eCommerce
Payment Systems

Zugriffskontrolle für Server Wallets
Vorteile separater Authentisierung

Autoren: **Jürgen Weiß, Stefan Risto**
Version: **1.0 vom 11.02.2002**

Zusammenfassung:
Momentan kristallisieren sich Server Wallets als die mächtigste Architektur im ePayment-Bereich heraus. Umso wichtiger ist es, sich mit den Themen Identifikation und Transaktionsfreigabe auseinander zu setzen, die zweifellos in jeder Server Wallet eine zentrale Rolle spielen. Dabei stellt sich unweigerlich die Frage, welche der vielen am Markt verfügbaren Identifikations-/Transaktionsfreigabeverfahren in die Server Wallet integriert werden sollen. Neben den klassischen Verfahren wie beispielsweise PIN/TAN oder idToken werden zukünftig mobile Verfahren immer mehr an Bedeutung gewinnen. Somit besteht die Notwendigkeit, bei Bedarf alte Identifikations- und Transaktionsfreigabemechanismen auszutauschen und/oder neue zu integrieren. Dieses Dokument gibt Anhaltspunkte, wie die Verwaltung der Wallet effizienter gestaltet und die Flexibilität bezüglich der zu unterstützenden Mechanismen gesteigert werden kann.

NOVOSEC
Aktiengesellschaft

Sulzbacher Straße 29-39
65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0
Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Grundlagen

Momentan kristallisieren sich Server Wallets als die mächtigste Architektur im ePayment-Bereich heraus. Umso wichtiger ist es, sich mit den Themen Identifikation und Transaktionsfreigabe auseinander zu setzen, die zweifellos in jeder Server Wallet eine zentrale Rolle spielen. Der Hauptgrund hierfür ist die räumliche Trennung der Kunden von den Systemen.
Eine sichere Zahlungstransaktion über das Internet benötigt insbesondere die folgenden drei Teilprozesse:

- Identifikation
- Transaktionsfreigabe
- Autorisierung

Identifikation

Erster Schritt einer solchen Transaktion ist die zweifelsfreie Feststellung der Identität des Kunden. Dazu muss dieser einen Beweis seiner Identität liefern. Dies kann durch verschiedene Verfahren geschehen; weit verbreitet sind Benutzername/Passwort, PIN und idToken. Zukünftig werden auch andere Challenge-Response-Verfahren, z.B. mit digitalen Signaturen, sowie biometrische Verfahren an Bedeutung gewinnen.
Die verschiedenen Verfahren bieten unterschiedliche Sicherheitsniveaus und sollten deshalb dem jeweiligen Anwendungsfall entsprechend ausgewählt werden.

Transaktionsfreigabe

Unter der Transaktionsfreigabe versteht man das verbindliche Auslösen einer Zahlungstransaktion durch den Kunden. Für die Freigabe stehen u.a. die gleichen Verfahren zur Verfügung wie bei der Identifikation. Obwohl möglich, ist es dennoch nicht ratsam, identische Verfahren für die Identifikation und die Transaktionsfreigabe einzusetzen (z.B. zweimal die gleiche PIN). Dadurch wäre es nämlich einem potenziellen Angreifer leichter möglich, Transaktionen unter dem Namen des Opfers auszulösen. Durch die Verwendung eines anderen Verfahrens (z.B. TAN) zur Transaktionsfreigabe wird ein Missbrauch erschwert – es müssten zwei verschiedene Verfahren kompromittiert werden, um eine Transaktion auszulösen. Verbreitete Verfahren zur Transaktionsfreigabe sind TANs, idToken, paybox und digitale Signaturen. In Zukunft werden sich neue Verfahren unter Verwendung von Mobiltelefonen etablieren.

Autorisierung

Die Autorisierung ist die Zahlungsfreigabe seitens der Bank. Sie erfolgt nach der Transaktionsfreigabe durch den Bankkunden. Dazu werden von Banksystemen Prüfungen z.B. des Limits, der Bonität, etc. vorgenommen, anhand derer entschieden wird, ob eine Zahlung ausgeführt wird oder nicht.

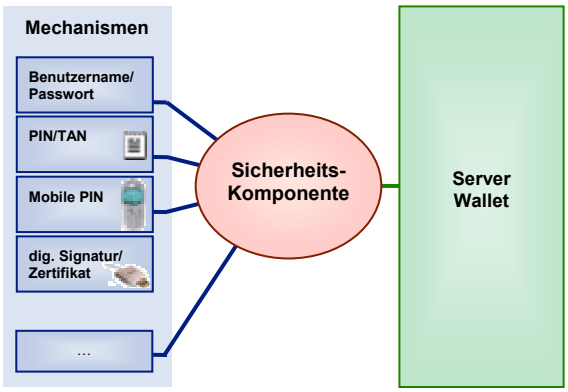
Von diesen drei Teilaufgaben, Identifikation, Transaktionsfreigabe und Autorisierung, übernimmt die Server Wallet die ersten zwei, während die Autorisierung der Zahlungen durch die Backend-Systeme vorgenommen wird.
In erster Linie benötigen Server Wallets daher Mechanismen zur zweifelsfreien Feststellung der Identität des Kunden. Je nach benötigter Sicherheit für die Wallet und regionalen Gegebenheiten kommen verschiedene Varianten in Frage. So sind normalerweise nicht alle Verfahren in allen Ländern etabliert.
Um auf die Dienste der Server Wallet zurückzugreifen, muss ein Kunde zunächst registriert werden. Dies erfordert die Aufnahme persönlicher sowie für den Zahlungsverkehr notwendiger Daten. Danach erhält der Kunde die Zugangsdaten, die nötig sind, um bei späteren Transaktionen seine Identität zu beweisen. Diese sind je nach verwendetem Identifikationsmechanismus unterschiedlich und können auch Soft- und Hardwarekomponenten einschließen.

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Viele existierende Server Wallets beschränken sich auf den Einsatz von nur einem Mechanismus. Gerade für länderübergreifende Lösungen ist es aber sinnvoll, mehrere Varianten anzubieten. Um dies sauber und effizient umzusetzen, benötigt man eine Architektur, wie sie der folgende Abschnitt beschreibt.

Ansatz mit separater Authentisierung

Betreiber von Server Wallets mit hoher Nutzerzahl bieten meist verschiedene Identifikations- und Transaktionsfreigabeverfahren. Da sich die Menge der am Markt verfügbaren Verfahren permanent ändert, muss ein Weg gefunden werden, möglichst einfach neue Verfahren in die Wallet zu integrieren und nicht mehr benötigte Verfahren abzuschalten. Genau diesen Aspekt berücksichtigt der folgende Ansatz.
Eine Server Wallet vereinfacht sich stark, wenn sich ihre Funktionalität auf die reinen Payment-Aufgaben beschränkt und sie sich nicht um Identifikation und Transaktionsfreigabe kümmern muss. Deswegen trennt man die Wallet von den Sicherheitsmechanismen. Die notwendige Identifikation und Transaktionsfreigabe wird von einer der Wallet vorgelagerten Sicherheitskomponente übernommen. Diese Komponente sendet die aufbereiteten und geprüften Identifikations- und Freigabedaten an die Wallet.
Ein wesentlicher Punkt ist demnach die Sicherheitskomponente. Sie ist so zu gestalten, dass neue Verfahren jederzeit ohne Beeinflussung der bereits laufenden Mechanismen integriert werden können. Besonders interessant sind hierbei neue Verfahren zur mobilen Transaktionsfreigabe, z.B. Mobile PIN.
Das folgende Bild gibt einen kurzen Überblick über die eben beschriebene Architektur:



Bei der Registrierung eines Kunden (automatisch oder manuell) werden lediglich die für die Zahlungsabwicklung nötigen Daten an die Wallet übermittelt. Alle Daten, die im Zusammenhang mit der Identifikation und Transaktionsfreigabe stehen, werden von der Sicherheitskomponente gespeichert.

Vorteile der Lösung

Als großer Vorteil für den Betreiber der Server Wallet ergibt sich die getrennte Administration der Wallet-Daten und der Sicherheitskomponente. Die Sicherheitskomponente ist modular aufgebaut und kann so um weitere Verfahren zur Identifikation und Transaktionsfreigabe erweitert werden, ohne bestehende Verfahren zu beeinflussen. Auf diese Art können neue eingeführte Verfahren parallel zu bisher installierten betrieben werden. So können Kunden langsam von alten Verfahren auf neue umsteigen. Nach einer gewissen Übergangszeit können nicht mehr benötigte Verfahren abgestellt werden. Ein praktischer Nebeneffekt einer solchen Sicherheitskomponente ist, dass sie auch für andere Bankanwendungen benutzt werden kann.
Für den Bankkunden stellt sich als Vorteil dar, dass er nach der Einführung eines neuen Verfahrens dafür unkompliziert, eventuell automatisch, freigeschaltet werden kann.

NOVOSEC Aktiengesellschaft

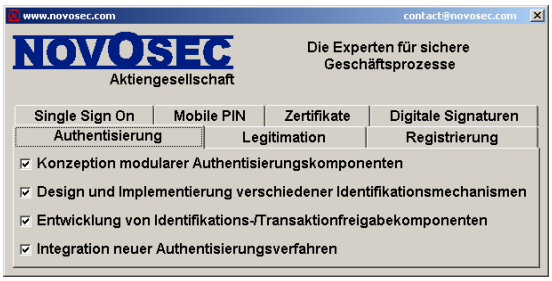
Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Beispiel: Ablauf einer Identifikation/Tranasaktions-freigabe mit PIN/TAN

Eine beispielhafte Darstellung einer Transaktion unter Verwendung von PIN/TAN befindet sich auf Seite 5 (Abbildung 1).

Wünschen Sie nähere Informationen zu diesem Thema? Wir freuen uns auf Ihre Anfragen.

juergen.weiss@novosec.com



Weitere Artikel finden Sie unter:
http://www.novosec.com/downloads

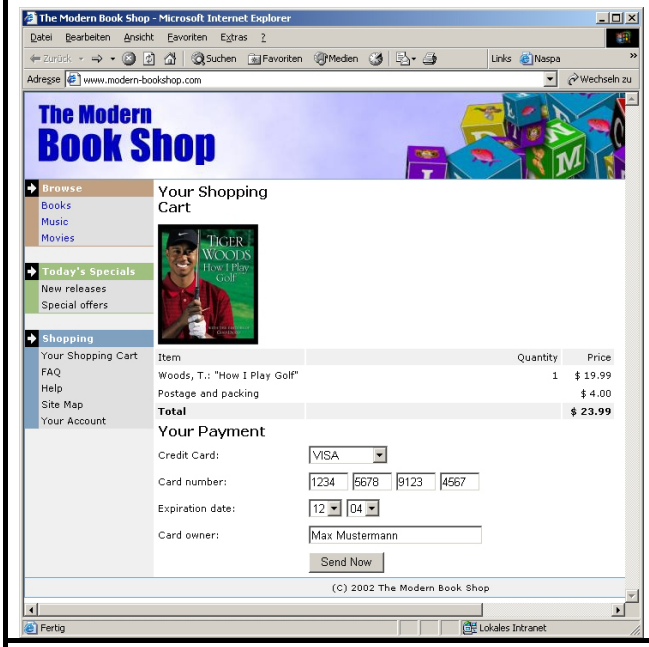
NOVOSEC Aktiengesellschaft

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Deutschland
Telefon +49 (0) 6196/88289-0, Telefax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Abbildung 1 – Kreditkarten-Payment-Transaktion mit PIN/TAN

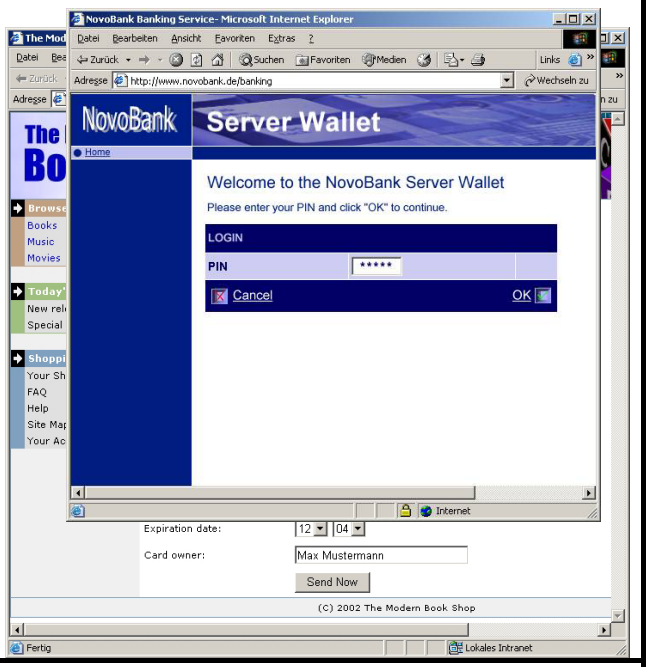
Schritt 1:

Kunde gibt Kreditkartendaten ein



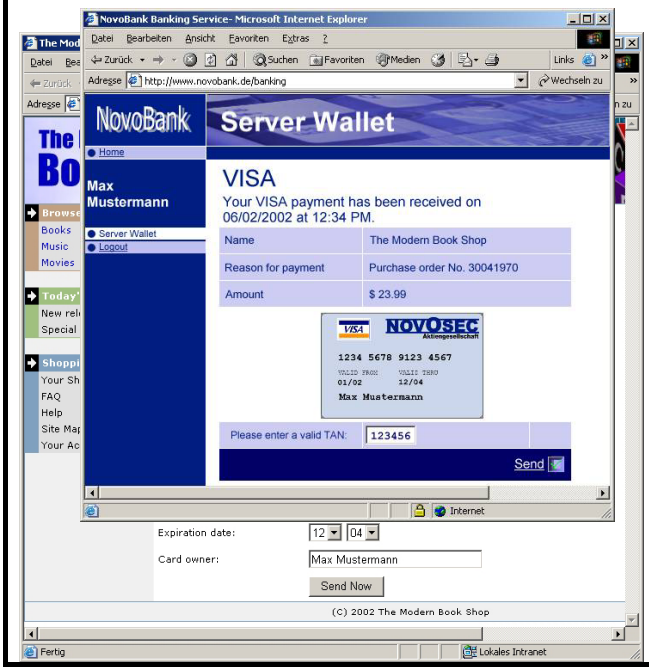
Schritt 2: Identifikation

Die Server Wallet startet automatisch und fragt den Kunden nach der PIN



Schritt 3: Transaktionsfreigabe

Die Server Wallet zeigt die Transaktions-daten an und fragt den Kunden nach einer TAN



Schritt 4: Autorisierung

Die Transaktion wurde erfolgreich ausgeführt