



# **CLASS**

## **Conference 2012**

Cloud Assisted Services

## **Can eGovernment work in the Cloud?**

Some examples from Digital Austria

**Peter Reichstädter**  
**Federal Chancellery of Austria**  
**ICT-Strategy**  
**Bled, 23<sup>rd</sup> October 2012**  
[peter.reichstaedter@bka.gv.at](mailto:peter.reichstaedter@bka.gv.at)

# Topics

- Definition
  - general features
- Opportunities and risks
  - Legally
  - Structurally
  - Economically
  - Technically
- example: eID and cloud
- possible approach / requirements for Austria

# Definition - general characteristics

- Cloud computing represents a (more) responsive and flexible deployment of IT resources
- Cloud computing is not a technology but a business model for providing IT services – however this demands for new technologies/ privacy considerations/ resource management/ law enforcement considerations
- the central feature is the consumption-based billing and the provision of IT services of shared resources (infrastructure, platforms, software, business processes/services)
- IT-requirements need to be decoupled from the IT infrastructure
- Cloud computing (Public cloud) is a form of outsourcing of ICT infrastructure

# Opportunities and risks - Overview

- **legal**
  - Data protection issues, ...
  - Influence on contract, ...
  - Procurement law
- **structural**
  - + faster service provisioning,
  - + Flexible bandwidth, ...
  - LockIn effects and silo solutions
  - Compliance with governance rules, ...
- **economical**
  - + standardization of IT infrastructure and services, ...
  - functional adaptation cost adjustments,
  - +/- operating costs vs. investment costs
- **technical**
  - + standardization, scalability, ...
  - Identity management, technical audit, ...

# Legal aspects

- **Public Cloud:**  
processing of personal data largely excluded,  
no possibility of contractual adjustment
- **Virtual Private Cloud:**  
only minor customization options compared to public  
cloud model
- **Private Cloud:**  
offers the best conditions to meet data protection  
requirements
- non-personal or not 'very' sensitive data are an  
option for Cloud usage
- **Contractual issues and procurement law issues!**

# Technical aspects 1/2

- **Standardization**
  - + competition between providers
  - without standards depending on the CSP operators
- **Scalability**
  - + almost unlimited resources by CSP
  - simultaneously load peaks in the worst case lead to a halt
- **Identity and rights management**
  - security concerns in the implementation of the CSP, especially the privileged user accounts (administrator)
- **Tenancy, security**
  - + is a core structure requirement for CSP, and should therefore be carried out "state of the art"

# Technical aspects 2/2

- **Cloud Management**

- + default management services are provided through web portals for convenient disposal
- Integration of tools to CSPs in customer-specific processes not yet tested

- **Technical revision**

- separation of customer-specific data (log files, ...) must be regulated by contract - currently, no standardized offers

- **Patch Management**

- + rapid roll out of standardized patch management patches through unified infrastructure
- difficulty of testing the compatibility of patches, consideration of specific customer requirements

# E-Government may be

- Informational processes
  - e.g. law information system
  - no immediate data protection dimension
- Transactional processes
  - Processing personal data
  - Authentication / quality eID plays a major role



# eID and the cloud – is there something new?

- The cloud as such is not bringing excitingly new technologies
  - It is the combination
  - It is the scale
  - It is the commercial aspect
  - It is the standard – the conformity
- By this the cloud might reach the “break through point”

# eID and the cloud – is there something new?

- It is changing some of the basic assumptions
- **The one to one model CLIENT-SERVER is no more possible**
  - it is CLIENT - CLOUD - SERVER
  - for legal considerations
  - for contractual considerations
  - for technology considerations
  - for data protection and privacy considerations
- **Most users will not yet recognize this difference**

# eID and the cloud – is there something new?

- **eID and security will bring highly impacting changes**
- **the cloud will show the need to react**
  - eID and technological quality
  - security and crypto-based technologies
  - policies and standards
- **yet there is a big difference**
  - encryption and crypto-based confidentiality hardly possible
  - user control on the physical level non-existent

transaction integrity

public data

trusted identity

reading manipulating Data

authorizing the transaction

eID

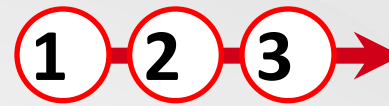


privacy - access



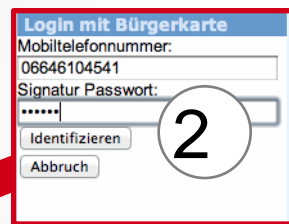
eSig

# eID and simplification



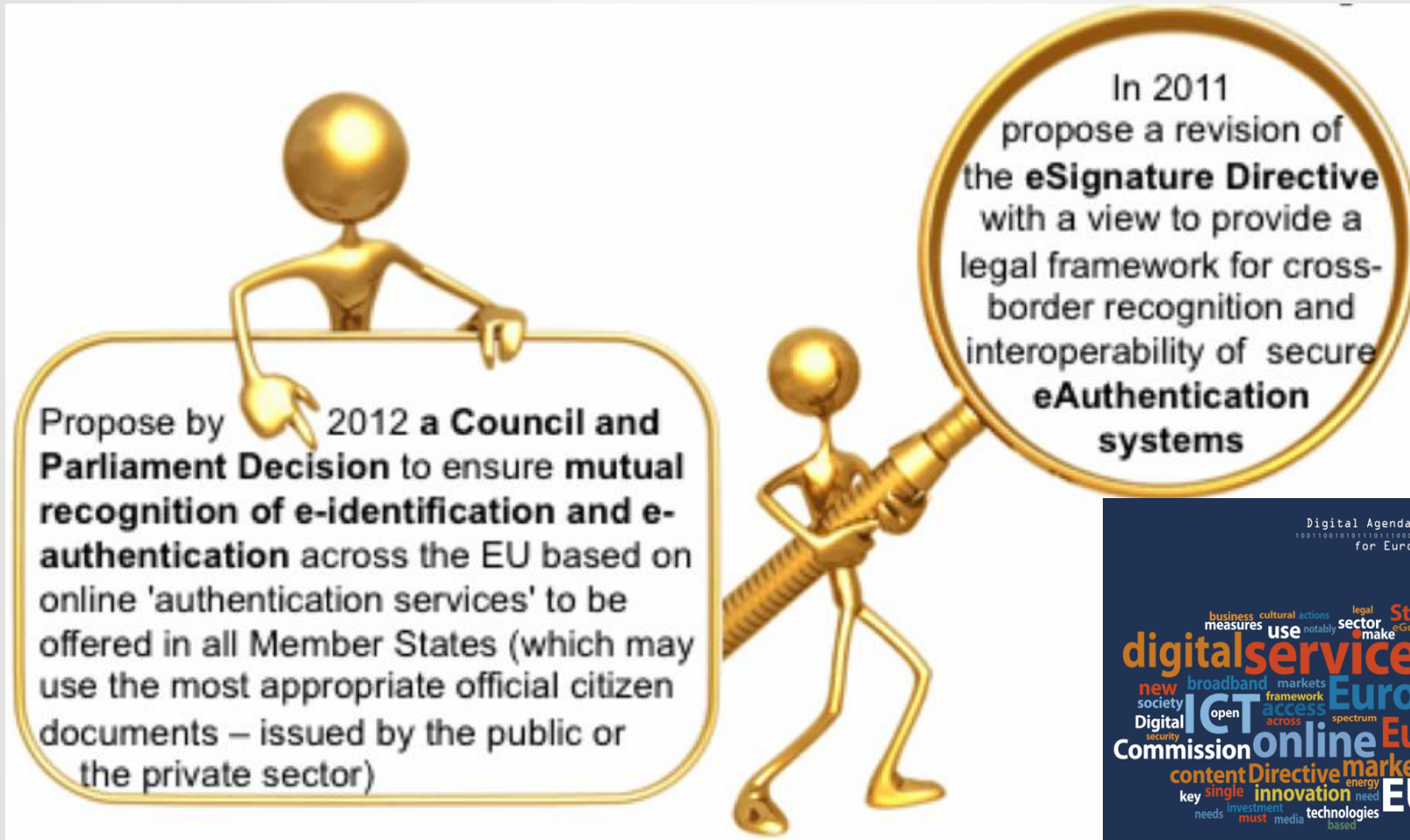
enhance usability by using one method for qualified signatures and eID

enhance acceptance by using ubiquitous devices e.g. standard mobile phones



- \* OBSERVING DATA PROTECTION
- \* ENABLING CLOUD COMPUTING

# National strategy alone? Digital Agenda for Europe

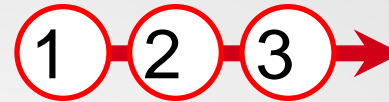


# STORK on EU eID interoperability



- Interoperability framework on top of national eID infrastructure
- To a large extent relies on MS-to-MS trust
  - SP trusting MS PEPS
  - MS-to-MS protocol shielding IdPs
  - Different in “MW-model”
- **How can a Cloud fit in?**

# the potential to extend cross border

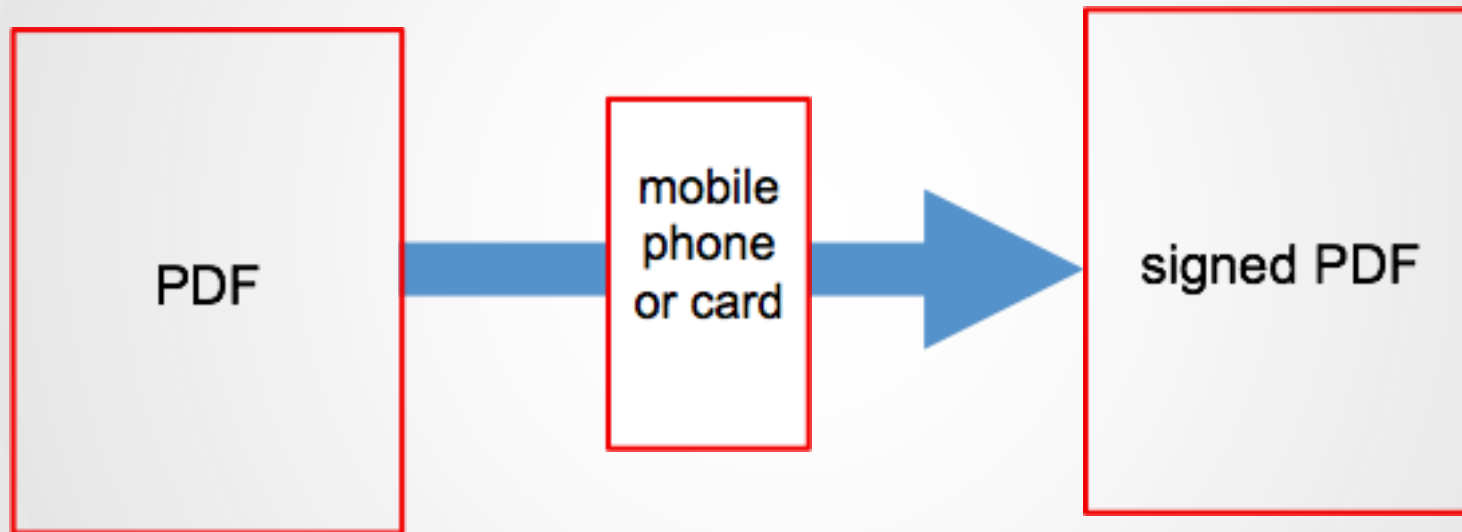
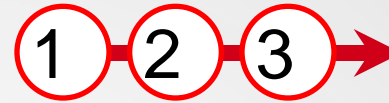


- STORK has developed to be a most recognized eID project
- managing eID for several Member States and for ECAS
- the future shall include even more MS and non natural persons (MANDATES)
- being a mostly legal and liability challenge





# coping with the dynamics of user devices



# Impacts of Cloud Computing on eID

- **new approaches (like eID) must be “cloud compatible”**
  - from the point of view of security
  - from the point of view of privacy and intellectual property protection
- **we might possibly need to twist on both ends**
  - in the eID domain
  - in the cloud domain
  - to yield contractual, legal/regulatory, commercial and technical acceptance

# Cloud - Chance and Risk

- CLOUD will enable and enforce broad usage of crypto-based services
  - eID and access control
  - storage and confidentiality of data
  - standard security for all
- **at the same time knowledge and with this awareness will be lowered at the users side**

## possible approach / requirements for Austria (1)

- **pilot and analyse cloud projects (,FRCC/BLSG‘)**
  - exchange of information and experience
  - Studying and experimenting on cloud solutions e.g. eID SSO etc.
- **,Cloud-compliant application‘**
  - develop new applications cloud ready
  - establishment of criteria, what defines "cloud compliant“
- **suitability criteria for cloud**
  - definition of suitable criteria for applications for assessing which cloud model they fit
- **Cloud standards**
  - definition of standard requirements for Cloud Providers
  - definition of a standard process model in the implementation of cloud applications

# possible approach / requirements for Austria (2)

- **Cloud assessment**
  - definition of criteria catalogue and development of models for assessment
- **Cloud sustainability and openness**
  - implement applications in the cloud so that migration is defined / assessed and / or service for alternative cloud is feasible (service runs at two different cloud providers)
- **Cloud in the administration**
  - evaluation and assessment of one / several government cloud(s) for Austria and across borders
- **Cloud – next steps:**
  - identify potential services, pilot them, learn, share, ...
  - European Cloud Partnership (ECP)

## Conclusions

- Cloud Computing on E-Government “radar”
  - Promises of cost reductions
  - Thus might assist getting efficiency gains
- Legal, technical, organizational issues
  - Citizen’s personal data in transactional services
  - May not interfere with citizen fundamental rights
  - Challenging with current public cloud contracts
- Quality eID in the Cloud to be addressed



Cloud Computing | 23.10.2012

# Thank You

## Cloud Computing / Austria

Thank you!

Peter Reichstädter

Federal Chancellery of Austria  
ICT-Strategy

Ballhausplatz 2  
A-1014 Vienna  
Phone: +43 53115 7477  
[peter.reichstaedter@bka.gv.at](mailto:peter.reichstaedter@bka.gv.at)