KATHOLIEKE UNIVERSITEIT LEUVEN A-SIT lawfort

Modinis Study Lot 3 - Study on Identity Management in eGovernment

*Modinis*IDM Overview

SEVECOM Workshop

Paris, 26 June 2006

Danny De Cock

modinis IDM

K.U.Leuven, A-SIT and Lawfort

Outline

- Introduction
- Phase I: Status of IDM
  - Country Profiles
  - Good Practice Cases
- Phase II: Barriers to Pan-European IDM
  - Organizational
  - Technical
  - Legal
- Phase III: Conceptual Framework
  - Scope
  - Consequences of Pan-European IDM
- Activities

Introduction to Modinis^{IDM}

Consortium Summary

- ***Lead contractor – K.U.Leuven Research & Development, Belgium***
  - Project manager: COSIC, prof. Bart Preneel
  - Subproject manager: ICRI, prof. Jos Dumortier
- ***Sub-contractor – Secure Information Technology Center, Austria***
  - Sub-contractor director: A-SIT, prof. Reinhard Posch
- ***Project dates & duration***
  - Start date: 1 January 2005
  - End date: 28 February 2007
  - 26 months
- ***EU Funding:***
  - € 249.970,00

Scope of the Modinis^{IDM} Study

- ***Assess impact of IDM initiatives***
  - 25 Member States
  - Cross-border and cross-sector eGovernment Services
    - Registration of persons (legal + natural)
    - Citizen mobility
  - Considering existing results from EU programs and other studies

- ***Goal***
  - Prospective analysis of possible initiatives and solutions at European level
  - Provide information on identity technologies-related market developments and technical requirements
  - Analyze good practices and use cases
    - Addressing key issues
      - Authentication, attributes, interoperability, privacy and future needs
    - From a technical, legal and organizational perspective

About Modinis^{IDM}

- ***To reach the goal – three pillars:***
  - Gathering information on national IDM infrastructures, policies and projects
  - Assessing existing difficulties and potential solutions
  - Formulating recommendations based on own and existing analysis

  ► Charting existing national solutions and policies
  ► Proposing potential solutions to the existing needs

- ***Target: Interoperable Pan-European IDM for eGovernment applications***

About modinis*IDM*

Project Structure

- ***Phase I: Status of IDM***
  - Through collection of country profiles
  - Through the good practice cases and the Good Practices Framework (GPF)
  - Resulting in:
    - The IDM Initiative Report (D3.5)
    - The Good Practice Lists (D3.7)

- ***Phase II: Identification of Barriers to Interoperable Pan-European IDM***
  - Organizational, technical and legal
  - Defining the parameters of the conceptual framework
  - Resulting in the IDM Issue Report (D3.9)

- ***Phase III: Conceptual Framework***
  - Based on the input and constrictions above
  - Finding a model that would allow existing solutions to interoperate
  - Resulting in the Yearly Reports (D3.19)

Phase I
Status of National Identity Management Systems

Phase I: Status of IDM Approach

- ***Starting point***
  - An acute need for accurate and up to date information on national IDM status
  - Dual informational track:
    - General national IDM policies and planning
    - Key IDM projects and programs
  - Through various sources: own research, public resources, other initiatives, local national experts, …

Country Profiles

Phase I: Status of IDM Country Profiles

- ***General status and most significant systems in each Member State***
  - History, scope and goals:
    - General purpose systems, …
  - Technology:
    - Used standards, choice of tokens, …
  - Applications
  - Existing issues and lessons learnt
  - Expected future developments:
    - Planned use of biometrics, …

- ***Report on 25 countries including preliminary analysis and categorization***

Phase I: Status of IDM Categories of Solutions

- ***Countries focusing on public/private partnerships:***
  - The Scandinavian countries, Austria, Malta, (the Netherlands)
  - Pro: Easier market penetration and deployment, attractive applications
  - Risks: Privacy issues, dependence on private industries
- ***Countries using/planning to use smart cards:***
  - Austria, Belgium, Finland, France, Spain, UK, Estonia, Italy,…
  - Pro: Standardized solution, potentially easy to deploy nationally/cross-border
  - Risks: Relies on public perception, dependant on use of traditional cards (importance of PR), risk of inflexibility

Phase I: Status of IDM Categories of Solutions

- ***Countries using/planning to use biometrics:***
  - France, Spain, UK, …
  - Pro: Offers advanced functionality, potentially increased reliability and security
  - Risks: Generally not politically high regarded, (even) greater importance of correct implementation

- ***Countries using/planning to use unique identifiers:***
  - Austria, Belgium, Czech Republic, the Netherlands, Ireland, Luxembourg, …
  - Pro: Easier to link data, increased governmental efficiency
  - Risks: Perceived privacy risk (diminished in the case of sectoral identifiers, such as Austria and to a lesser extent the Netherlands

- ***Other categories: mobile solutions, inclusion of non-nationals, sector-based solutions, focus on local services, token issuing, …***

Good Practice Cases

Phase I: Status of IDM Good Practice Cases

- ***Good Practice Cases: Vehicle to achieve the objectives***
  - Passive collection
    - Extracted from existing information
    - Participation in events or workshops and follow-up of other projects
  - Active collection
    - Contacting authorities and sending out our questionnaire

- ***Some already in the Good Practice Framework (GPF), others entered by us***
  - Some “very good” practice cases selected for further analysis
  - Selection based on relevance for IDM
  - GPF is about eGovernment in general
  - Lessons learned will lead to recommendations
  - After selection more information through people directly involved

- ***Selected cases published on our website***

Phase I: Status of IDM Good Practice Cases

- ***Good Practice Cases***
  - Open Portal Guard (Italy),
  - eID cards governmental employees (Slovenia)
  - DigiID (the Netherlands)
  - eID in Italy (Italy)
  - Identification Service tunnistus.fi (Finland)
  - Enforcement of eGov regulations…(Hungary)
  - Spanish Administrations Open Source (Spain)
  - French Citizen Portal (France)
  - …
- ***Selected as very good practice***
  - Austrian Citizen Card (Austria)
  - Crossroads Bank Social Security (Belgium)
  - Irish Public Service Broker System (Ireland)
  - Distributed Authentication and Authorization (Czech Republic)
  - WPKI (Sweden)

Phase II
Identified Barriers to Pan-European Identity Management

Phase II: Barriers
Technical Problems

- ***Multitude of standards / lack of common standard***
  - Applicable to almost any technical issue
  - Key goal: allowing for differences
- ***Temporary character of most solutions***
  - Typically, technical choices are “medium-term”
- ***The middleware issue***
  - Always a problem when eIDs can take many different forms…
- ***Management of authorizations***
  - In a cross-border context: sometimes difficult to scale efficiently
- ***Mapping of partial identities***
  - Depends on local technical choices: what data is available, and how should it be managed?
- ***Free choice of tokens***
  - An eID is not equal to a token
  - Not everyone wants to use smart cards (only)

Phase II: Barriers Organizational Problems

- ***Multitude of digital identities***
  - Local vs. international services, and the need for a harmonious user experience
- ***Reliability and trust***
  - Objective assessment of these qualities?
- ***The issues of delegation/representation***
  - How to model and manage this?
- ***Possible conflict between technology and socio-cultural background***
  - e.g. biometrics => potential benefit, but at what cost
- ***Tendency towards conservation of local choices***
  - Protection of investments sometimes prohibit large strategy changes
- ***Public perception ('PR')***
  - Importance of attractive applications
- ***Lack of a common terminology***
  - Enabling dialogue and exchange of best practices

Phase II: Barriers
Legal Problems

- ***Availability and use of one or more unique identifiers***
  - Obligatory issuing is sometimes illegal
- ***Mismatch between technical/legal concepts***
  - E.g. the mandate dilemma
- ***Diversity of legal frameworks vs. the need for technical interoperability***
  - Respecting legal autonomy becomes difficult when cross-border infrastructures are created...
- ***eID and European legal competence***
  - Article 18.3 of the EC Treaty: no ID cards, residence permits, social security cards…
- ***Federation and the law***
  - Core concept: circles of trust. However, the law doesn't "trust"…
- ***Varying attention to privacy issues***
  - ID cards, data exchange or access…
  - Respect socio-cultural backgrounds

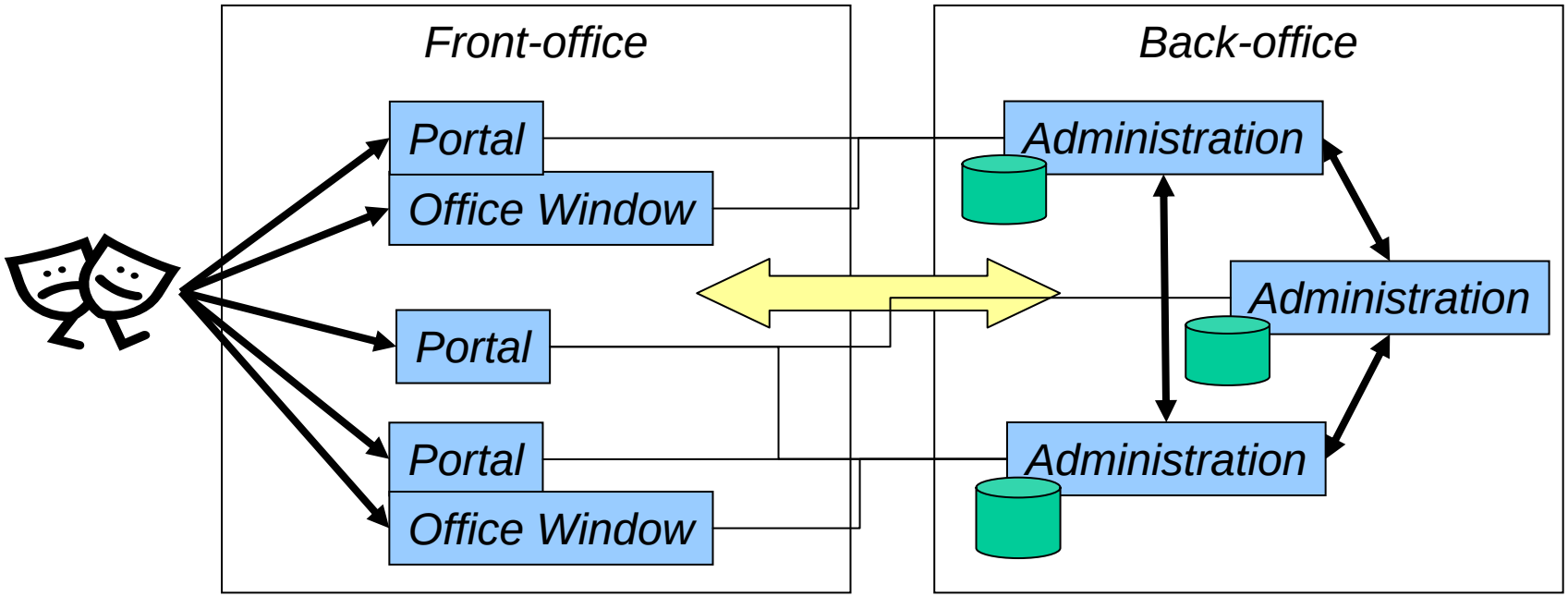
Phase III
Conceptual Framework

Phase III: Conceptual Framework Limited Scope

- ***Goal: Specify a Framework that is Compatible with all Member States' Visions***
  - One member state considers another member state as a sector in a particular context
  - A member state
    - Regulates the existence and use of context specific identifiers for its citizens on its territory
    - Cannot forbid that another member state issues context specific identifiers for its citizens within a particular context
- ***Conceptual Framework for Electronic Identity Management***
  - Link between the paper world and the electronic world
    - Non-electronic identity management is already in place: Everyone can be electronically identified within government contexts

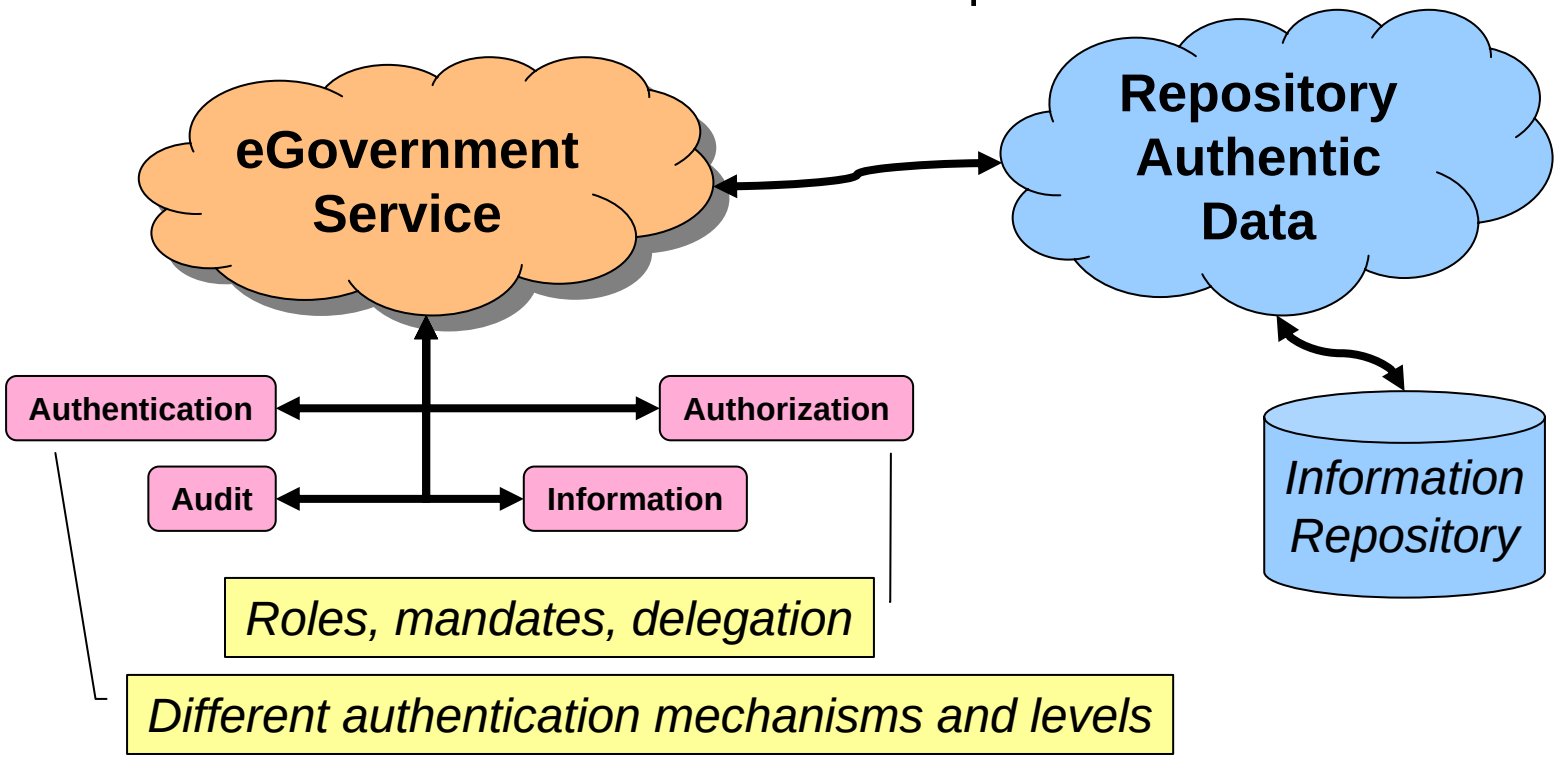
Phase III: Conceptual Framework eGovernment IDM

- ***It is about eGovernment***
  - Services offered to citizens and digitalization of information
  - eGovernment should reduce costs
  - Public sector consists of many different administrations and organisation that have 2 faces:
    - Front-office
    - Back-office
  - Note that there are different sectors: sectors are active within contexts



Phase III: Conceptual Framework Authentic Sources in eGovernment

- ***Concept of authentic sources and repositories with authentic data***
  - Information is believed to be correct
  - Information is collected only once
  - Information is reused whenever possible



Phase III: Conceptual Framework eGovernment IDM

- ***It is about Identity Management***
  - Management of personal information
  - Identity: need to be able to identify someone
    - Identifiers are unavoidable!
      - Different approaches in the Member States.
      - Who cares?!

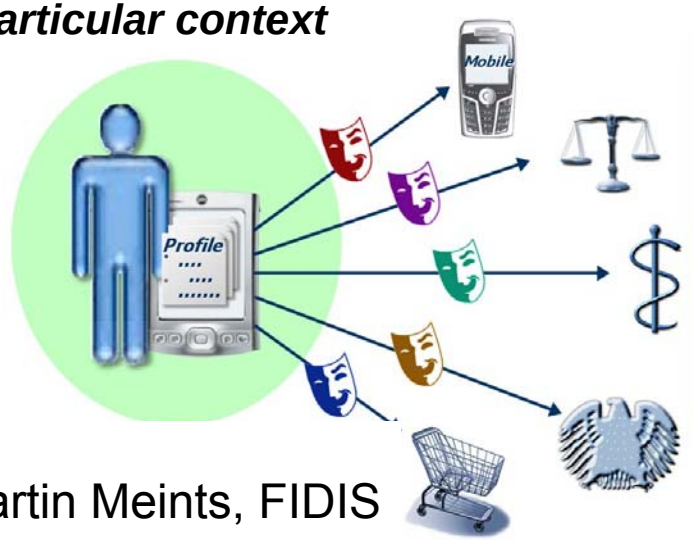
- ***But Identity Management for eGovernment***
  - Brings new challenges:
    - Need to be able to identify someone electronically, remotely
  - With divergent approaches:
    - Different electronic identities: certificates, digital signatures
    - In different forms: eID (smart) cards, hard and soft tokens
    - Depends on identifiers!
    - Sometimes backed up by private sector solutions or built on public-private cooperation
  - Different sectors and different contexts

modinis IDM

Cross-Context Pan-European Identity Management

Phase III: Conceptual Framework Essentials

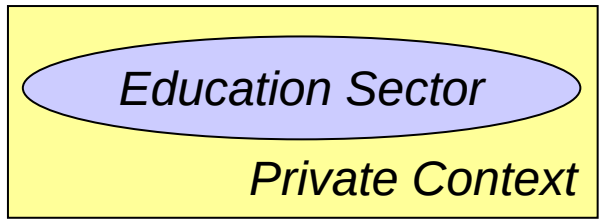
- ***Strong link between* identity management *and* semantic interoperability**
  - Context-specific information is exchanged from one sector to another
    - Information has a *TYPE* and a *VALUE*
    - All information needs to be *uniquely identified*
  - Requires a mapping and conversion of information exchanged between different contexts
  - Semantics are only a cross-context issue!
  - Identifiers should not be shared among contexts
- ***There is a clear need to have***
  - ***Unique identifiers*** for entities within ***a particular context***
    - National insurance number (UK),
    - Sectoral identifiers (AT)
    - National registry number (B)
    - Social security number (NL)
  - ***Roles*** and ***mandates***
    - A person acts **within** a context:
    - civil servant, lawyer, father,…

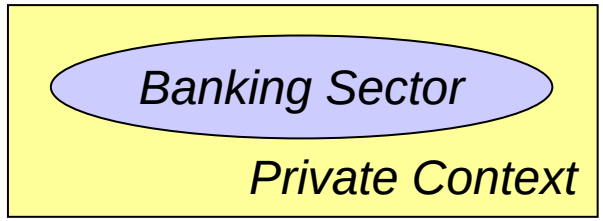


Picture © Martin Meints, FIDIS

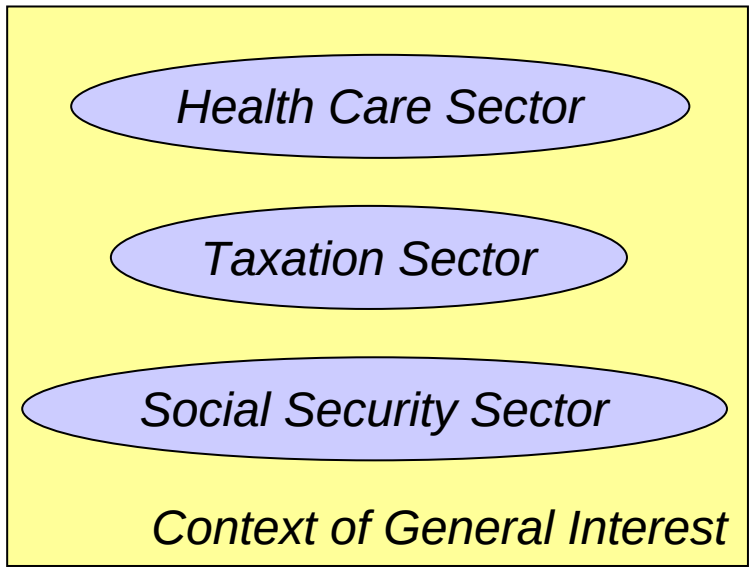
Phase III: Conceptual Framework Essentials

- ***Discrepancy between*** context ***and*** sector
  - A context spans one or more sectors
    - All sectors within one context share identifiers
  - Providers of energy resources, telephony services, bank services, etc.
  - Heated debates about identifiers per sector or per context
    - Austria tends towards “Context = Sector”
    - Belgium tends towards “One or more sectors in one Context”

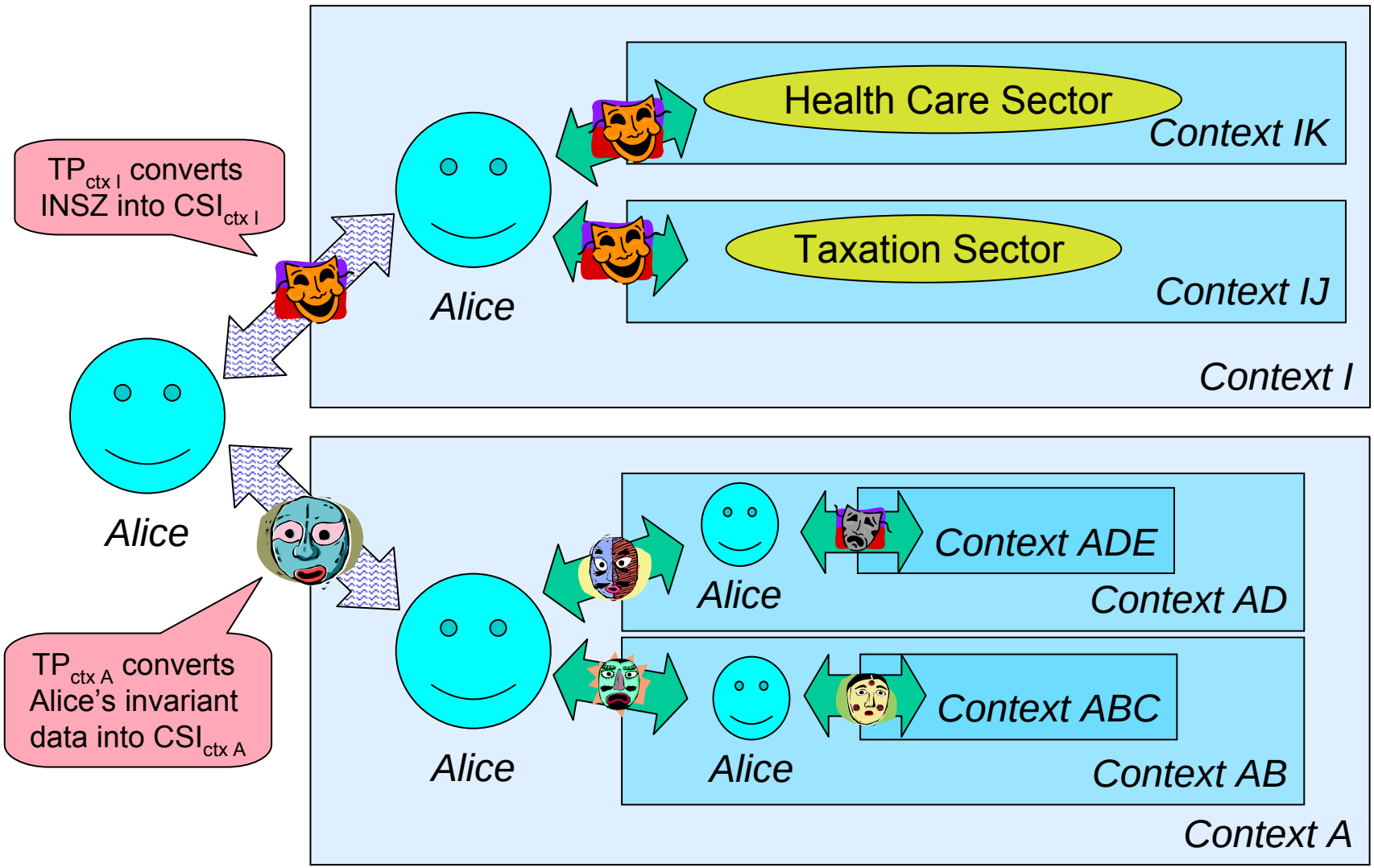




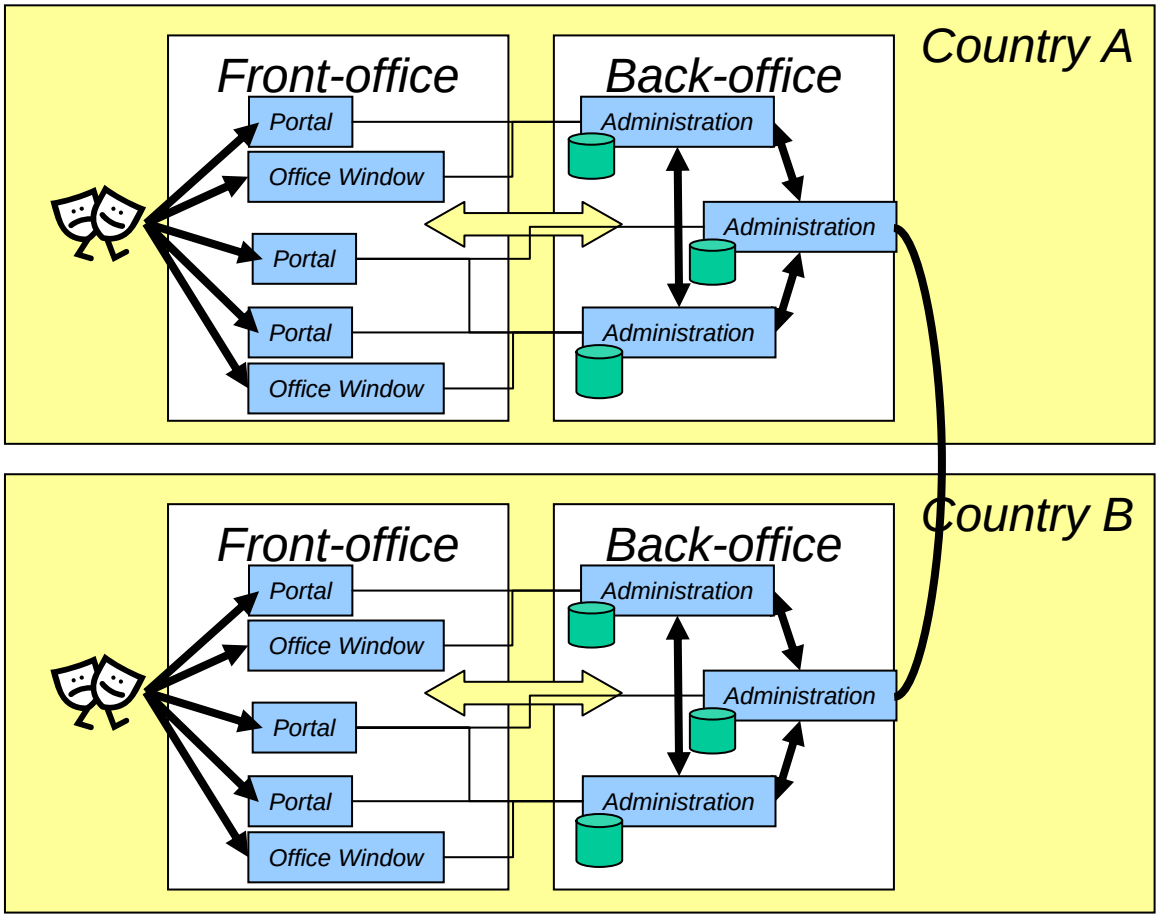
- ***Pan-European eGov IDM***
  - Expand eGovernment identity management
  - to multiple nations interacting and communicating with each other



Phase III: Conceptual Framework
Context-Specific Identifiers (CSIs)



Phase III: Conceptual Framework Pan-European IDM



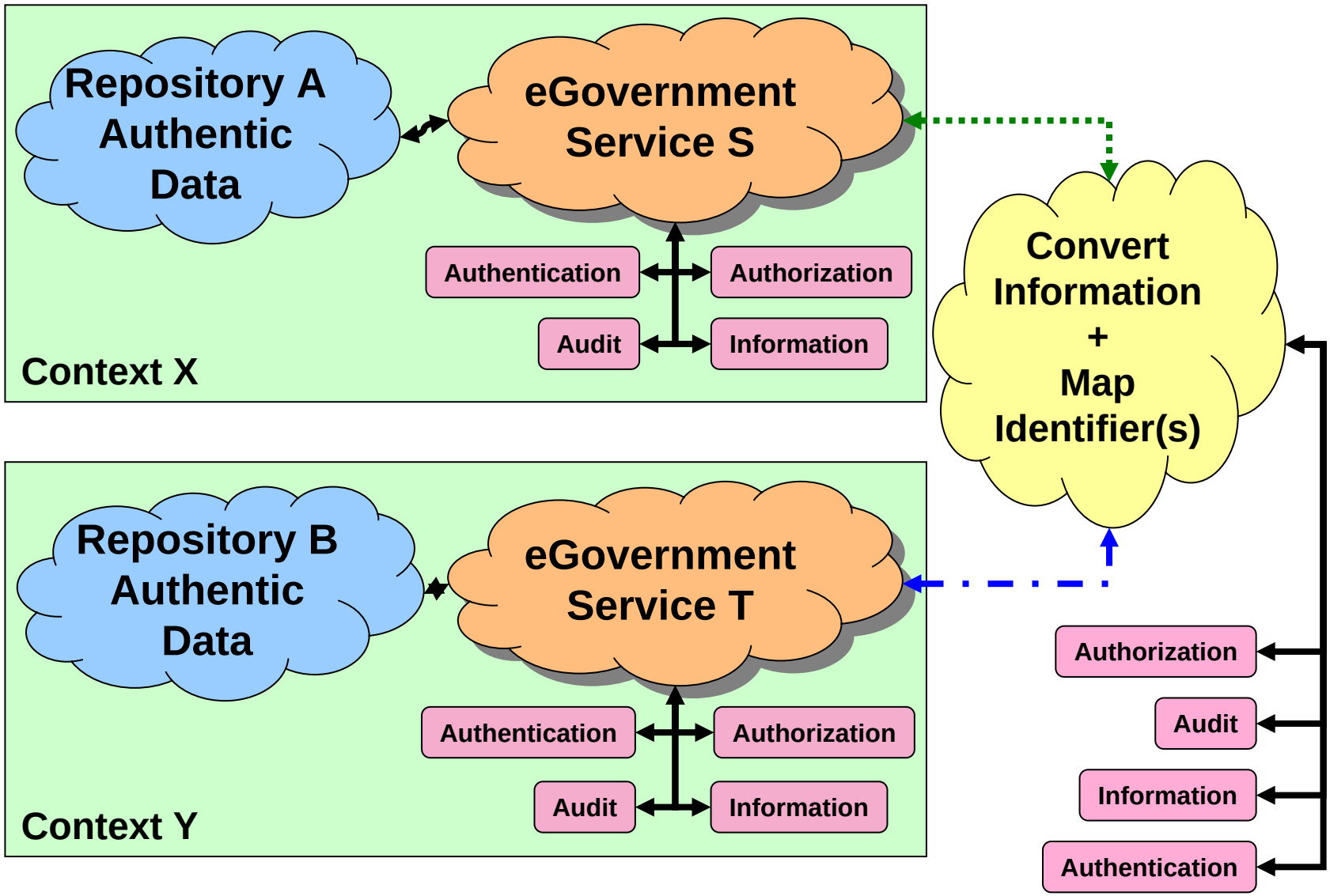
Member States communicate

Administrations may communicate directly

How is irrelevant! EU mediating service?

Do not forget the citizen: Pan-EU generic portal?

Phase III: Conceptual Framework Pan-European IDM



modinis IDM

Consequences of Pan-European Identity Management

Phase III: Conceptual Framework Consequences of Pan-EU IDM

- ***Semantic interoperability: Talk about the same concepts***
- ***Identifier mapping: Talk about the same entity***

There is more!

- ***Look at facilities for eGovernment services:***
  - Authentication, authorization, information, auditing
- ***Authentication prior to authorization***
  - No need to register citizen or user in foreign system
  - Limited roaming of authentication to avoid abuses
    - (applying for benefits in more than 1 country?)
  - To work with other member states, use their identifying solutions

Phase III: Conceptual Framework Consequences of Pan-EU IDM

- ***Federation***
  - Authentication:
    - I.e., assertion by another member state that the entity is as claimed
  - Authorization:
    - Federation of competences and mandates
    - Example in Czech Republic, authorization federation, apply on EU level
    - As many different solutions for authorisation as there are solutions for identifiers, authentication, ...
  - Federation of information
    - Where do we find the correct information?
    - Service registration or registration of European authentic sources
- ***Technology independence guarantees IDM interoperability***

Phase III: Conceptual Framework Summary

- ***It is an interoperability problem!***
  - Let member states talk to each other
  - Learn them how
  - How do you know where to fetch authorization or authentication information?
  - What about logging?
  - Who decides what?
  - Privacy consequences of all this?
  - Mobile citizens
- ***Do not change the way member states do it***
  - Is harmonization possible?
  - Again: it is an interoperability problem
  - Do not make things more complicated
- ***Concepts to remember***
  - eGov: public sector, digitalization, services, authentic source
  - IDM: identity, identifier, information, contexts and sectors
  - eGov IDM: electronic identity, authentication, authorization, …
  - Pan-EU eGov IDM: identity federation, shared or forwarded authentication/authorization/authentic sources, mediators

Phase III: Conceptual Framework MS Requirements

- ***Each member state should:***
  1. Be able to identify the natural persons on its territory
  2. Be able to identify the legal persons on its territory
  3. Issue the means to each entity to identify itself electronically
  4. Register competences of the identified entities on its territory
  5. Register mandates of a natural person regarding other persons
  6. Support online validation mechanisms of competences and mandates
  7. Agree on a dictionary with semantically compatible concepts for electronic IDM

Activities

… 1st Workshop …

- ***Scope:***
  - To propagate the initiative
  - To determine the study's scope and goals
  - To discuss a vision for interoperable Identity Management in eGovernment
  - Intention was to investigate which topics the experts consider to be most important – which we then can further investigate in the two years and the four follow-up workshops to come

To draft the study's scope and goals, mostly from a public sector perspective

… 2nd Workshop …

- ***Scope:***
  - More practical focus
  - Identification of potential issues and solutions for programs on this scale
  - Presentations of
    - Member State representatives
    - Representatives of the industry introducing different approaches towards a interoperable IDM systems

► Identifying the perceived difficulties and potential solutions
► From all stakeholders' perspectives (i.e., public sector, academic, industry, …)

… 3rd Workshop …

- ***Scope:***
  - Conclusions of the first year of Modinis*IDM*
  - Presenting the current status of the conceptual framework for interoperable identity management
  - 3 speakers presenting different experiences:
    - Czech Republic
    - Estonia
    - France

► **Gain experiences from Member States**
► **Disseminate project results**

… 4th Workshop …

- ***Scope:***
  - Focus on success and solutions
  - Presenting
    - Draft Conceptual Framework
    - Good Practice Cases
    - Draft Roadmap based on gathered input
  - Active contribution of the audience to the roadmap

► **The first steps towards interoperable pan-EU IDM**
► **Drafting a roadmap**

… 5th Workshop …

- ***Scope:***
  - Conclusions of the study
  - Presenting final report and dissemination of the project results:
    - IDM initiatives and issues, good practice cases
    - Conceptual Framework
    - Roadmap

- **Conclusion and roadmap**
- **Dissemination of results**

KATHOLIEKE UNIVERSITEIT LEUVEN A-SIT lawfort

Modinis Study Lot 3 - Study on Identity Management in eGovernment

Thank you

https://www.cosic.esat.kuleuven.be/modinis-idm/

bart . preneel @ esat . kuleuven . be

Leuven, Belgium

modinis IDM

K.U.Leuven, A-SIT and Lawfort