E-Banking

Philipp Gühring
pg@futureware.at

Dieses Konzept soll einen Weg zeigen, wie E-Banking einfach und trotzdem sicher realisiert werden kann, und wie das System dann erweitert werden kann.

1. Vorhandene Infrastruktur:

1.1. Bank

Die grundsätzliche Annahme des Konzeptes ist das bestehen einer engen und sicheren Verbindung des Kunden mit seiner Bank. Die Bank bietet jedem Kunden eine gesicherte Verbindung für Online Banking, die von jedem Browser aus verwendet werden kann, und meistens eine Mischung aus HTML und Java Applets ist.

Innerhalb dieser gesicherten Umgebung bietet die Bank bereits jetzt dem Kunden folgende Funktionen an:

- Erfassen von Transaktionen (HTML Formular)
- Transaktions-Vorschlagsliste
- Bestätigungen von vorgeschlagengen Transaktionen mittels TAN
- Ausdruckbare Bestätigung der Transaktion

1.2. Verkäufer

Hier gehen wir von 3 Szenarien aus.
Die Hauptzielgruppe sind Webshops, also Geschäfte, die zum Großteil im Internet ohne Medienbruch abgehandelt werden.
Daneben gibt es den B2B Bereich, der auch im Internet funktioniert, nur eben automatisiert, und nicht manuell
Und schließlich Geschäfte, die nicht hauptsächlich im Internet abgewickelt werden.

Dieses Konzept behandelt primär die erste Zielgruppe, die Webshops.
Der B2B Bereich wird automatisch mit abgedeckt, und wird vorerst besonders behandelt.
Den Nicht-Internet Bereich wird man in weiterer Folge untersuchen müssen, inwieweit man das Konzept auch auf den Bereich anwenden kann.

Bei den Webshops wird davon ausgegangen, daß die Verkäufer bereits einen grundsätzlich funktionierenden Webshop haben, der bereit ist, an Zahlungssysteme angebunden zu werden.

1.3. Kunde

Wir gehen davon aus, daß der Kunde einen Computer mit Internetzugang und einen Browser hat, mit dem er Zugang zum Onlinebanking seiner Bank hat.

2. Grundkonzept des Systems

Das System orientiert sich an den Zahlschein und Erlagschein Systemen.

Nachdem der Warenkorb gefüllt ist, und der Kunde sich entschieden hat zu bestellen fängt das System zu laufen an:

1. Der Verkäufer stellt dem Kunden einen Zahlschein aus, und läßt den Kunden den Zahlschein downloaden. Der Kunde downloadet den Zahlschein, und speichert ihn auf der Festplatte ab.

2. Der Kunde steigt in sein Online-Banking System ein, und importiert dort den Zahlschein. Dadurch wird der Zahlschein fertig ausgefüllt. Dann kann der Kunde die Daten der Transaktion wie üblich noch kontrollieren und verändern, bevor er sie mit einer TAN unterschreibt.

3. Nachdem der Kunde die Transaktion gestartet hat, stellt die Bank die Transaktionsbestätigung auch in digitaler Forma als Download zur Verfügung.

4. Der Kunde loggt sich wieder beim Verkäufer ein, und uploadet die Bestätigung der Bank, wodurch der Verkäufer die Bezahlung bestätigt bekommt, und die weitere Lieferung auslösen kann.

2.1. Eigenschaften

Betrachten wir nun verschiedene Eigenschaften des hier aufgestellten Systems:

3. Vereinfachung für den Kunden

Das Grundkonzept hat die Schwäche, daß der Benutzer dauernd irgendwelche Dateien auf dem Computer abspeichern muß, und die dann wieder uploaden muß. Da muß er dann jedesmal einen Dateinamen vergeben, ...
Dem kann Abhilfe geschaffen werden:
Der Kunde installiert sich einen Transaction-Handler, den er von seiner Bank zur Verfügung gestellt bekommt.

3.1. Transaktionshandler

Ein Transaction Handler ist ein kleines Programm, das Dateien, die man downloadet entgegen nimmt, und dann auf Anfrage an eine vorbestimmte URL schickt.
Das heißt, wenn der Kunde beim Verkäufer auf den Link zum downloaden des Zahlscheines klickt, kommt vom Transaction Handler die Frage, ob dieser Zahlschein automatisch an seine Bank geschickt werden soll. Wenn der Kunde dies mit Ja beantwortet, wird der Zahlschein verschlüsselt an das Online Banking System geschickt, und dort genauso behandelt, wie es mit dem Upload passiert wäre. Das Online-Banking System stellt den Zahlschein in den Pool der Transaktionsvorschläge, wo er auf die Bestätigung des Benutzers mit der TAN wartet.
Der Zahlschein enthält zusätzlich die URL, an die der Verkäufer dann die Bestätigung geschickt bekommen haben will.
Derselbe Transaktionshandler nimmt dann die Transaktionsbestätigung entgegen, und schickt sie wieder zum Verkäufer.

Der Transaktionshandler wird dem Kunden entweder von der Bank zur Verfügung gestellt, oder ist eine Standardlösung, die entsprechend von der Bank Online konfiguriert wird.

4. Sicherheit

Nun, zum Thema Sicherheit gibt es eine große Menge an Dingen, die möglich sind, und glücklicherweise relativ einfach realisiert werden können.

Viele davon können von der SET (Secure Electronic Transaction) Spezifikation übernommen werden.

Betrachten wir die einzelnen Sicherheitsaspekte:

4.1. Datenübertragung

Wir haben hier grundsätzlich gesehen 2 Datenübertragungsmöglichkeiten: HTTP und SMTP
HTTP hat den großen Vorteil, daß SSL praktisch fast überall zur Verfügung steht, und die Datenintegrität und auch die Vertraulichkeit bei der Datenübertragung sicherstellt.
Bei SMTP hat sich leider bis heute keine End-zu-End Sicherung wirklich durchgesetzt, S/MIME und OpenPGP sind beides mögliche Optionen, sind aber beide nicht verbreitet genug.
Im Allgemeinen muß man außerdem davon ausgehen, daß Verschlüsselung ein relativ schlechtes Image hat, und bei Emails schwer durchzusetzen sein wird.
Ich schlage daher vor, soweit möglich HTTPS (SSL) einzusetzen.

4.2. Integrität

Die Integrität der Daten ist durch das Systemdesign nicht immer unbedingt notwendig, kann aber sehr leicht durch transparente Signatur angeboten werden. Hierfür sollte der Verkäufer und die Bank die jeweiligen Dokumente entsprechend digital signiert zur Verfügung stellen. Der Kunde braucht keine eigene Möglichkeit, zu signieren, da die Transaktionen ja über PIN und TAN zwischen Kunde und Bank abgesichert sind. Dadurch kann man ein relativ kleines PKI System für alle Banken und optional die Händler aufziehen, und muß nicht jedem Kunden eine digitale Identität verpassen. Hier könnten auch bestehende Infrastrukturen genutzt werden, wie X509v3 Zertifikate, oder OpenPGP.

4.3. Vertraulichkeit

Weder die Vertraulichkeit der Zahlscheine, noch die Vertraulichkeit der Zahlungsbestätigungen ist sicherheitskritisch. Wer versteckt schon unausgefüllte Zahlscheine im Safe?
Beide sind für die Privatsphäre des Benutzers notwendig, aber eine Veröffentlichung von Zahlscheinen oder Zahlungsbestätigungen sollte außer der möglichen Verletzung der Privatsphäre kein weiteres sicherheitskritisches Problem dar. Ein einfacher Zugriffsschutz wie es Online-Banking durch die Benutzerauthentifizierung bietet, Verschlüsselung der Leitungen, und das nicht-abspeichern der Daten auf der Festplatte durch den Transaktionshandler müßten ausreichenden Schutz bieten.

4.4. Anonymität

Der Verkäufer und die Bank bestimmen gemeinsam den maximalen Anonymitäts-Level.

Grundsätzlich gibt es 3 Bemühungen des Kunden auf Anonymität:
Daß der Verkäufer nicht weiß, bei WELCHER Bank der Kunde ist, und welche Identität er dort hat
Daß die Bank nicht weiß, WO der Kunde WAS gekauft hat
Daß auch keine dritte Partei die Daten bekommt, wer wo was gekauft hat, und diese verknüpfen kann.

Auf folgende Art und Weise kann die Sicherheit des Systems gewährleistet werden, und ein hoher Level an Anonymität garantiert werden:

Jedes Dokument wird in mehreren Stufen signiert.

Stufe 1 sind die ganz zentral notwendigen Daten. (Welches Konto, wieviel Geld)
Stufe 2 sind für die Transaktion notwendige Daten. (Transaktionsnummer)
Stufe 3 sind nicht notwendige Daten. (Verwendungszweck)

Jede Stufe wird zusammen mit den vorhergehenden Stufen signiert:

Daten1
Signatur(Daten1)
Daten2
Signatur(Daten1,Daten2)
Daten3
Signatur(Daten1,Daten2,Daten3)

Dadurch können die Daten stufenweise getrennt werden, sind aber trotzdem gemeinsam signiert.

Dadurch kann sich der Kunde entscheiden, bis zu welcher Stufe er die Daten weitergeben will, die Integrität der Daten ist aber trotzdem gewährleistet.

4.5. Denial of Service

Hier besteht wahrscheinlich die Möglichkeit, eine grofle Anzahl von Zahlscheinen automatisiert an die Bank zu schicken, und damit vielleicht die Benutzung des Online-Bankings für den Kunden unmöglich macht. Es ist daher beim Design des Online-Bankings darauf zu achten, dafl das Online-Banking in der Vorschlagsliste mit einer großen Anzahl an Vorschlägen arbeiten können muß. Geeignete Maßnahmen, einen Mailbomben-Effekt zu verhindern, wären, nur jeweils 50 Einträge der Vorschlagsliste anzuzeigen. Sobald die notwendige Infrastruktur bei den Händlern aufgebaut worden ist, könnte man beim automatischen Import nur signierte Zahlscheine zuzulassen. Doppelte Zahlscheine (Rechnungsnummer) sind beim Import grundsätzlich zu ignorieren.

4.6. Single-Point of Failure

Der Single-Point of Failure, was die Sicherheit betrifft ist auf jeden Fall bei der Bank. Die Bank trägt eine große Verantwortung, das Online-Banking entsprechend sicher zu gestalten.

4.7. Wiederholungsangriffe

Ein Wiederholungsangriff geht davon aus, daß ein Angreifer Transaktionsdaten bekommt, die er dann in modifizierter Form wiederholt an ein automatisiertes System schickt, um daraus einen eigenen Vorteil zu erhalten. Wiederholungsangriffe sind durch das Systemdesign für einen Angreifer nicht sonderlich sinnvoll, da er nur schwer einen direkten Vorteil erhält, da jede Transaktion vom Benutzer unterschrieben werden muß, und er dadurch nur schwer dem Benutzer eine Transaktion unterjubeln kann.

4.8. Allgemeines Angriffsmodell

Beteiligte Parteien:
- Verkäufer
- Käufer
- Bank des Käufers
- Bank des Verkäufers
- CA (Zertfifizierungsstelle)

Beteiligte Objekte:
- Online-Banking Server
- Signaturserver
- Webshop

- Client Computer ohne Transaktionshandler
- Client Computer mit installiertem Transaktionshandler

Kommunikationsverbindungen:
- Zwischen dem Online-Banking Server

Ein Angreifer kann grundsätzlich:
- Sich als eine der beteiligten Parteien ausgeben
- Die Kontrolle über eines der Objekte übernehmen
- Kommunikationsverbindungen passiv abhören, oder aktiv manipulieren

5. Fallbeispiele

5.1. Lion.CC

Lion.CC ist ein österreichischer Online Versandhandel für Bücher und Multimedia. Lion ging den aufwändigen Weg, mit den verschiedenen Banken direkte Schnittstellen zu schaffen, und die Kunden direkt zu den Banken zu verweisen. Hier ein Auszug aus den Oft gestellten Fragen auf der Webseite von Lion:

> Kreditkarte Wir akzeptieren gerne Visa und EuroCard/MasterCard. Ihre Kreditkarte wird erst am Tag der Auslieferung belastet. Die Übertragung der Kreditkartendaten ist durch modernste Verschlüsselungstechniken (SSL 3-Verschlüsselung) absolut sicher.
>
> Erlagschein (ausgenommen Bestellungen von LIONtickets) Sie erhalten mit Ihrer Lieferung einen Erlagschein und bezahlen damit. Bei dieser Art der Bezahlung wird eine Bearbeitungsgebühr von 0,50 EUR (ATS 6,88) verrechnet. ACHTUNG: Die Bezahlung mit Erlagschein ist erst ab Ihrer zweiten Bestellung bei LION.cc möglich.
>
> Bankeinzug (ausgenommen Bestellungen von LIONtickets) Mit dem Bankeinzug erledigt sich die Bezahlung Ihrer Rechnung von selbst. Alles, was Sie tun müssen, ist Ihre Bankverbindung und Ihre Kontonummer bekanntzugeben. Die Zahlung per Bankeinzug funktioniert nur über österreichische Bank- und Kreditinstitute.
>
> Nur LIONtickets: Bank Austria Online-Konto Hier erfolgt die Bezahlung über eine speziell entwickelte Software der Bank Austria. Nach der Kartenreservierung leiten wir Sie in den Bank Austria HOST, wo Sie Ihre Kontonummer, Verfügernummer und Ihre TAN eingeben und so Ihre Tickets sicher bezahlen.

Das grundsätzliche Problem an allen diesen Zahlungsmethoden ist, daß der Kunde Lion ja grundsätzlichermaßen nicht trauen kann, zur richtigen Bankseite sicher weitergeleitet zu werden. Es wäre ja möglich, daß Lion den Kunden zu einer Seite schickt, die für den Benutzer so wie die Bank aussieht, aber nur alle Eingaben des Benutzers protokolliert. Dadurch mußten alle beteiligten Banken das von Lion entwickelte System detaillierten Kontrollen unterziehen, um sicherzustellen, daß alles in Ordnung ist, und diese Sicherheitsbestätigungen dann an ihre Kunden weitergeben.
Eben dieses grundsätzliche Problem wurde mit diesem Konzept gelöst, weil hier nicht der Verkäufer den Kunden zu seiner Bank schickt, sondern der Kunde selber von sich aus (oder vom Transaktionshandler, den er von seiner Bank bekommen hat) zu seiner Bank geht, weil er einen Zahlschein bekommen hat. Dadurch kann der Verkäufer den Kunden grundsätzlich nicht "irgendwohin" schicken.

5.2. NaN (Not A Number)

NaN ist eine holländische Firma, die 3D Software entwickelt, und über ihren Webshop Bücher, CDs, Lizenzen und Merchandising Artikel anbietet. NaN bietet neben Kreditkarten auch normale Banktransfers

als Zahlungsmöglichkeit an. Nachdem man bestellt hat, sieht man eine Webseite, auf der alle notwendigen Transaktionsdaten stehen. Diese kann man dann selbst im Onlinebanking seiner Bank abtippen, oder auf eine andere Art seiner Bank zukommen lassen. Ausdrucken und am Schalter vorbeibringen müßte auch funktionieren. Sobald NaN dann das Geld am eigenen Konto empfangen hat (was einen Monat dauern kann), wird die Lieferung in Gang gesetzt.
Dieses System ist grundsätzlich nicht schlecht, nur gibt es einige Schwachstellen:
- Man könnte sich beim Abtippen der Transaktionsdaten vertippen (-> Zahlschein)
- Es dauert lange, bis es endlich zur Lieferung kommt (-> Zahlungsbestätigung)

Die Vertrauensbeziehung vom Kunden zum Händler ist problematisch, da der Kunde vom Zeitpunkt der Überweisung bis zum Erhalt der Ware lange warten muß

5.3. Kreditkarten

Bei Kreditkartentransaktionen gibt es derzeit 3 Systeme im Internet:
1. Man gibt dem Händler die Kreditkartennummer
2. Der Händler leiteten den Kunden um zu einem Aquirer Bei der Umleitung des Händlers zum Aquirer entstehen 2 Sicherheitsfragen: Wir der Kunde richtig umgeleitet? Dies kann durch aufwändige Kontrollverfahren durch den Aquirer beim Händler großteils sichergestellt werden. Ist der Aquirer für den Kunden vertrauenswürdig? Ich habe bisher in der Praxis keinen Maßnahmen beobachtet, die dieses Vertrauen aufbauen würden.
3. SET

6. Auswirkungen

6.1. Vorteile des Systems

6.1.1. Vorteile für den Kunden

Die Zahlscheine stellen sicher, daß die Transaktionsdaten richtig übermittelt werden. Die Probleme falsch eingegebener Bankleitzahlen, Kontonummern, Transaktionshöhen oder Währungen beim Online Banking fällt weg, kann aber trotzdem vom Benutzer kontrolliert werden.

Zeitersparnis, weil das abtippen von Transaktionsdaten sehr lästig und zeitraubend sein kann

Die Möglichkeit, Dinge im Internet zu bestellen, ohne eine Kreditkarte zu besitzen.

Der Kunde hat jederzeit vollen Überblick über den Status seiner Transaktion.

Der Kunde hat die Möglichkeit, die Transaktion zu anonymisieren

6.1.2. Vorteile für den Verkäufer

Die Kosten des Kreditkartenhandlings fallen wahrscheinlich weg

6.1.3. Vorteile für die Bank

Erschließung des Marktsegments der Online-Transaktionen, die sonst an Kreditkartenfirmen oder Mobilnetzbetreiber verloren gehen

Keine Sicherheitsprobleme, da keine direkte Kommunikation mit dem Verkäufer passiert

6.2. Nachteile

Die Banken erfüllen derzeit keine (oder nur wenig) Versicherungsfunktionen, wie dies die Kreditkartenfirmen tun. Allerdings ist dies kein grundsätzliches Problem dieses Konzeptes, sondern eher eine Chance. Der Kunde ist ja nicht daran gebunden, mit dem Zahlschein zu seiner eigenen Bank zu gehen, er kann sich dann möglicherweise zwischen seiner Bank und anderen Versicherungsanbietern entscheiden, wodurch eine Transparenz der Versicherungsfunktion entstehen kann. Der Kunde ist nicht mehr gezwungen, die Versicherungsleistung der Kreditkartenfirmen in Anspruch zu nehmen.

7. Implementierung

Was ist an welcher Stelle zu tun, um das Konzept in die Realität umzusetzen?

7.1. Bank

Die Bank sollte:

7.1.1. Schnittstellen zum Einspielen von Zahlscheinen

Eine davon mittels Datei Upload in einem HTML Formular
Eine automatisierbare über eine definierte CGI Schnittstelle (könnte auch XMLRPC oder SOAP werden)
Wichtig neben der Schnittstellen ist die Funktionalität des Ausfüllens mit den Kundendaten, und das Ablegen in der Vorschlagsliste.

7.1.2. Signaturserver

Das zweite wichtige ist das zur Verfügung stellen der Transaktionsbestätigung. Hierfür ist das Einrichten eines internen Signatur-Services sinnvoll, um alle Transaktionsbestätigungen automatisiert zu signieren. Hierfür wird wahrscheinlich ein eigener Server notwendig sein, der entsprechend physisch und softwaretechnisch abgesichert sein muß.
Zum Design des Signaturservers:

Der Signaturserver sollte
- asynchron einzelne und größere Mengen (Batch) von Zahlscheinen entgegennehmen können
- die einlangenden Zahlscheine einer kurzen semantischen Kontrolle unterziehen
- mehrere verschiedene Signaturverfahren parallel anwenden, damit bei der Verifikation nur eine der Signaturen erfolgreich kontrolliert werden muß (OpenPGP/X509/...)

die signierten Zahlscheine
- synchron zurückliefern
- auf einem anderen System abliefern
- per Email verschicken (SMTP)

Als Transportprotokoll kann TCP, HTTP, XMLRPC, SOAP herangezogen werden.

7.1.3. weitere Dienste

In weiterer Folge kann und sollte die Bank einige weitere Services anbieten:
- Allen Kunden den Transaktionshandler zur Verfügung stellen (individualisierter Download, Marketing Aktion)
- Zertifizierung von vertrauenswürdigen Verkäufern, und informieren des Kunden über die Vertrauenswürdigkeit des Verkäufers beim Import des Zahlscheines

7.2. Verkäufer

Der Verkäufer sollte:
Dem Webshop beibringen, bei der Bestellung downloadbare Zahlscheine zur Verfügung zu stellen.
Diese können in weiterer Folge digital signiert werden, müssen aber nicht unbedingt.

Wesentlich schwieriger ist dann das Akzeptieren der Transaktionsbestätigung, hier wird eine ausgefeilte

PKI notwendig. Oder ein Verifikationsservice der Bank des Verkäufers.

7.3. Kunde

Der Kunde hat es wohl am einfachsten. Er kann entweder schon jetzt die Zahlscheine abspeichern und uploaden, oder dann mit dem Transaktionshandler arbeiten.
Wichtig wird es, den Kunden soweit zu schulen, daß er mit dem System umgehen kann.

8. Zertifizierungsstellen

Die Zertifizierungsstellen müssen die notwendige Infrastruktur zur Verfügung stellen, alle beteiligten Banken, Versicherungs-institutionen und Händler zu zertifizieren.

9. Protokolldefinition

9.1. Bank->Verkäufer:

```
<BANKACCOUNT>
  <BLZ>35000</BLZ>
  <ACCOUNT>106485048001</>
</BANKACCOUNT>
```

9.2. Bank->Kunde:

```
<BANKACCOUNT>
  <BLZ>35000</BLZ>
  <ACCOUNT>35356738998</>
</BANKACCOUNT>
```

9.3. Verkäufer -> Kunde:

```
<PAYMENT>
 <ID>455678</ID>
 <DATE>20020526T0740</DATE>
 <BANKACCOUNT>
   <BLZ>35000</BLZ>
   <ACCOUNT>106485048001</>
 </BANKACCOUNT>
 <AMOUNT>100.40</>
 <CURRENCY>EUR</>
 <SUBJECT>Einkauf</SUBJECT>
</PAYMENT>
```

9.4. Kunde -> Bank

```
<TRANSACTION>
 <PAYMENT>
 <ID>455678</ID>
 <DATE>20020526T0740</DATE>
 <BANKACCOUNT>
   <BLZ>35000</BLZ>
   <ACCOUNT>106485048001</>
 </BANKACCOUNT>
 <AMOUNT>100.40</>
```

```
   <CURRENCY>EUR</>
   <SUBJECT>Einkauf</SUBJECT>
  </PAYMENT>
  <BUYER>
   <BANKACCOUNT>
    <BLZ>35000</BLZ>
    <ACCOUNT>35356738998</>
   </BANKACCOUNT>
   <TEXT>Käufer</TEXT>
   <TAN>346D5FFIL</TAN>
  </BUYER>
</TRANSACTION>
```

9.5. Bank -> Kunde (-> Verkäufer)

```
<DIGSIG>
 <DATE>20020527T1730</DATE>
 <PAYMENT>
  <ID>455678</ID>
  <DATE>20020526T0740</DATE>
  <BANKACCOUNT>
   <BLZ>35000</BLZ>
   <ACCOUNT>106485048001</>
  </BANKACCOUNT>
  <AMOUNT>100.40</>
  <CURRENCY>EUR</>
  <SUBJECT>Einkauf</SUBJECT>
 </PAYMENT>
</DIGSIG>
```

10. Offene Probleme

Unterjubeln von Zahlscheinen
DigSig