LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LFE Medieninformatik • Max-Emanuel Maurer

Oberseminar - Abschlussvortrag Diplomarbeit

SeCuUI - Secure and Fast Data Submission to Public Terminals Using an Autocomplete Mechanism

Responsible Professor:	**Prof. Dr. Heinrich Hußmann**
Supervisor:	**Dipl. Medieninf. Alexander De Luca**
Start:	**February 01 2009**
End:	**June 30 2009**

7. Juli 2009

Overview

Source: sxc.hu

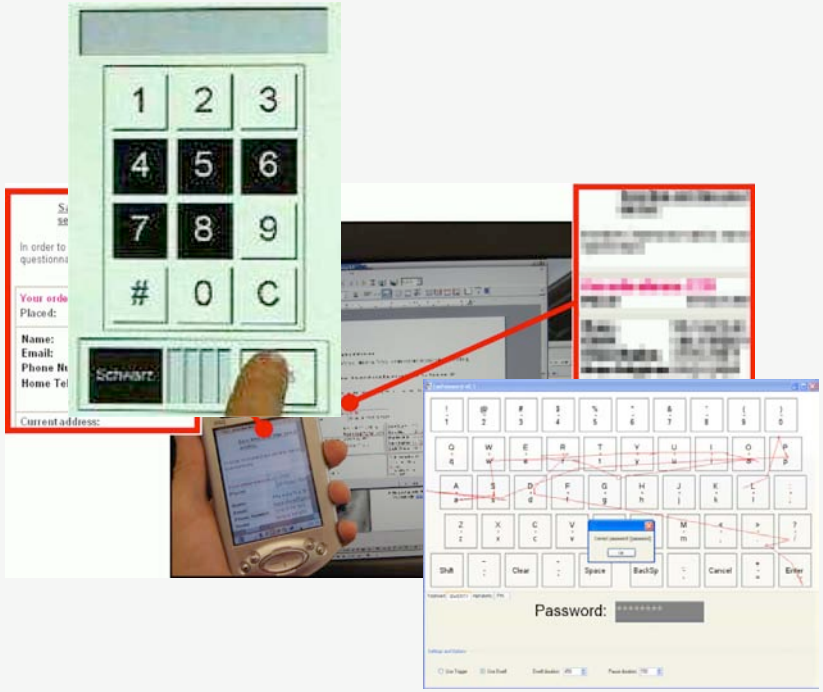
- Goals
- Related Work
- Explanation of SeCuUI
  - XUL
  - Autocomplete Function
  - Connection methods
- User study
- Conclusion

Goals

- Develop a system using mobile devices for terminal input
  - Client development
  - Not one specific server, but a framework
- Optimize the client and framework usage
  - External GUI information (XUL)
  - Faster input using autocomplete mechanism
  - Modularity throughout the system
    - Connection methods
    - Connection types

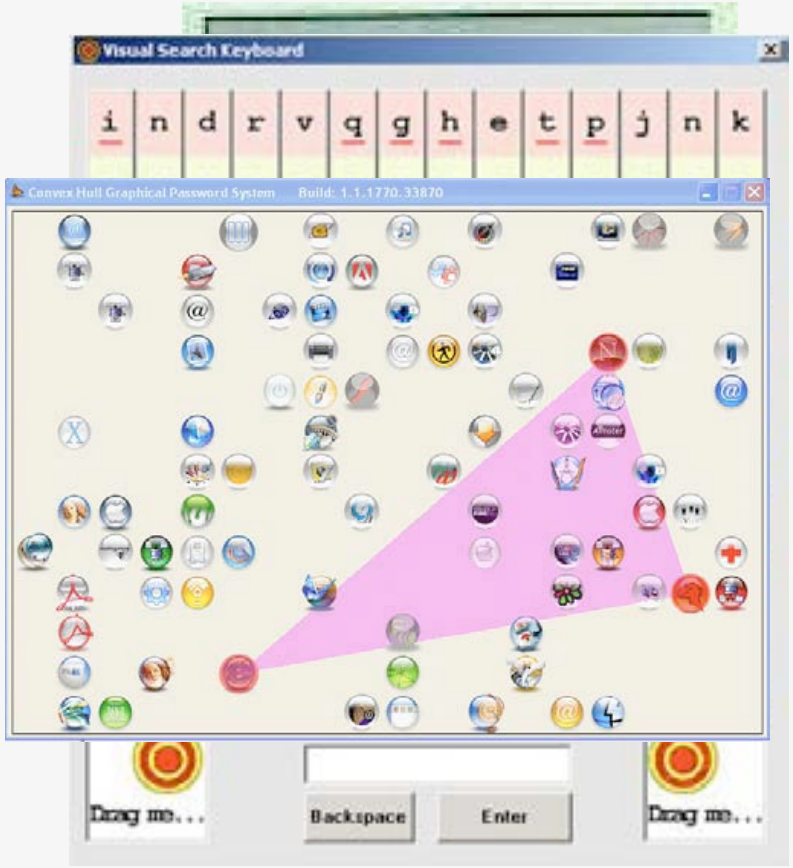
Related Work

- Either macroscopic / microscopic
  - Password entry alternatives
  - Remote control systems
- Missing happy medium
- 3rd group of biometric approaches



Related Work (Microscopic)

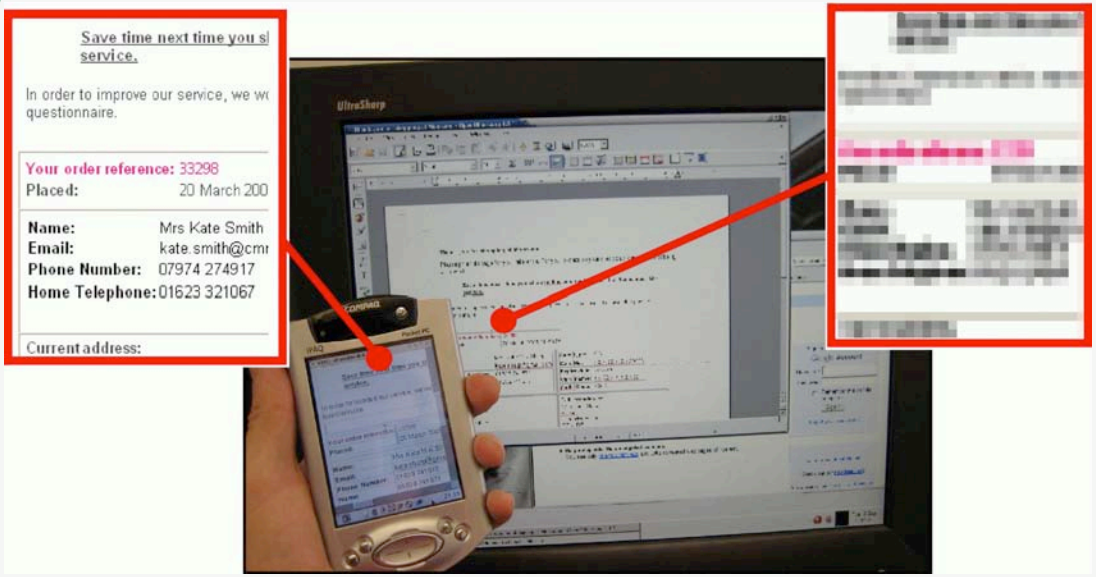
- Black and White PIN Pad
  - Roth et al. (2004)
- Spy-Resistant Keyboard
  - Tan et al. (2005)
- Convex hull password
  - Sobrado & Birget (2006)



Source: Roth et al. (2004), Tan et al. (2005), Sobrado & Birget (2006)

Related Work (Macroscopic)

- Secure Mobile Computing
  - Sharp et al. (2004)
- Other more general approaches
  - Opportunistic Annexing of Handheld Devices Pierce, Mahaney (2004)



Source: Sharp et al. 2004

Related Work (Biometrics)

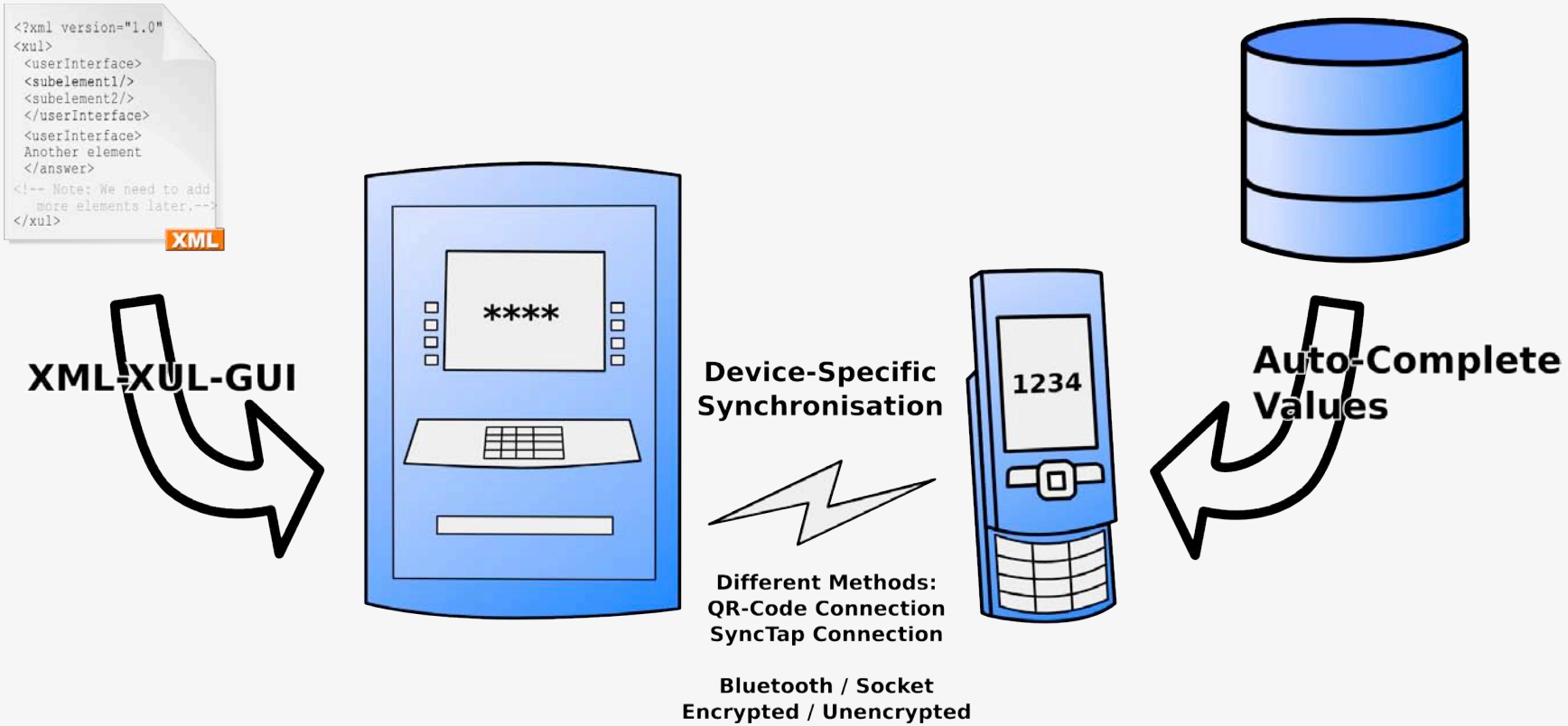
- Biometric Verification at the ATM interface
  - Coventry et al. (2003)
- Already used in some areas
  - DVD rental

Source: Lenovo.com

SeCuUI - Secure Custom User Interface

- Entering data to public terminals using the own mobile device
  - Smaller screen
  - Closer proximity
  - Can not altered by someone else
  - Distributed risk
- Public terminal changes based on connection state
- Usage of a mobile device is not obligatory

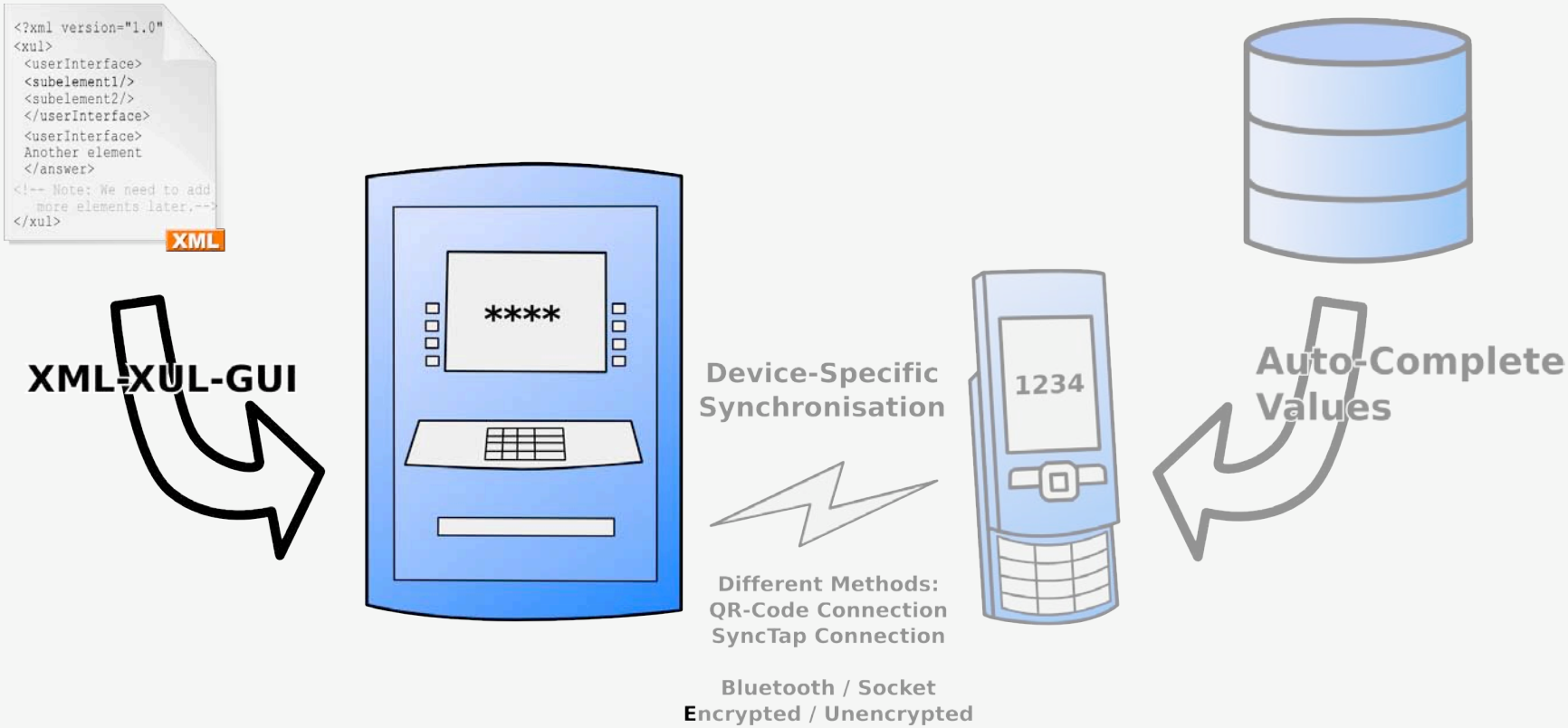
SeCuUI - Secure Custom User Interface



SeCuUI - User Perspective

- User has to perform only three simple steps
- One client software for all framework conform terminals
- Autocomplete values used for all applications

SeCuUI - Secure Custom User Interface



XML-GUI

- Autonomous server application
- Transferable GUI parts not “hard coded”
- Framework parses external XML-File
  - Returns GUI container
  - Handles and synchronizes components
  - Programmer has direct access but does need to care about connected devices
- XUL (XML User Interfaces) used as a container format

XUL (XML User Interface Language)

- Created by Mozilla
- Very powerful but only some part used for SeCuUI
- Additional attributes for SeCuUI

```
1  <?xml version="1.0"?>
2  <?xml-stylesheet href="chrome://global/skin/" type="text/css"?>
3  <window id="findfile-window"
4          title="Find Files"
5          orient="horizontal"
6          xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">
7
8    <label id="lblAccountValue"/>
9    <textbox
10     id="tfInput"
11     value="Eingabetext"
12   />
13   <button id="btnNext" label="Next"/>
14
15 </window>
```

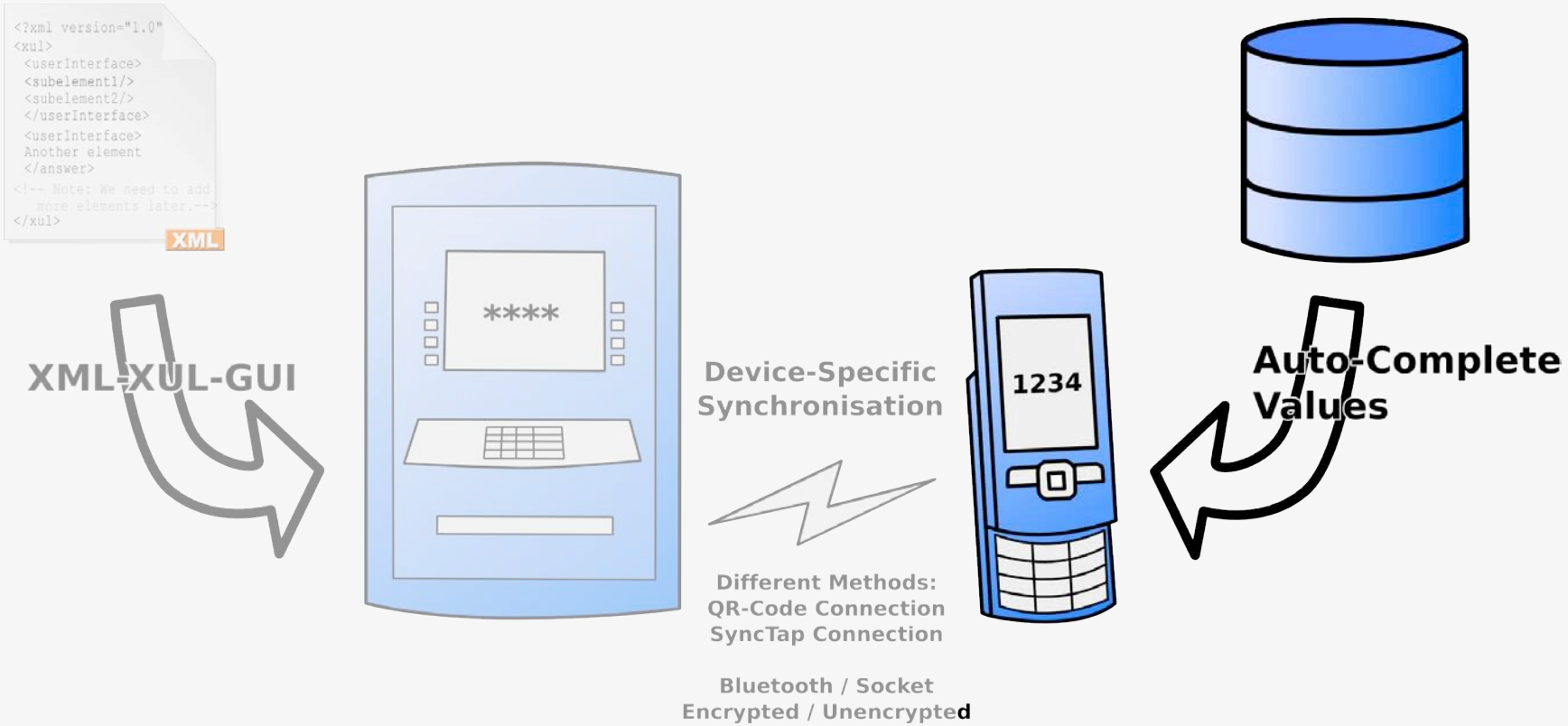
XUL (SeCuUI attributes)

```
6          xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">
7
8    <label id="lblAccountValue"/>
9    <textbox
10     id="tfInput"
11     value="Eingabetext"
```

- **`asterisk:`** Used to replace contents with echo characters (Possible values: `ASTERISK_NEVER`, `ASTERISK_LOCAL`, `ASTERISK_OPTIONAL`, `ASTERISK_BOTH`)
- **`security:`** Used to force input on the mobile device (Possible values: `SECURITY_INSECURE`, `SECURITY_BOTH`, `SECURITY_SECURE_OPTIONAL`, `SECURITY_SECURE_FORCED`)
- **`dataType:`** Used to define the type of data for this field (e.g.: `TYPE_VISA_CARD_NUMBER`, `TYPE_ADDRESS`)

```
12   />
13   <button id="btnNext" label="Next"/>
14
15 </window>
```

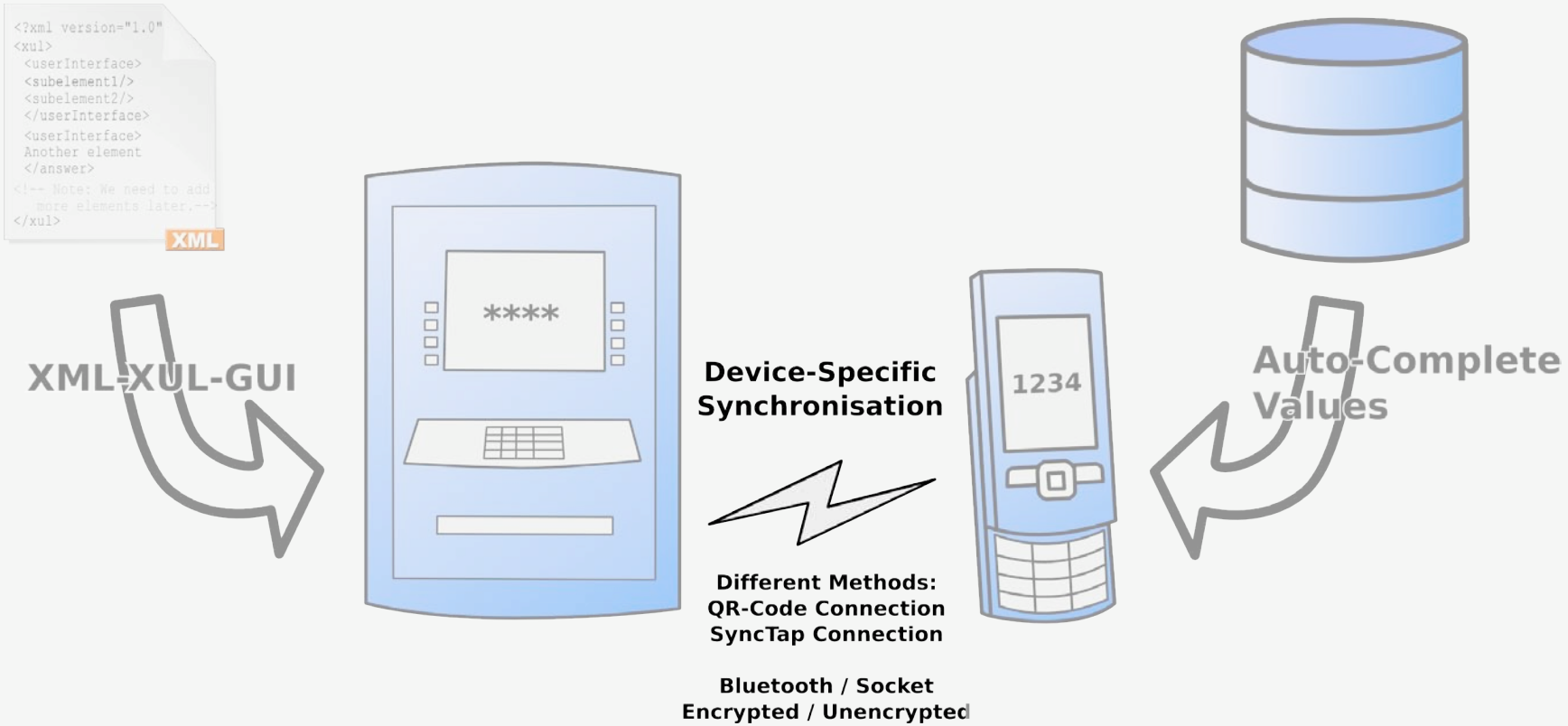
SeCuUI - Secure Custom User Interface



Autocomplete mechanism

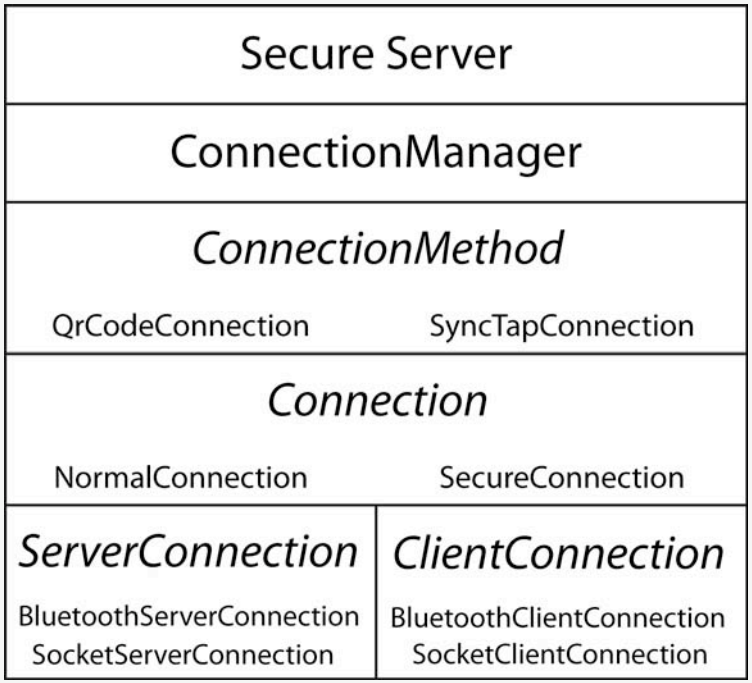
- `dataType` attribute is processed
- all matching entries that have been previously entered are displayed beneath the corresponding input field
- no direct access for any server application
- possibility to disable autocomplete
- saving of new values on submit of a form

SeCuUI - Secure Custom User Interface

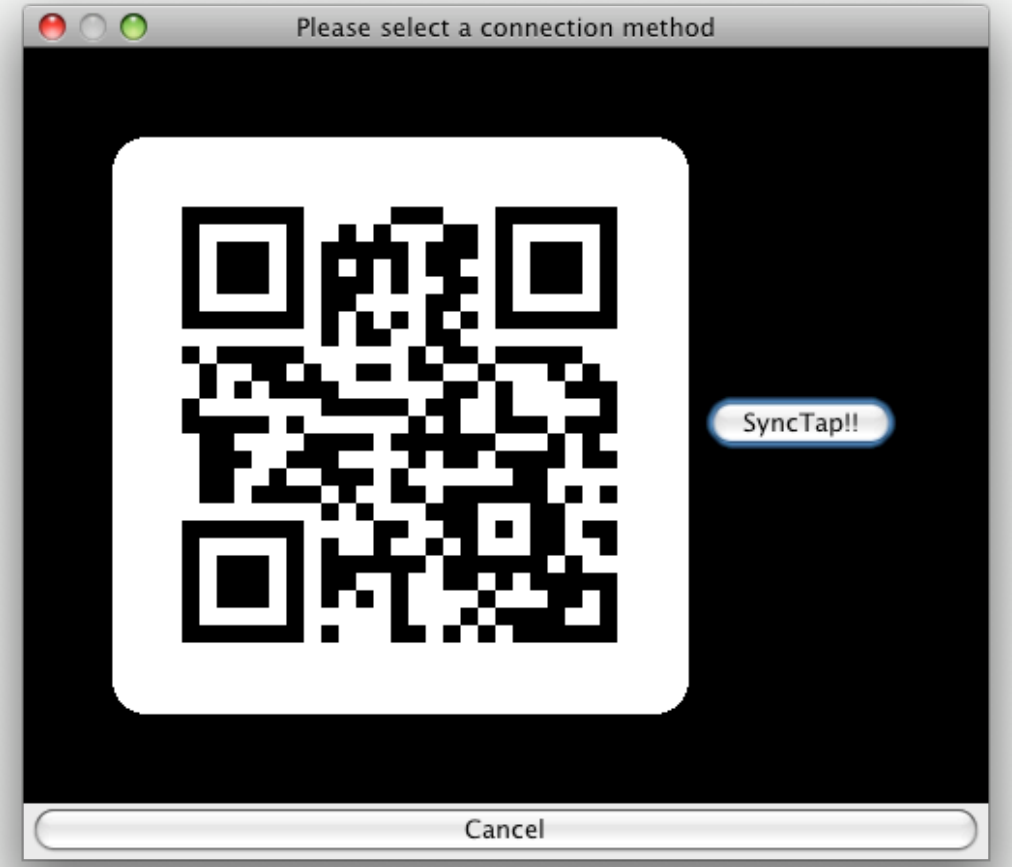


Modularity

- Connection process is very modular
- Module stack
- Three layers:
  - connection method
  - connection type
  - connection medium
- Connection independent message stack is used after connecting
- Protocol classes use simple MessageTransmitter

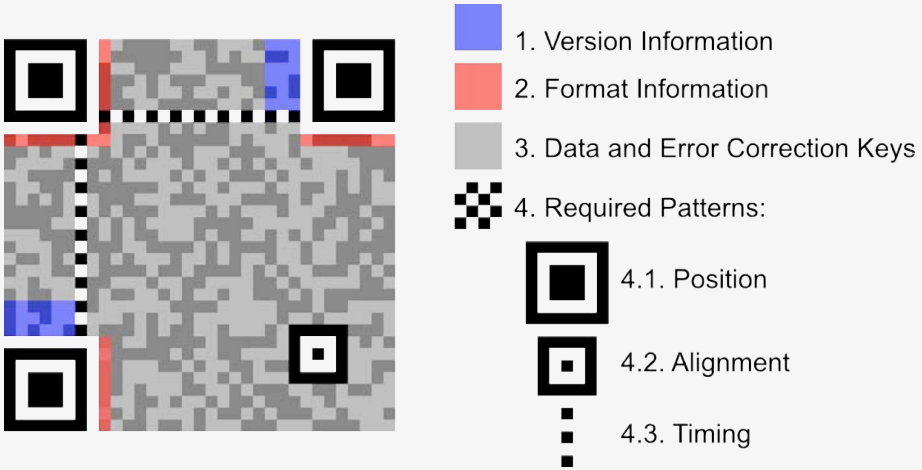


Connection Manager



QrCodeConnection

- One completely implemented connection method
- Many different methods can be imagined

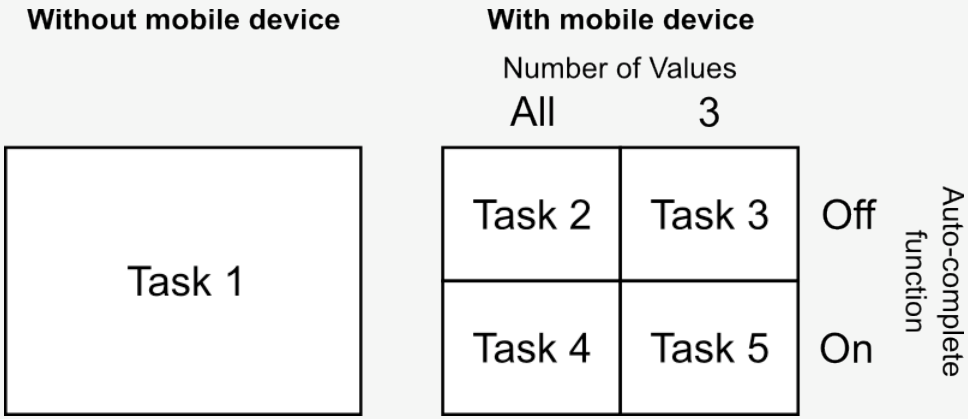


Userstudy

- Userstudy with client and test server was conducted
- 21 participants
- Scenario: Buy a product out of three different products and enter personal data
  - Shipping address
  - Payment details
- Two fake companies to demonstrate the portability

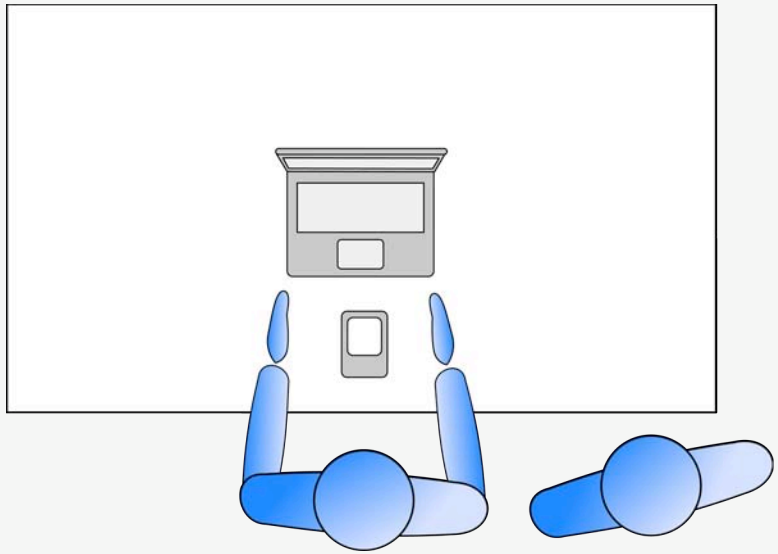
Userstudy - Variables

- Two independent variables
  - Autocomplete: On/Off
  - Number of values entered on the phone
    - Security related only
    - All values
- Fifth reference task: No phone connection at all
- Questionnaire at the end of the study



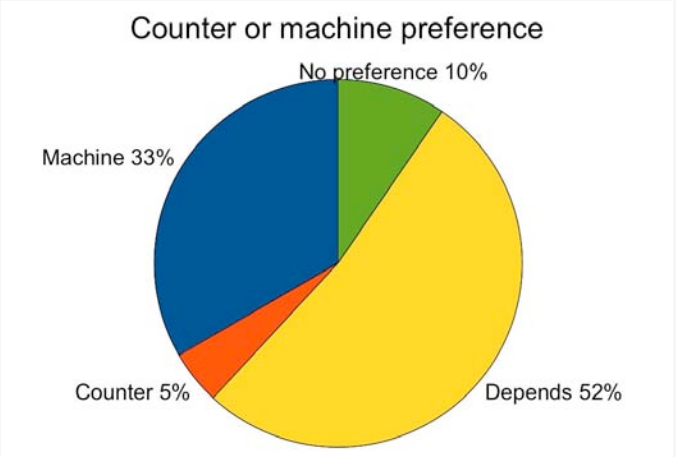
Userstudy - Setup

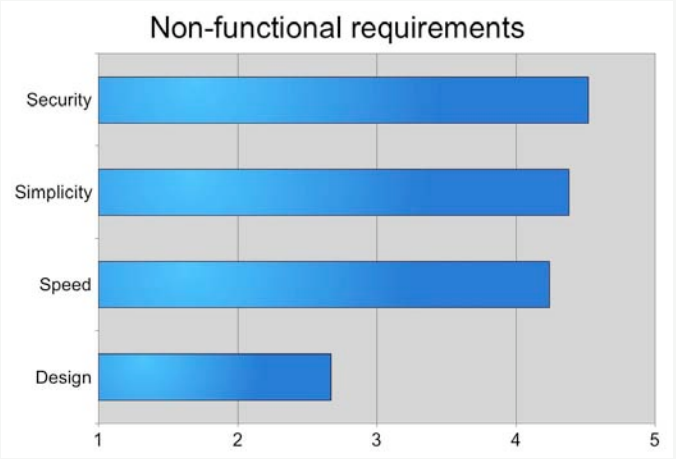
- MacBook served as Public Terminal
- Nokia N80 as mobile device
- Users could practice as long as they wanted to
- Issues noticed during test:
  - No real public terminal
  - Sitting instead of standing
  - Computer keyboard much faster



Userstudy - Vending machine usage

- People tend to use machines very often
- 62% are worried about their security at such machines
- Using a machine or ordering at a counter depends on the situation for most of them
- Security was also the highest rated non-functional requirement





Userstudy - Task results

Without mobile device

Task 1

With mobile device

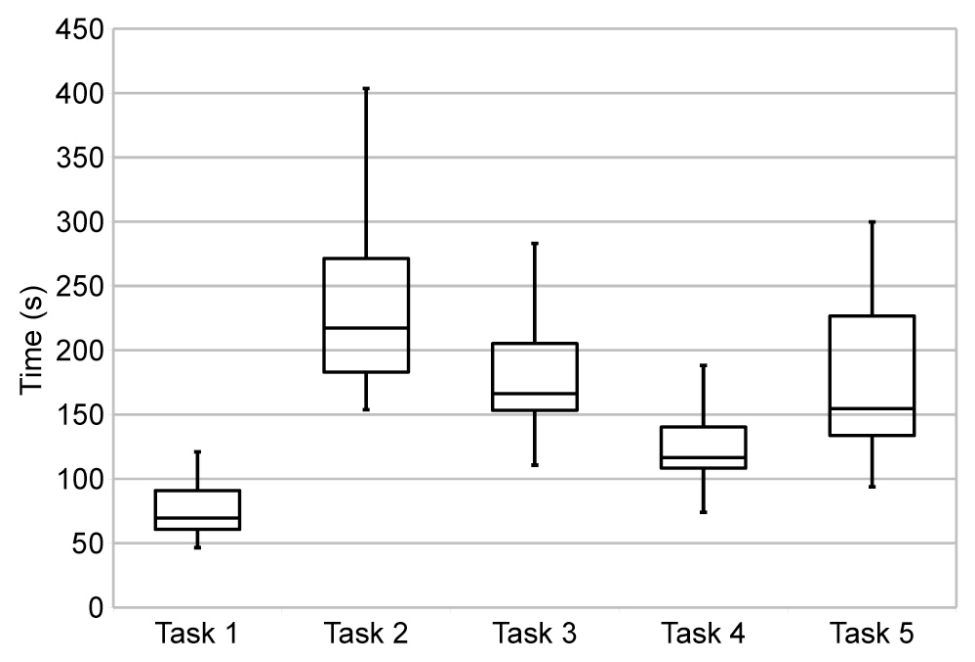
Number of Values	All	3
Auto-complete function: Off	Task 2	Task 3
Auto-complete function: On	Task 4	Task 5

time in seconds	Average connection	Average overall	Task 1 ratio
Task 1	0	76	
Task 2	28	238	3,3
Task 3	27	178	2,4
Task 4	35	129	1,8
Task 5	29	163	2,3

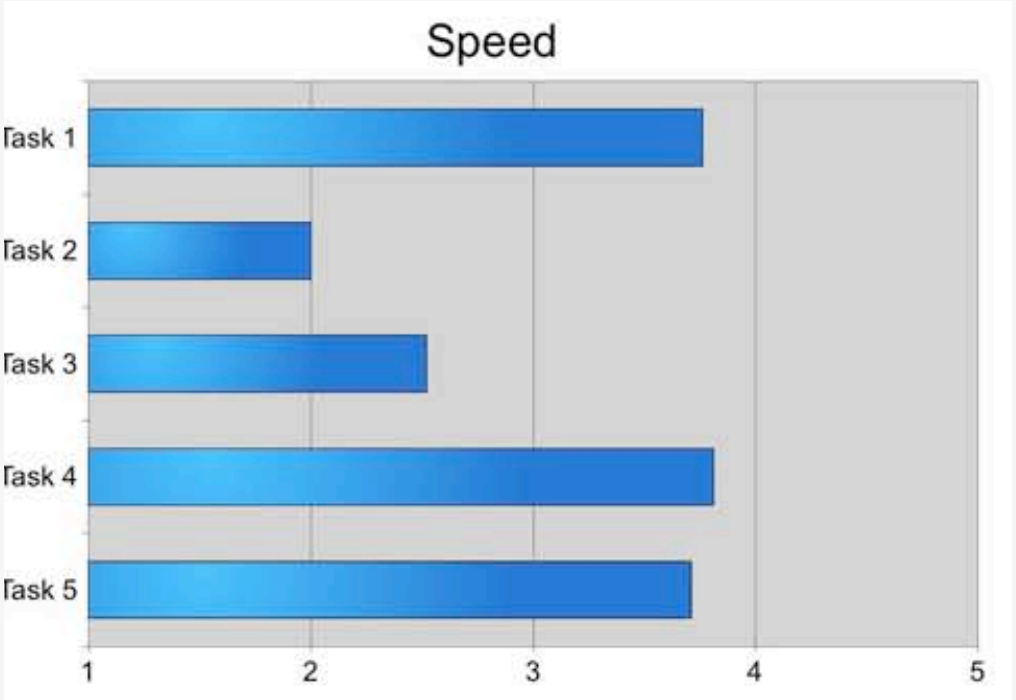
Average connection time 29,74

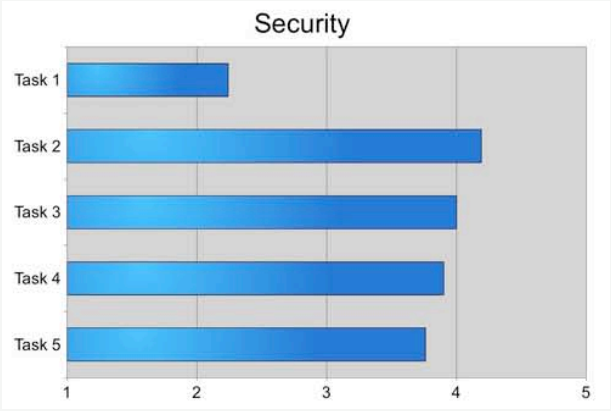
Userstudy - Task interpretation

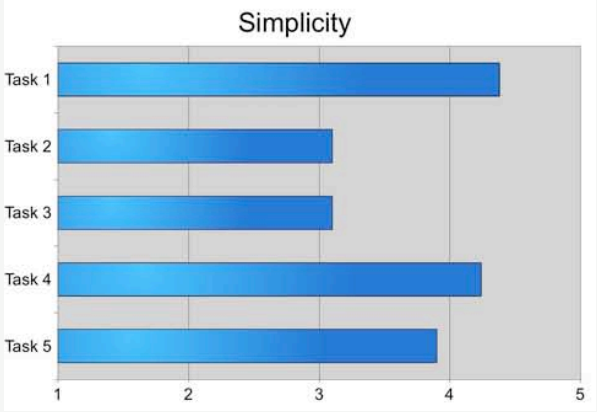
- Task 1 fastest
  - Probably due to laptop usage
- But task 4 significantly faster than task 2
  - Autocomplete speeds up data entry
- Participants had a different feeling



Userstudy - Task interpretation



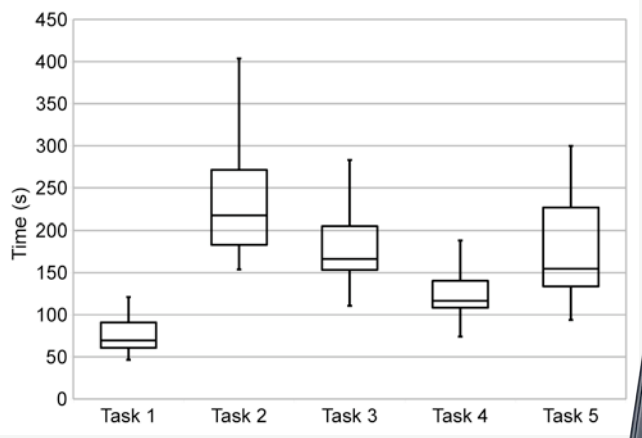




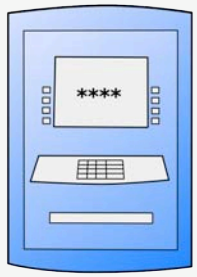
Conclusion

- People are aware of security risks at public terminals
- Still PINs at ATMs as in 1967
- SeCuUI is a new approach between macroscopic and microscopic ideas
- Autocomplete feature increases the input speed whilst still more secure

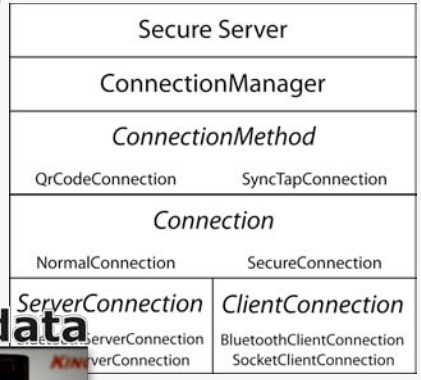
Thank you!

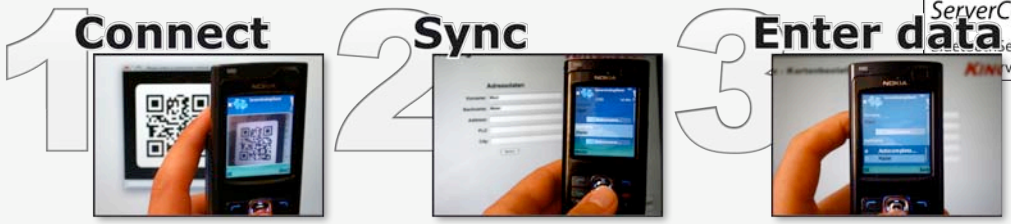

Time (s)
450
400
350
300
250
200
150
100
50
0
Task 1
Task 2
Task 3
Task 4
Task 5

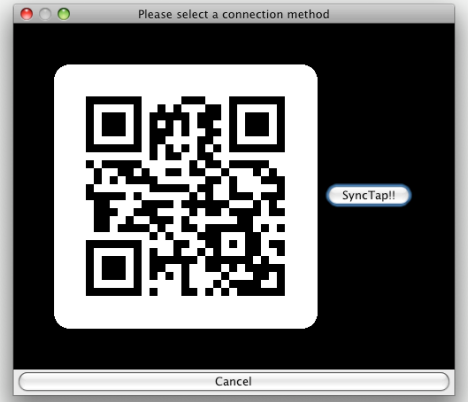

XML


****
XML-XUL-GUI
Device-Specific Synchronisation
1234
Auto-Complete Values
Different Methods:
QR-Code Connection
SyncTap Connection
Bluetooth / Socket
Encrypted / Unencrypted


NOKIA
Autocomplete....
Maier
OK
Back


Secure Server
ConnectionManager
ConnectionMethod
QrCodeConnection
SyncTapConnection
Connection
NormalConnection
SecureConnection
ServerConnection
ClientConnection
BluetoothClientConnection
SocketClientConnection


1
Connect
2
Sync
3
Enter data


Please select a connection method
SyncTap!!
Cancel