



Security in Mobile banking and mCommerce

- in practice

Norsk UMTS Forum

June 4, 2008

Bjørn Sloth



Outline

Security and threats in

- Internet Banking and e-commerce
- Mobile Banking and mCommerce

Presentation will cover

- Secure authentication
- Secure communication
- Security hazards
- "End-to-end" security
- Example applications and demo



From Internet to Mobile Banking

Internet banking is now a commodity

- no public bank can exist without offering a full-service internet bank to the customer

In few years, mobile banking will be just as important to the customer

- and will be more frequently used!

- Will be used everywhere
- But can we expect the same level of a security from a mobile terminal?
- Can mobile terminals be used for transactions?
- And what if we loose the mobile terminal?



Secure authentication



2-factor authentication in Internet Banking

- Possession factor
- Knowledge factor





2 – factor authentication in e-commerce

- BankAxept
- 3D Secure
 - Verified by Visa
 - MasterCard® SecureCode™
- BankAxess





Secure Communication

https over:

- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

Transport Layer Security (TLS) and its predecessor, **Secure Sockets Layer (SSL)**, are cryptographic protocols that provide secure communications

(Source: Wikipedia)



But remember...

→ Security is no better than the weakest link!





Security hazards

- Hacking
- Rootkit
- "Single sign-on"?
- DDOS
- Phishing
- "Man-in-the-middle"
- "Laura at the counter"
or
"Kent the self-made"





Applying all this to the mobile....

- How to apply the internet security to the mobile channel?
- Can we make it even better?



Mobile banking authentication

- BankID Mobile
- Mobile OTP solutions
 - Mobile generated OTP
 - Server generated OTP
 - Open Source solutions

BankID



ENCAP

todos[®]



mCommerce authentication

- 3DSecure / Mobile OTP



ENCAP

todos[®]

MasterCard.
SecureCode.

VERIFIED
by VISA

- BankAxxess / BankID Mobile

BankID

bank
axess



Secure mobile communication

Https over:

- SSL
- TLS
- WAP TLS
- ~~WTLS~~

➔ And how to implement it securely on the mobile?

➔ What about terminals not supporting SSL/TLS?



WTLS and end-to-end security

➔ **Reminder: SMS is not a secure channel!**

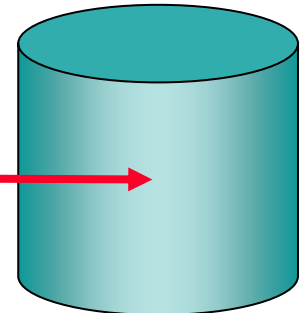
User

Client

Transport

Termination

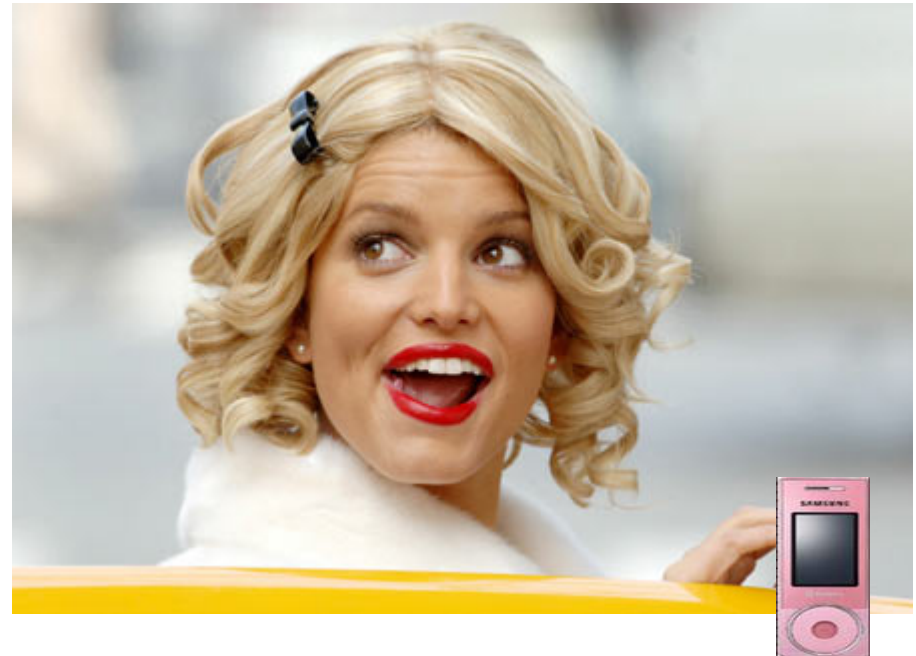
Server





Security hazards

- Midlet hacking
- Rootkit
- "Single sign-on"?
- DDOS
- Phishing
- "Man-in-the-middle"
- "Laura at the counter"
 - with a mobile!
 - with all her money in it!





Denial of Service (DDOS)

Requires that someone can steal your ID

→ Tie the mobile service to the mobile terminal!



Phising and "man-in-the-middle"

"Social hacking"

- The user must be "fooled" to browse to a hackers web site/server

- Mobile services should use fixed server address

- Mobile services should not give Laura or Kent any possibilities to make mistakes



Other attacks

Web/WAP browsers and visible (X)HTML

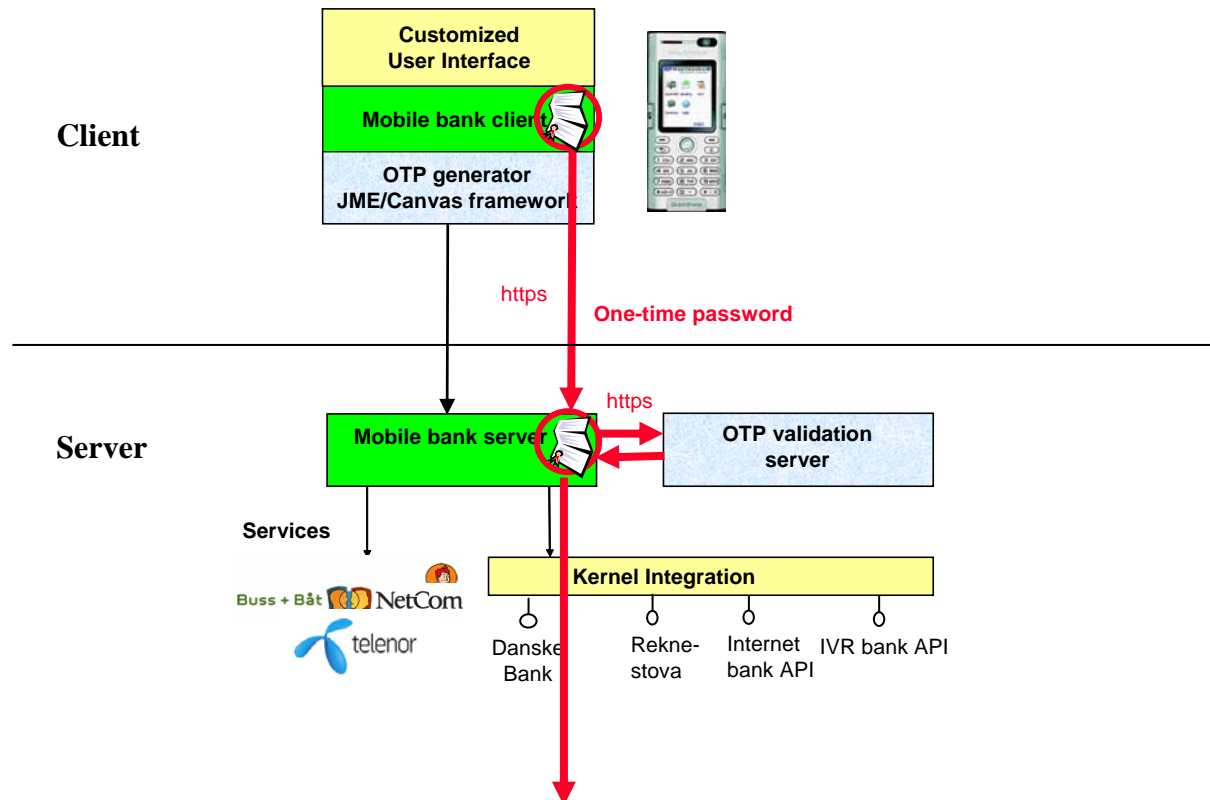


Does clients on the mobile add security?

- End-to-end security
 - Can avoid mobile browser security flaws
 - Can integrate with Mobile OTP
 - Rich clients cannot be fooled as easily as Laura or Kent
- ➔ Still, security is no better than the weakest programmer!

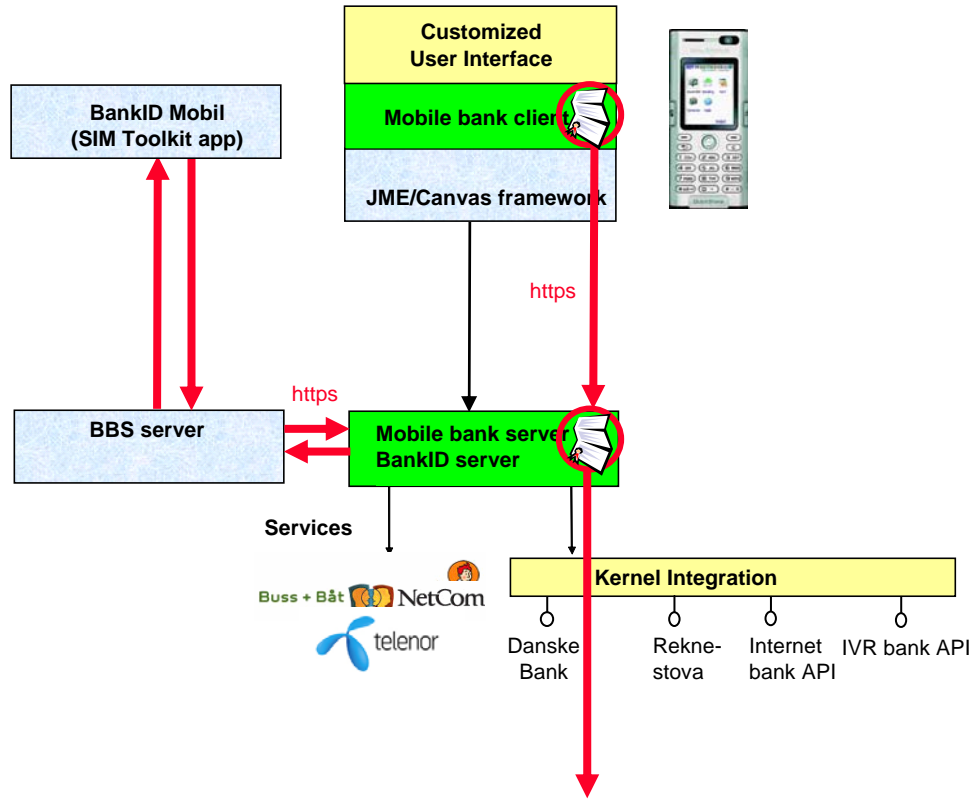


”End-to-end” security – Client-based application and Mobile OTP





With BankID Mobile





Demo

- Mobile OTP integrated in a Midlet
- Midlet using BankID Mobile





Summary

- Mobile authentication
- Secure mobile communication
- How to avoid security hazards



Thank you!

Bjørn Sloth

sloth@systemek.no

9095 2228