



# Designing Secure Security Applications and Service Oriented Applications

**Danny De Cock**

Danny.DeCock@esat.kuleuven.be

Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)

Computer Security and Industrial Cryptography (COSIC)

Kasteelpark Arenberg 10

B-3001 Heverlee

Belgium

# Outline

- Typical Crypto Applications
- Typical Security Issues
- Benefits of Secure Software Development?
- Core Security Problems
- Secure vs. Security
- Two Examples
- So what?
- Good practices...

# Typical Crypto Applications

- Many applications rely on cryptographic primitives and use security protocols:
  - e-Banking & e-Payments: DigiPass, Proton, Isabel,...
  - Integrity protection: Code signing, Electronic signatures, eID cards
  - Confidentiality protection: Encrypted file systems, email,...
  - Wireless: GSM, Bluetooth, ZigBee, WiFi,...

# Typical Security Issues

- Errors in the cryptographic primitives are rare causes of non-secure security applications
  - Bad use of cryptographic primitives/protocols kills the application
- Causes of Major security flaws
  - Everybody believes he/she is a cryptographer ☹️
  - Very primitive key management
  - User's lack of security awareness

# Benefits of Secure Software Development

- Application security
  - Important emerging requirement in software development
  - Controls potential
    - Severe brand damage
    - Financial loss
    - Privacy breaches
- Risk-aware customers (financial institutions, governmental organizations) want to
  - Assess the security posture of products they build or purchase
  - Plan to ultimately hold vendors accountable for security problems in their software
  - Procure reliable and secure software
    - Hold vendors accountable for security problems in software

# Core Security Problems

- Software development lifecycle does not deal well with security:
  - Software developers lack structured guidance
  - Books on the topic are
    - Relatively new
    - Collections of good practices
- Security is not a feature that demos well
  - Developers tend to focus on core functionality features
- Security is addressed in an ad hoc manner during development
  - Developers typically provide a minimal set of security services given their limited security expertise
- Applications are too complex to comprehend

# Secure vs. Security Software Development

## ■ Secure software

- Application acts according to its specifications
- Provable features of the application
- Software design is the bottleneck

## ■ Security software

- Relies on secure software
- Application uses secret and private information
  - Electronic payments, voting, signing,...
  - Protection of privacy, confidentiality, integrity,...
- Critical use of the user/device/... credentials

# SSL/TLS Example

- Fact: SSL/TLS is the most popular way to provide data confidentiality and integrity services for data in transit
  - Drop-in for traditional sockets
- But: Most SSL/TLS deployments are susceptible to network-based attacks
  - Technology is widely misunderstood
  - Self-signed server certificates
  - No decent validation of server certificates
  - Insecure client configuration

# “Our system is secure: we use the AES”

- What about
  - Key management
    - “Random” keys?
    - Authenticated (?) key agreement
  - Implementation
    - Modes of encryption, initialization vectors,...
    - Attacking the implementation
- Who holds the keys?
  - Who can use the keys?
  - Stored in the clear?
  - Key archives?

# What to do about it?

- Large software vendors make lots of effort
  - Ongoing effort to improve security through its development process
    - Involves training and process improvements
  - Good practices:
    - Initial approach: freezing the current status
    - Only allow change that improve the security
- Good system design relies on embedded security
  - Simplifies security issues: no add-on
  - Hides complexity of cryptographic protocols

# Good Practices

- Centralize security knowledge in software architects and application designers
  - Implementers should not have to make delicate security decisions
  - Cryptographic algorithms and protocols should be considered as modular building blocks
  - Consistent deployment of a security vision saves time and money
  - Security expertise concentrated in a few of the most trusted members of the development organization
  - Allows for better depth of knowledge
  - Results in more effective and secure results
- Good initial security design avoids hard to solve security issues
  - Security patches do not deal with inherent design flaws
  - Simple design is easily understandable/testable/auditable



# Towards Secure Service Oriented Architectures

Partially based on slides of  
Frank Robben, cf.

[www.law.kuleuven.be/icri/frobben](http://www.law.kuleuven.be/icri/frobben)

# Structure

- General Overview of User and Access Management applied to Belgian Public & Social Security Sector
  - Basic concepts related to User and Access Management
  - Identification
  - Belgian eID Card
  - Policy Enforcement Model
  - User Management for citizens, professionals and companies
  - Access Management
  - Federated Principle of “Circles of Trust“
- Future SOAs
  - TAS3 – Trusted Architecture for Securely Shared Services

# General Overview

- 3 Target Groups
  - Citizens
  - Professionals
  - Companies and other Service Providers
- Different Aspects
  - User Management
    - Registration of the Identity
    - Authentication of the Identity
    - Registration of Characteristics and Mandates
    - Verification of Characteristics and Mandates
  - Access Management
    - Registration of Authorizations
    - Verification of Authorizations

# User Management: 3 Basic Concepts

## 1. Identity of an Entity

- A number or a set of attributes of an entity that allows to know precisely who or what the entity (physical person, company,...) is
- An entity has only one identity, but this identity can be determined by several numbers or sets of attributes
- E.g., VAT number, Social Security Identification Number

## 2. Characteristic of an Entity

- An attribute of an entity, other than the attributes determining its identity, such as a capacity, a function in an organisation, a professional qualification,...
- E.g., Doctor, Lawyer, Teacher

## 3. Mandate

- A right granted by an identified entity to another identified entity to perform well-defined legal actions in her name and for her account
- Is essentially a relationship between two entities

# User Management: 3 Basic Processes

1. Registration of Entity, Characteristic, Mandate
  - Determining the identity/characteristic/mandate of an entity with sufficient certainty, before
  - Issuing means by which the identity can be authenticated, or the characteristic or the mandate can be verified
2. Authentication – Verifying the Identity
  - Checking whether the identity that an entity pretends to have in order to use an electronic service, corresponds to the real identity
  - Uses the means issued during the registration process
3. Authorization – Verification of a Characteristic or a Mandate
  - Checking whether a characteristic or a mandate that an entity pretends to have in order to use an electronic service, corresponds to a real characteristic or mandate of that entity
  - Verification of a characteristic or a mandate can be done by
    - Using the authentication means of the entity
    - Consulting a trusted database with characteristics of mandates of identified entities

# Access Management: Basic Concepts

## ■ Authorization

- A permission to an entity to perform a defined action or to use a defined service

## ■ Authorization Group

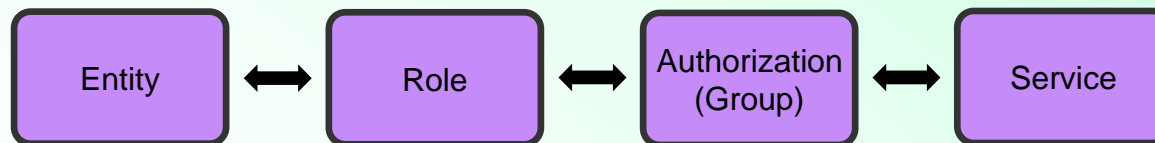
- A group of authorizations

## ■ Role

- A group of authorizations or authorization groups related to a specific service

## ■ Role Based Access

- A method of assigning authorizations to entities by means of authorization groups and roles, in order to simplify the management of authorizations and their assignment to entities



# Choices made in Belgium

- Identification
- Policy Enforcement Model
- User Management for
  - Citizens
  - Professionals
  - Companies
- Access Management
- Federated Principle of “Circles of Trust“

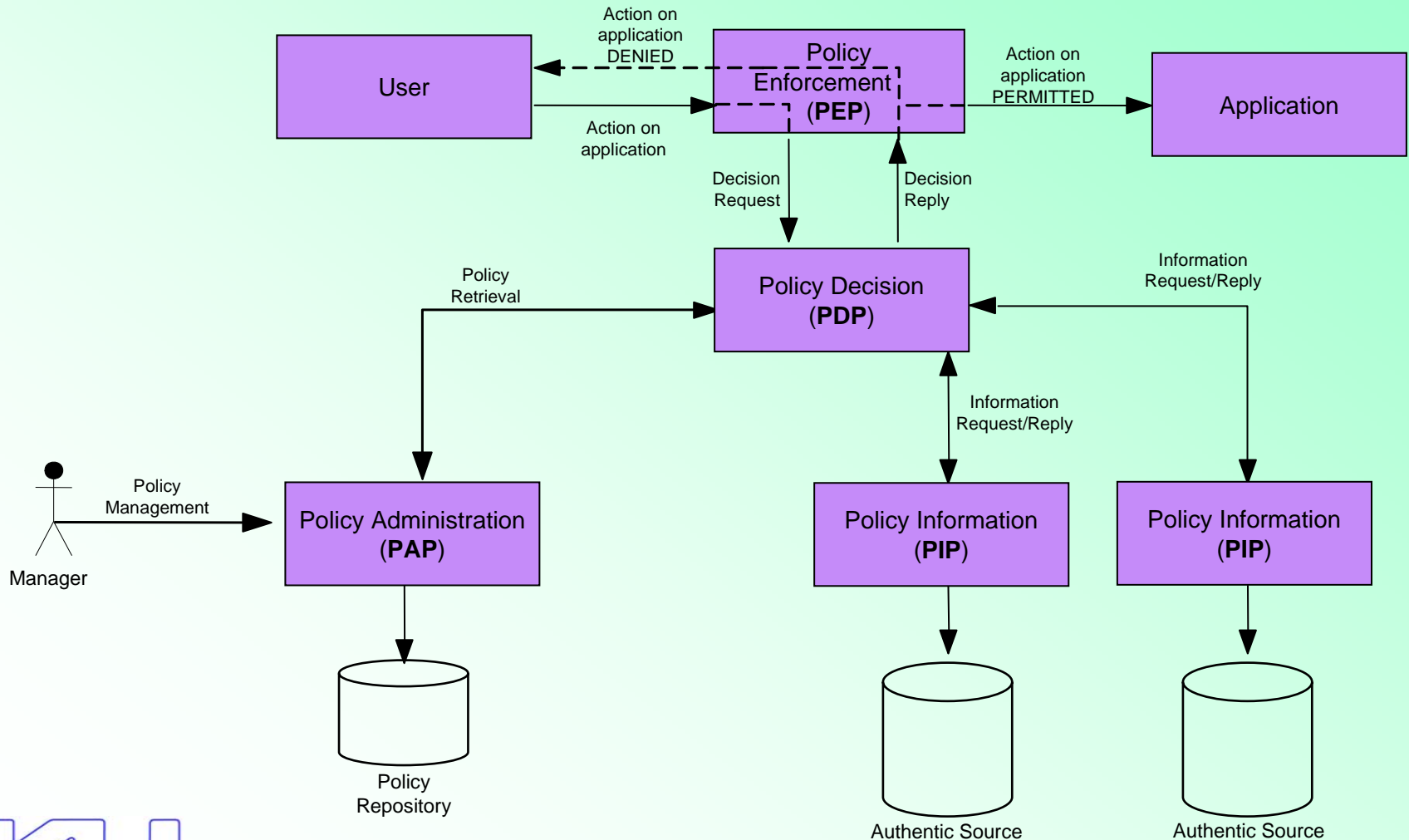
# Identification Numbers

- Numbers for every citizen and every company
  - Characteristics
    - Unique
      - Every entity in principle only has one identification number
      - The same identification number is not assigned to several entities
    - Exhaustive
      - Every entity to be identified has an identification number
    - Stable over time
      - Identification number should not contain variable characteristics of the identified entity
      - Identification number should not contain references to the identification number or characteristics of other entities
      - Identification number should not change when a quality or characteristic of the identified entity changes

# Identification

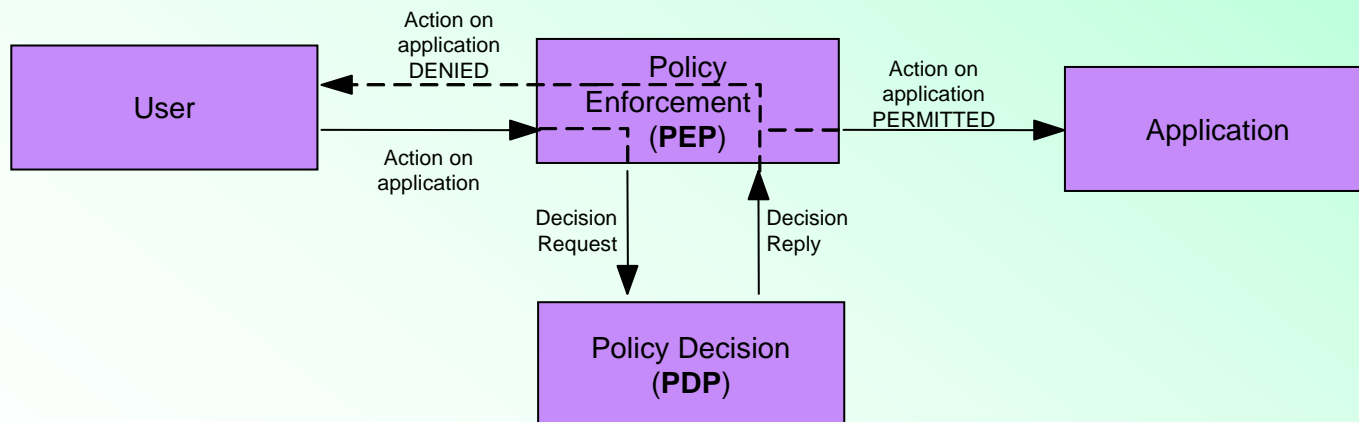
- Art. 8, 7 Directive 95/46/EC: "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed"
  - Evolution towards meaningless identification numbers
  - Unique identification numbers of citizens can only be used by instances authorized by a sectoral committee of the national privacy commission
  - In some sensitive sectors (e.g. justice, health, ...), the identification number can be a specific number derived from the unique number of the citizen
  - Regulation on interconnection of personal data
- Registration of the identity of citizens by the municipalities
- Registration of the identity of companies by company counters

# Generic Policy Enforcement Model – XACML-based



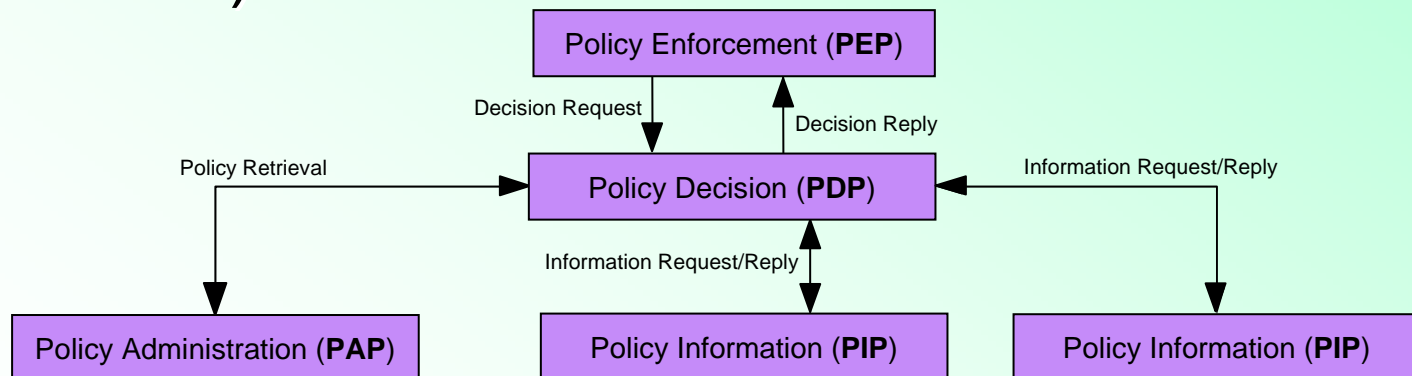
# Policy Enforcement Point (PEP)

- Intercepts the request for authorization with all available information about the user, the requested action, the resources and the environment
- Passes on the request for authorization to the Policy Decision Point (PDP) and extracts a decision regarding authorization
- Grants access to the application and provides relevant credentials



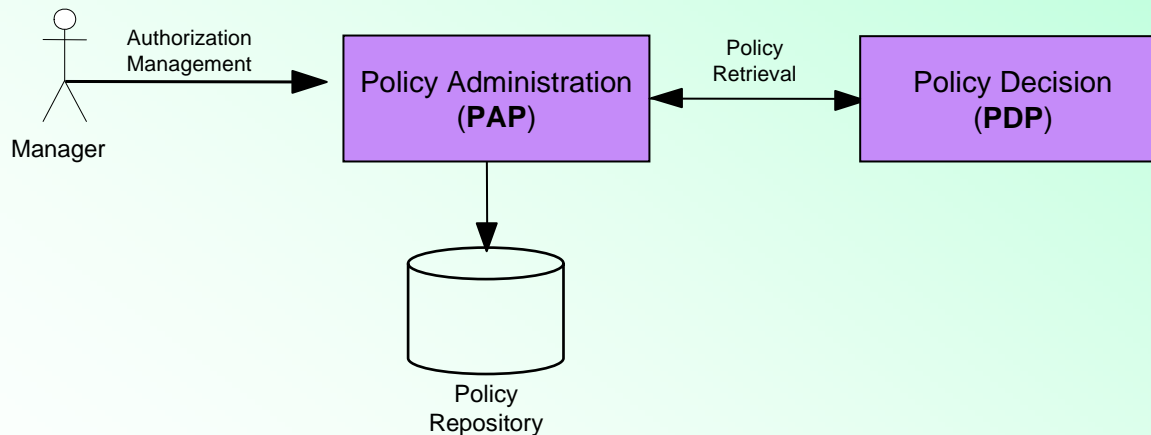
# Policy Decision Point (PDP)

- Based on the request for authorization received, retrieves the appropriate authorization policy from the Policy Administration Point(s) (PAP)
- Evaluates the policy and, if necessary, retrieves the relevant information from the Policy Information Point(s) (PIP)
- Takes the authorization decision (permit/deny/not applicable) and sends it to the PEP



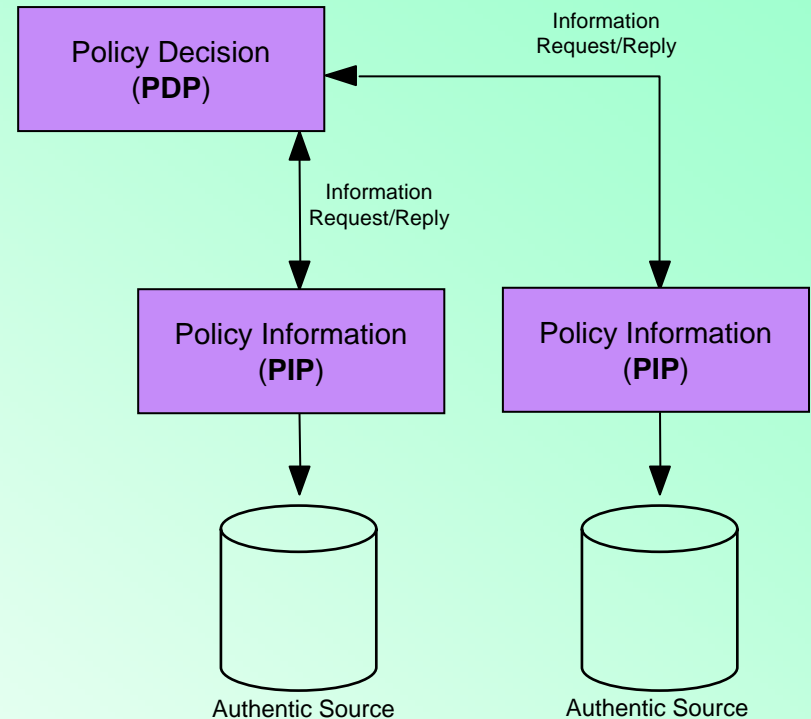
# Policy Administration Point (PAP)

- Environment to store and manage authorization policies by authorised person(s) appointed by the application managers
- Puts authorization policies at the disposal of the PDP

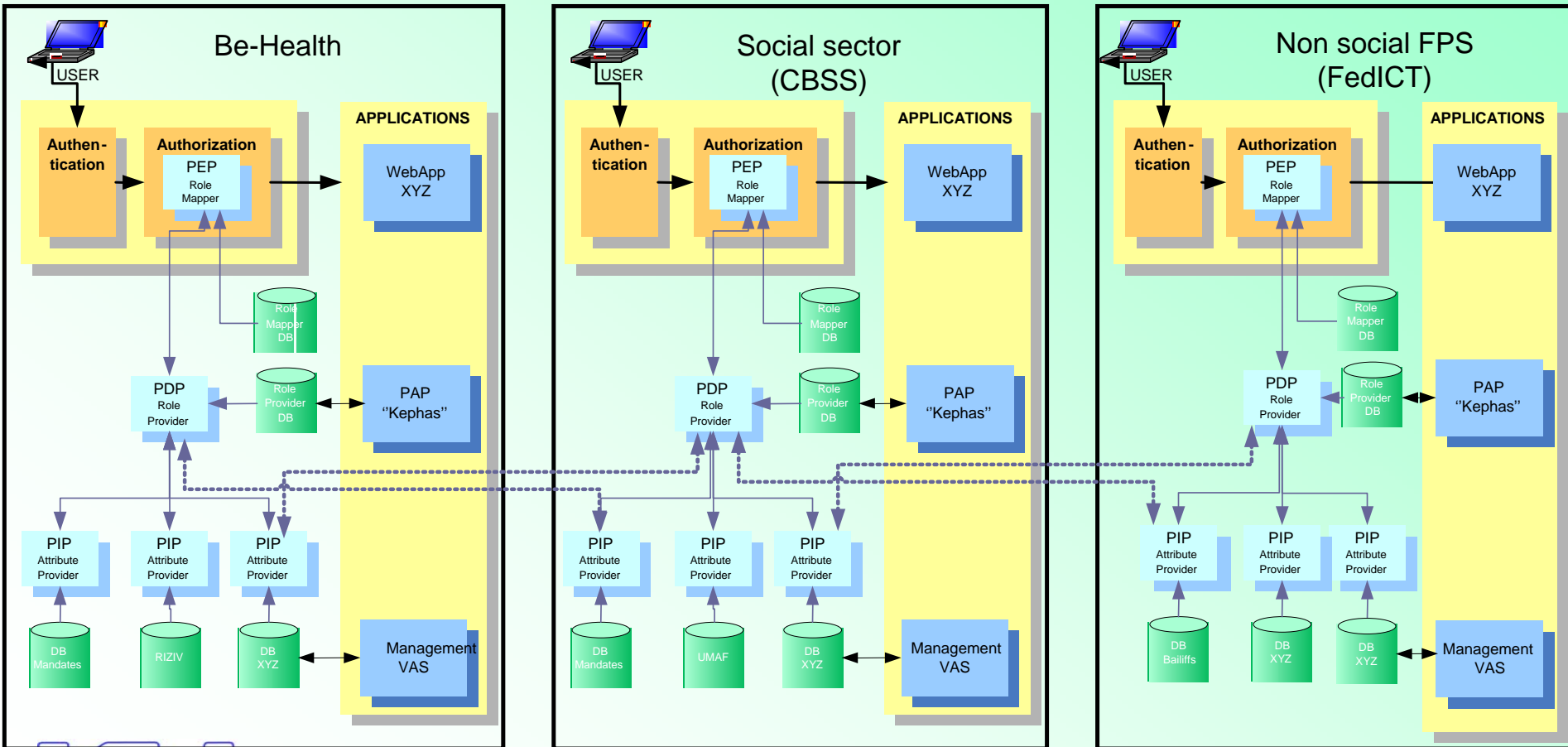


# Policy Information Point (PIP) – Authentic Sources

- Puts information at the disposal of the PDP in order to evaluate authorization policies (authentic sources with characteristics, mandates, etc.)



# Architecture



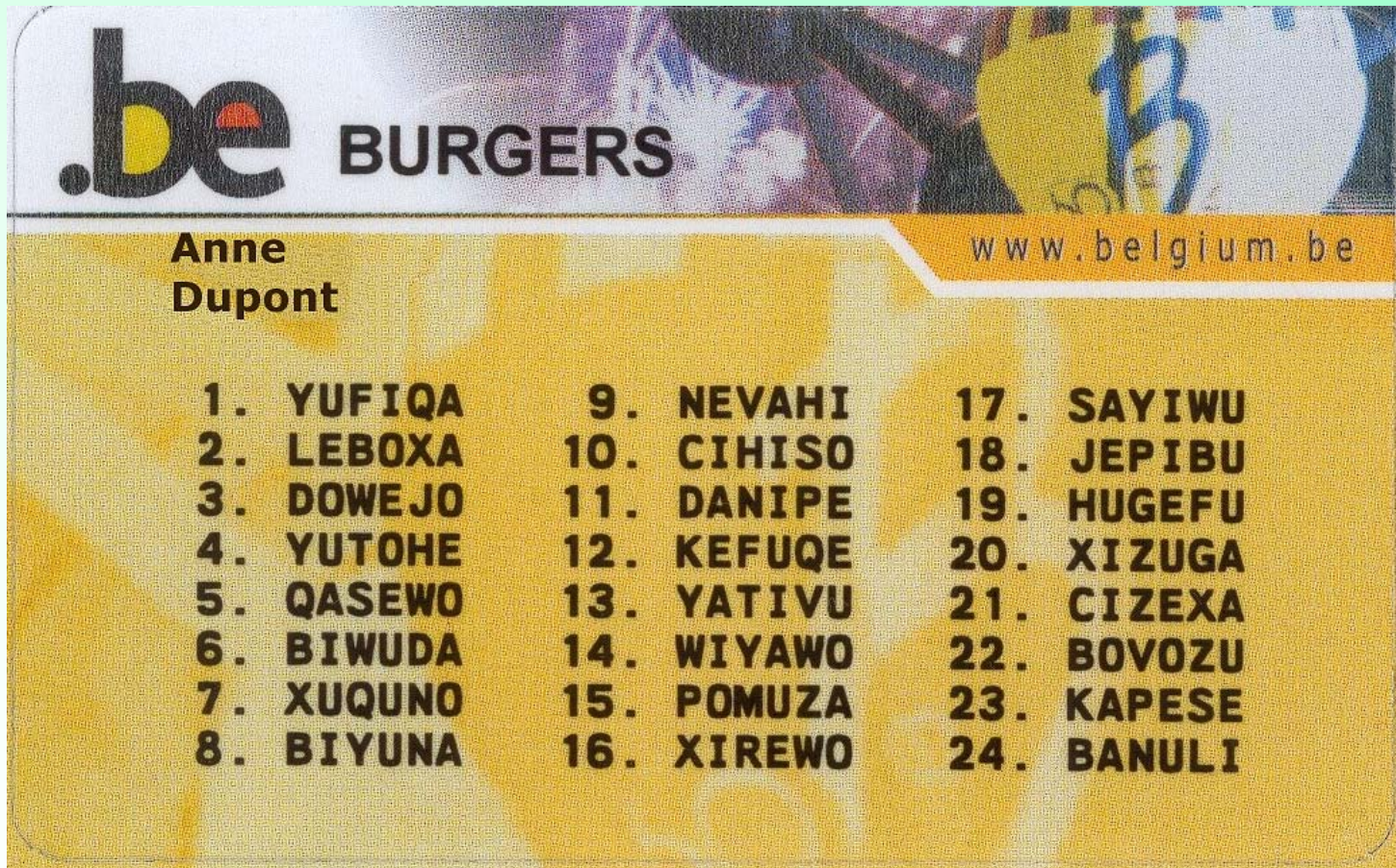
# Citizens, Services & Authentication Levels

Level	Registration Identity citizens	Authentication Identity citizens	Services
0	None	None	Public information/services
1	Online by input national identification number, number of the identity card and number of the social security card	User number and password chosen by the user	Lowly sensitive information/services
2	Level 1 + e-mail with URL for activation sent to an e-mail address mentioned by the citizen and paper token sent to the residence of the citizen as registered in the national register	Level 1 + input of an arbitrarily asked string mentioned on the paper token (contains 24 strings)	Medium sensitive information/services
3	Physical visit at the municipality in order to get the eID	Authentication certificate of the eID + password per session	Highly sensitive information/services
4	Physical visit at the municipality in order to get the eID	Authentication certificate of the eID + signature certificate on the eID + password per transaction	Services requiring an electronic signature

# eID – Level 3 + 4



# Citizen's Paper Token – Level 2



# Professionals

## ■ Who?

- Employees of public services and social security institutions
- Specific professions: health care providers (medical doctors, pharmacists,...), notaries, bailiffs, accountants,...
- ...

## ■ Registration and Authentication of the Identity

- In principle same system as the citizens system
- For employees of public services and social security institutions, the paper token at level 2 is sent to the information security officer of the public service or the social security institution that employs the employee and is delivered to the employee by this information security officer

# Professionals

- Registration of characteristics and mandates
  - Designation by the government, for every (type of) characteristic(s) or mandate(s), of an appropriate body (called the registration authority) that has the responsibility to register the characteristic or the mandate with sufficient certainty
  - Storage of the characteristic or the mandate by the registration authority into an authentic source (PIP) accessible to all interested parties
- Verification of characteristics and mandates
  - Consultation of the relevant authentic sources (PIPs) accessible to all interested parties
  - In case of use of the paper token, also arbitrarily requested string mentioned on the paper token

# Companies, Services & Authentication Levels

Level	Identity Registration of mandataries of companies	Identity Authentication of mandataries of companies	Services
0	None	None	Public information/services
1	Local administrator: signed (electronic) form to the National Office for Social Security by the company for whom the person acts as a local administrator other mandataries: registration by the local administrator	User number and password chosen by the user	Lowly or medium sensitive information/services
2	Physical visit at the municipality in order to get the eID	Authentication certificate on the eID + password per session	Highly sensitive information/services
3	Physical visit at the municipality in order to get the eID	Authentication certificate on the eID + signature certificate on the eID + password per transaction	Services requiring an electronic signature

# How to Choose a Security Level?

- Responsibility of the provider of an electronic service under supervision of the Privacy Commission
- Based on a **risk assessment** and dependent from a.o.
  - The type of processing: communication, consultation, alteration,...
  - The scope of the service: does the processing only concern the user or also concern other persons ?
  - The degree of sensitivity of the data processed
  - The possible impact of the processing
- On top of the security level, the use of an electronic signature might be needed in order to preserve the service provider against disputes
- In the social sector and the federal government: decision of the Board of Directors of the Crossroads Bank for Social Security set down in a user regulation

# Federated Principle of “Circles of Trust”

- Aim
  - Avoid unnecessary centralization
  - Avoid unnecessary privacy threats
  - Avoid multiple similar controls and registration of loggings
- Method: division of tasks between the entities associated with the electronic service, including clear agreements on
  - Who is in charge of which authentications, verifications and controls by which means
  - How the results of the authentications, verifications and controls can be safely exchanged electronically between the entities concerned
  - Who keeps which log files
  - How to ensure that in case of an investigation, on one’s own initiative or in response to a complaint, a complete tracing can be realized in order to know which physical person has used which service or transaction concerning which citizen or company, when, through which channel and for which purposes

# Intermediate Conclusion

- An integrated system for user and access management for citizens, professionals and companies exists in Belgium
- Electronic identities for natural and legal persons are the first & crucial steps towards efficient user and access management
- Based on a well coordinated assignment of tasks to the most appropriate bodies
- Accessible via open standards
- The federated system permits the use of common basic services without loss of autonomy
- The system permanently evolves according to ever changing user requirements



Trusted Architecture for  
Securely Shared Services



# *Generic Architecture for Securely Managing Employability & Healthcare Personal Information Services*

Web: <http://tas3.eu>

Email: [tas3@ls.kuleuven.be](mailto:tas3@ls.kuleuven.be)

TAS<sup>3</sup> is an IST FP7 funded Integrated Project

TAS<sup>3</sup> contract number 216287

Duration: 1 Jan 2008 - 31 Dec 2011

Research budget: 13.200.000 €

EC Funding: 9.400.000 €



# TAS<sup>3</sup> Consortium

## ■ Coordinators:

- K.U.Leuven & Synergetics

## ■ 9 Research Institutes:

- Universities of Eindhoven, Karlsruhe, Kent, Koblenz-Landau, Leuven, Nottingham, Brussel, Zaragoza
- Consiglio Nazionale delle Ricerche

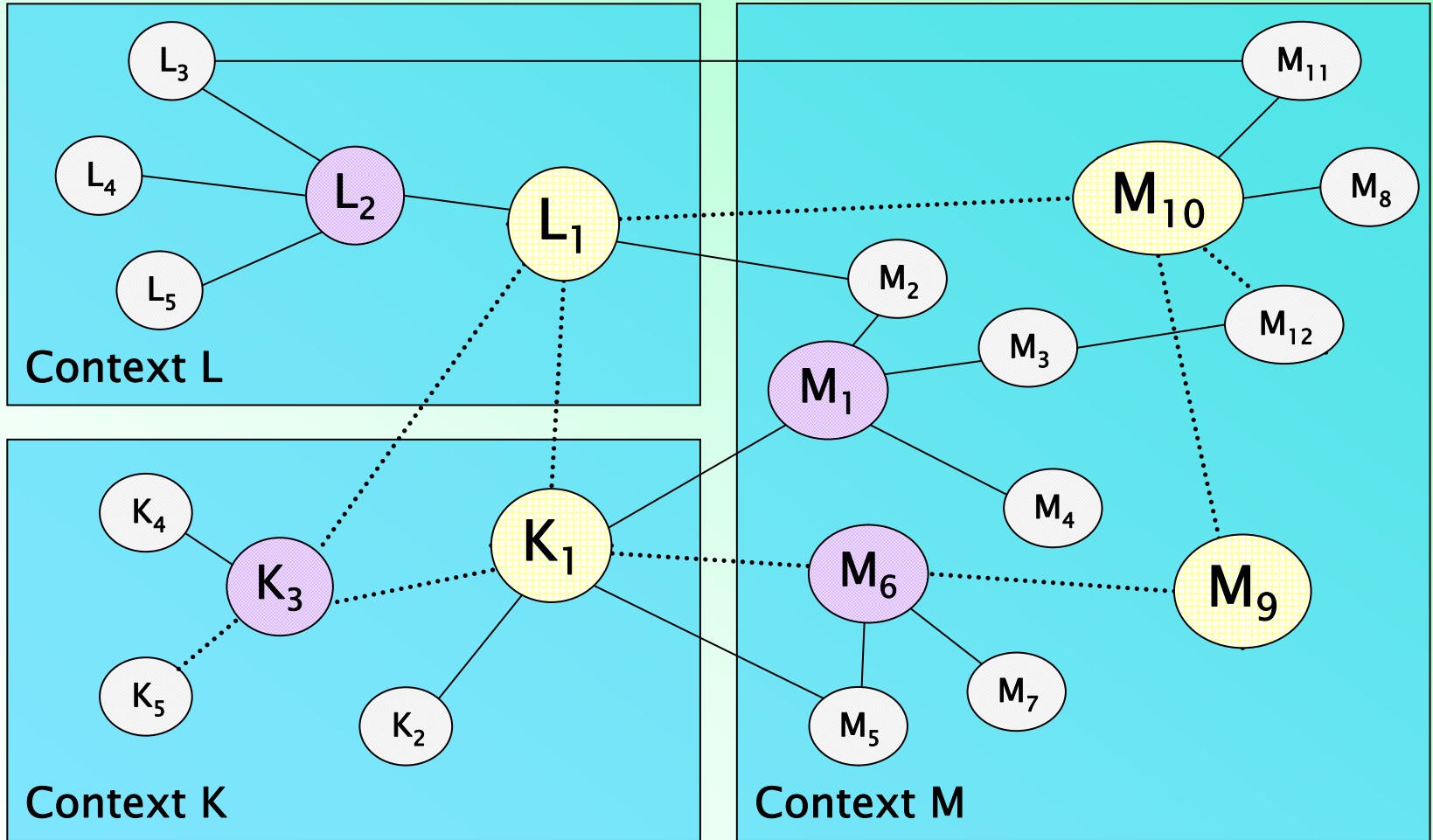
## ■ 9 Companies & Organizations:

- Custodix, Eifel ASBL, Intalio Ltd, Kenteq, Medisoft, Oracle, Risarid Ltd, SAP Research, Synergetics

# TAS<sup>3</sup> Project Motivation

- TAS<sup>3</sup> **consolidates** scattered research in
  - Security, Trust, Privacy, Digital identities, Authorization, Authentication...
  
- TAS<sup>3</sup> **integrates** adaptive business-driven end2end Trust Services based on personal information:
  - Semantic integration of Security, Trust, Privacy components
  
- TAS<sup>3</sup> **provides** dynamic view on application-level end2end exchange of personal data:
  - Distributed data repositories

# Support for Cross-Context Adaptable Business Processes!

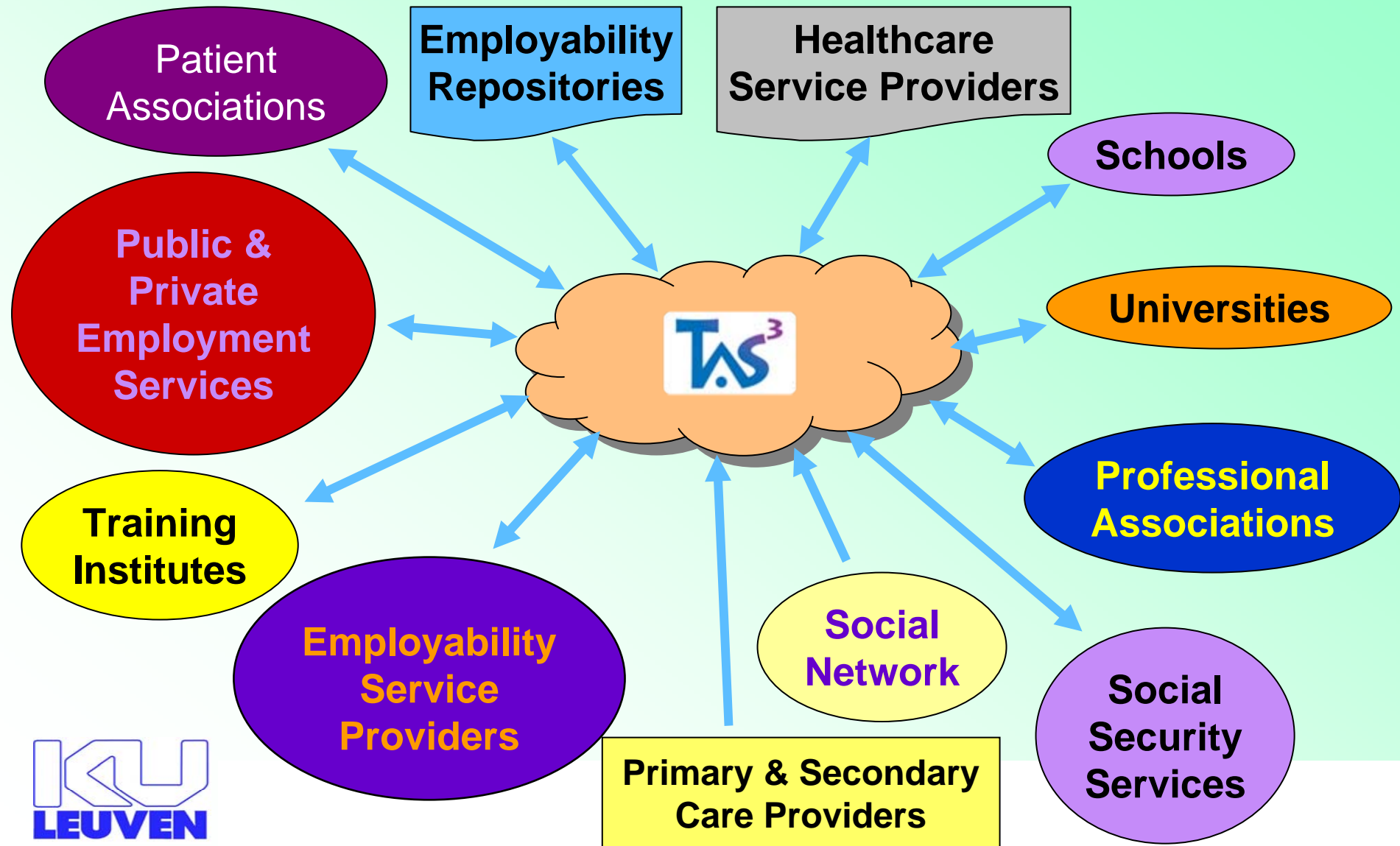


# TAS<sup>3</sup>'s 4 Layers

- Layer 1 – **Authentication**
  - Federated identities
- Layer 2 – **Authorization**
  - Federated attributes
- Layer 3 – **Compliance with Trustworthiness profile**
  - End-user controlled
  - Fine-grained role-based
- Layer 4 – **Compliance with Data-protection regulation**
  - Sticky policies associated with information elements

# Objective – User-centric SOA

## Employability & Healthcare Use Cases



# Business Process



Frontend Service

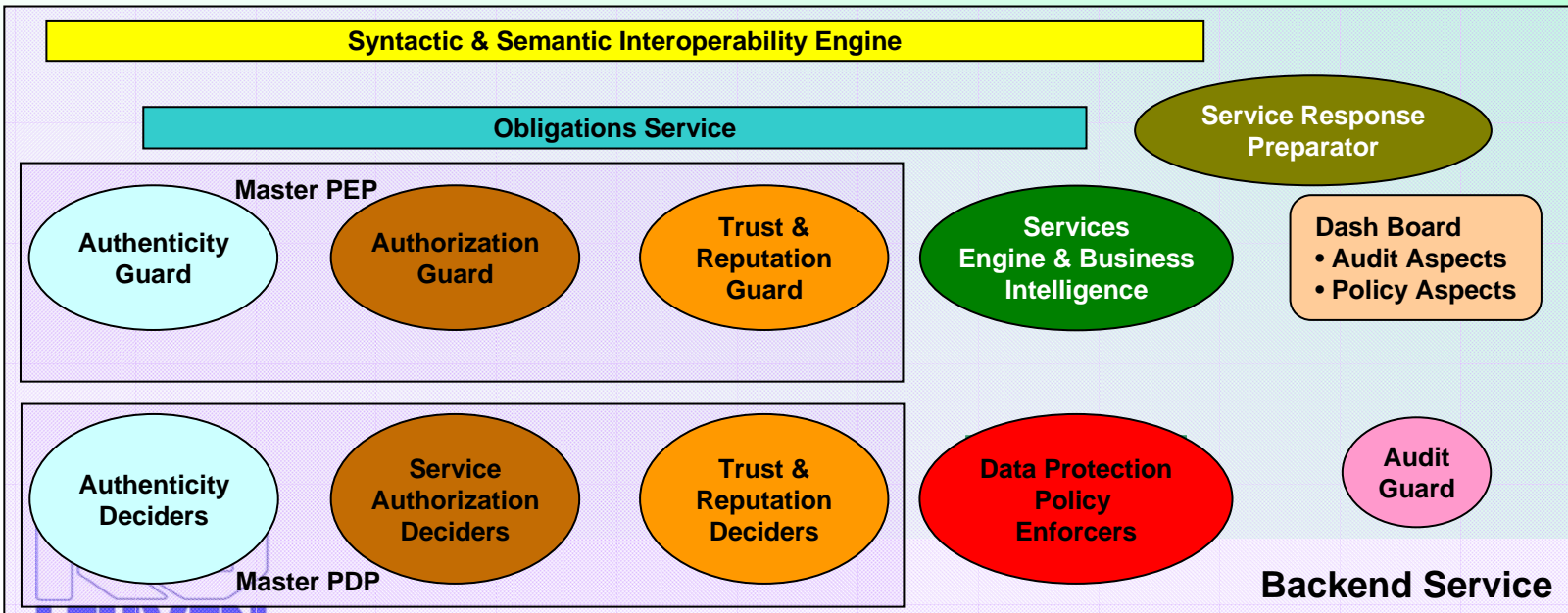
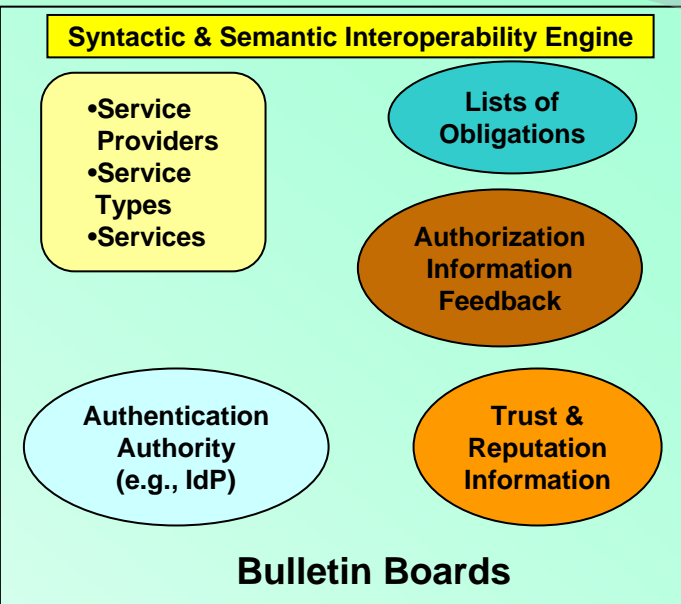
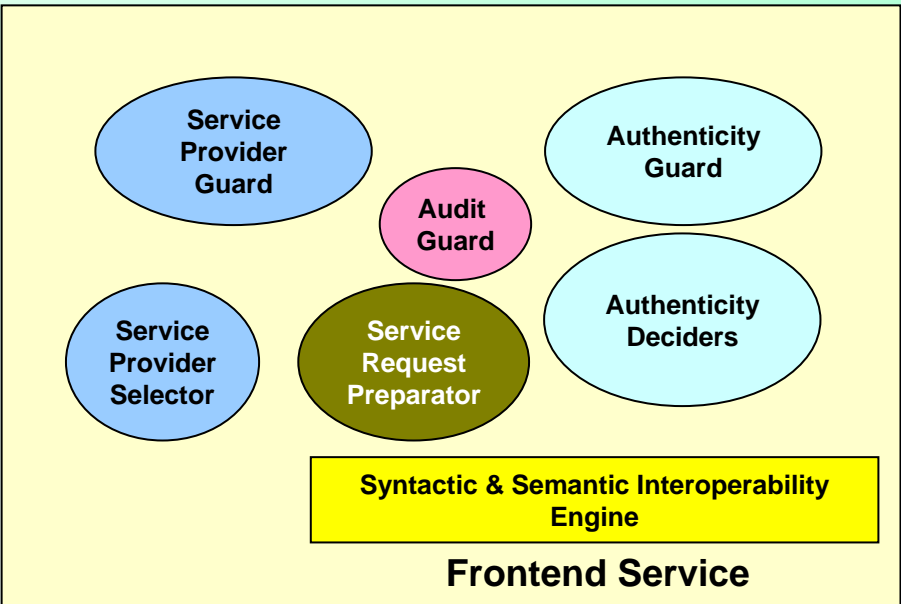
Bulletin Boards

Backend Service

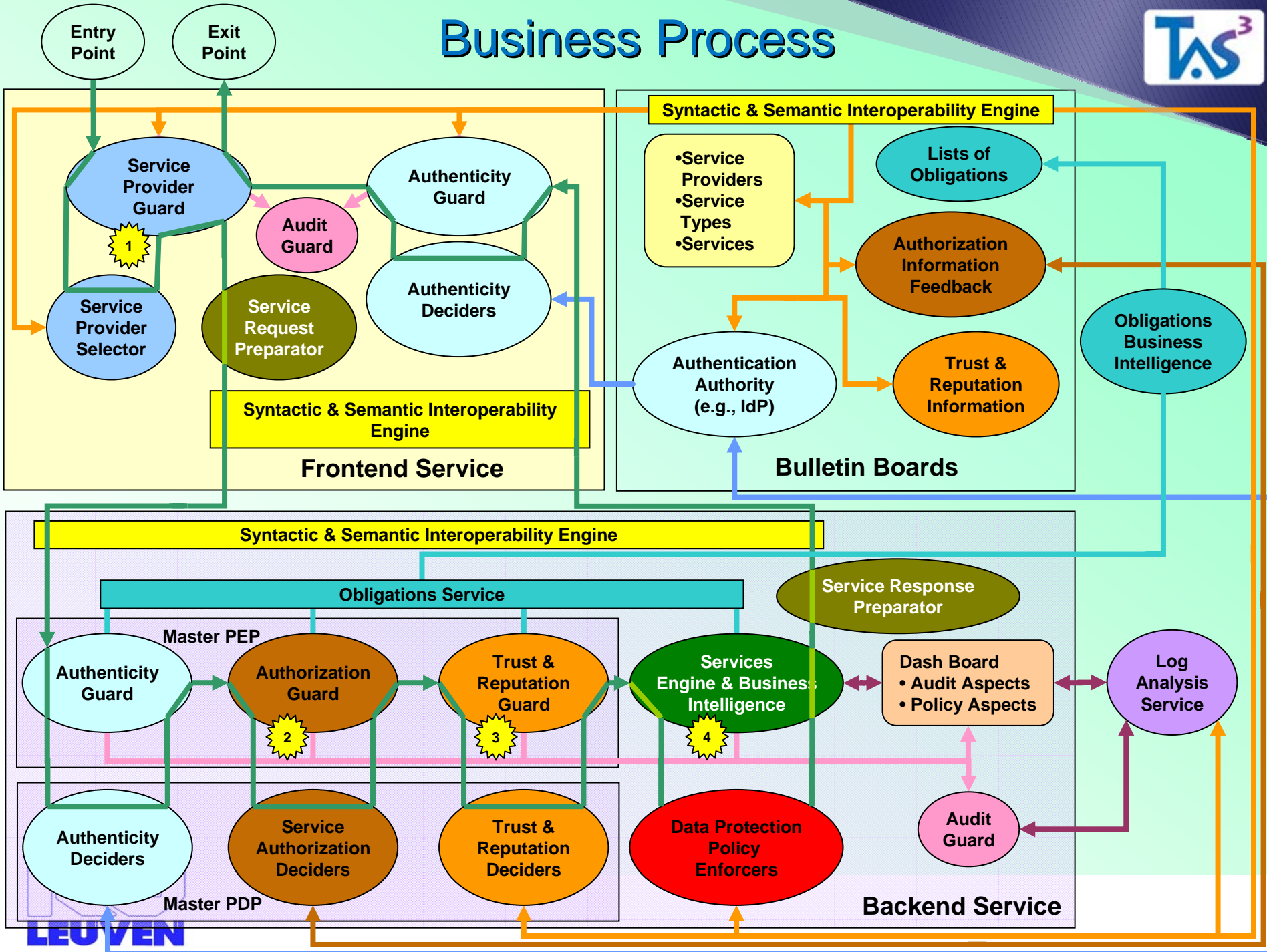
# Business Process

Entry Point

Exit Point



# Business Process

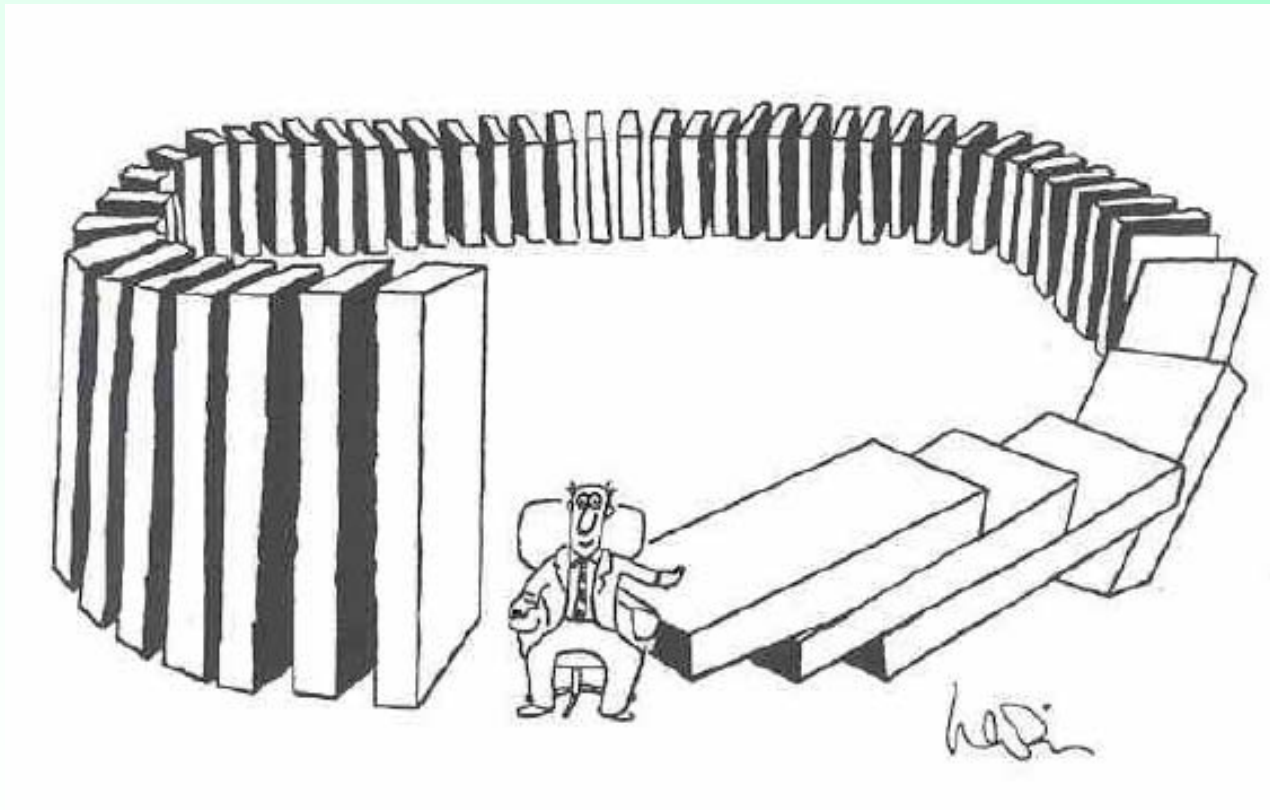


# TAS<sup>3</sup> – Innovation & Impact

- Open and interoperable *4-layered* service oriented architecture enforcing
  - authentication, authorization, trustworthiness, data protection policies and regulation
  - **semantically interoperable & trust-driven** adaptable business processes
  - instantiated in employability and healthcare contexts
- *User-centric* management of personal information
  - **optimize** information processing with **sticky policies** and **fine-grained policy tags**

# Food for Thought

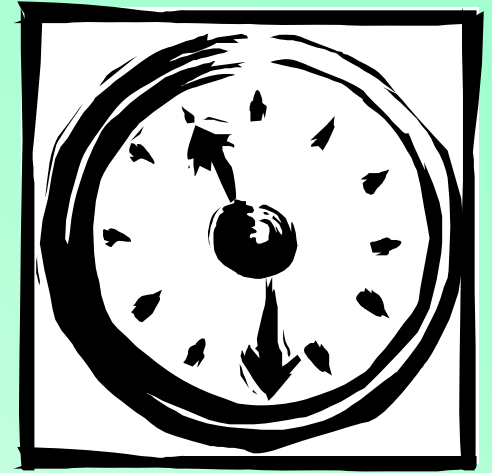
- Fully automated Trust Decision making undermines Trust Perception
- Trust is Good – Control is Better!



# More Information

- Personal websites
  - <http://www.law.kuleuven.be/icri/frobbe>
  - <http://www.esat.kuleuven.be/~decockd>
  
- Website Trusted Architecture for Securely Shared Services
  - <http://tas3.eu>
  
- Website Crossroads Bank for Social Security
  - <http://www.ksz.fgov.be>
  
- Website Federal Public Service for Information and Communication Technology (FedICT)
  - <http://www.fedict.be>
  
- Belgian Electronic identity card
  - <http://godot.be/eid>

Th@nk you!



Any questions?