Eigenschaften von Protokollen im Elektronischen Handel

1. Atomarität
    - Geldatomarität
    - Warenatomarität
    - Zertifizierte Auslieferung (Quittung)
2. Anonymität

Atomarität

Zur Erinnerung: Atomarität erlaubt es mehrere Operationen logisch so zu verknüfen, daß entweder aller oder keine der Operationen ausgeführt werden.

```
<begin-transaction>
state-changing operation 1;
state-changing operation 2;
...
state-changing operation n;
<end-transaction>
```

In der Regel treten dann Probleme auf, wenn die Transaktion wie hier in einer verteilten Umgebung ausgeführt wird: Kommunikation kann ausfallen, dann muß die **komplette** Transaktion zurückgesetzt werden.

Problem mancher Protokolle: Wird die Kommunikation zwischen Käufer und Händler unterbrochen, so kann es passieren, daß beide das "Geld" haben (der eine noch, der andere schon).

Geld-Atomarität (GA)

- Transfer von "Geld", wobei es keine Möglichkeit geben darf, Geld zu erzeugen oder zu vernichten.
- Klassisches Beispiel: Austausch von Bargeld oder EC-Karten.
- Grundlegende Eigenschaft, die jedes Protokoll erfüllen sollte.

Waren-Atomarität (WA)

- WA-Protokolle sind GA. Sie gewährleisten zusätzlich den vollständigen Austausch von "Geld und Waren".
- Ich erhalte die Ware genau dann wenn der Händler sein Geld erhält, d.h. es ist ausgeschlossen, daß ich zahle, aber nichts erhalte und daß ich etwas bekomme ohne zu zahlen.
- WA ist besonders wichtig für Informationsgüter, denn hier kann der Transfer unterbrochen werden (ftp-Abbruch); Unsicherheit auf beiden Seiten.
- Klassisches Beispiel: Nachnahme bei der Post.

Zertifizierte Lieferung (ZL)

- ZL-Protokolle sind GA und WA.
- Käufer und Händler können genau überprüfen, welche Ware geliefert wurde.
- Klassisches Beispiel: Nachnahmepaket, das im Beisein des Boten ausgepackt und quittiert wird.

ECash ist nocht nicht einmal GA.
SSL und SET sind nicht WA.

NetBill – Ein atomares Protokoll

- unterstützt alle drei Ebenen der Atomarität.
- läuft zwischen drei Parteien ab: K (Käufer), H (Händler) und N (NetBill-Server).
- N fungiert als eine Art Notar (von beiden Seiten als vertraulich akzeptiert).
- Schlüsselidee: Zwei-Phasen-Commit-Protokoll
- CyberCash benutzt es

Skizze des NetBill Protokolls (Wdh.)

1. K erfragt den Preis einer Ware bei H.
2. H mach K ein Angebot.
3. K akzeptiert das Angebot.
4. H schickt das mit S verschlüsselte Informationsgut W an K.
5. K bereitet einen EPO (electronic purchase order) vor, der eine digitale Signatur für <Preis, chiffrierte Signatur des verschlüsselten W, Zeitstempel> enthält.
   K schickt den unterschriebenen EPO an H.
6. H zeichnet den EPO gegen und signiert S. H schickt beides an N.
7. N überprüft die Signatur und Gegensignatur des EPO.
   N überprüft den Kontostand von K und den Zeitstempel des EPO.
   Wenn alles ok ist, transferiert N das Geld von Ks auf Hs Konto.

N speichert den Schlüssel S und die chiffrierte Signatur von W.
N bereitet eine signierte Empfangsbestätigung, die S enthält, vor und schickt sie an H.

8. H speichert eine Kopie der Empfangsbestätigung und schickt sie an K weiter. K kann nun die Ware W entschlüsseln.

Korrektheit

1. GA: Geldtransfer erfolgt nur im NetBill-Server.
   Somit ist dies eine ganz normale Transaktion mit ACID-Eigenschaft!
2. WA: Commit-Punkt ist Schritt 7:
   - Fehler vor Schritt 7: Es erfolgt kein Geldtransfer und K erhält S nicht!
   - Fehler nach Schritt 7: N und H speichern S. Falls etwas schiefläuft, kann K S entweder von N oder H erhalten.
3. ZL:
   - Annahme: K behauptet, etwas anderes als W erhalten zu haben.
   - N hat eine chiffrierte Signatur des verschlüsselten W (von K und H gegengezeichnet).
     N und H haben S.
     Somit kann eine Schiedsstelle feststellen, ob K das chiffrierte W verändert hat.
     Außerdem kann W nach Entschlüsselung mit Hilfe von S inspiziert werden.

Verhalten bei Käuferreklamationen

- Falsche oder beschädigte Ware
  - Dies ist nicht, was ich bestellt habe.
  - Die Ware war unvollständig oder fehlerhaft.
  - Der Entschlüsselungs-Schlüssel war falsch.

  In diesen Fällen benötigt man einen Menschen, um zu entscheiden, wo der Fehler liegt an Hand von

  1. der vom Käufer signierten EPO und des Schlüssels S des NetBill-Servers und
  2. der Kopie der Ware W vom Käufer und des Schlüssels S.

  - Ich habe die Ware bezahlt, aber nie den Schlüssel S erhalten.

  In diesem Fall kann der Schlüssel vom Händler oder dem NetBill-Server nach einer erneuten Anfrage ausgeliefert werden.

- Die Ware entspricht nicht dem Angebot.

  In diesem Fall kann das Protokoll nicht helfen.

- Streit über die Transaktion
  - Ich habe einem Preis von X DM zugestimmt, es wurden aber Y DM abgerechnet.
  - Ich habe nur für X DM Ware gekauft, aber mein Konto wurde mit Y DM belastet.

  In diesen Fällen kann der NetBill-Server an Hand der vom Kunden signierten EPO beweisen, wieviel DM der Käufer zugestimmt hat.

  - Ich habe dies nicht gekauft, auch wenn es so aussieht.
  - Ich habe das Angebot des Händlers abgelehnt, aber er hat es dennoch weitergeleitet.

  In diesen Fällen kann der NetBill-Server an Hand der vom Käufer signierten EPO den Handel nachweisen. Existiert dieser Nachweis nicht, wird das Geld zurückerstattet.

– Mir wurde mitgeteilt, daß die Transaktion abgebrochen wurde, aber mein Konto wurde dennoch belastet

Für abgebrochene Transaktionen teilt der NetBill-Server signierte Abbruchnachrichten aus. Kann vom Käufer keine solche Nachricht vorgelegt werden, geht man von der Korrektheit der Transaktion aus.

Verhalten bei Händlerreklamationen

- Ich habe Ware für X DM geliefert, aber nur Y DM erhalten.
- Die Transaktion wurde bestätigt, aber ich habe niemals Geld erhalten.

Da der NetBill-Server für alle Transaktionen Erfolg oder Abbruch mit einer signierten Nachricht bestätigt, können diese Fragen an Hand dieser Nachrichten geklärt werden,

Protokolle zur Unterstützung von Anonymität

- Gründe?
- In den USA sind Käufe über 10.000 $ meldepflichtig.
- Klassisch: Kauf einer Ware am Automaten.
- Problem: Ist Protokoll nicht GA, so ist in der Regel auch die Anonymität nicht gewährleistet.

Anonymes Protokoll

1. Käufer bezieht von seiner Bank ein Geldtoken.
2. Käufer behandelt das Token krypthographisch so, daß der Händler zwar die Validität nicht aber die Identiät checken kann.
3. Käufer gibt das Geld einem Händler, die Identität des Händlers wird zusätzlich in das Token hineinkodiert.
4. Händler checkt, ob das Token schon einmal benutzt wurde.
5. Händler schickt die Ware zum Kunden.
6. Händler gibt irgendwann seine eingenommenen Token zur Bank.
7. Bank checkt, ob das Token zum ersten Mal eingelöst wird. Ist dies der Fall, bleibt der Käufer anonym. Sonst wird der Käufer wegen "Fälschung" angezeigt.

Was passiert, wenn die Transaktion in Punkt 3 abgebrochen wird?

Offene Fragen

- Gibt es andere Arten der Atomarität, die für den elektronischen Handel notwendig sind (außer GA, WA und ZL)?
- Gibt es eine formale Definition dieser Atomaritäten?
- Wie kann man beweisen, daß ein Protokoll bestimmte atomare Eigenschaften hat? Gibt es formale Methoden?
- Wieviele Nachrichten müssen bei einem Protokoll mit bestimmten atomaren Eigenschaften mindestens ausgetauscht werden?
- Wie kann man verhindern, daß die Ware vom Käufer weiterverteilt wird?
- Kann man digitale Wasserzeichen erstellen, die Raubkopien identifizieren?
- Kann man anonym spenden und dennoch eine Spendenquittung erhalten?

Weitere Anwendung: Elektronische Briefmarken

- Kann man GA ohne eine zentrale Kontrollstelle erreichen?
- Ja, z.B. mit Hilfe von spezieller Hardware: Geräte, die Informationen speichern und Prozesse ausführen können und in dem Sinne sicher sind, daß bei einem Versuch, sie zu knacken, sie unbrauchbar gemacht werden.
- Anwendungsfeld Briefmarken: Frankierautomaten.
- Es ist leicht eine von einem Frankierautomaten erzeugte Briefmarke einzuscannen und den Wert bzw. das Datum zu manupulieren.
- Entwicklung eines "Secure-Coprocessor":
  - Speichert einen Wert und vermindert diesen bei der Produktion von "Briefmarken".

- Die "Briefmarke" ist eine verschlüsselte Nachricht, die Senderadresse, Empfängeradresse, Datum und eine fortlaufende Nummer enthält.
- Post an eine bestimmte Adresse wird grundsätzlich von der gleichen Poststelle sortiert.

  Diese Poststelle testet, ob die Adresse auf dem Umschlag der verschlüsselten Adresse entspricht, ob die Nummer eindeutig ist und ob die Marke "aktuell" ist(Der Wert der Briefmarke bleibt 6 Monate erhalten).

  Der Datenserver kann alle gespeicherten Nummern von Sendungen, die älter als 6 Monate sind, regelmäßig wegwerfen.

- mögliche Angriffe:
  - Kopieren von "Briefmarken": Wird nur für gleiche Adresse gehen und an der Poststelle auffallen.
  - Versuch, den Schlüssel für die digitale Signatur zu brechen, benötigt das Öffnen des Koprozessors und zerstört ihn so.