Mobile Government

AK IT-Sicherheit 1 (WS14)
Agenda

- Part 1: Mobile Government: Basics

- Break

- Part 2: Mobile Signature Solutions
Part 1: Mobile Government: Basics
Control Questions

- What is mobile government?

- What are the benefits, success factors, acceptance factors, and challenges of mobile government?

- What are the main differences between m-government in developing countries and developed countries?

- What are typical m-government solutions in developing countries and in developed countries?
Mobile Government

Mobility

E-Government

Mobile Government (m-Government)
Definition „Mobility“

- **Device Mobility**: „[…] the continued access to services with a device while moving’.“

- **User Mobility**: „[…] refers to location- and device-independent service access apart from the mobility without physical constraints.”

- **Service Mobility**: “[…] the capability to provide a certain service irrespective of device and user.”

[ Roggenkamp, 2004 ]
Mobile Government

- m-Government “may be defined as a strategy and its implementation involving the utilization of all kinds of wireless and mobile technology, services, applications and devices for improving benefits to the parties involved in e-government including citizens, businesses and all government units”
  
  [Kushchu, 2003]

- “m-Government is largely a matter of getting public sector IT systems geared to interoperability with citizen’s mobile devices”
  
  [Antovski, 2005]

- “m-Government involves the provision of public sector services via mobile technologies […] m-Government involves interaction where the contexts are unknown, where accessing government services might be one of several activities being undertaken and where the physical constraints of interacting with mobile devices limit the amount and type of information that might be located and accessed”
  
  [Carroll, 2005]
What is Mobile Government?

- Mobile government refers to the use of mobile technologies in the context of e-government with the aim to improve existing services and to provide new solutions.

- Mobile government is a subset but not a substitute of e-government.
What M-Government Should NOT Be…
Reasons for Mobile Government

- Enables access to e-government services everywhere and anytime („Always-on Society“)

- Makes citizens contactable 24/7

- Improves the usability of e-government services
Reasons for Mobile Government

- Cutting-edge technologies enable new types of application
  - Location-based services
  - Services relying on short-range communication
  - ...

- Increased opportunities for personalized services, as mobile end-user devices are usually not shared

- Because it is sometimes the only alternative
Relevant Success and Acceptance Factors

- Infrastructure
- Legal basis
- Security and Privacy
- User acceptance
  - Availability
  - Usability
  - Trustworthiness
Challenges

- Security
- Accessibility
- Usability
- High development costs
- Dynamic mobile market
  - Frequent technical innovations
  - Fast changing markets
Mobile Government in Developing Countries
M-Government in Developing Countries

- Wired communication networks are often underdeveloped
- Mobile communication networks are usually better developed
- Mobile government is often the only alternative

[Matthes, 2012]
Case Study: Text to Change

- Launched in 2008 as health-education program

- Distribution of information via SMS

- Ongoing enhancements
  - Interactive quiz
  - SMS- and app-based surveys
  - etc..

- http://www.texttochange.org/
Case Study: M-Pesa

- Cashless payments via mobile phones
  - No bank account required
  - M-Pesa agents act as interface to virtual accounts
  - Enables mobile user-to-user transactions
- Developed by Safaricom and Vodafone
- Introduced in Kenya in 2007
- Expanded to other countries
  - Tanzania (2008)
  - South Africa (2010)
- [http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa](http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa)
Case Study: text2teach

- Provision of teaching material (videos, etc.) via mobile networks

- Goal: Improve education of children in underdeveloped regions

- http://www.text2teach.org.ph/
**M-Government in Developing Countries**

- M-government in developing countries focuses on certain sectors
  - m-health
  - m-education
  - ...

- Simple mobile technologies still predominating
  - Voice
  - SMS

- Further case studies
  - http://www.mgovworld.org/
Mobile Government in Developed Countries
M-Government in Developed Countries

- Mobile communication technologies usually complement well-developed wired communication networks

- Mobile solutions are nice feature, but not a must

- Mobile communication networks and end-user devices are typically more developed than in developing regions
Case Study: Smartphone Apps

- In most cases pure informational services
  - City maps with points of interest
  - Information on public transport
- Different providers
  - Public sector
  - Private sector (Open Government Data)
- Few apps that enable interaction between citizens and public administrations
  - BuitenBeter (NL): Reporting of issues in public space via app
- Austria: https://www.bka.gv.at/site/6490/default.aspx
Case Study: SMS-Based Solutions

- **Disaster alert systems**
  - etc.

- **Teacher-parent-student communication**
  - TextaParent (Ireland): [https://www.textaparent.ie](https://www.textaparent.ie)

- **Process enhancements**
Case Study: Mobile Signatures

- Electronic signatures are key component of transactional services (e-government, e-business, etc.)
- Especially important in Europe (EU Signature Directive, EU eIDAS Regulation)
- Mobile signatures are alternative to smart card based approaches
- Available in various European countries
  - Austria: Mobile Phone Signature ([http://www.handy-signatur.at/](http://www.handy-signatur.at/))
  - Estonia: Mobiil ID ([http://mobiil.id.ee/](http://mobiil.id.ee/))
  - Norway: BankID ([https://www.bankid.no/](https://www.bankid.no/))
  - etc.
M-Government in Developed Countries

- M-Government Solutions need to bring additional value for citizens
  - Location awareness
  - Always-on characteristic
  - etc.

- Use of established and innovative technologies
  - SMS
  - Smartphone apps

- Special relevance: Mobile signature solutions
Break
Agenda

- Part 1: Mobile Government: Basics
- Break
- Part 2: Mobile Signature Solutions
Mobile Government – Key Facts

- Use of mobile technologies in the context of e-government with the aim to improve existing services and to develop new applications

- Various benefits, success criteria, acceptance criteria, and challenges

- Increasing use in both developing and developed countries

- Various use cases and application scenarios
Part 2: Mobile Signature Solutions
Control Questions

- Why are electronic signatures important for e-government?
- How are mobile technologies employed by current mobile signature solutions?
- What are pros and cons of current mobile signature solutions?
- Which approaches are conceivable to create electronic signature on smartphones?
- What are advantages and disadvantages of these approaches in terms of security and usability?
Electronic Signatures

- Electronic equivalent to handwritten signatures
- Useful features
  - Data integrity
  - Authenticity
  - Non-repudiation
- Rely on asymmetric cryptography
  - RSA
  - ECDSA
- Public Key Infrastructure (PKI)
  - CA issues certificates
  - Certificates establish link between user‘s identity and his/her keys
Electronic Signatures - Applications

- **E-Banking**
  - User authentication
  - Transaction authorization

- **E-Government**
  - User authentication
  - Signing of applications
  - Signing of official notifications and administrative rulings

- **Private Affairs**
  - Signing of contracts
Electronic Signatures – Legal Aspects

- **Legal basis**
  - EU level: EU Signature Directive/eIDAS Regulation
  - National Level (Austria): Signature Act

- **Advanced vs. qualified signatures**

- **Requirements for qualified signatures**
  - Based on qualified certificates
  - Created in secure/qualified signature creation device (SSCD/QSCD)

- **Two-Factor Authentication!**
Electronic Signatures with Smart Cards

Require a smart card

Require a card-reading device

Require software for smart-card access
Idea: Use a mobile phone instead of a smart card!
Realizations

- Mobile Phone implements factor possession in two-factor authentication

- Central question: How to implement the SSCD/QSCD?

- Currently two approaches
  - Use the SIM as SSCD/QSCD
  - Use a central hardware security module (HSM) as SSCD/QSCD
SIM-Based Solutions

- SIM implements SSCD/QSCD

- Keys on SIM are protected by means of a PIN (two-factor authentication)

- Data-to-be-signed are sent to mobile phone and signed by the SIM

- ETSI Standard: *Mobile Signature Service, M-COMM*

- Available in various countries: EE, FI, NO, etc.
Case Study: Mobiil-ID (Estonia)

Pros and Cons

+ Signatures are based on SSCD/QSCD (SIM)

+ Two-factor authentication (SIM + PIN)
  - Special SIM required
  - Data-to-be-signed are present on the mobile device
  - Depending on concrete solution potentially limited to own mobile-network operator (no roaming)
Server-Based Mobile Signatures

- SSCD/QSCD implemented by central server and HSM
  - Storage of user-specific keys
  - Signature creation

- Access to user-specific keys protected by means of two-factor authentication

- Mobile phone implements factor „possession“ by receiving a one-time password
Case Study: Mobile Phone Signature (Austria)

Pros and Cons

+ No need for a special SIM
+ Reliance on a highly secure central HSM
+ Roaming support
+ Data-to-be-signed are never present on the mobile device
+ Additional security due to separated communication channels
  - SMS technology used to implement factor possession
Mobile Signatures on Smartphones
Challenges

- Smartphones are more prone to malware than classical mobile phones
- Smartphones do not necessarily represent an additional end-user device
  - Used to access applications (e.g. via integrated browser)
  - Used to create electronic signatures
- Smartphones support various additional technologies that can be used for signature-creation processes
Approaches

SIM-based approach

Server-based approach

Secure element based approach
Security? Usability?
Security Analysis

- Assets: Data-to-be-signed, credentials

- Security depends on various aspects, hence no clear „winner“

- Security depends on application scenario and smartphone platform
  - Can data be protected appropriately on the smartphone?
  - Can data be sent securely to the SIM?
  - Can credentials be entered securely?
  - Can SMS messages be reliably protected?
  - ...
# Relevant Security Aspects

<table>
<thead>
<tr>
<th></th>
<th>Secure Element</th>
<th>SIM</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Internal App</td>
<td>External App</td>
<td>Internal App</td>
</tr>
<tr>
<td>Platform support for background tasks</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Supported application sources</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Secure input of credentials to mobile apps</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Secure input of credentials to SIM applications</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Credential input via API</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Secure Processing of DTBS by mobile apps</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Secure Processing of DTBS by SIM</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Secure SMS Processing</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
Usability Analysis

- Usability is crucial acceptance factor and hence needs to be especially considered

- Aspects
  - Hardware independence
  - Software independence
  - Complexity of signature-creation process
  - Roaming support
  - ...

Graz, 2014-12-03
Mobile Government
## Relevant Usability Aspects

<table>
<thead>
<tr>
<th></th>
<th>Secure Element</th>
<th>SIM</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Independence</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Software Independence</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Efficiency</td>
<td>HIGH</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>Roaming Support</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>
Conclusions

- Electronic signatures are important tool for security-critical applications

- Mobile signature solutions are important alternative to smart card based approaches

- Mobile signature solutions are already in productive operation
  - SIM-bases approaches (Estonia, etc.)
  - Server-based approaches (Austria)
Conclusions

- Smartphones provide new opportunities to realize electronic-signature solutions
- Three approaches are basically conceivable
  - SIM
  - Server
  - Secure element
- Security heavily depends on underlying smartphone platform
- Server-based solutions are advantageous in terms of usability
Time for questions…
…and to give it a try!

https://www.handy-signatur.at/
References


- Ibrahim Kushchu and M. Halid Kuscu: From E-government to M-government: Facing the Inevitable


- Text to Change: http://www.texttochange.org/, 2013

- M-Pesa: http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa

- Handy-Signatur: http://www.handy-signatur.at