

Schein und Sein sicherer Authentisierung

Forum 2: Authentisierung von Mitarbeitern, Kunden und Dritten in offenen Systemen

Aspekte des m-Bankings

René Müller

UBS AG, e-Access & Shared Services



Disposition

- **Thematik 'Technologie und Anforderungen des Markts'**
- **Thematik 'Revenue Stream'**
- **Thematik 'Personal Trusted Device'**
- **Diskussion**

Stand der Mobilkommunikation in der Schweiz*

Einige Eckdaten

- ◆ **Fast 50% der Benutzer wollen auch privat immer erreichbar sein**
- ◆ **v.a. Anschaffung des Handys aus geschäftlichem Grund, dann aber private Nutzung**
- ◆ **40% benutzen SMS mind. 1x wöchentlich, 20% regelmässig beruflich**
- ◆ **Nur 16% nutzen ab und zu Datendienste, 40% haben dazu das nötige Equipment (Grund: zu hohe Kosten, zu geringe Bandbreiten, unzulängliche Displays)**

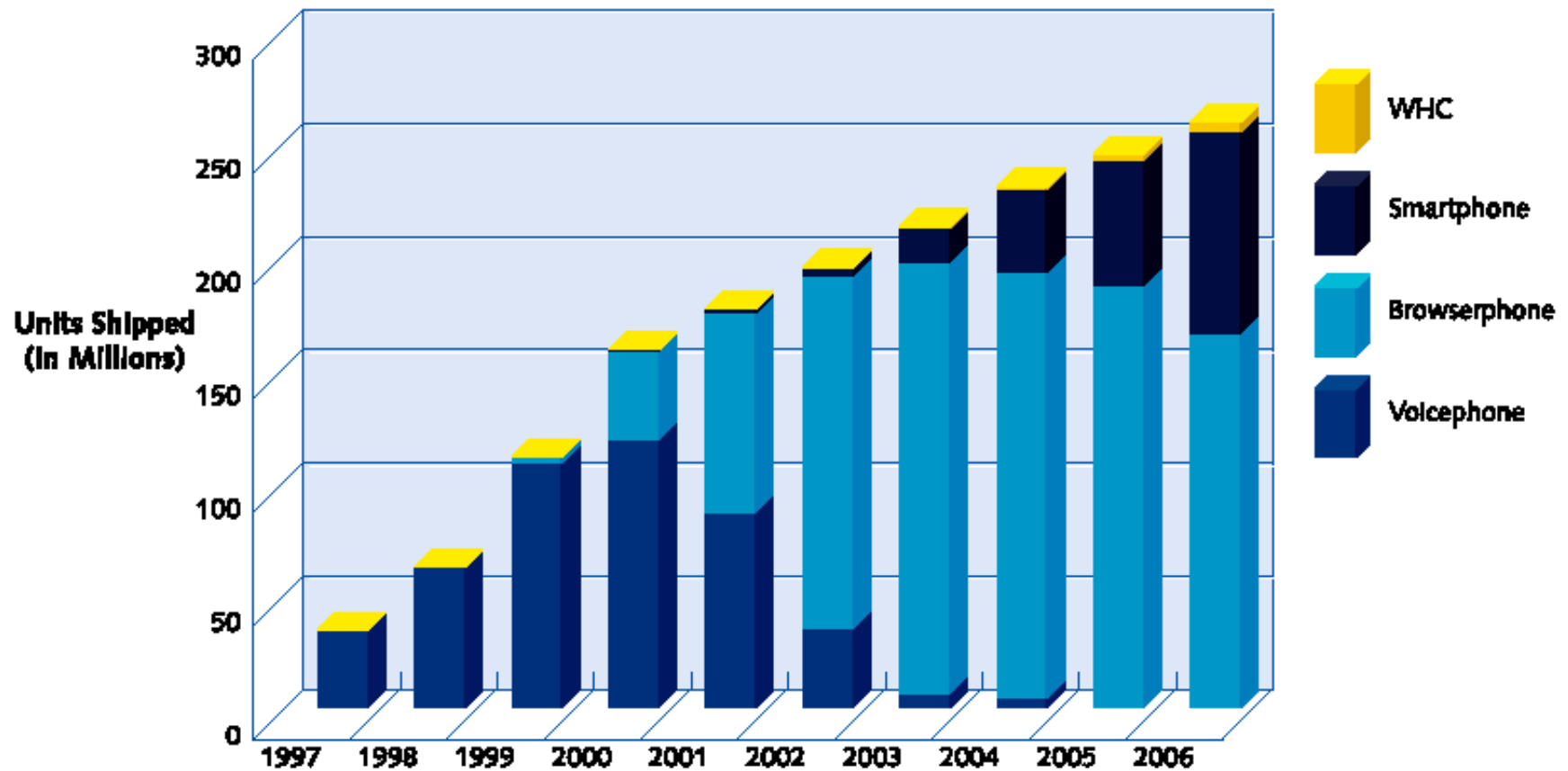
Thesen

- ◆ **Messaging stösst auf grosse Akzeptanz (asynchrone Dienste, Push-Services)**
- ◆ **Ortsabhängige Informationen können sich durchsetzen, wenn sie einfacher werden**
- ◆ **Die Übermittlung von Bildern wird ein Erfolg, selbst bei schlechter Qualität**
- ◆ **Identifikation von Benutzern für zB. Freigabe von Mikrobeträgen könnte für mobile Endgeräte wichtig werden**
- ◆ **Computerspiele für mehrere Benutzer werden keine Killer- m-Services**



***) Quelle: Gleichnamige Studie von Dr. Pascal Sieber & Partners AG, Nov. 2001**

Verbreitung mobiler Geräte in West Europa*



Note: This shows the total annual shipments of cellular terminals in western Europe, split by the intelligence and functionality resident in the handset.

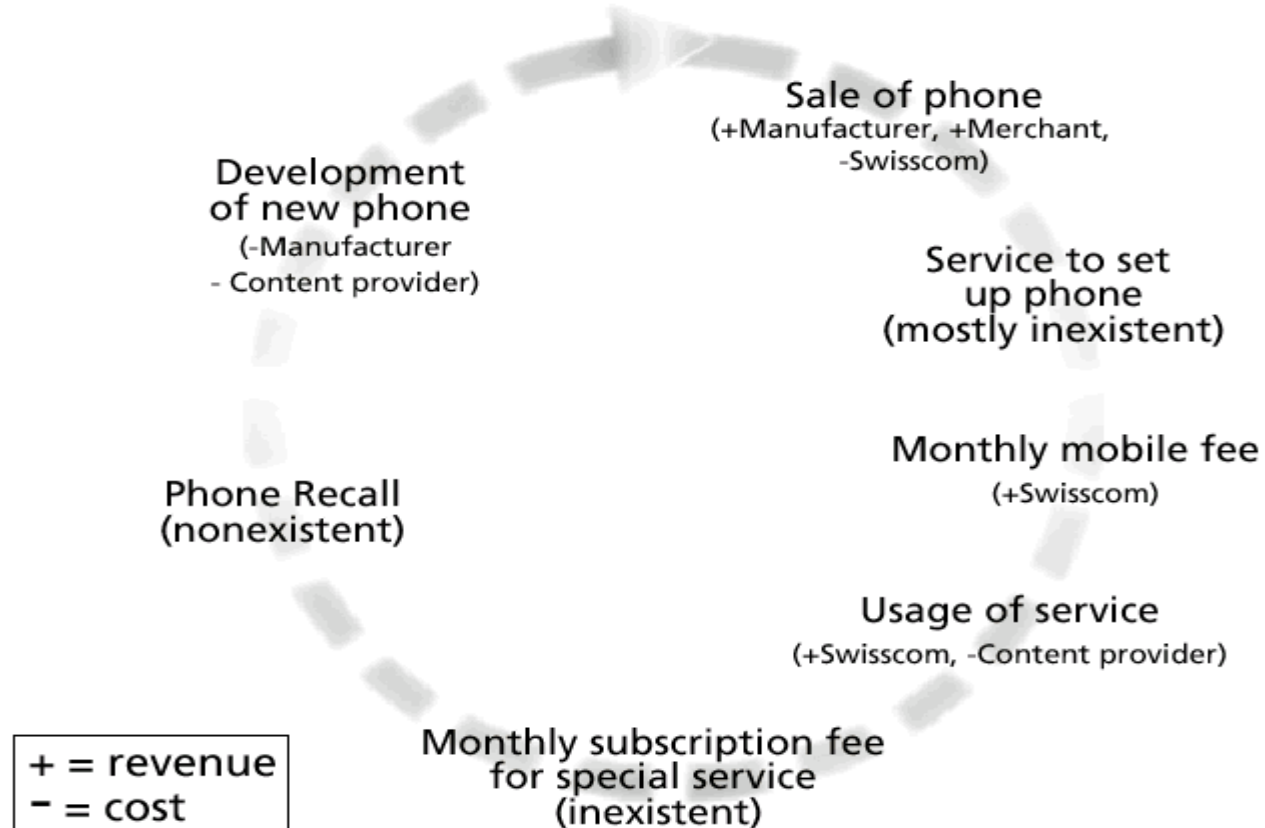
Wichtigste Kunden-Bedürfnisse

- ◆ **Nutzung der e-Channels als Comodity-Dienstleistung mit Value Add zum traditionellen Bankgeschäft**
- ◆ **Höchste Ansprüche in bezug auf Trust, Liability und Verfügbarkeit der Systeme**
- ◆ **Keine oder nur minimale Bereitschaft für Installationen**
- ◆ **Einfachheit und Geschwindigkeit in den Anwendungen**
- ◆ **Mobile Information/Nutzung, stationäre Konfiguration/Hauptnutzung**
- ◆ **Möglichst wenig zusätzliche Geräte/Listen/Passwörter**
- ◆ **e-Payments → (noch) wenig Bedürfnisse; Kartenlösungen bevorzugt.**

Disposition

- Thematik 'Technologie und Anforderungen des Markts'
- **Thematik 'Revenue Stream'**
- Thematik 'Personal Trusted Device'
- Diskussion

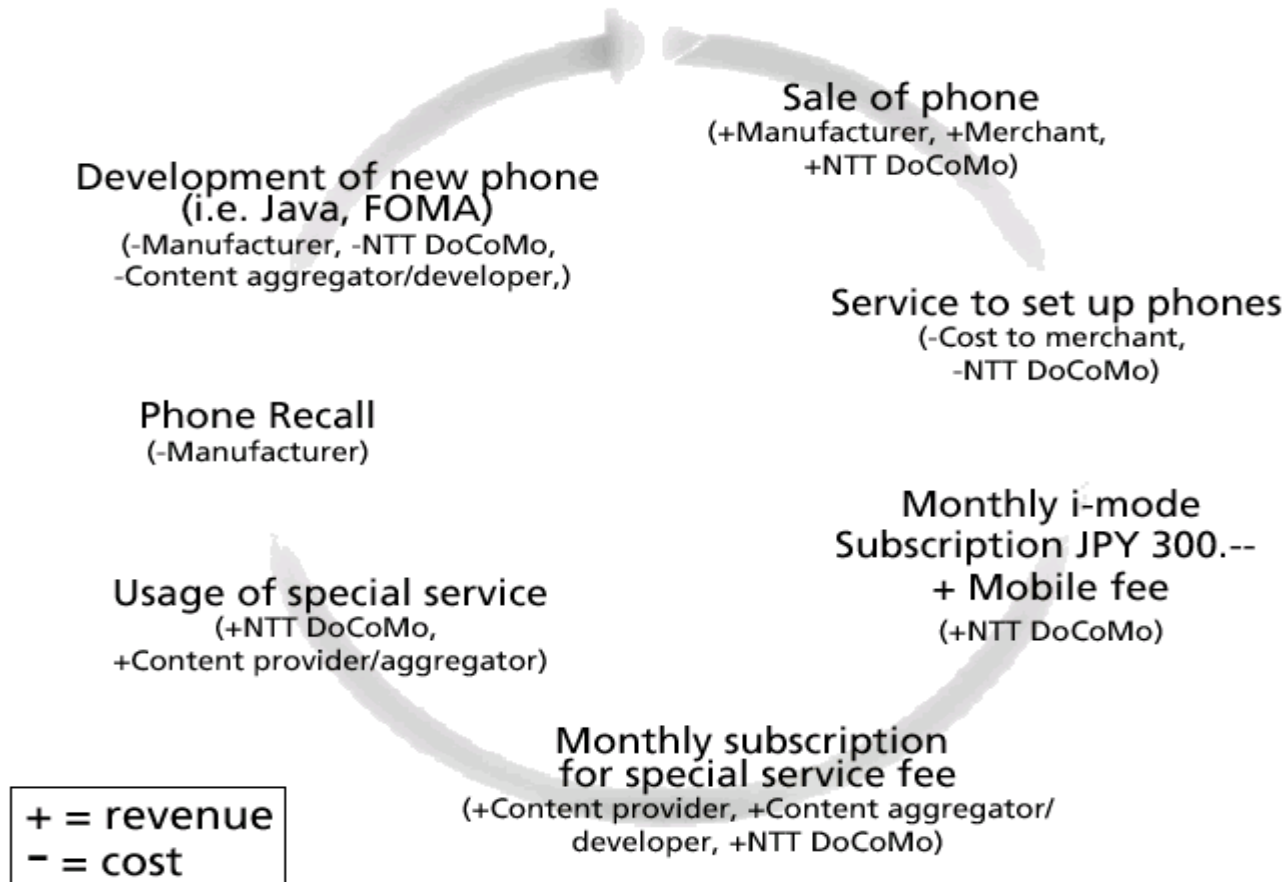
Revenue Stream: das Beispiel GSM (Schweiz)



Es gibt noch immer kaum einen positiven Business Case für den Content Provider und Entwickler!

→ GPRS wird einiges an Veränderungen bringen!

Revenue Stream, zum Vergleich: i-mode



Es profitieren alle, da die Einnahmen und Kosten verteilt werden; allerdings besteht eine grosse Abhängigkeit/Monopolsituation

Erkenntnisse

- ◆ Auf ‚mobile‘ zugeschnittener Content und Marketing/Branding als wichtigstes Element
- ◆ Umfassender Service reicht vom Set-up bis zum Support
- ◆ Hohe Funktionalität im Device (zB. vorinstallierte Java-Classes) erlaubt geringeren Bandbreitenbedarf → Modell i-Mode kaum anwendbar in Europa, da nicht die selbe Monopol-Situation (NTTDoCoMo)
- ◆ Interesse aller Beteiligten, falls alle daran verdienen: Verkäufer, Operatoren, Content-Entwickler und -Anbieter, uam.
- ◆ Kulturelle Unterschiede spielen eine wichtige Rolle (zB. Japan nur 11% PC-Verbreitung, lange Gesprächszeiten, Technologie-Akzeptanz, uam.)
- ◆ Bereitschaft des Marktes laufend beurteilen - ist in raschem Wandel!

Disposition

- Thematik 'Technologie und Anforderungen des Markts'
- Thematik 'Revenue Stream'
- **Thematik 'Personal Trusted Device'**
- Diskussion

WPKI Pilot

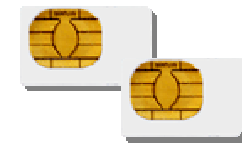
- ◆ Gemeinsames Pilotprojekt zw. **UBS** und **NOKIA**
- ◆ WIM-Karte und Perso-Software:
Oberthur Card Systems

WIM (Wireless Identity Module): "*Tamper proof token in the mobile client in which security information e.g. private keys are stored*"



SIM-Chip eines Operators

SIM



WIM

Bank Issued WIM

➔ **Der Bank-Chip wird hier nur als WIM genutzt; er ist aber ein Open Platform Chip, der noch weitere Module enthalten könnte !!! (siehe zB. NOKIA/Nordea/VISA-Pilot)**



Ziele und Zweck

- ◆ Test des dual-chip Konzepts mit interessierten Kunden: benutzerfreundlicheres Login auf UBS e-banking wap → WTLS Class 3 Authentisierung
- ◆ Vertiefung von Know-How und Sammeln von Erfahrungen
- ◆ Realisierung eines Elements der ‚Preferred Payment Architecture‘ und damit Umsetzung von Findings im Mobey-Forum (siehe www.mobey.org)
- ◆ On-board key generation (OBKG), der Private Key verlässt die Karte niemals
- ◆ Zur Vereinfachung: UBS self-signed CA, keine CRL
- ◆ Pilot-Beginn: April 2002
- ◆ Begrenzte Dauer von ca. 6 Monaten

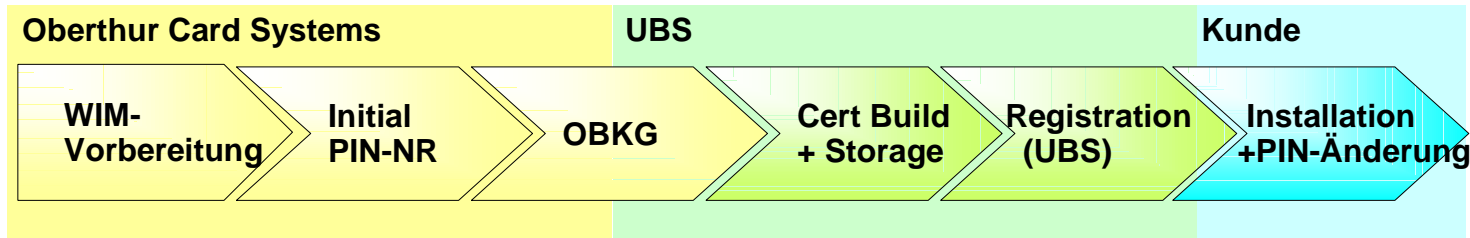


**WAP Handy mit
dual-chip
Technologie**

(Nokia 6310 mit WIM-
modul auf zweitem Chip)



Personalisierung und Login-Prozess



FIRST LOGIN

- Gateway-Aufruf mit dual-chip Device
- Login mit VNr/Pwd/StrL
- „Announce Cert“
- Service-Nutzung resp. Logout

CERT LOGIN

- Gateway-Aufruf mit dual-chip Device
- Login mit (VNr)/PIN-NR/signText)
- Service-Nutzung resp. Logout

(Zugang auf das Gateway mit beliebigem anderen Device führt zum normalen Login)



Einige Argumente für den Dual-Chip Approach

- ◆ **Klare Separierung der Zuständigkeiten und Verantwortlichkeiten**
 - keine Interessenkonflikte/Datenschutzprobleme mit Operator
 - Bank- und Operator-issued Chip, je unabhängig unter Kontrolle

- ◆ **Flexiblere Implementierung, Bewirtschaftung und Nutzung**
 - grundsätzlich nebst WIM auch weitere Anwendungen möglich
 - Kundennutzen: grösstmögliche Flexibilität

- ◆ **Grundsätzlich mögliche Integration in bestehende Systeme**
 - Chipkarten-Personalisierung
 - PKI-Management Systeme

Disposition

- Thematik 'Technologie und Anforderungen des Markts'
- Thematik 'Revenue Stream'
- Thematik 'Personal Trusted Device'
- **Diskussion**

Kontakt

UBS AG
e-Access & Shared Services
René Müller
Postfach
8098 Zurich

E-Mail: rene-za.mueller@ubs.com

Tel.: +41 1 236 01 36

<http://www.ubs.com/g/ebanking.html>

