Technological landscape behind Mobile Identity

June 21st, 2012

simalliance

Agenda

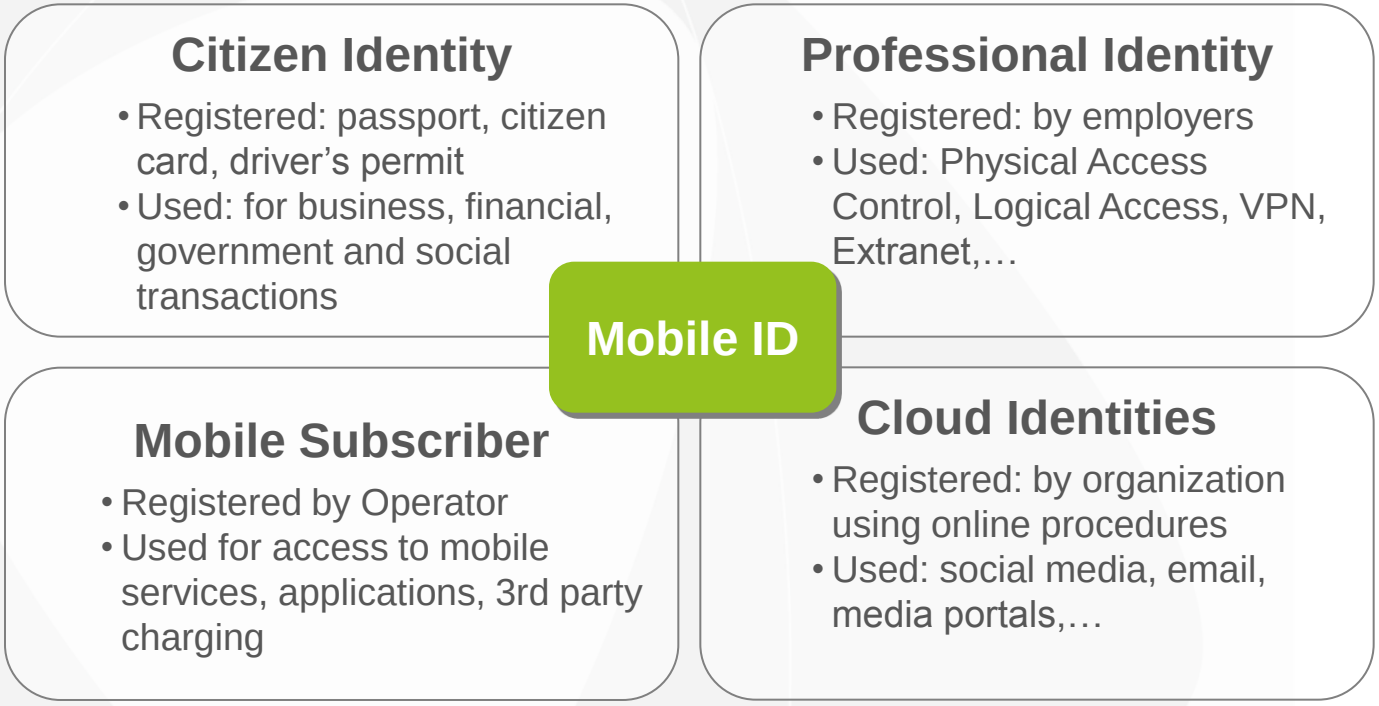
- Building trust In the Cloud
  - Introduction to identity and security issues
  - Secure Elements
- Strong authentication methods
  - 2G/3G Credentials
  - OTP,
  - Wireless PKI
- Enabling collaboration between Applications Developers, Service Providers and MNOs
  - Open Mobile API
  - Identity & Authentication Sharing and Credential Wallet

simalliance

Building trust In the Cloud



Defining Mobile Identity



Mobile Identity is the use of identities of all type in mobility use cases

simalliance

Usernames and passwords are not enough. How to add another factor to perform strong authentication?

Factors for Authentication

Something the user knows:
- PIN or a Password
- Shared secrets such as answers to questions or known images



Something the user has:
- Smart Card / Secure Element
- Password generating token
- USB token

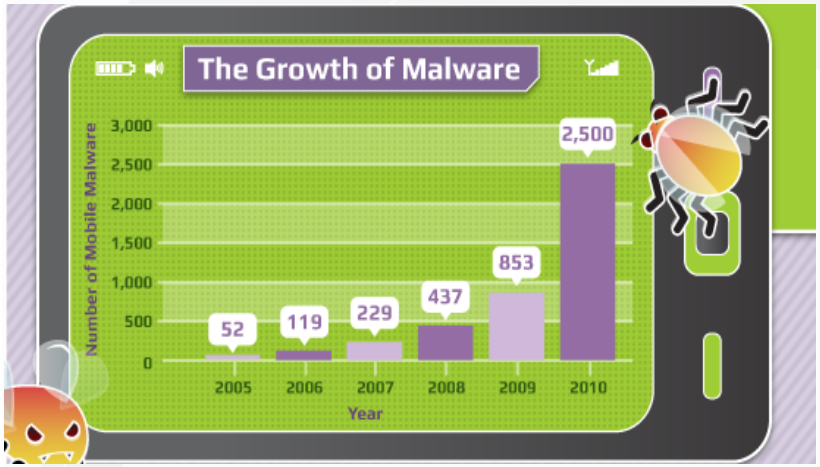
Something the user is such as biometric characteristics
- Fingerprint, face, voice, handwriting recognition, Finger and hand geometry, retinal scan, iris scan

Using the mobile device as a an authentication factor, with an OTP or PKI, is safe and convenient…

simalliance

Source: FFIEC, Guidelines for Authentication in Mobile Banking

..Mobile Internet Devices are vulnerable



Source:Bullguard 2011



The UICC is a secure element (SE) providing a safe execution environment for identity applications

- Highly **Secured** (Certifications: EMVCO, CC up to EAL5, CAST)
- Highly **customizable** Multi-services platform (java & GP OS)
- **Connected**: NFC(SWP) & Remotely manageable (OTA & OTI)
- **Multi-party** manageable: Secured domains managed independently by each entity +**dynamic** security domains creation
- **Standardized**
- **Interoperable** for mobile devices, for services hosting & management (TSM compliant)
- **Proven and mature** technology – **NFC Ready**



simalliance

Strong authentication methods

simalliance

Solutions available for authenticating mobile subscribers with secure elements

- **GSM/3G Credentials** to authenticate authorized subscriber devices
  - Using phone calls and SMS in 2G networks, GBA and EAP in 3G networks
- **One Time Password (OTP)**
  - Such application can be stored and executed in a secure element for a higher security level
- **Wireless Public Key Infrastructure (WPKI)**
  - PKI requires a second factor in the form of a secure element where the certificates are stored



Download SIMalliance White Paper « Secure Authentication for Mobile Internet Services: Critical Considerations » at ***www.simalliance.org***

simalliance

The basic use case of authentication with a 2G phone

A site performs a strong authentication
of a subscriber by sending an OTP via SMS

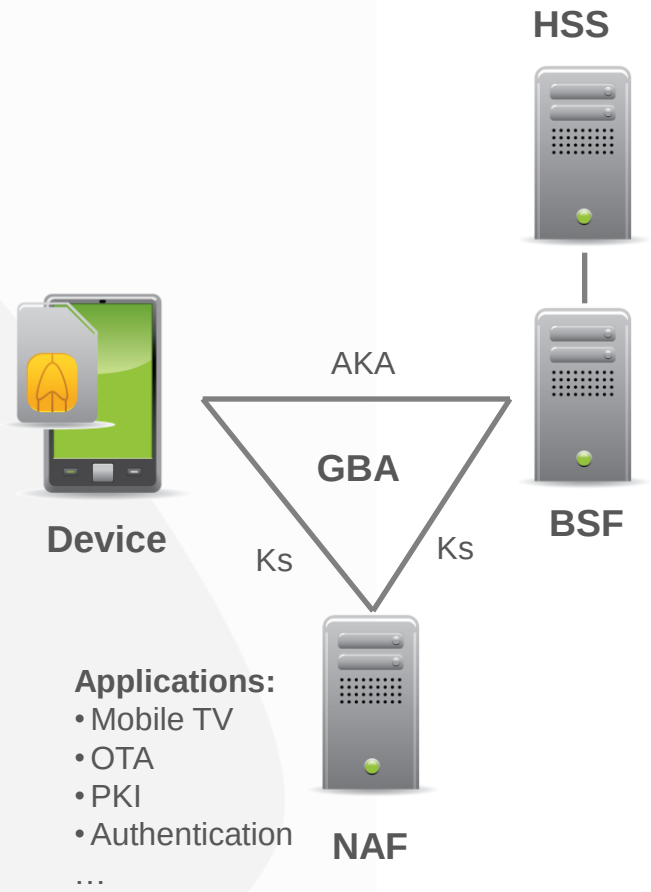


This approach is simple but not adapted to a frequent use in mobile internet applications. Its use is limited to risk-based scenarios such as recovering passwords for example

simalliance

Authenticating subscribers in mobile data networks using 3G credentials and GBA

- Generic Bootstrapping Architecture (GBA)
  - A shared secret (Ks) between a device and an application sever (NAF) is derived from 3G Authentication (AKA) using a bootstrapping server (BSF)
- The applications (NAF) of GBA include authentication for:
  - Service Platforms: Mobile TV, OTA platforms
  - Deployment of PKI: to request a subscriber certificate (SSC)
  - Cloud authentication service



The UICC can provide, using GBA (or EAP, …), a continuous and seamless factor of authentication for connected mobile applications

Standards: 3GPP TS 33.220 (GBA) 3GPP TS 33.221 (SSC)

The UICC can host a OTP service

- OTP Client on SIM
  - Support of Several Services
  - Java Card Applet
    - Use SHA-1 on the chip
    - Use STK menu on the mobile
  - Compatible standard HOTP: (RFC 4226)
  - Applet loaded during the personalization or OTA
  - Service activation via OTA



- Market Experience:
  - Used in mobile banking, business applications

simalliance

Wireless PKI use cases

- Privately Managed PKI
  - For use inside the corporation



User in the corporation



Email



VPN



Private Application

- Electronic Signature
  - Registration process with formal ID
  - Legally binding, presumed reliable
  - Common Criteria Certification



Legal Identity



Banking & Insurance



E-Government



Health



simalliance

Operator can play a role as a Registration Authority

- Operators perform registration already,
  - To manage fraud
  - Or comply with national security regulations
- …gain in dematerializing contracts in the process,
  - Credit Checks, Signature, Activation, Archive, Retrieval…
- …and add support for subscriber certificate
  - Generate certificate and store the SIM.



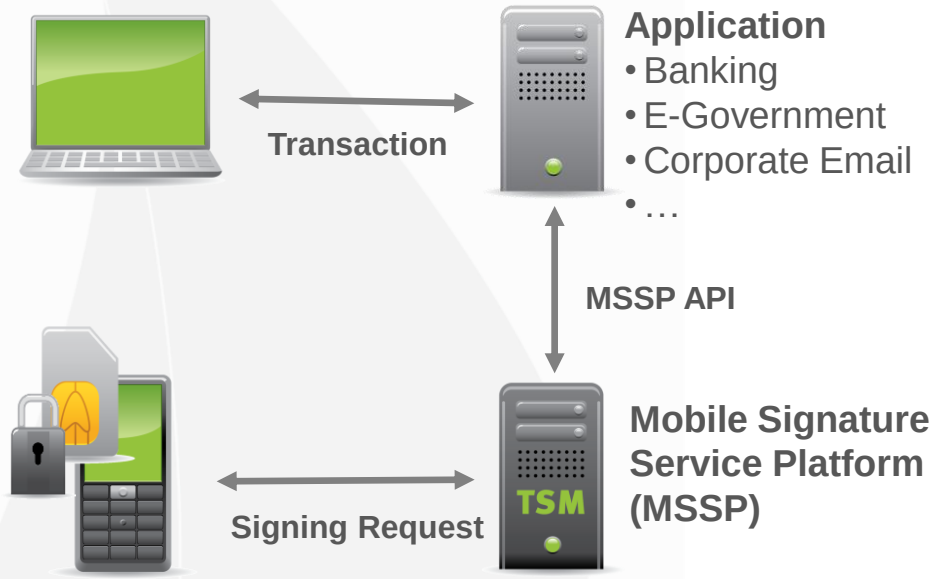
Registration Kiosk In Point of Sale



simalliance

The Secure Element enables a Mobile Signature Service

- Mobile Signature Service Platforms
  - Operated by MNOs
  - Signature Client on SIM
  - Standards:
    - ETSI TS 102 203, 102 204
- Market Experience
  - Turkey
  - Northern & Eastern Europe



simalliance

Enabling collaboration between Applications Developers, Service Providers and MNOs

simalliance

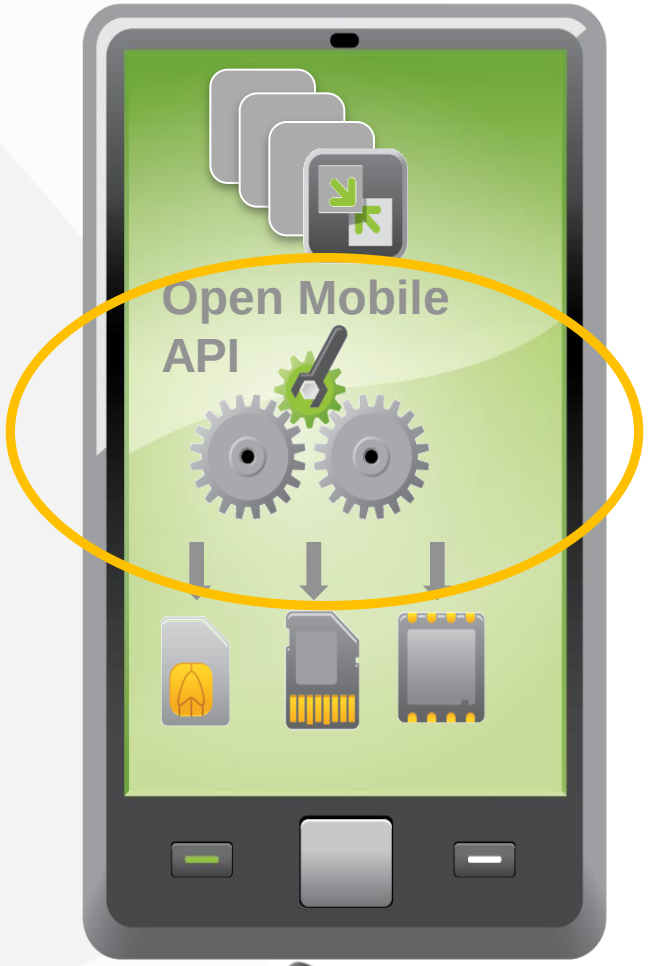
OpenMobile API enhances the customer experience in a Smartphone World an opens the SE to developers

The **Open Mobile API** is a software interface on the phone that

- Adds the missing link between mobile applications and the Secure Elements
- Provides access to all kinds of Secure Elements via a single interface
- Defined in an OS and programming language agnostic way

The Open Mobile API is specified by the SIMalliance

Open Mobile API is mandatory part of GSMA NFC Handset requirements



simalliance

Agreement between Service Provider and MNO: Identity and Authentication sharing approaches

Identity sharing

- Principle
  - MNO provides a full identity service from registration to authentication with SSO to 3rd party applications.
- Service Models
  - **Federated:** MNO, as ID provider ,controls where the ID is shared
    - ie Content partners, Liberty Alliance
  - Or **User centric:** User decides where the ID is shared.
    - ie OpenID, facebook connect

Authentication sharing

- Principle
  - MNO only authenticates the second factor (OTP, SIM,…) and not the full identity.
- Service Models
  - **Centralized token service model:** Many sites, 1 token service
    - Ie: OTP Service
  - Or **Distributed validation model:** Many sites, many token services with token lookup

In all of these approaches, the MNO is responsible for issuing, provisioning and validating credentials

simalliance

Source: OATH Reference Architecture, Release 2.0

Agreement between Service Provider and MNO: Credential Wallet approach

- **Principle:** Mobile device aggregates the credentials issued by different service providers and ID providers in a wallet secured by the UICC
- The **Global Platform 2.2** framework enables Service Providers and MNO to manage credentials on the UICC
  - Amendment A: Confidential Card Content Management
    - Create Security Domains (SD) and allocate keys, load trusted applications, and personalize cards remotely
  - Amendment B: Remote Application Management over HTTP
    - Manage remotely larger files such as large keys
- **Trusted Service Manager (TSM)**
  - Manages the lifecycle of secure elements, trusted applications and credentials

In this approach, deployed for NFC, the SP issues and validates the credentials and the MNO provisions and hosts them on the UICC

Source: OATH Reference Architecture, Release 2.0; Global Platform

Conclusion

- Secure Element are necessary to store and manage user credentials, to counter security threats and meet certification requirements
- The Secure Element provide convenient authentication to connected, with improved security compared to other methods using:
  - GSM/3G Credentials, OTP, Wireless PKI
- The operator can play a role as Registration Authority for qualified signature services and use the SIM as a certified vehicle
- Technology options (form factors and Global Platform) enable Service Provider and MNO to support the identity service model best adapted to their business
  - Identity and authentication sharing, credential wallet

simalliance

Appendix A: Support Slides

simalliance

Do you trust Mobile Identities?

How Private Is Your Smart Grid Data?

2:38 PM Wednesday October 13, 2010
by Usman Sindhu | Comments (1)

[For more, visit Tomorrow's Smart Grid.]

Privacy is not security, but it's an equally important an issue to smart grid integrity. And like security, much needs to be worked out to ensure privacy breaches don't expose consumers to malicious attacks, fraud or other invasive practices.

Sony Hacked Again, 1 Million Passwords Exposed

Hacker group LulzSec releases 150,000 Sony Pictures records, including usernames and passwords, in latest setback for consumer electronics giant.

By **Mathew J. Schwartz** InformationWeek
June 03, 2011 11:36 AM

Hack Attack Exposes 1.3 Million Sega Accounts

LulzSec says to watch your Facebook, Gmail, and Skype passwords, though no one ha responsibility for the Sega breach.

By **Mathew J. Schwartz** InformationWeek
June 20, 2011 06:13 PM

The Gazette
montrealgazette.com

HOME | NEWS | OPINION | BUSINESS | SPORTS | ARTS | LIFE | HEALTH | TECHNOLO

Experts raise alarm over Citigroup cyber attack

Hackers access credit-card data

REUTERS JUNE 10, 2011

Recommend | Tweet 1 | Shar

Major U.S. banks came under growing pressure from banking regulators to improve the security of customer accounts after Citigroup Inc. became the latest high-profile victim of a cyber attack.

STORY TOOLS
E-mail this
Print this Art

Could DigiNotar Hack Lead to a Cyberatt You?

By Jeremy A. Kaplan
Published September 06, 2011 | FoxNews.com

Print | Email | Share | Recommend 78 | Tweet 104



Hackers colluding with the Iranian government to spy on democratic activists may have made it easier for cybercrooks to spy on you, a security expert told FoxNews.com.

The Dutch government over the weekend seized control of DigiNotar --

THE CYBERCRIME ECONOMY

More than 6 million LinkedIn passwords stolen

By David Goldman @CNNMoneyTech June 7, 2012: 9:34 AM ET

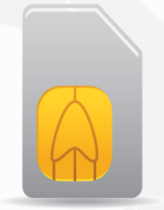
CNNMoney

325 comments

simalliance

Secure Element (SE) are in different form factors





UICC (SIM)

> Includes the application that authenticates the user in the network

> **Distributed by the Network Operator (MNO)**



Secure MicroSD

> SE embedded in µSD form factor and featuring large memory

> **Distributed by the Service Provider (SP)**



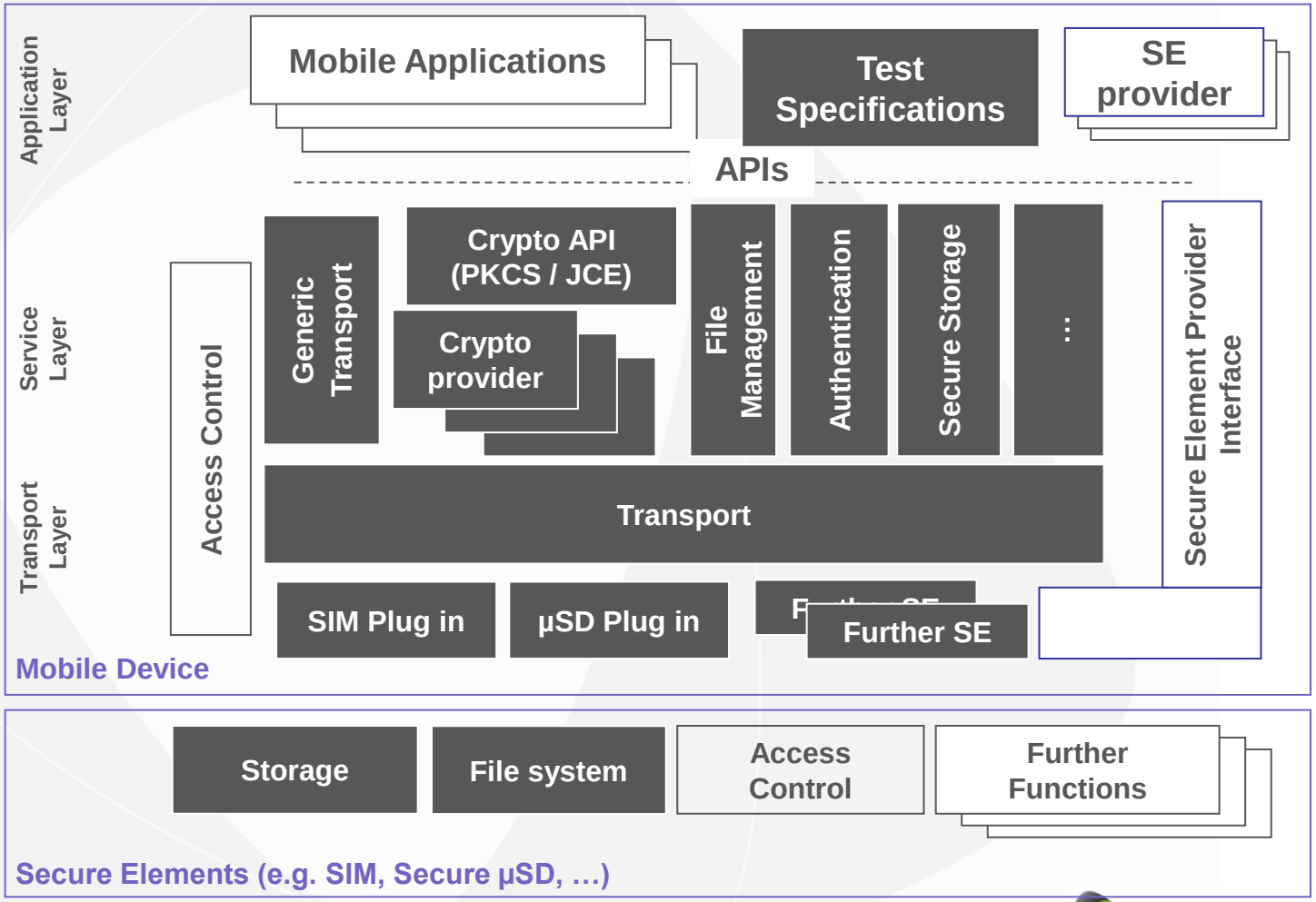
Embedded Secure Element (eSE)

> SE embedded in the mobile at the time of manufacturing

> **Distributed by the Device Maker (OEM)**

simalliance

Architecture of Open Mobile API



Open Mobile API is gaining adoption

- Currently available for Android
  - http://code.google.com/p/seek-for-android/
- Featured devices: (as of june 2012)
  - SAMSUNG Galaxy S2 NFC
  - ACER Liquid Express
  - Huawei T20
  - ZTE P728
  - LG Optimus Net NFC
  - …

Open Mobile API is mandatory part of GSMA NFC Handset requirements

simalliance

Mobile ID is rolled out in different business models: The SE distribution models

- **Model 1: The SE is the UICC, owned by the MNO**
  - UICC available in every 3GPP handset.
  - Requires agreement between MNO and service provider*
- **Model 2: The SE is a microSD card, issued by the Service Provider**
  - One SE per service ? or cooperation between SPs ?
  - Additional cost for distributing SE
- **Model 3: The SE is embedded in the handset (eSE), distributed by the OEM**
  - Provisioning of credentials ?
  - Agreements between OEM and SPs

***The agreement between MNO and Service Provider may have different approaches: Identity & authentication sharing, credential wallet,…**

simalliance

The link between the Service Provider and the SE:

Trusted Service Manager (TSM)

Why a TSM ?
Avoid application issuer dealing with multiple entities, phones, OS



Which functions does a TSM provide?
Activation, provisioning and life-cycle management

What does a TSM manage?
Credentials and applications stored on the various SE's

Who could be the TSM?
MNO, application issuer, personalization bureau, 3rd party…

simalliance

Appendix B: Use Cases

simalliance

Corporate –
Cloud applications and company network access



Local



Cloud



http://www2.sfdcstatic.com
f
http://www.salesforce.com/
crm/



Microsoft Office 365

- Apps access customer and company data, and employees feed data from their mobile devices
- Employees access the company network and applications through their mobile device (BYOD – Bring Your Own Device / consumerization of IT)

Is the access to those resources secured?

simalliance

User- centric – Data sharing services

Today, a smartphone user……

uploads mobile-created content



http://instagr.am/

access content created anywhere



https://www.dropbox.com/android

synchronizes across all its devices



http://evernote.com/

- All my life is in the cloud
- Service providers require only a login and a password to access my account

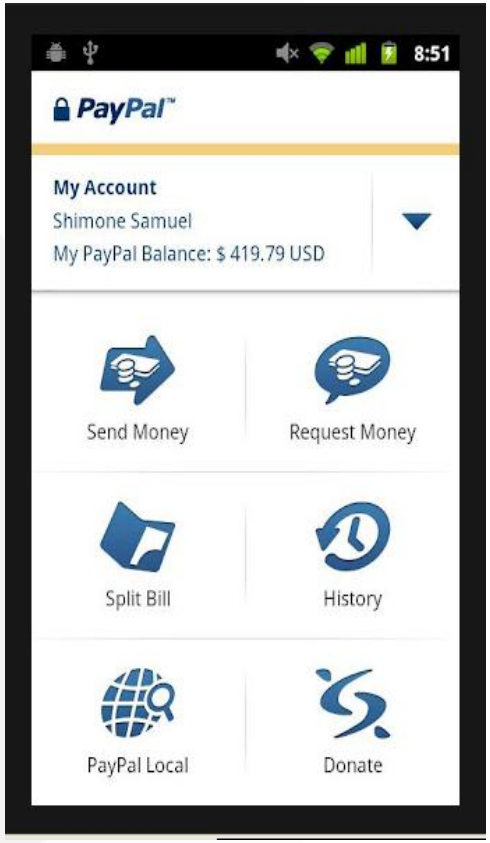
Am I the only one who can access or manage access rights to my data?

Mobile Transactions

- Access your balance, add a bank account, wire money to a friend, trade your stocks, subscribe a new contract….
- So many possibilities at your fingertips…

… but with the right level of security?

- Most apps simply use Login/Password



simalliance

E-Goverment







- Governments are fostering mobile services to reach their citizens and cut costs
- Possible use cases: Tax payments, voting in elections, license/permit management, healthcare right access…

Highest level of security is needed to deliver government-grade services

simalliance