



The SIM as an Enabler for Security, Privacy, and Trust in Simple Mobile Services

Smart Card Web Server based User Data Management

Carsten Rust, Sagem Orga GmbH

■ ■ ■ ■ Agenda



4 Introduction

4 SIM Integration in Simple Mobile Services

4 SIM Enabled Basic Services

4 Application Examples

4 Conclusion



4 Introduction

4 SIM Integration in Simple Mobile Services

4 SIM Enabled Basic Services


4 Application Examples

4 Conclusion

Simple Mobile Services

New class of services
meeting the specific
needs of mobile users:

- § simple to find
- § simple to use
- § simple to trust
- § simple to set-up



*Discovery of airport services:
„Where can I buy a tie ?“*

Support for Check-In

*Personal reminder:
„Boarding in 20 min.“*

*Mobile Messages:
„Hi, I am already at gate
7. - Pete“*

At the airport

SMS: What's here ?




SMS: Take me-2



Simple Mobile Services

New class of services
meeting the specific
needs of mobile users:

- § simple to find
- § simple to use
- § simple to trust
- § simple to set-up



*Discovery of airport services:
„Where can I buy a tie ?“*

Support for Check-In

*Personal reminder:
„Boarding in 20 min.“*

*Mobile Messages:
„Hi, I am already at gate
7. - Pete“*

At the airport



Benefit from the (U)SIM as a Trusted Personal Device



- 4 Secure management of personal user data
 - User Identity (Multi-Identities)
 - Personal data
 - Public/Private keys, Digital Certificates
- 4 Portability of personal profile data and identity
- 4 Signing / Signature verification for MEMs and Mails
- 4 Service trust verification
 - Service identification
 - Trust level management for known services
 - Support of Trust level evaluation during service discovery
- 4 Secure User Authentication
- 4 Platform for Services



■ ■ ■ ■ Agenda



4 Introduction

4 SIM Integration in Simple Mobile Services

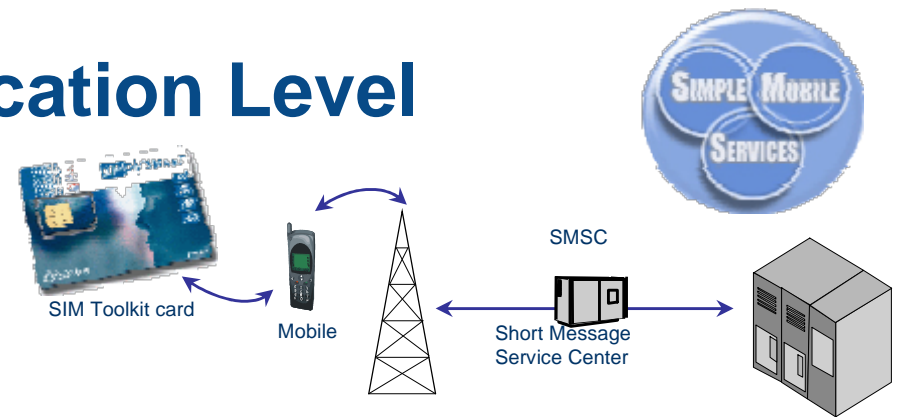
4 SIM Enabled Basic Services

4 Application Examples

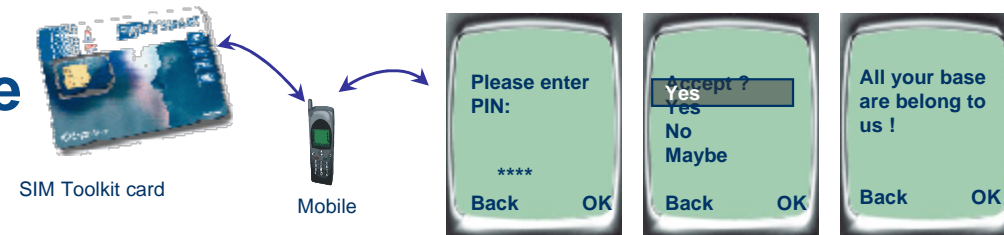
4 Conclusion

■ Interfacing the SIM on Application Level

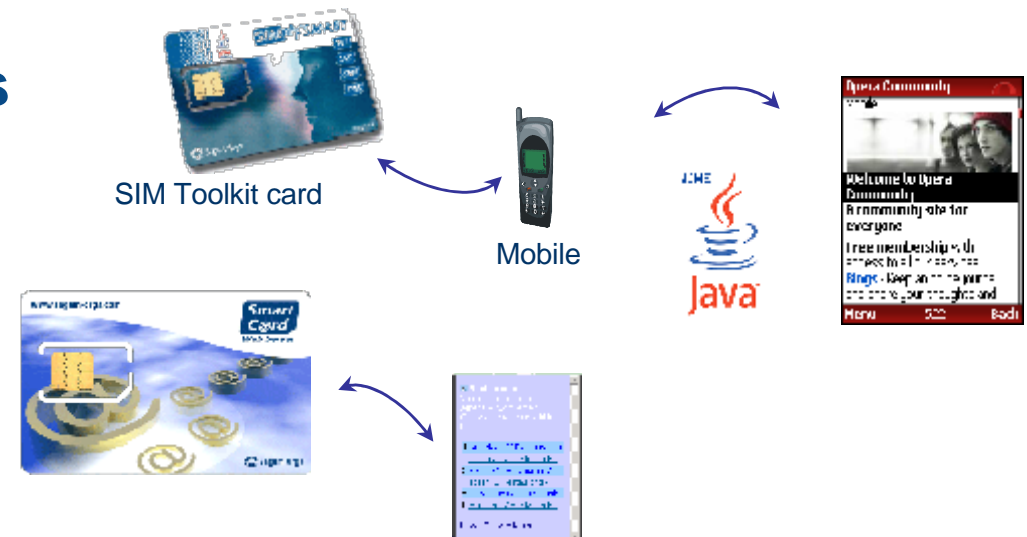
4 SIM Short Messages / BIP (GPRS)



4 SIM Toolkit Graphical User Interface



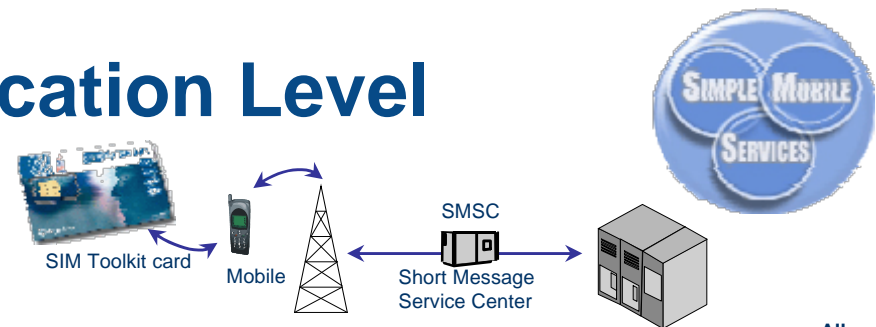
4 JSR-177 / Other proprietary APIs



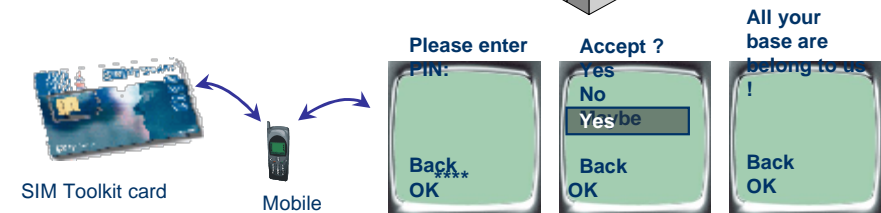
4 Smart Card Web Server (SCWS) Java Card 3.0

Interfacing the SIM on Application Level

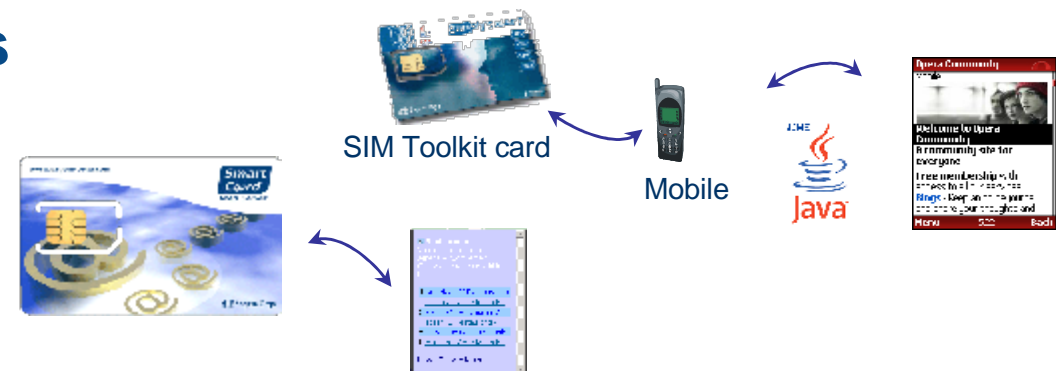
4 SIM Short Messages / BIP (GPRS)



4 SIM Toolkit Graphical User Interface



4 JSR-177 / Other proprietary APIs



4 Smart Card Web Server (SCWS) Java Card 3.0

Related Specifications

- 4 ETSI SCP TS 102 223: Card Application Toolkit (CAT)
- 4 ETSI SCP TS 102 588 Application Invocation API by a UICC Webserver on a Java Card (R7)
- 4 ETSI SCP TS 102 483 Internet protocol connectivity

SCWS in Simple Mobile Services



4 Smart Card Web Server with remote administrable *webpace* and *Extension Interface*

4 Open Mobile Alliance (OMA) Smartcard-Web-Server V1.0

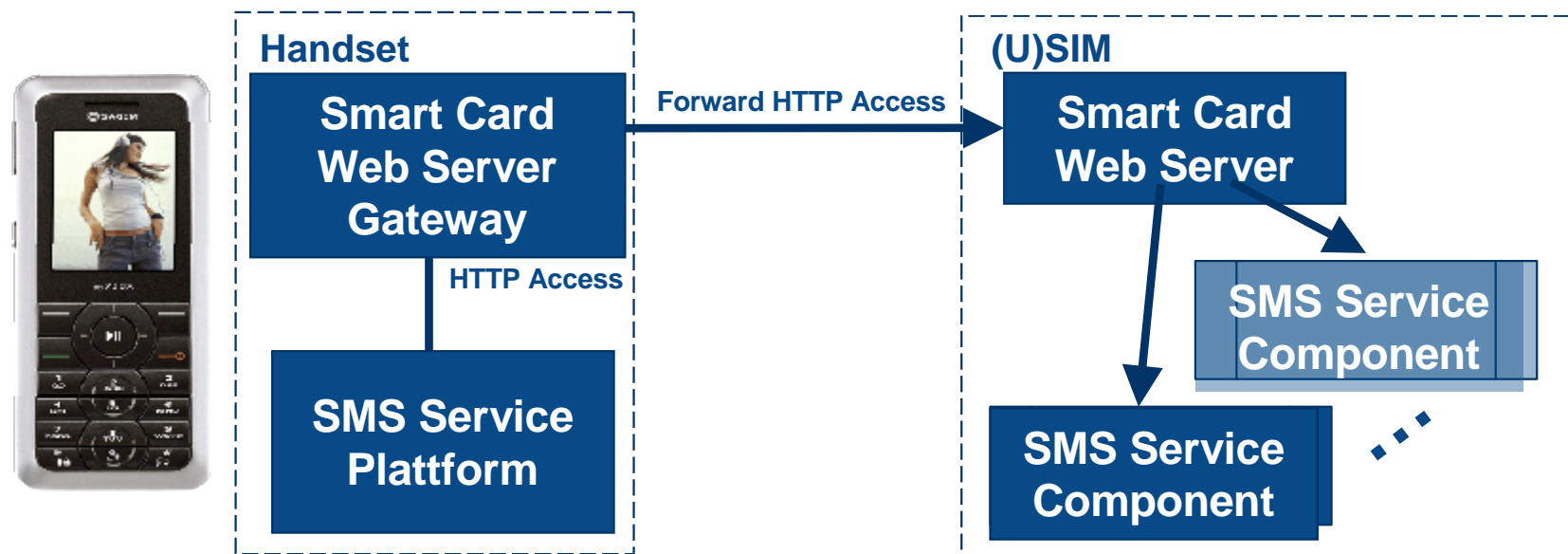
4 Platform independent access to (U)SIM

4 HTTP(S) interface to access Simple Mobile Service components on the (U)SIM from applications on the handset

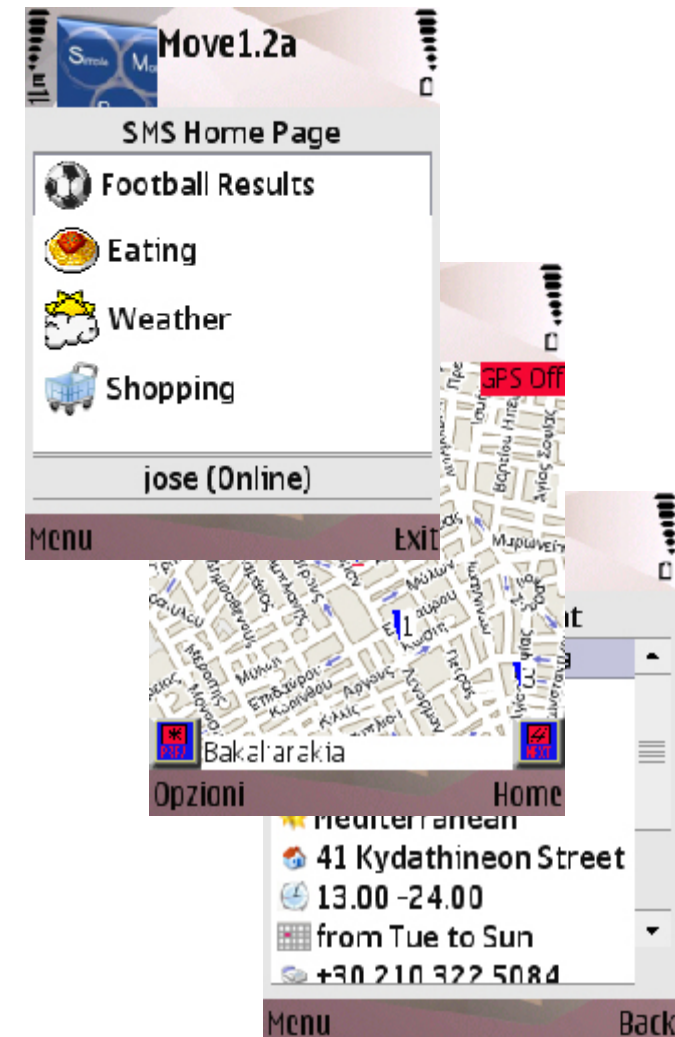
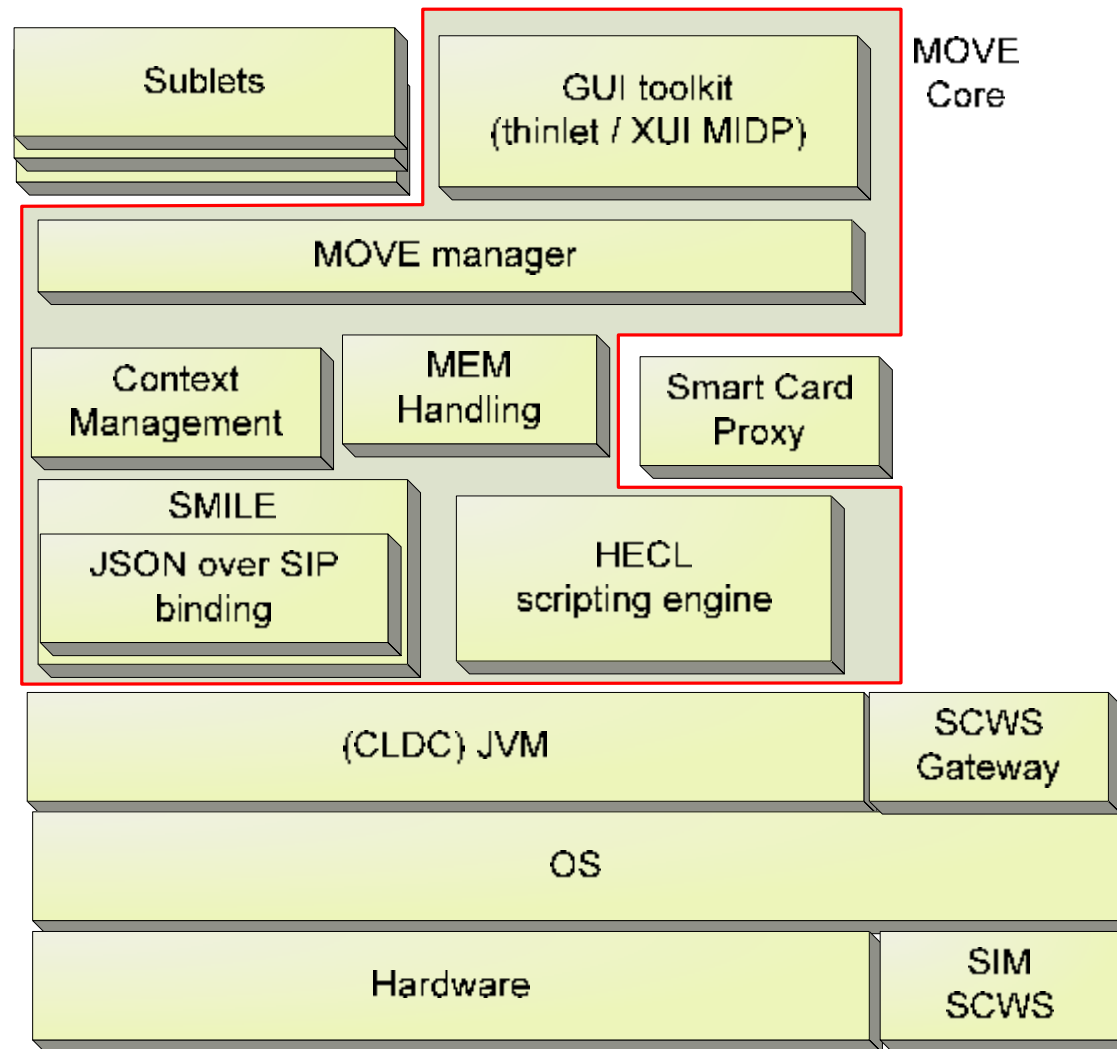
4 Connection to `http://127.0.0.1:3516/smsService`

4 Extensible service components implementation

4 ETSI SCP TS 102 588 Application Invocation API by a UICC Webserver



SMS: Client Architecture



Next Generation SIM cards



4 Java Card 3.0

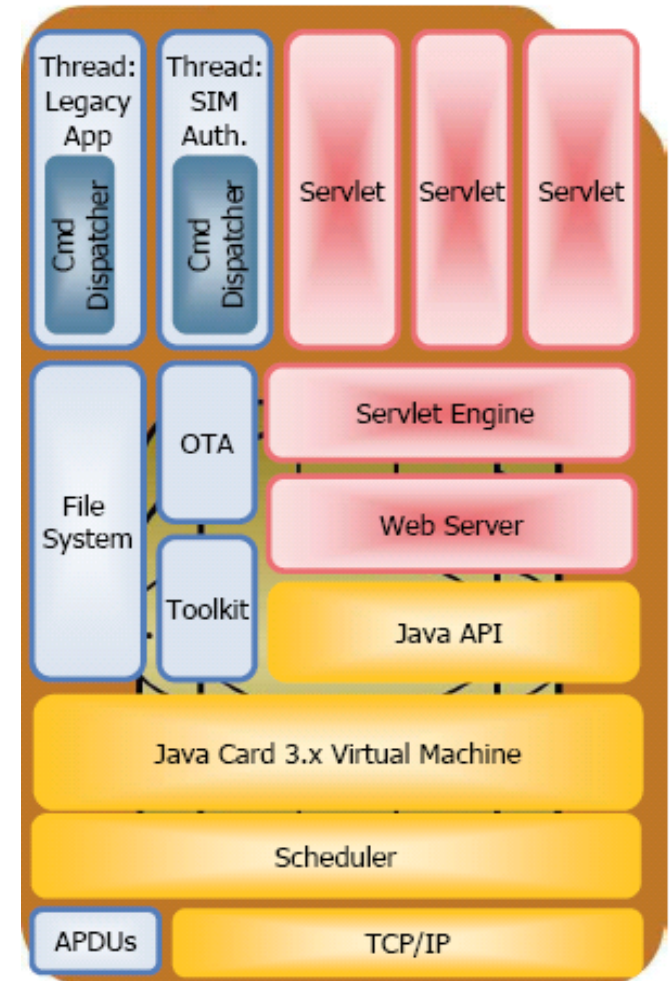
- OS architecture =
Multithreaded Java™ Virtual Machine
+ TCP/IP
+ General Purpose APIs

4 Key benefits

- New application model: Web Apps
- Network aware (TCP/IP)
- Security Framework

4 Major evolutions

- USB High-speed protocol
- NAND Flash mass storage



Sun Microsystems

■ ■ ■ ■ Agenda



4 Introduction

4 SIM Integration in Simple Mobile Services

4 **SIM Enabled Basic Services**

4 Application Examples

4 Conclusion

User Data Service

4 Key/Value data records with namespace indicator and access rules

RentACar		
loginname	fullname	credit
johnnyq	John Q. Public	1234567890

4 Protect the personal user and keep it portable

- Identity Management (e.g. Single Sign On, convenient log-in)
- Bookmarks, Favorites, History, etc.

4 Data Storage of service provider

- Device Personalisation, Branding
- Service deployment: Loading Thinlets from SIM

Profile Information	
Name:	Smith
First Name:	Brian
Sex:	Male
Day of Birth:	04.09.1967
Address:	Private Drive London

Ok Next

SMS Home Page	
Football Results	
Eating	
Weather	
Shopping	
Registration Service	
orga (Online)	

Exit Menu

Signature Service

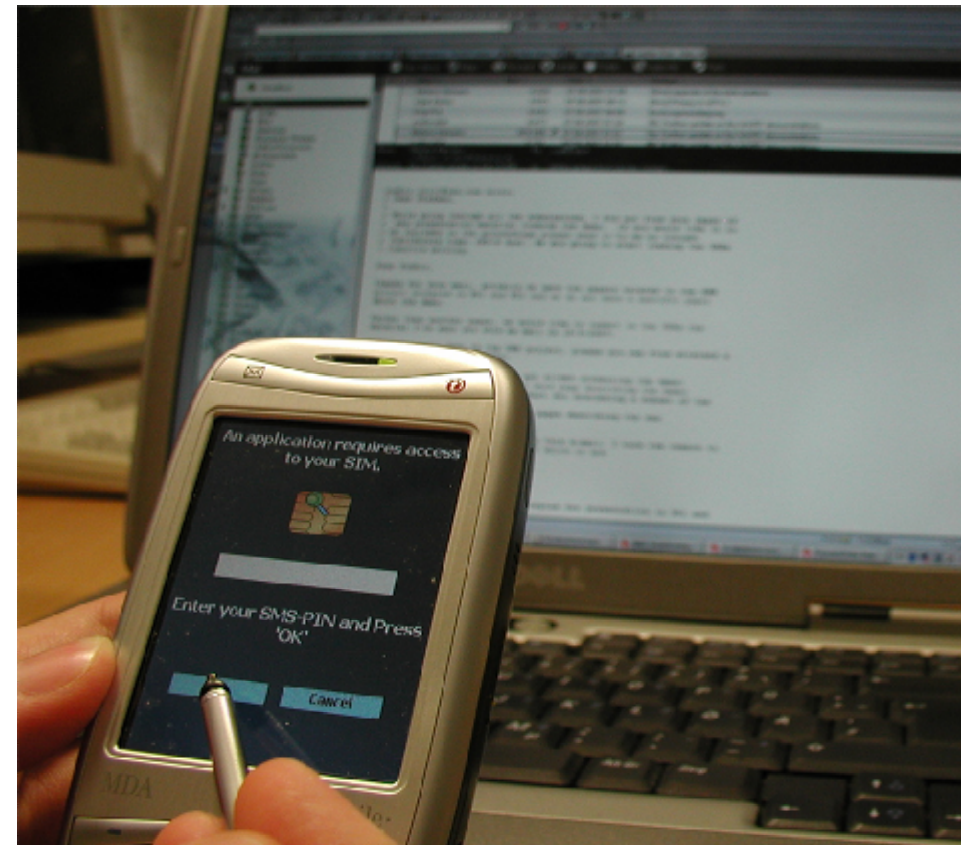
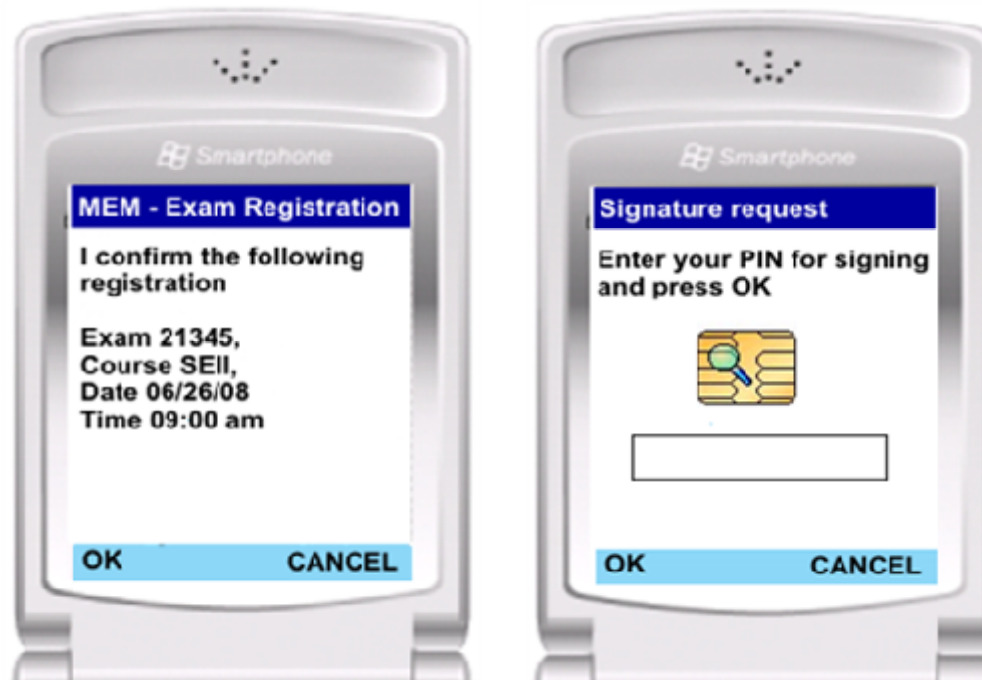


4 Services might require a digital signature, e.g.

- authentication, prove the identity of the originator
- verify data consistence

4 SIM card service

- generates a public/private key pair
- signs data (MEMs) on requests



■ ■ ■ ■ Agenda



4 Introduction

4 SIM Integration in Simple Mobile Services

4 SIM Enabled Basic Services

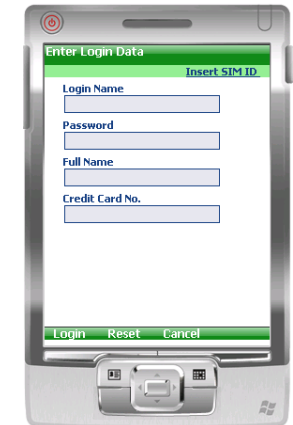
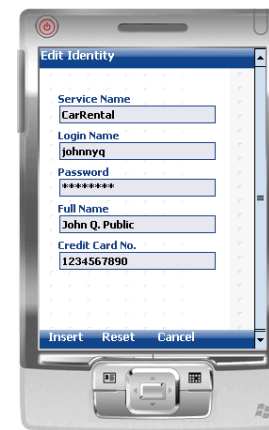
4 Application Examples

- Login Data Management
- Trusted MEMs
- Service and Trust Management

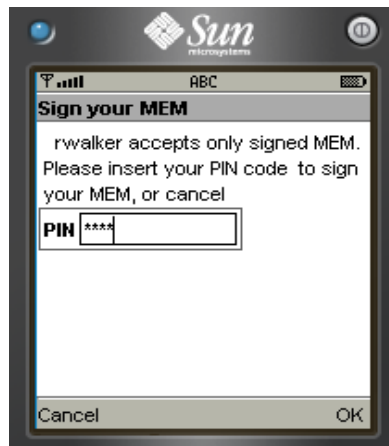
4 Conclusion

Application Examples

Login Data Management



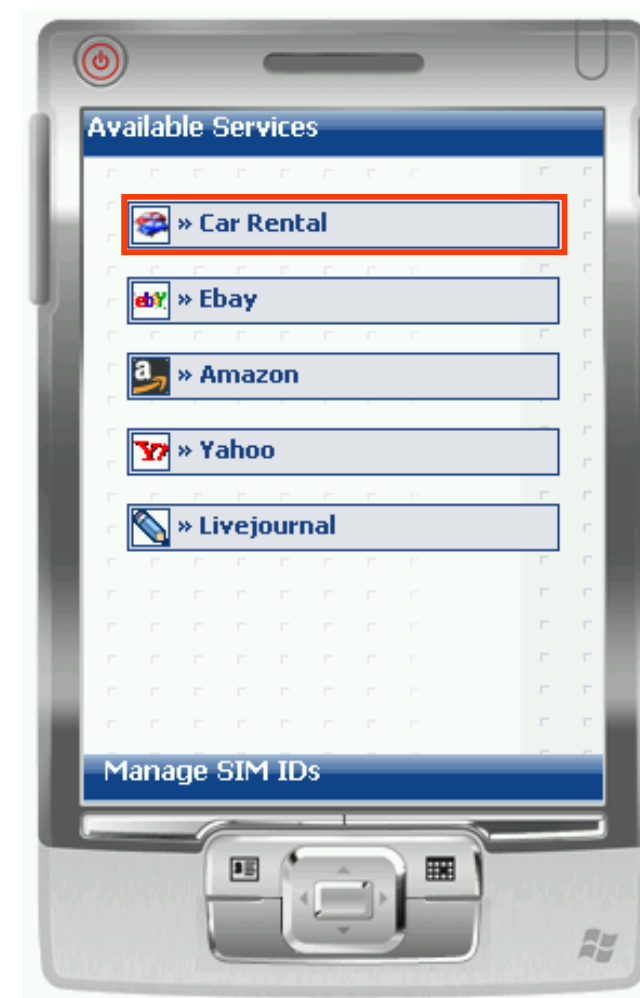
Trusted MEMs



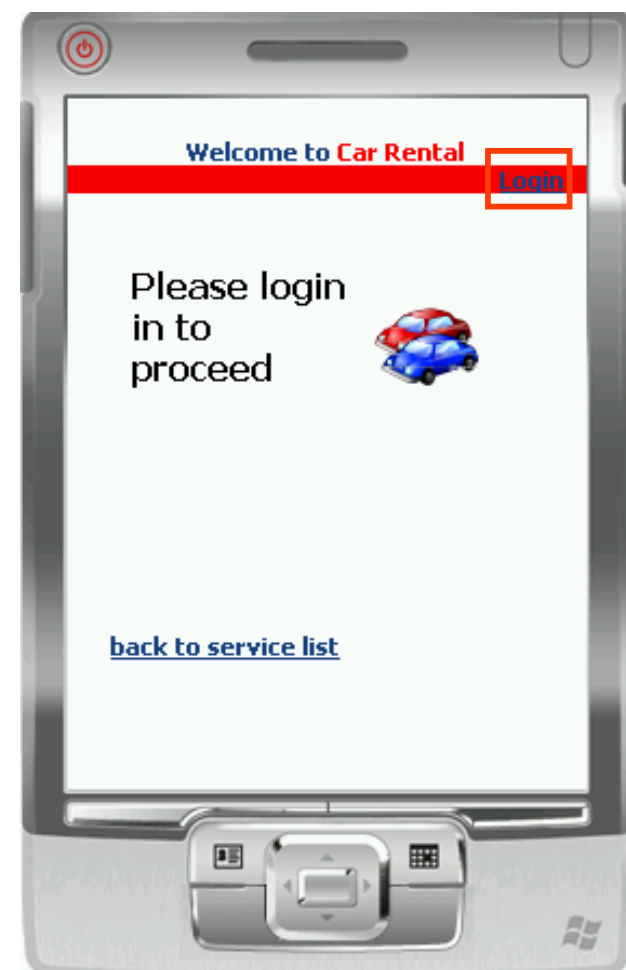
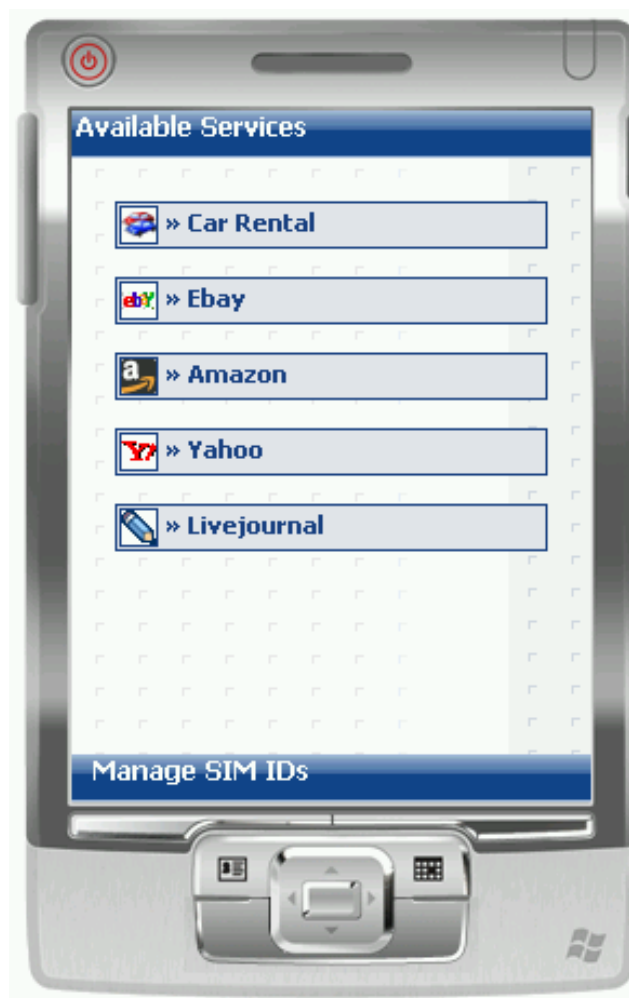
Service and Trust Management



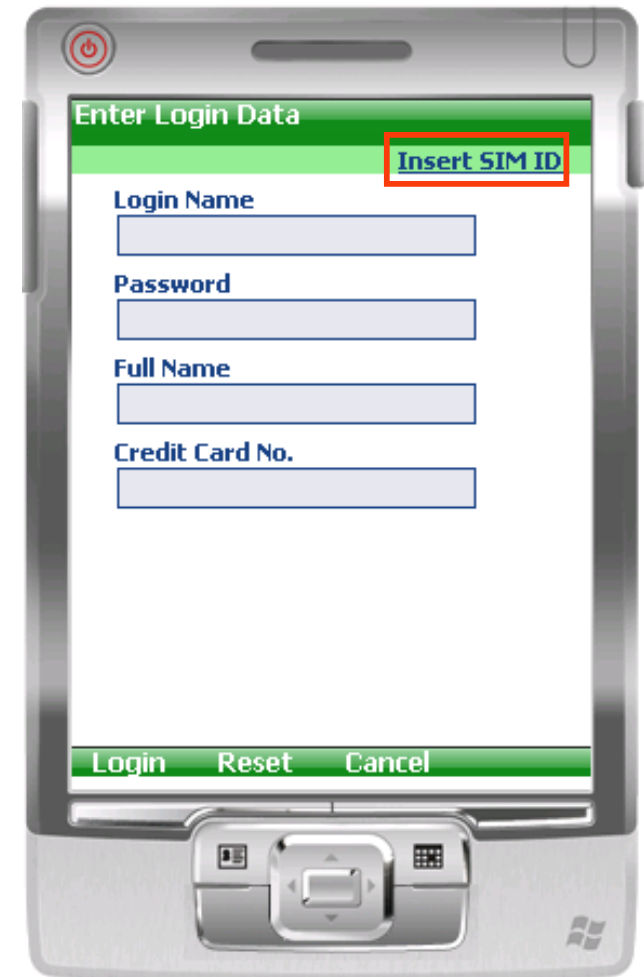
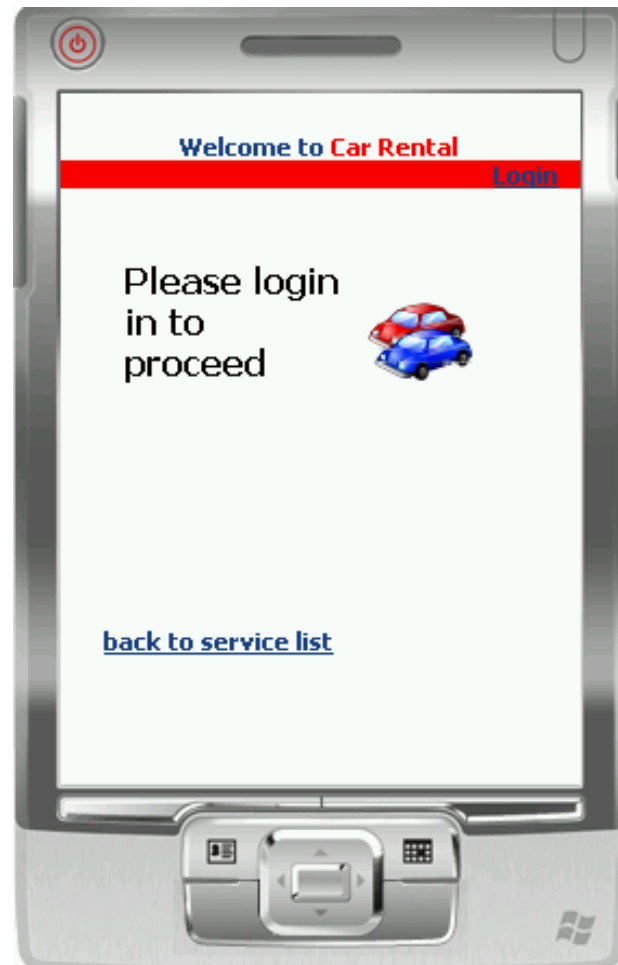
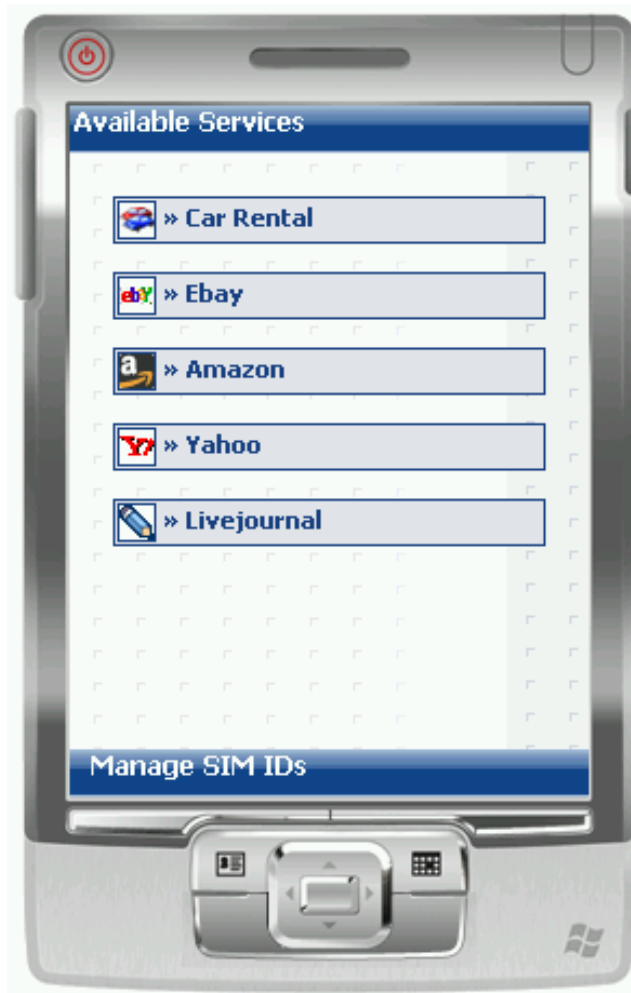
■ ■ ■ ■ Login Data Management



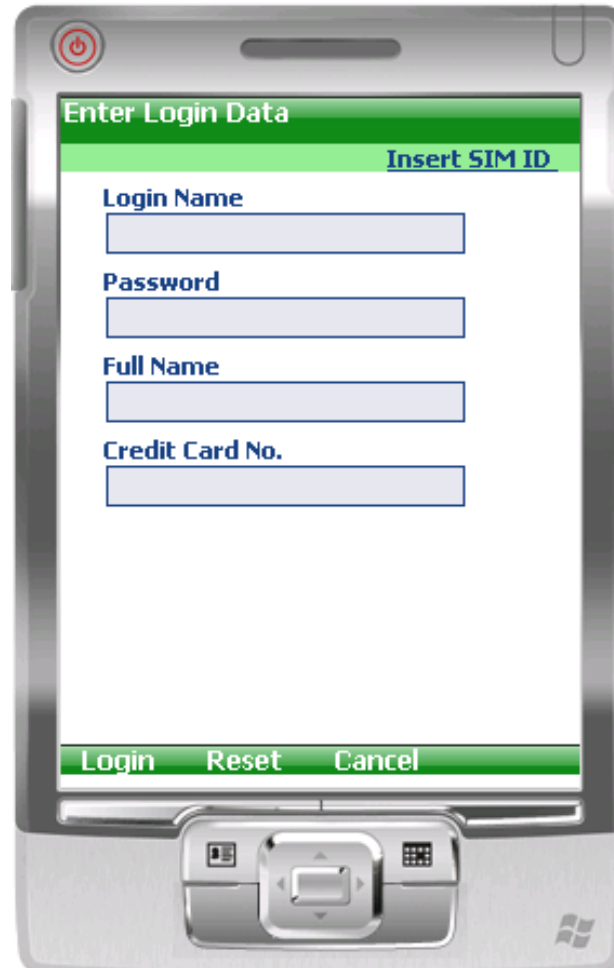
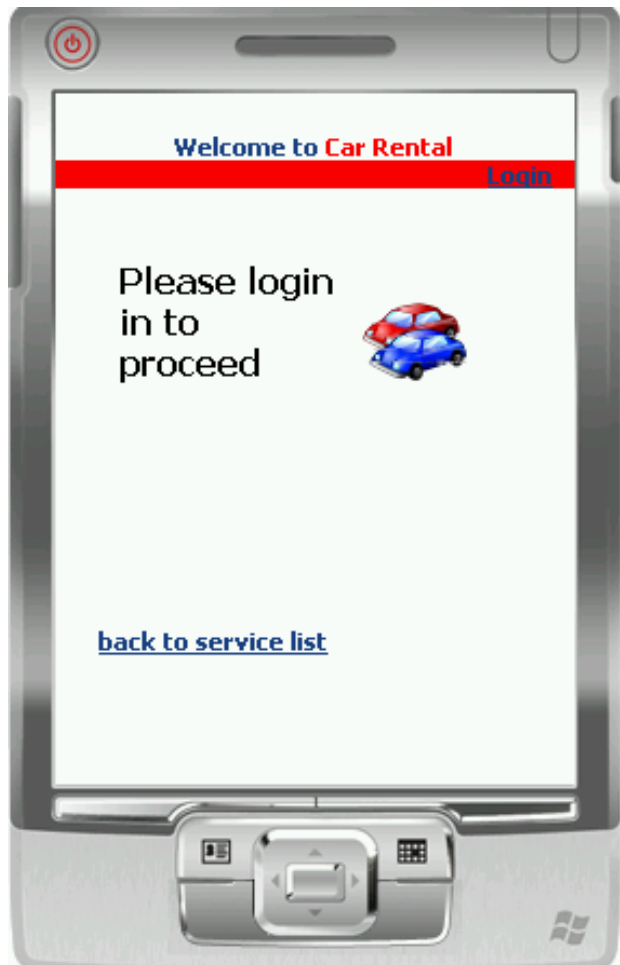
Login Data Management



Login Data Management



Login Data Management



Login Data Management



Enter Login Data

Insert SIM ID

Login Name

Password

Full Name

Credit Card No.

Login Reset Cancel

Authentication for SIM Card access required!

Please enter your PIN

Submit

Edit Identity

Service Name

Login Name

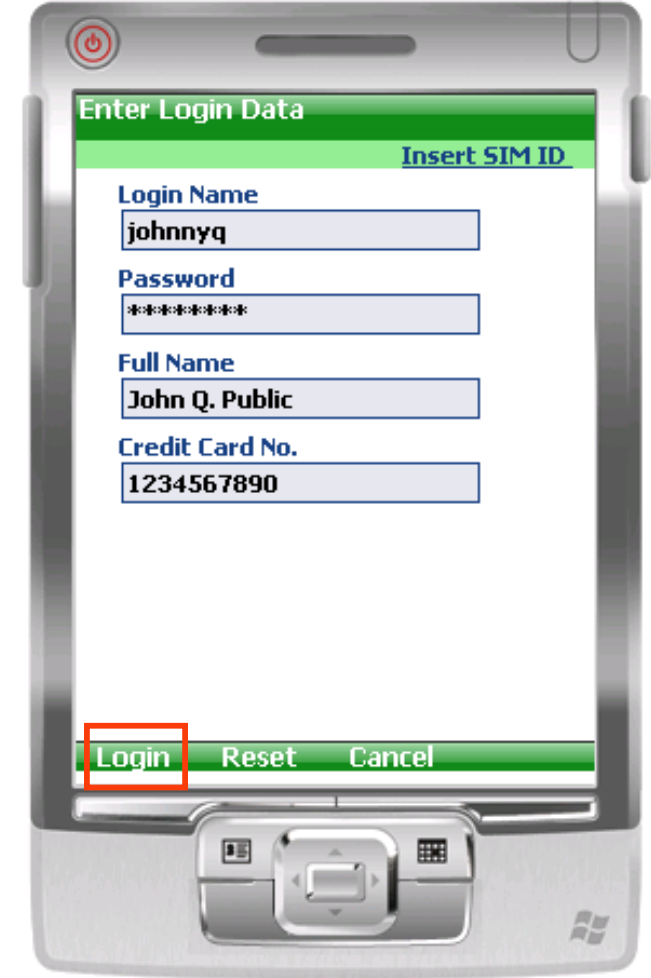
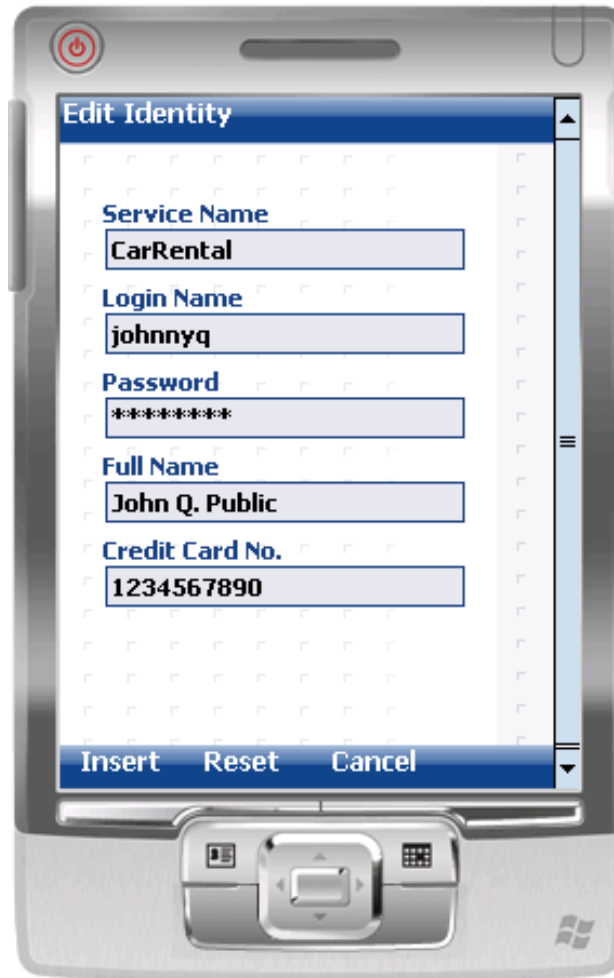
Password

Full Name

Credit Card No.

Insert Reset Cancel

Login Data Management



Login Data Management



Mobile phone screen displaying the 'Edit Identity' form. The form includes fields for Service Name, Login Name, Password, Full Name, and Credit Card No. The bottom navigation bar shows 'Insert', 'Reset', and 'Cancel' buttons.

Edit Identity

Service Name
CarRental

Login Name
johnnyq

Password

Full Name
John Q. Public

Credit Card No.
1234567890

Insert Reset Cancel

Mobile phone screen displaying the 'Enter Login Data' form. The form includes fields for Login Name, Password, Full Name, and Credit Card No. The bottom navigation bar shows 'Login', 'Reset', and 'Cancel' buttons.

Enter Login Data

Insert SIM ID

Login Name
johnnyq

Password

Full Name
John Q. Public

Credit Card No.
1234567890

Login Reset Cancel

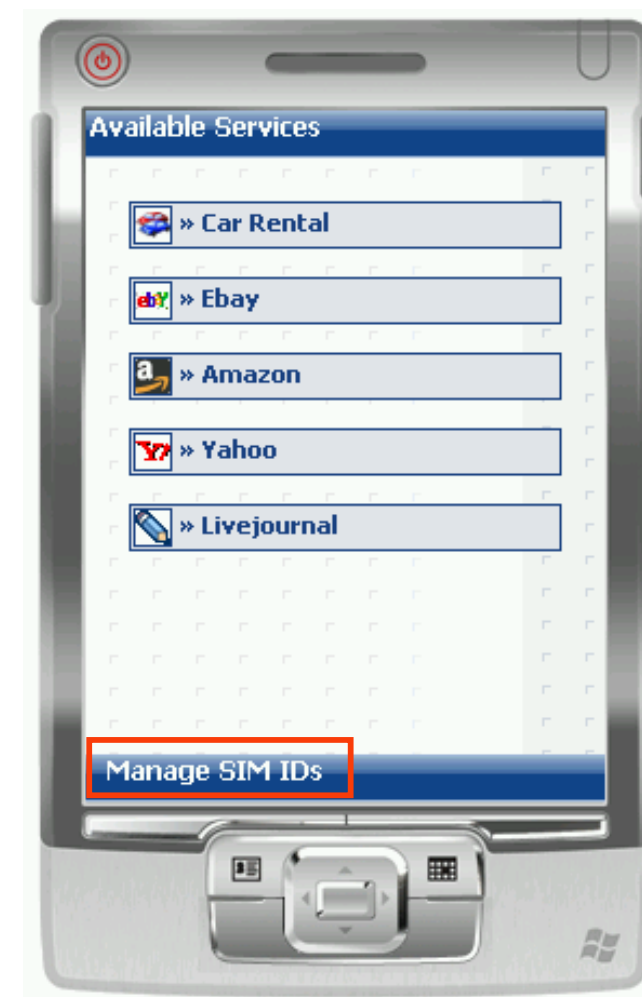
Mobile phone screen displaying the 'Welcome to Car Rental' message. The screen shows the user is logged in as 'johnnyq' and provides a 'Logout' link. A 'back to service list' button is visible at the bottom.

Welcome to Car Rental
logged in as johnnyq Logout

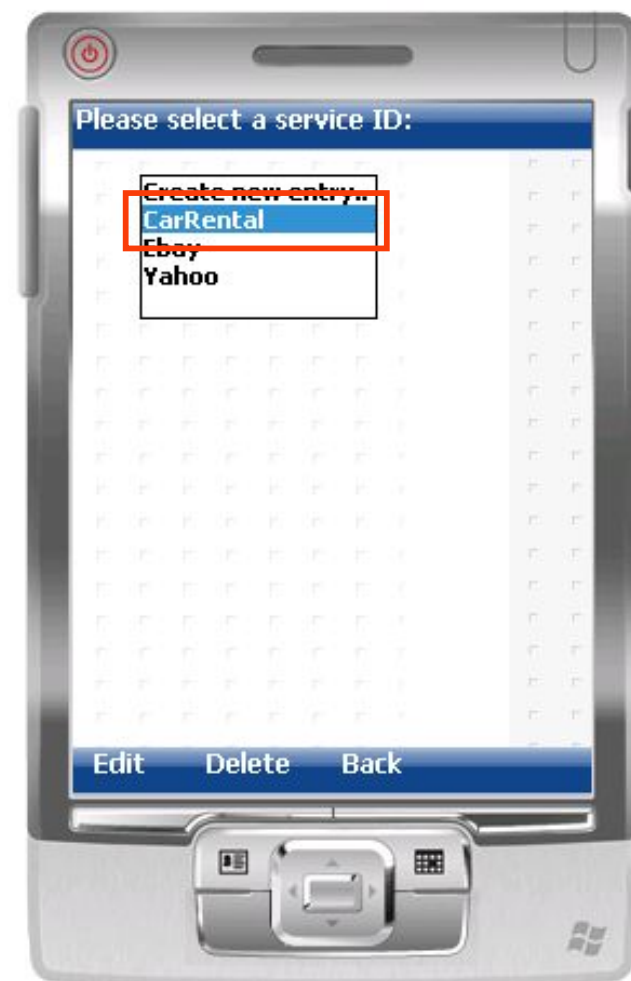
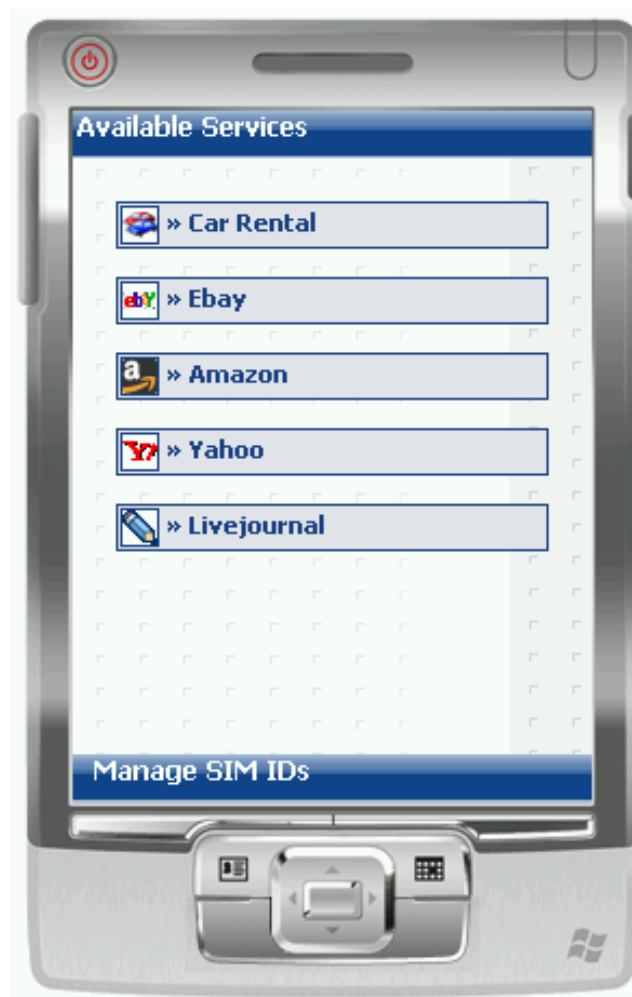
Welcome
johnnyq!

back to service list

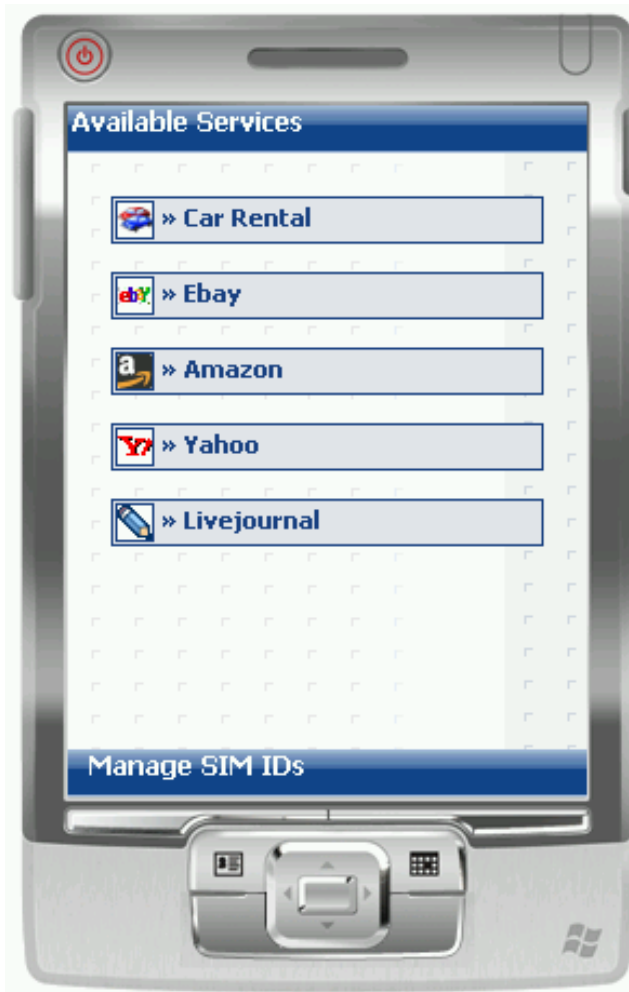
■ ■ ■ ■ Login Data Management



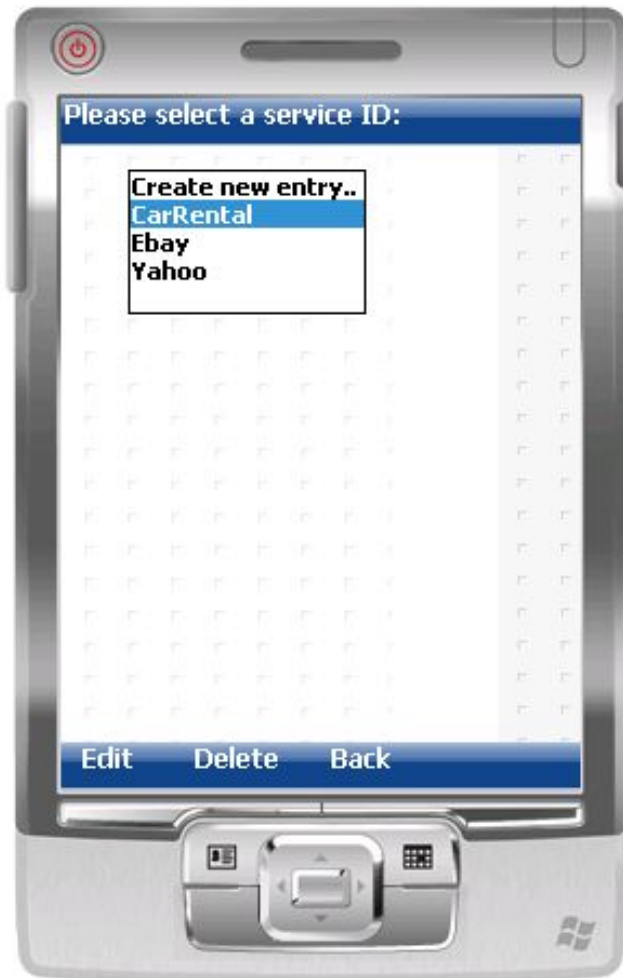
■ ■ ■ ■ Login Data Management



Login Data Management



■ ■ ■ ■ Login Data Management



Strong User/Client Authentication



- 4 In ICT, often only the *server side* is strongly authenticated (e.g. using RSA)
- 4 However there exist already some examples showing the need for a strong user/client authentication
 - Home Banking uses additional devices to implement RSA at client side
 - Skype uses strong client authentication in addition to user authentication
 - ...
- 4 Use cases in ICT
 - eCommerce: reputation and proof of purchase
 - eFinance: home banking
 - eGovernment: allowing to sign declarations by citizens
 - eHealth: allowing patients to proof their identity before accessing Hospital services
 - Social networking and p2p: recommendations from friends and local people (e.g. a good restaurant, a nice hotel, a place to visit)

Mobile Electronic Memos (MEMs)



- 4 Mobile Electronic Memos (MEMs) are electronic notes consisting of a data structure associated with a specific class of information
 - location, person, service, shops, events...
- 4 MEMs are used to capture context information from the environment or from services. They can be
 - stored for future use
 - shared them with other users
 - given as input to services and applications
- 4 MEMs may implement non-repudiation capability. They may be signed by users directly from their mobile phones using a secret key contained in their USIM

Trusted MEMs

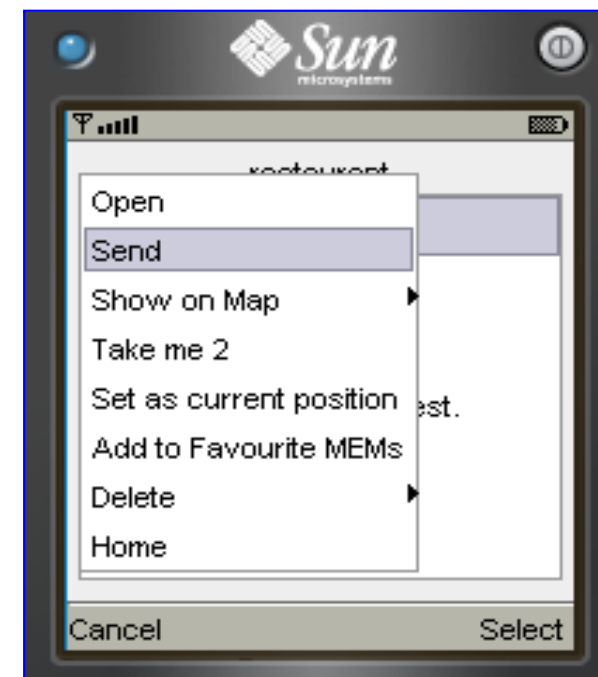


- 4 User A sends a MEM to user B
- 4 ...but User B accepts only signed MEM (user's B preference)
- 4 A warning message is displayed to User A
- 4 User A is requested to sign the MEM (or cancel the transaction)
- 4 User A sign the MEM using the PriK in the SIM
- 4 The signed MEM is sent to User B
- 4 User B checks whether the signature is authentic using the SMS PKI
- 4 The signature is authentic
- 4 ... thus the received MEM is trusted
- 4 User B is finally notified about the received MEM

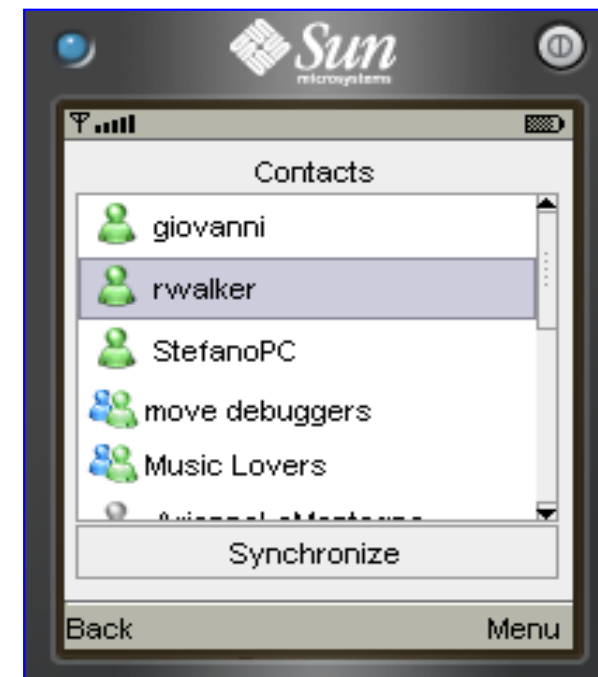
■ Signing MEMs



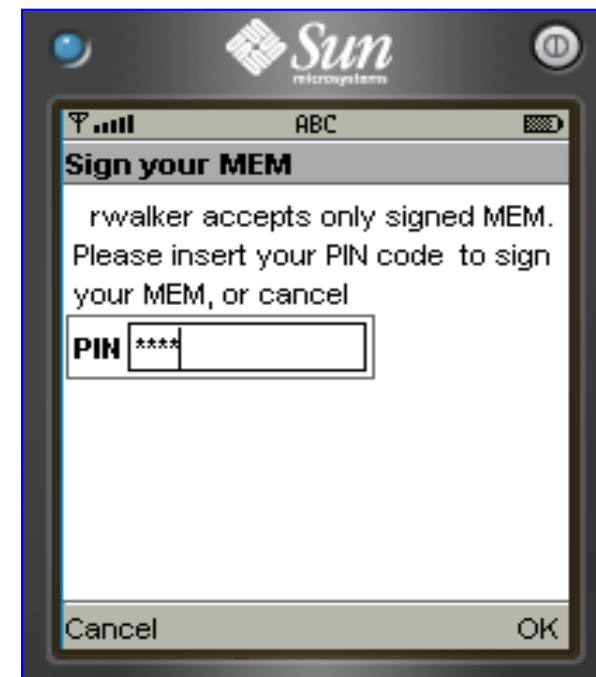
Signing MEMs



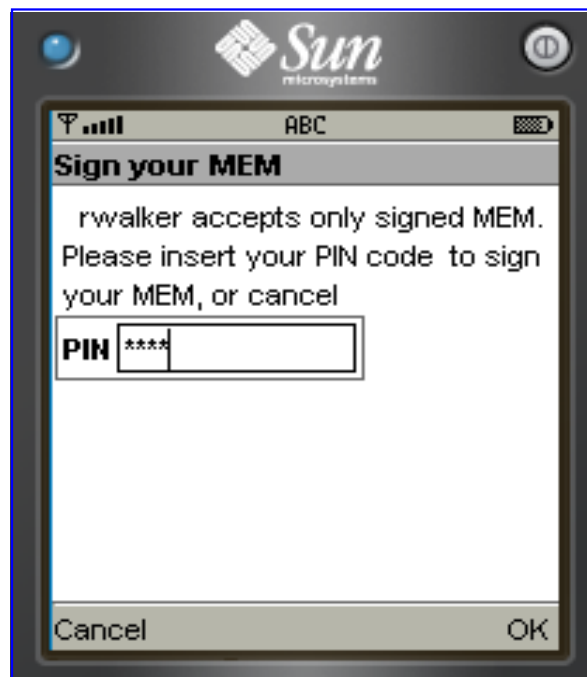
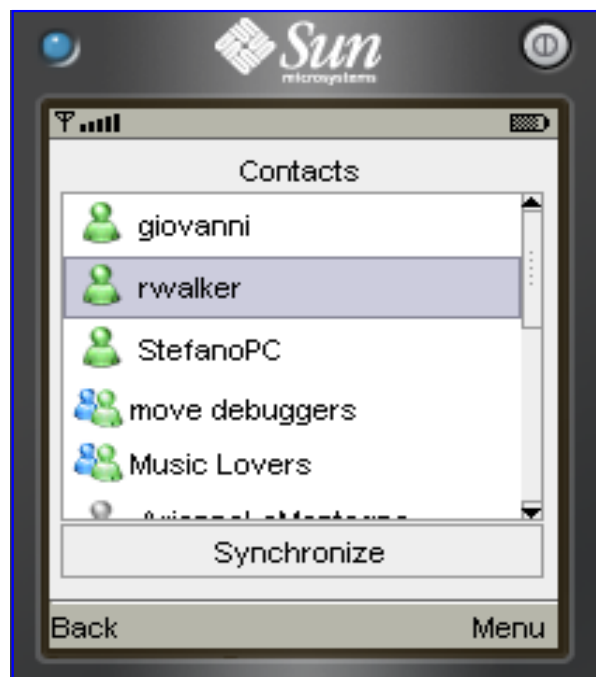
Signing MEMs



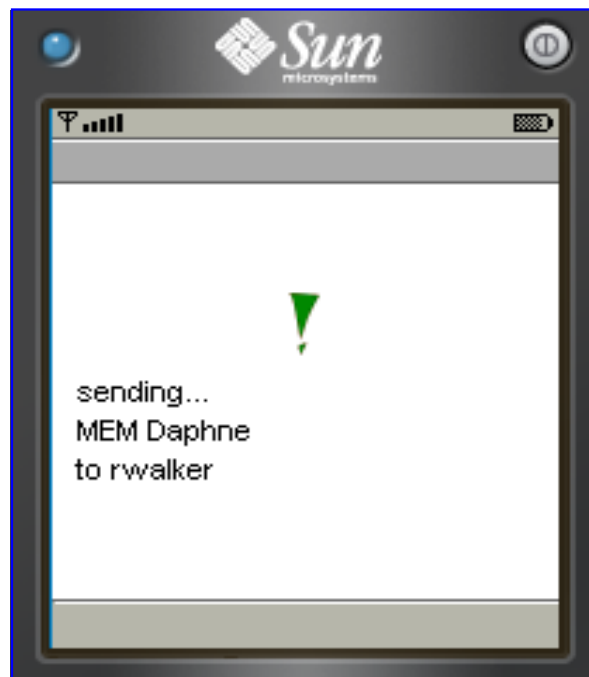
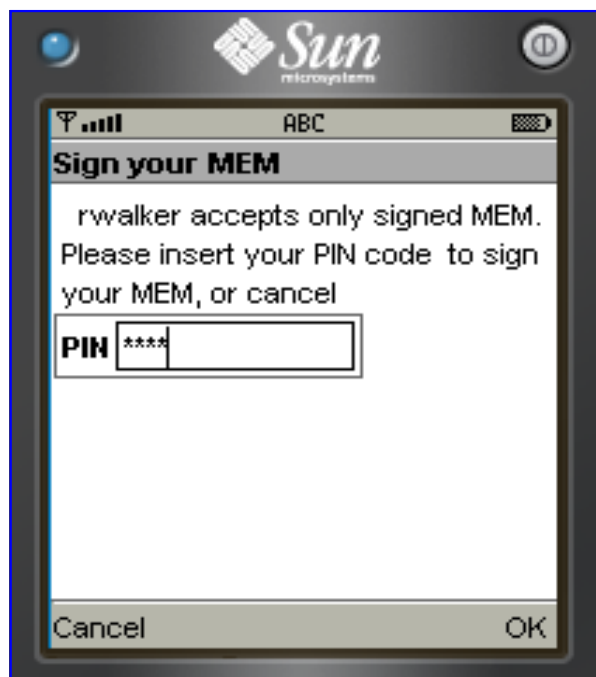
Signing MEMs



Signing MEMs

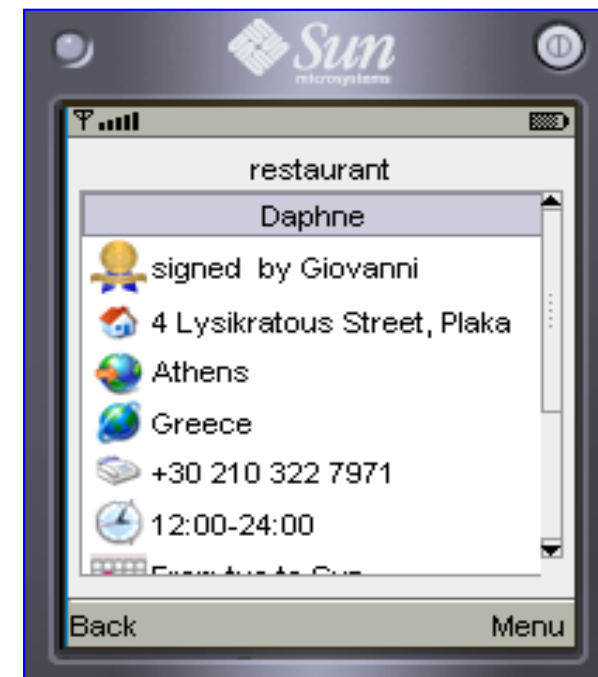
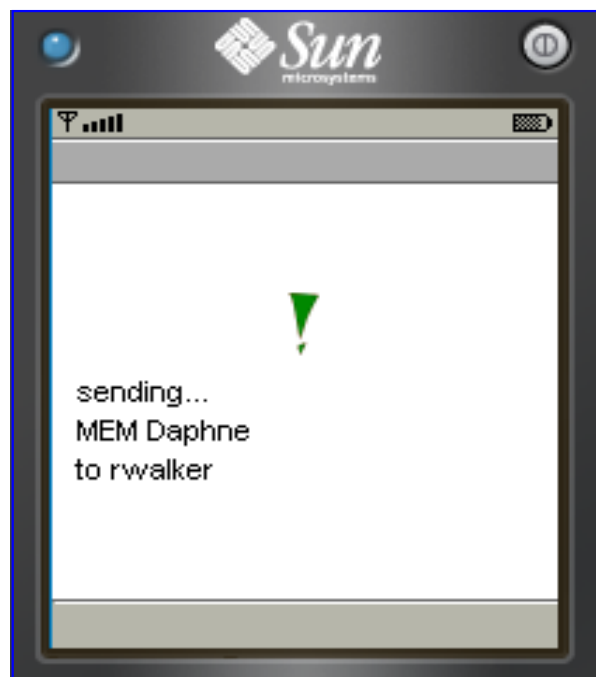


Signing MEMs



user B

Signing MEMs



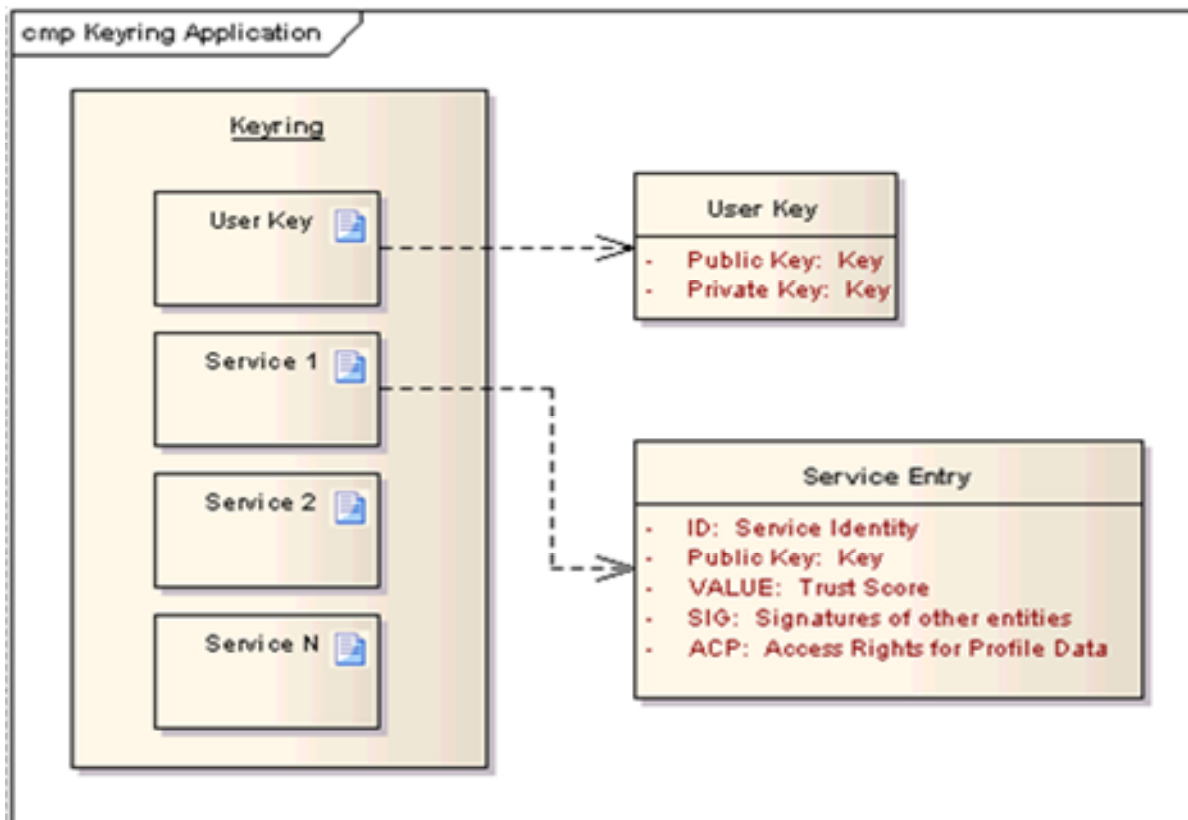
user B

Service and Trust Management on Card



On-card signature service:

- digital sign with your identity
- proof the signature of other entities



Editor Application

First implementations of
OpenPGPCard on Java Card™

SIM based service verification



Trust verification Service



Service Discovery



Trials at the University of Roma

- 4 Three SIM Applications for Trials:
- 4 User Data Management: Secure Storage on SIM
- 4 Digital Signature Service: Building Signature with SIM identity
- 4 Software Deployment Service: IMEI Tracking by SIM

- 4 Factory Production of 100 Test SIM Cards
- 4 including Telecom Italia Subscription Data
- 4 Gateway Software for Windows Mobile Phones

- 4 Ongoing work !



■ ■ ■ ■ Conclusion



4 Introduction

4 SIM Integration in Simple Mobile Services

4 SIM Enabled Basic Services

4 Application Examples

Conclusion



4 Introduction

4 SIM Integration in Simple Mobile Services

4 SIM Enabled Basic Services

4 Application Examples

**Thank you for
your attention!**

