Elektronisches Bezahlen

- DELL verkauft Computer im Wert von mehr als 3 Millionen Dollar am Tag über ihre Web-Site.
- amazon.de verkauft in Deutschland US-Literatur zu wesentlich günstigeren Preisen innerhalb von 14 Tagen Lieferzeit porto- und zollfrei.
- Quelle bietet einen Service an, Blumen über ihre Web-Site zu “versenden” und bezeichnet diesen Service als erfolgreich.

	herkömmlicher Handel (in Milliarden $)	elektronischer Handel (in Milliarden $)
1994	5150	245
2000	8500	1650
2005	12000	2950

Man rechnet damit, daß $2/3$ des EC im Bereich business-to-business und $1/3$ im Bereich business-to-custumer liegen werden.

Elektronisches Bezahlen – Charakteristika

- Verläßt sich auf IT und schnelle Netze, um "Werte" zu speichern, zu übertragen und zu empfangen.
- Verläßt sich auf Verschlüsselung, um Sicherheit in offenen Netzen zu gewährleisten.
- Versucht Kosten zu reduzieren durch technologische Fortschritte (z.B. Papier, Zeit).
- Benötigt eine zentrale Stelle im finanziellen System, von der "Geld" abgehoben werden kann. (Es wäre ja zu schön, selbst Geld erzeugen zu können)

Transaktionssicherheit (Wdh.):

Anforderung	Bedeutung
Vertraulichkeit	Die während einer Transaktion übertragenen Daten dürfen nur für autorisierte Personen zugänglich sein.
Authentizität	Die Identität des jeweiligen Geschäftspartners (und der Nachricht) muß eindeutig bestimmbar sein.
Verbindlichkeit	Mündliche Absprachen und schriftliche Dokumente gelten unter bestimmten Rahmenbedingungen als rechtlich bindend. Dies muß auch für Transaktionen im Internet möglich sein. Insbesondere dürfen die Geschäftspartner nicht abstreiten können, an einer Kommunikationsbeziehung teilgenommen zu haben.
Integrität	Die Integrität der bei einer Transaktion übertragenen Daten muß gewährleistet sein. Die Daten dürfen, außer von autorisierten Personen, in keiner Weise modifiziert werden können.
Anonymität	Wenn gewünscht, müssen die Geschäftspartner bei einer Transaktion anonym bleiben können. Dies ist insbesondere ein Wunsch von vielen Konsumenten, die nicht wollen, daß Unternehmen, Banken oder sogar die Regierung nachvollziehen können, wofür sie ihr Geld ausgeben.

Vertraulichkeit, Authentizität und Integrität durch kryptographische Absicherung der Kommunikationskanäle (z.B. bei S-HTTP und SSL).

Verbindlichkeit durch digitale Signaturen (z.B. bei S-HTTP, SET und NetBill).

SSL

- Secure Socket Layer
- Von Netscape entwickeltes Verfahren zur Absicherung der Internet-Protokolle auf der Transportschicht.
- erlaubt es, Anwendungsdienste (z.B. HTTP) ohne Modifikation um symmetrische Verschlüsselung der Nutzlast und Authentifizierung der Kommunikationspartner zu ergänzen.
- Es werden nach einem Austausch des Sitzungsschlüssels *alle* übertragenen Daten verschlüsselt.

Initialisierungsphase von SSL

Unmittelbar nach Abschluß des TCP/IP-Verbindungsaufbaus findet der sogenannte *SSL-Hanshake* statt:

1. Client baut Verbindung zum Server auf und schlägt eine Reihe von kryptographischen Verfahren vor (DES (40 Bit), DES(56 Bit), IDEA (128 Bit), Triple-DES (168 Bit) . . .).
2. Server sendet Auswahl von Verfahren, die beide unterstützen an den Client.
   Server sendet sein digital unterschriebenes X.509-Zertifikat an den Client.
   Server kann vom Client ein Zertifikat anfordern.
   Server sendet abhängig von gewählten Schlüsselaustauschprotokoll seinen Beitrag zum Schlüssel.
3. Client überprüft Zertifikat des Servers.
   Client sendet, falls angefordert, sein digital signiertes Zertifikat.

Client sendet, falls Server nicht schon den gesammten symmetrischen Schlüssel geschickt hat, seinen Anteil am Schlüssel.

4. Server überprüft evetuell das Zertifikat des Clients.
   Server bestätigt dem Client den erfolgreichen Abschluß der Initialisierungsphase (Handshake). Dies erfolgt bereits mit dem ausgehandelten Verschlüsselungsverfahren.
   Jetzt steht die sichere Verbindung dem Anwendungsprotokoll zur Verfügung.

Zusammenfassung:

- Sichert in der einfachsten Fassung nur die Übertragung, keinerlei Sicherheit über die Endpunkte! Dies kann durch Erweiterung um Zertifikatsprüfung erreicht werden.
- Idee: Einfacher, sichere Server zu zertifizieren, als Public-Key-Infrastruktur aufzubauen.
- Da symmetrische Verschlüsselung eingesetzt wird, keine Verbindlichkeit.

S-HTTP

- Secure Hypertext Transfer Protocol
- Absicherung auf der Anwendungsebene.
- Erweiterung von HTML und HTTP, welche die Übertragung von verschlüsselten und/oder digital unterschriebenen MIME-Entitäten in beide Richtungen vorsieht.
- Server und Client handeln für jede Verbindung die Absicherung der Übertragung neu aus.
- Erlaubt den applikationsspezifischen (die tatsächlichen Sicherheitsbedürfnisse reflektierend) Einsatz kryptographischer Verfahren, z.B.:
  - Unwichtige Dokumente im Klartext ohne digitale Unterschrift übertragen.
  - Bei verbindlichen Daten kann der Client eine Unterschrift oder auch eine Verschlüsselung durch den Server fordern.
  - Server kann z.B. bei Ausfüllen von Formularen durch den Client eine digitale Unterschrift verlangen (Verbindlichkeit im Gegensatz zu SSL möglich).

Kurzausflug: Zertifikate

- eine Art elektronischer Personalausweis
- **Zertifikat**: Der öffentliche Schlüssel eines Benutzers gemeinsam mit zusätzlicher Information, unfälschbar gemacht durch Verschlüsselung mit dem privaten Schlüssel der Zertifizierungsstelle.
- **Zertifizierungsstelle**: Eine Institution, der einer oder mehrere Benutzer die Erstellung und Zuweisung von Zertifikaten anvertrauen.
- nach X.509-Standard (ITU-T der UN)
- Erweiterungen:
  - Einsatzgebiet des Zertifikates einschränken
  - beliebige alternative Namen (neben dem eindeutigen DN-Namen (distinguished name): cn=reinert, ou= informatik, o=uni-kl, c=de) cn=person, ou=organisational unit, 0=organisation, c=country.
  - Sperrlisten
- VeriSign, Thawte, BelSign.

X.509 Version

Seriennummer

Unterschrifts-Algorithmus

Gueltigkeit

Name des Ausstellers

Name des Benutzers

Oeffentlicher Schluessel

Austeller-ID

Benutzer-ID

Erweiterungen

Digitale Unterschrift

X.509-Zertifikat Version 3

(X.509v3)

Lebenszyklus eines Zertifikates

1. Registrierung des Benutzers bei einer Zertifizierungsstelle
   - entweder erzeugt Benutzer sein Schlüsselpaar selbst und schickt öffentlichen Teil an die Zertifizierungsstelle oder
   - Schlüsselpaar wird von der Zertifizierungsstelle erzeugt (Key Escrow, Schlüsselhinterlegung möglich, ist umstritten).
2. überprüfung der Identität nach den bekannten Geschäftsbedingungen der Zertifizierungsstelle.
3. Seriennummer, eindeutiger Name, Gültigkeitsdauer werden vergeben und das Zertifikat mit Unterschrift der Zertifizierungsstelle wird erstellt und einem Verzeichnisdienst übergeben (für möglichst viele zugänglich)
4. Bei Einsatz, kann es mit dem öffentlichen Schlüssel der Zertifizierungsstelle geprüft werden.
5. Nach Anlauf (meist unterhalb der Dauer einer Brute-Force-Attacke) oder Sperrung neu zu beantragen.

SET

- Secure Electronic Transactions
- gemeinsame Entwicklung von Mastercard und Visa
- The World of Visa Secure Electronic Commerce (Eine Demo)
  `http://www.visa.com/cgi-bin/vee/nt/sec/no_shock/entry_L.html?2+0`
- Public-Key-Infrastruktur zur sicheren Abwicklung von Kreditkartentransaktionen über das Internet.
- benutzt X.509-Zertifikat
- Idee: SET ist ein Container, der Daten vom Käufer über den Händler zur Bank sicher über das Internet schickt. (Drei-Personen-Protokoll)
- Verbindlichkeit durch elektronische Unterschrift.
- Neu: Der Händler sieht nicht alle Daten des Käufers, z.B. nicht die Kreditkartennummer.

SET-Funktionsprinzip

1. Der Kunde beantragt ein *Digital Wallet*: Software für
   - Kommunikation mit Händlern
   - Verifikation der Zertifikate der Händler

   und digitale Zertifikate (vergleichbar mit Ablaufdatum der Kreditkarte)

2. **Bestellung**: Karteninhaber wählt bei seiner Bestellung via Internet Zahlungsart "Kreditkarte". Er übermittelt die Transaktion elektronisch zum Händler.

3. **Verifizierung**: Der Kunde (seine Software) prüft das Zertifikat des Händlers (z.B. wird es mit dem Angebot geschickt). Hat der Händler kein Zertifikat, so wird der Kunde gewarnt und kann die Bestellung rückgängig machen.

4. **Payment Transfer**: Hierfür benötigt der Kunde ein Zertifikat, das ihm sein Finanzinstitut zur Verfügung stellt (elektronische Kreditkarte). Das Zertifikat des Bestellers wird zusammen mit der Bestellung übermittelt. SET verschlüsselt die Information und fügt eine digitale Unterschrift hinzu.

5. **Quittung**: Der Händler kann den Karteninhaber, nicht jedoch die Kartendaten, überprüfen. Die Daten werden weitergeschickt an die dritte Partei (Acquirer).

6. **Autorisierung**: Der Acquirer entschlüsselt die ganze Information und autorisiert die Karte beim Aussteller (dies erfolgt z.B. über das VISANet).

7. **Versand**: Nach der Autorisierung wird diese dem Händler mitgeteilt, der die Bestellung bestätigt und die Ware versendet.

Elektronisches Bezahlen – Arten

- Smart-Cards
- Micropayments
- Elektronisches Geld

Smart-Cards

Verbindung von klassischen Methoden

- Banktransaktionen wie z.B. Überweisungen, Schecks, Bankeinzüge.
- Elektronische Geldbörse
- Kreditkarten

mit weiteren Funktionen

- Schlüssel speichern
- Zertifikate speichern
- Zusatzprogramme mit Händlern (Flugbonusmeilen, Versicherungen, Ermäßigungen).
- uvm.

mit dem Fernziel alles auf einer Karte zu haben.

R. Anderson, M. Kuhn: Low Cost Attacks on Tamper Resistant Devices, In: Security Protocols, Springer 1997

Micropayments

- "Amerikaner tätigen pro Jahr mehr als 237 Milliarden Käufe für über 600 Milliarden \$ von denen 84 % weniger als 20 \$ kosten." (Master Card)
- Kreditkartenzahlungen sind für solche Käufe ungeeignet, da für den Verkäufer zu gebührenintensiv (2 -2,25 % + 30 - 50 cent).
- Man benötigt ein Abrechnungssystem für kleine Beträge (< 1 cent !) für die Informationsleistungen des Internet (Zeitungsberichte, Börsenkurse, Suchergebnisse, . . .).
  - kosteneffektiv und skalierbar, einfach und sicher
  - Kontoführung, Mikroschulden überwachen und ausgleichen.
  - Beträge vieler kleiner Transaktionen sammeln und innerhalb einer großen Transaktion abbuchen.
- Es gibt derzeit 2 Kategorien:
  - Zertifikate (vergleichbar mit Bargeld, wer es hat besitzt es)
  - über eine dritte Partei (Bank)
- CyberCash, ECash (DigiCash), Netbill, Millicent, MicroMint, Payword

Elektronisches Geld – Anforderungen

- Sollte bank-zertifiziert sein.
- Sollte mit anderen Währungen tauschbar sein.
- Sollte fälschungssicher sein.
- Sollte über das Netz zugänglich sein.

Beispiel: E-Tokens, die von einer dritten Partei (Bezahlungsservice) gespeichert und verwaltet werden. (Eine Art Bank für Kontos mit elektronischem Geld)

Stand: Cybercoins haben sich nach einem optimistischen Anfang bisher nicht durchsetzen können.

Problem: Funktioniert in der Regel nur, wenn beide Seiten angeschlossen sind.

CyberCash

- Projekt von Commerzbank, Dresdner Bank, Hypovereinsbank und einigen Landesbanken
- Info unter www.cybercash.com

- Jede Kommunikation wird verschlüsselt (derzeit DES 56 Bit).
- Erhöhte Sicherheit durch Prüfsummen, die mit RSA (1024 Bit) verschlüsselt werden.
- benutzt häufig speziell eingebaute Hardware: CyberCashWallet.

1. Käufer sendet Bestellung und Zahlungsart per WWW zum Händler.
   Händler schickt die aufgearbeiteten Bestelldaten mit seinem Angebot zurück.
   Beides geschieht verschlüsselt z.B. mit SSL oder CyberCashWallet.
2. Käufer verifiziert die Bestellung und sendet sie mit "pay" zurück.
   Die Bestellung wird digital signiert (RSA 1024 auf Prüfsumme)
3. Händler erhält nur die Bestelldaten.
   Er schickt die verschlüsselte Zahlungsinformation digital signiert zum CyberCash Server.
4. CyberCash erhält das Paket und bringt es in "Sicherheit" (Firewall).
   Die Information wird entschlüsselt und über einen sicheren Kanal der Bank der Händlers mitgeteilt.
5. Händlerbank setzt sich mit Kundenbank oder Kreditkartenorganisation in Verbindung und sendet das Ergebnis (gedeckt oder nicht gedeckt) zu CyberCash.
6. CyberCash informiert den Händler, der wiederum den Kunden.

- Dauer: 15 – 20 Sekunden.
- weiterer Vorteil: sowohl das System des Kunden als auch das des Händlers protokollieren alle durchgeführte Transaktionen mit. Bei Problemen können beide ihre Daten offenlegen, um den Zahlungsvorgang zu rekonstruieren.

ECash

- Deutsche Bank
- Wie bei Banknoten kann ein Kunde "Geld" von seinem Konto abheben.
- Man kann diese elektronischen Banknoten auch an andere Personen weitergeben.
- Aber im Gegensatz zu echtem Bargeld, spielt die Bank eine wichtige Rolle.

1. **Geld abheben**:
    - Abgehobenes elektronisches Geld wird von der Bank an den elektronischen Geldbeutel des Kunden geschickt.
    - Den echten Geldstücken entsprechen (verschiedene) Zeichenketten mit Werten, die von der Bank signiert wurden (vergleichbar mit den Seriennummern der Banknoten).

- Die Software des elektronischen Geldbeutels “verwaltet” dieses Geld und “bezahlt” damit. Sie informiert den Kunden auch, wenn ihr das “Kleingeld” ausgeht.

2. **Einkaufen**:

   - Der Händler **muß** ein Konto bei derselben elektronischen Bank haben.
   - Entscheidet sich der Kunde zum Kauf und Bezahlen, so stellt der elektronische Geldbeutel die entsprechenden Geldstücke zusammen und schickt sie an den Händler.
   - Der Händler schickt das Geld an die Bank.
   - Gibt die Bank ihr ok, so sendet der Händler die Ware an den Kunden, das Geld wird seinem Konto gutgeschrieben.
   - Die Bank merkt sich, welches “Geld” des Kunden schon verbraucht wurde.
   - Der Händler selbst kann auch “Geld” von seinem Konto abheben. Dazu erzeugt die Bank für ihn neues “Geld”.

3. **Anonymität**:

   - Benutzt “blinde Signaturen”.
   - Die Geldbörse des Kunden erzeugt das “Geld” (die Zeichenkette) und packt es ein.
   - Die Bank signiert den “Umschlag”, in dem das Geld steckt, und belastet das Konto des Kunden.
   - Die Unterschrift “schlägt” sich durch den Umschlag durch auf das Geldstück.

   Mathematisch:

   - Kunde erzeugt Zufallszahl und verschlüsselt sie mit ihm bekannten Verfahren.
   - Bank leistet digitale Unterschrift.
   - Kunde macht seine Verschlüsselung rückgängig und erhält signierte Zufallszahl.

   Rolle der Bank bei ECash oder elektronischem Geld generell: Sie muß sich merken, welches Geld schon einmal ausgegeben wurde.

Beobachtungen und Ausblick

- Im Internet hat man eine verteilte Verarbeitung zwischen Kunde, Händler und Bank.
- Wie läßt sich hier Atomarität (oder sogar ACID) erzielen?
- Schlüsselkonzept: Zwei-Phasen-Commit-Protokoll.