Stephanie Kretschmar

Elektronische Zahlungssysteme - Verbreitung und Akzeptanz im B2C Bereich

Diplomarbeit

Examicus

Fachhochschule für Ökonomie und Management

Essen

Diplomarbeit

zur

Diplom- Informatikerin

Thema

Elektronische Zahlungssysteme

Verbreitung und Akzeptanz im B2C Bereich

vorgelegt von: Stephanie Kretschmar

Marl, den 28.02.2005

Inhaltsverzeichnis

Abbildungsverzeichnis

Glossar

Acquirer Vertragsunternehmen eines Händlers, welches die Kartendaten autorisiert, erfasst und Zahlungen transferiert.

Authentifizierung Verfahren zur Überprüfung der Identität, dies kann mit Hilfe von Passwörtern, Chipkarten oder biometrischen Verfahren realisiert werden.

Asymmetrische Verschlüsselung Verschlüsselungsverfahren, bei dem zwei Schlüssel verwendet werden; ein Schlüssel zum Verschlüsseln und einer zum Entschlüsseln.

B2C Kurzform von Business-to-Consumer, bezeichnet Geschäftsbeziehungen zwischen Händlern und Privatkunden.

Challenge Response Verfahren, bei dem die Autorisierung über persönliches Geheimnis erfolgt; wird unter anderem bei EC-Karten mit PIN eingesetzt.

Digitale Signatur Daten, die elektronischen Nachrichten hinzugefügt werden und der Authentifizierung dienen.

Disagio Gebühr, die ein Händler für Kartentransaktionen an Acquirer oder entsprechendes Vertragsunternehmen zahlt.

Hash- Funktion Verfahren, welches zur Komprimierung von Nachrichten und Daten dient. Aus einer Nachricht wird ein Wert mit fester Länge berechnet, der so genannte Hash- Wert. Dieser ist der Nachricht eindeutig zuzuordnen, da eine Veränderung in der Nachricht zu einem veränderten Hash- Wert führt. Rückschlüsse vom Hash-Wert auf die Nachricht sind nicht möglich.

Hybride Verschlüsselung	Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Eine Nachricht wird symmetrisch verschlüsselt. Der verwendete Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, so dass nur der Empfänger (Inhaber des privaten Schlüssels) den Schlüssel und anschließend die Nachricht entschlüsseln kann.
Kerberos	Dienst der auf einem Server aktiviert ist und die Authentifizierung durch die Verteilung und Verwaltung von Sitzungsschlüsseln regelt.
Persönliche Identifikations-nummer (PIN)	Persönliches Geheimnis, welches aus Zahlen- und/ oder Buchstabenkombinationen besteht und der Authentifizierung dient.
Public Key Infrastructure (PKI)	Methode für die Erstellung, Ausgabe und Verwaltung von Zertifikaten und digitalen Signaturen.
Random Access Memory (RAM)	Speicher, der lesbar, adressierbar und beschreibbar ist; speichert die Daten nur solange eine Stromversorgung vorhanden ist.
Read Only Memory (ROM)	Speicher, der lesbar, aber nicht wieder beschreibbar ist.
RSA	Asymmetrisches Verschlüsselungsverfahren, 1978 veröffentlicht und nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman benannt.
Secure Electronic Transaction (SET)	Protokoll zur sicheren Datenübertragung im Internet, speziell für sensible Daten entwickelt. Verwendet Zertifikate bei allen Vertragspartnern und garantiert die eindeutige Identifizierung.