



Trusted Architecture for Securely Shared Services

*Generic Architecture
to Securely Manage
Employability, Healthcare &
Personal Information Services*

Web: <http://tas3.eu>

Email: tas3@ls.kuleuven.be

TAS³ is an IST FP7 funded Integrated Project

TAS³ contract number 216287

Duration: 1 Jan 2008 - 31 Dec 2011

Research budget: 13.200.000 €

EC Funding: 9.400.000 €



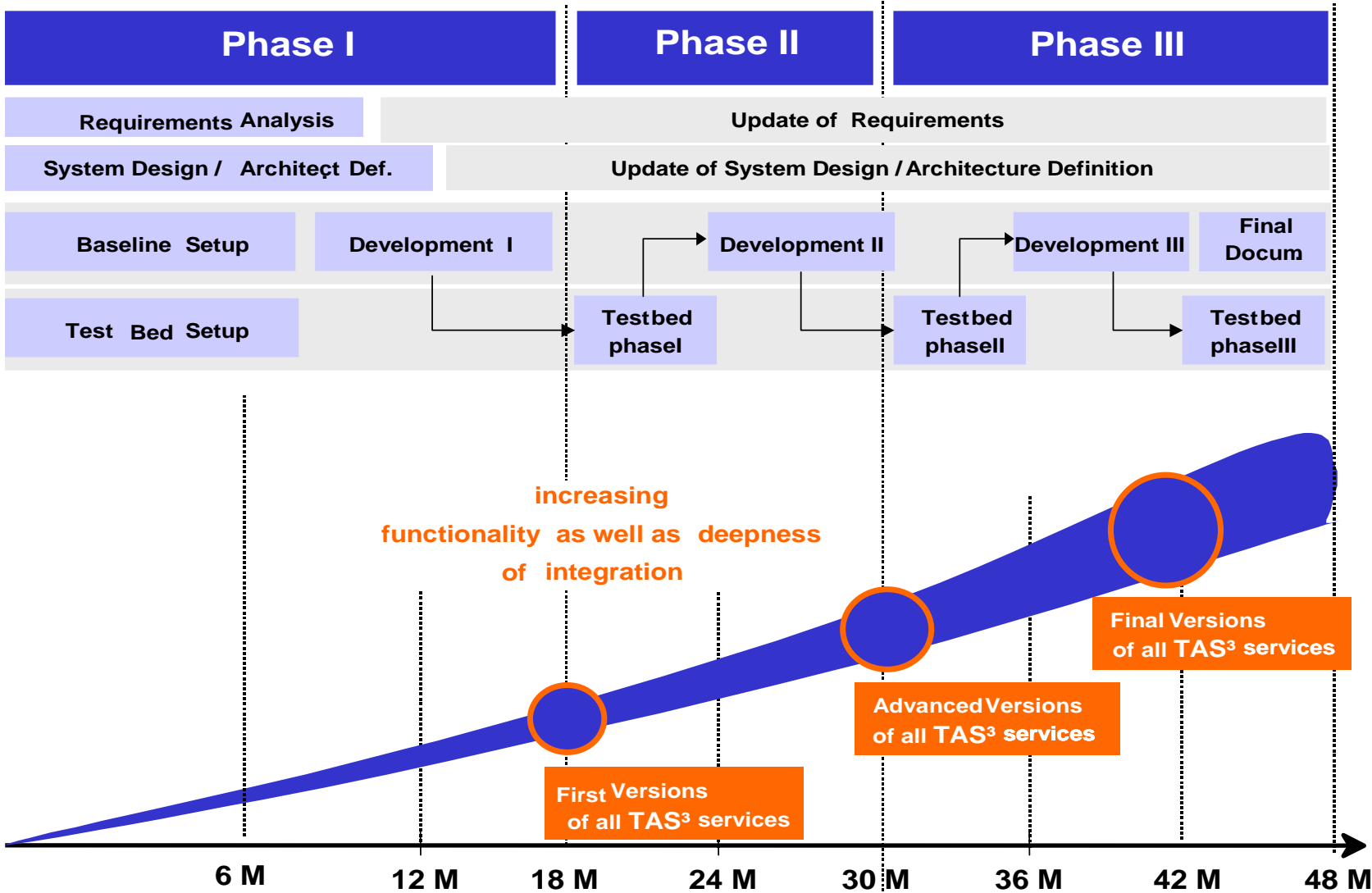
What is TAS³ About?

- TAS³ focuses **federated** identity management
- TAS³ consolidates **scattered research** in
 - Security, Trust, Privacy, Digital identities, Authorization, Authentication...
- TAS³ integrates adaptive business-driven **end2end** Trust Services based on personal information:
 - Semantic integration of Security, Trust, Privacy components
- TAS³ provides dynamic view on application-level **end2end** exchange of personal data:
 - Distributed data repositories

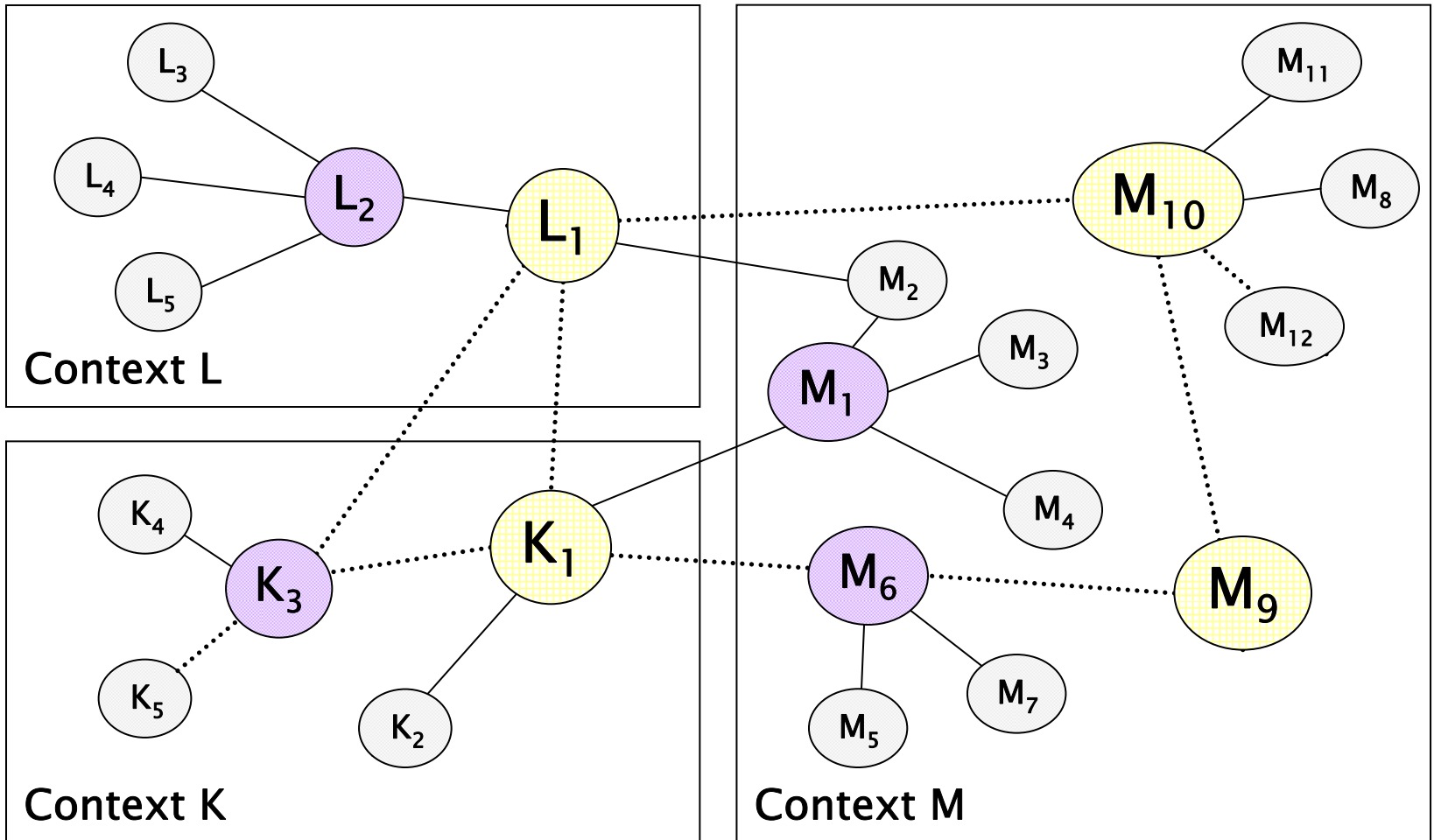
18 TAS³ Partners

- **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, Risaris Ltd, SAP Research, Synergetics

TAS³ Phased Approach



Support for Cross-Context Adaptable Business Processes!



TAS³'s 4 Core Layers

- Layer 1 – **Authentication**
 - Federated identities
- Layer 2 – **Authorization**
 - Federated attributes
- Layer 3 – **Trustworthiness & Reputation** scores
 - End-user controlled
 - Fine-grained role-based
- Layer 4 – **Data-protection** policy enforcement
 - Sticky policies associated with information elements

Business Process

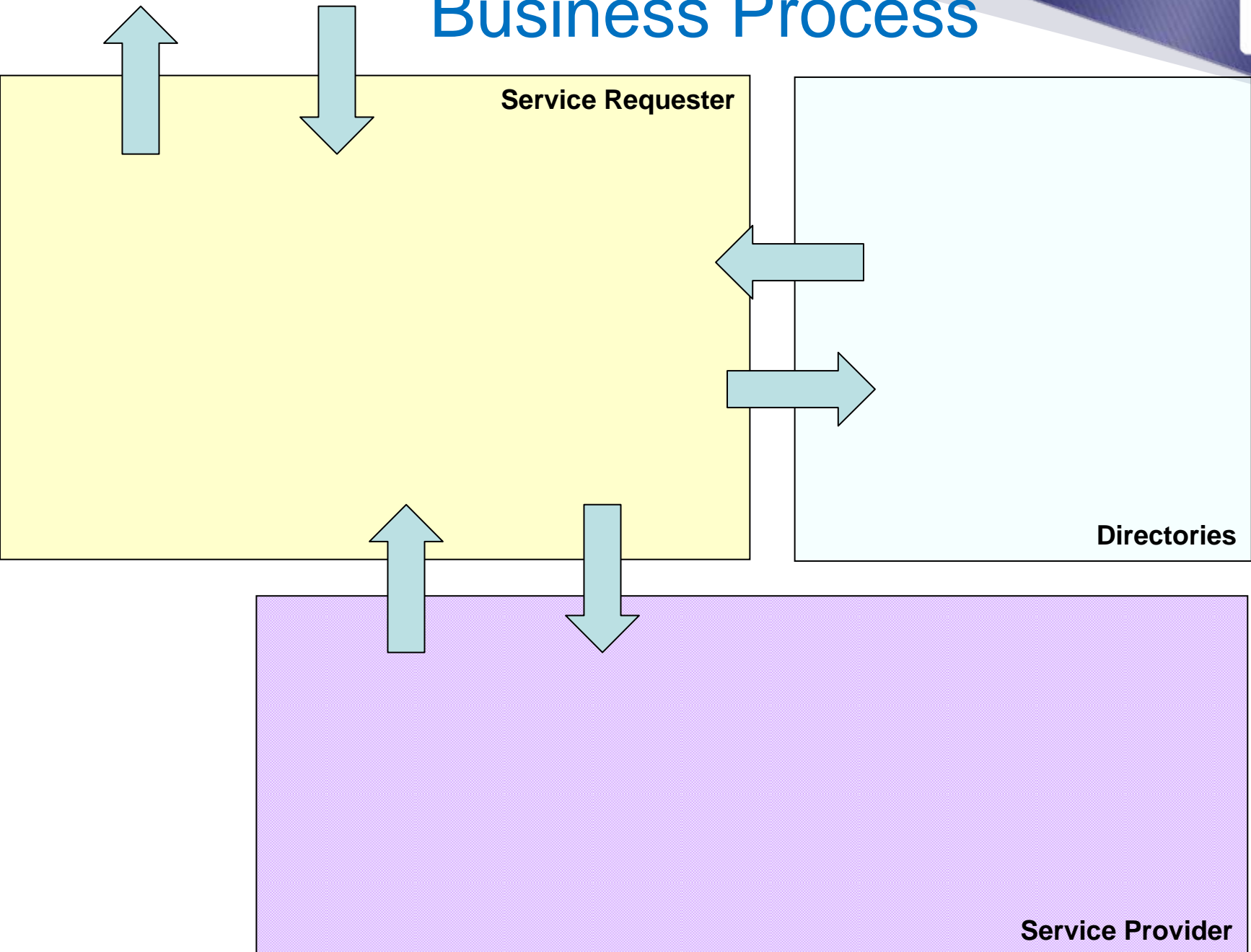


Service Requester

Directories

Service Provider

Business Process



TAS3 Entry Point

TAS3 Exit Point

Business Process



Service Requester

Service Requester Process Engine

Trust & Privacy Negotiator

Obligations Watchdog

Audit Guard

Policies Enforcement Point

Request Preparer

Response Verifier

Log Analysis Engine
• Audit Aspects
• Policy Aspects

TAS³ Registry
•Service Providers
•Service Types
•IdPs

Authentication Authorities (IdPs)

Authorization, Trust & Reputation Authorities

Directories

Request Verifier

Obligations Watchdog

Audit Guard

Response Preparer

Credentials Clearing PEP

Service Provider Process Engine

Policies Enforcement Point

Credential Clearing PDP

Actual Application Engine

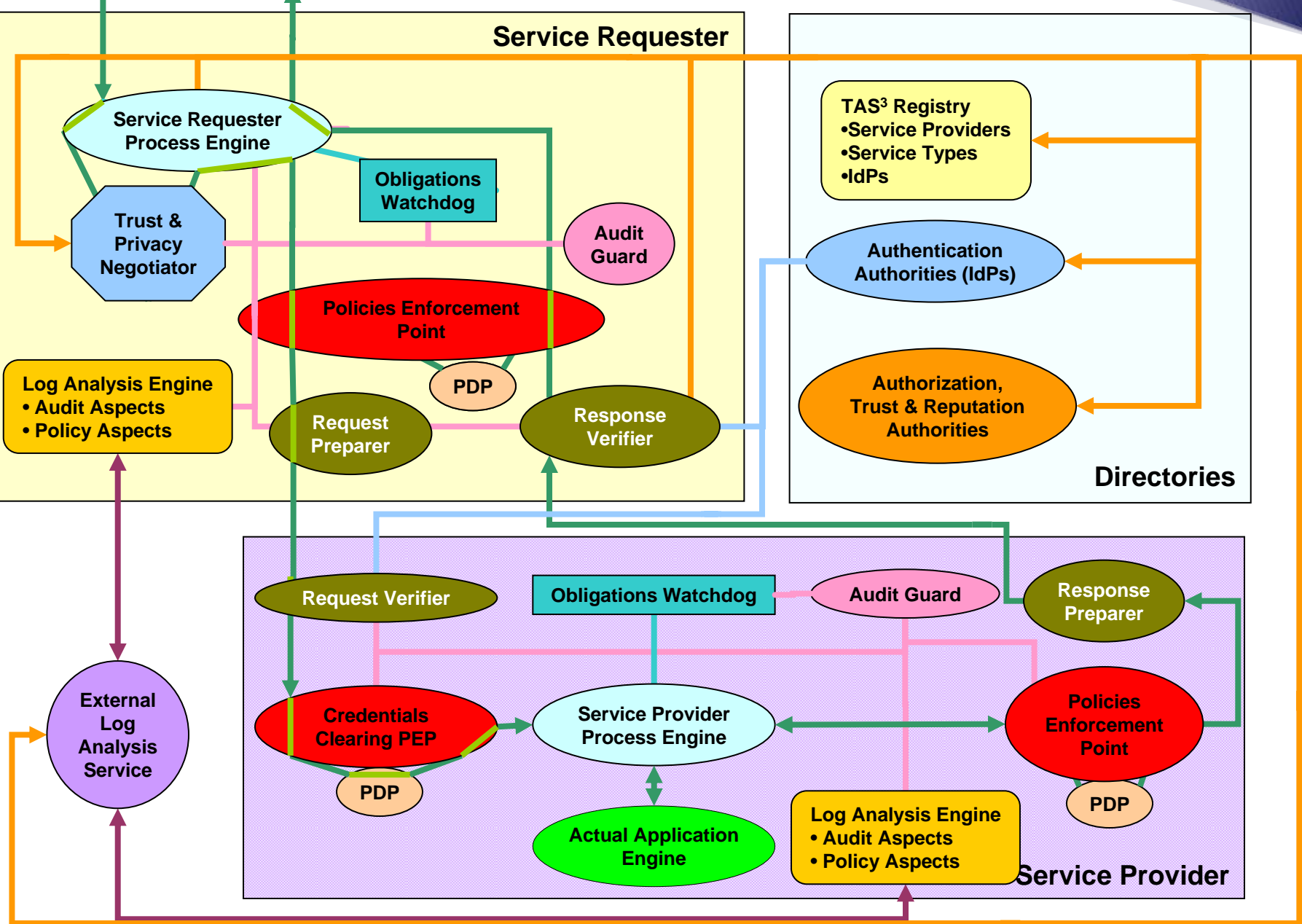
Log Analysis Engine
• Audit Aspects
• Policy Aspects

Service Provider

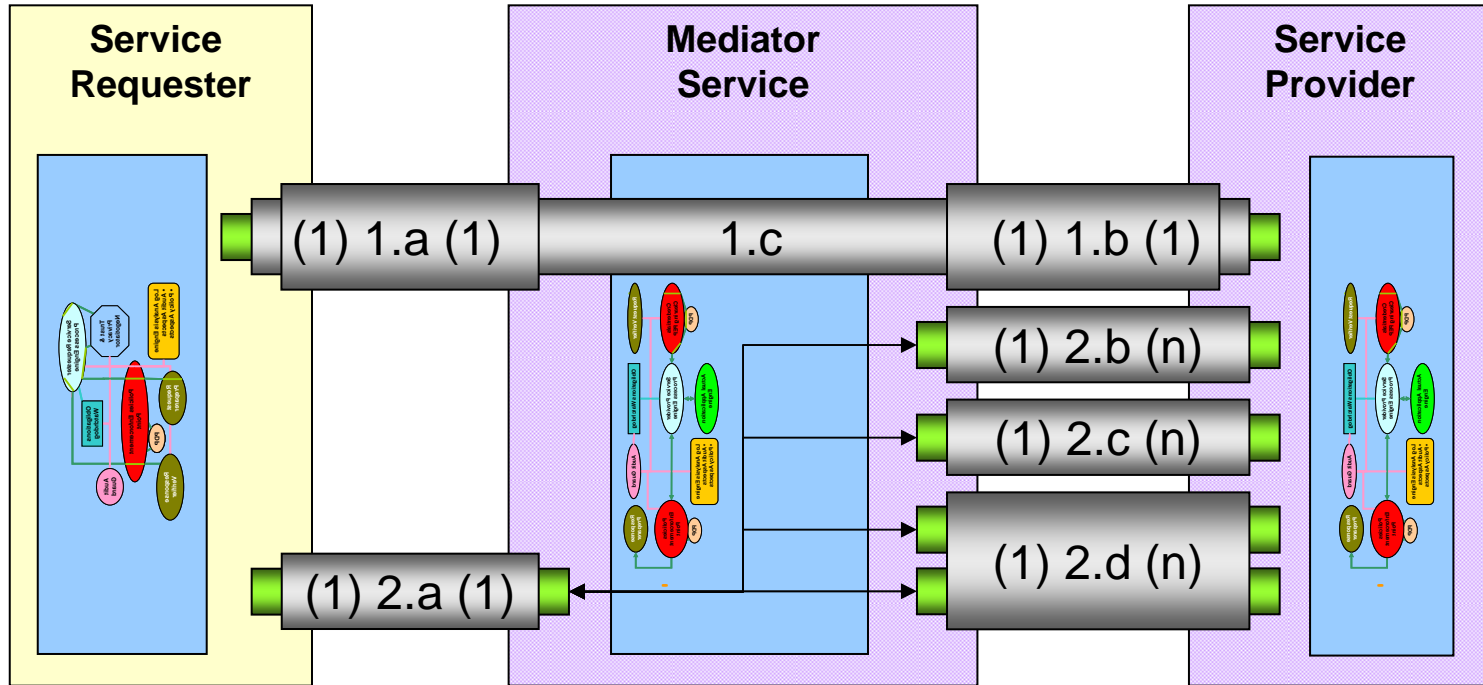
External Log Analysis Service

Business Process

TAS3 Entry Point TAS3 Exit Point



End-to-End Communications Options



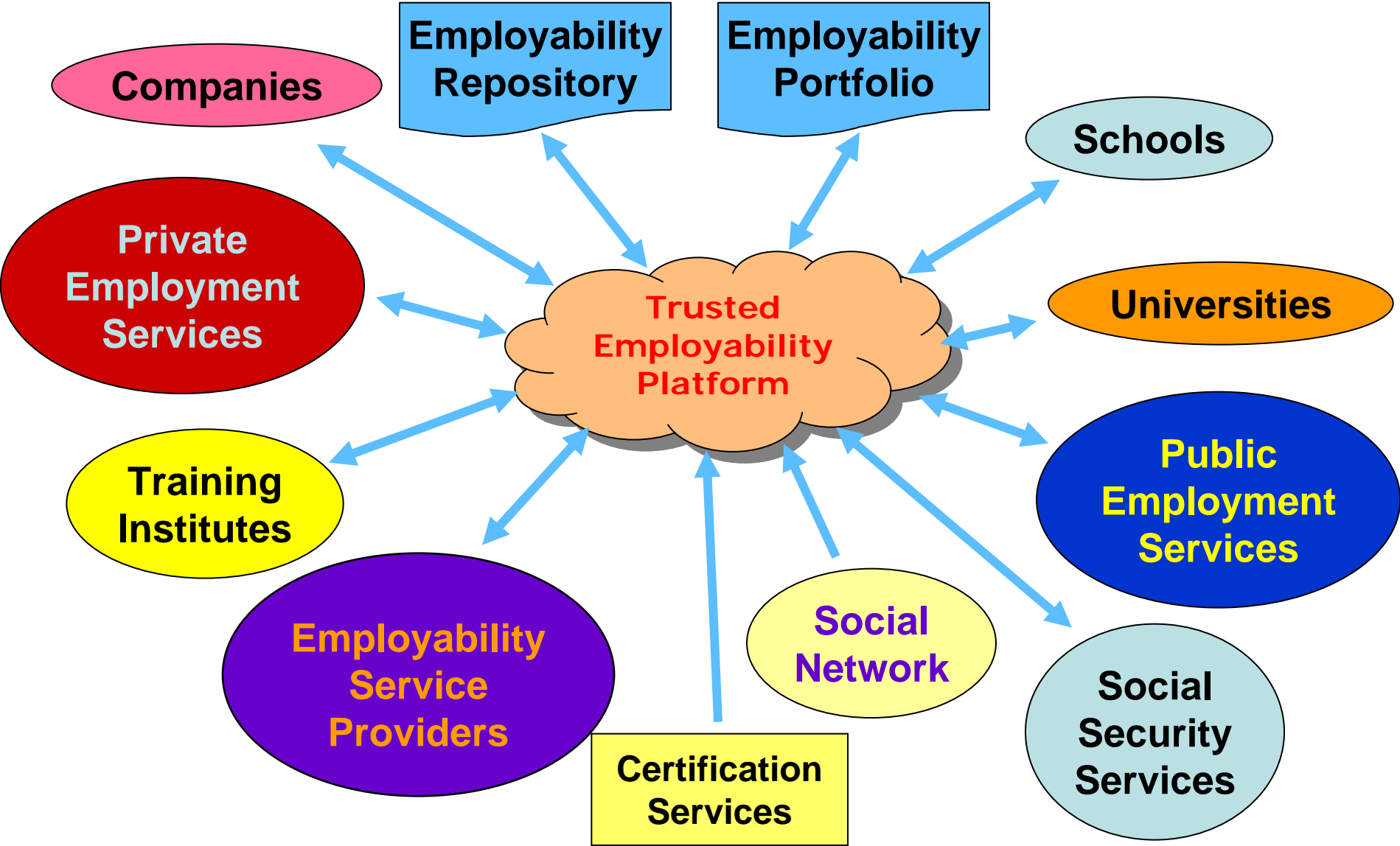
Application Data

- (1) Reference (1) → One to One
- (1) Reference (n) → One to Many
- (m) Reference (n) → Many to Many

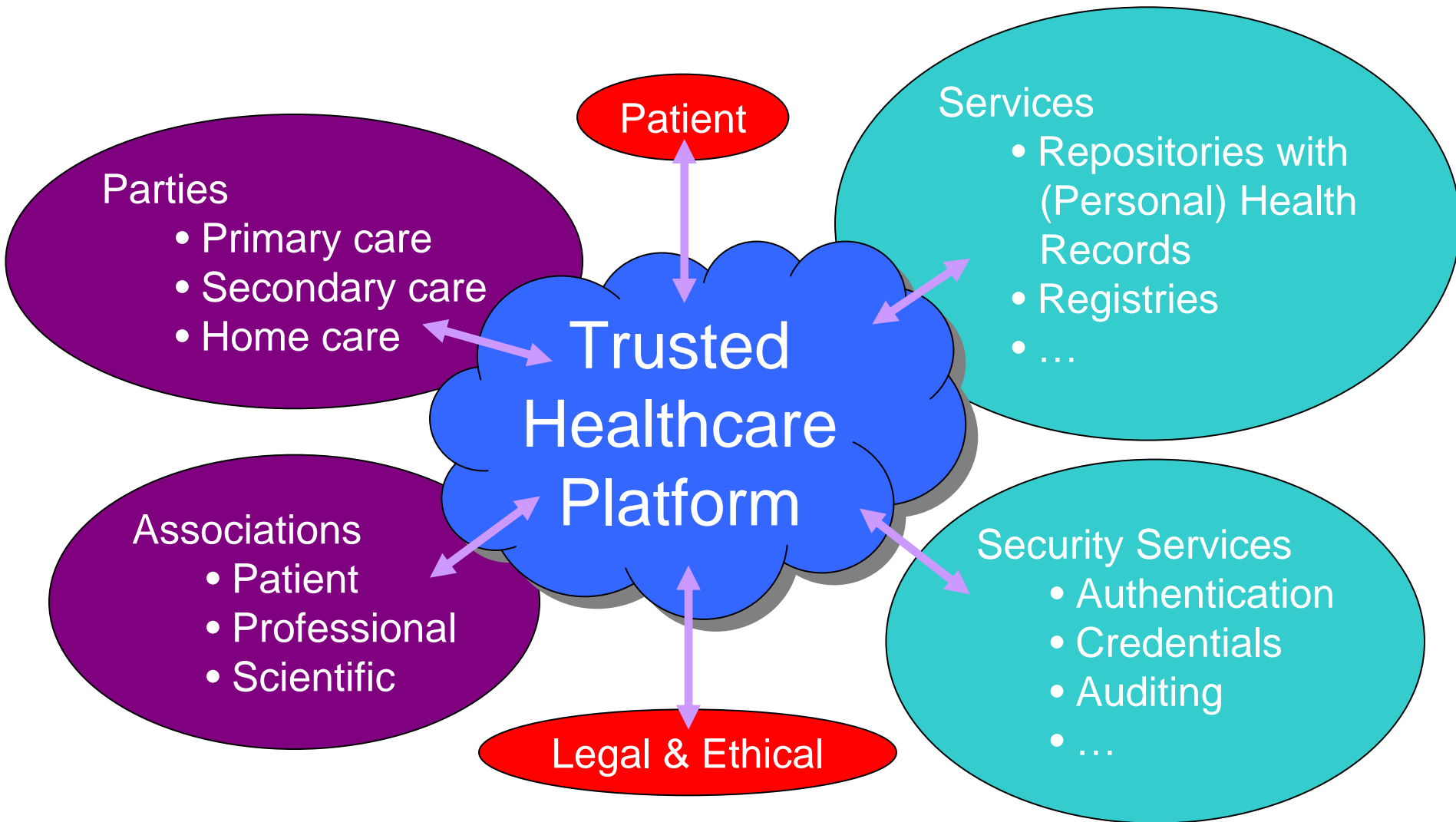
Communications Tube

- Some degree of anonymity (optional)
- Secure
- Confidential
- Data-origin
- Insecure

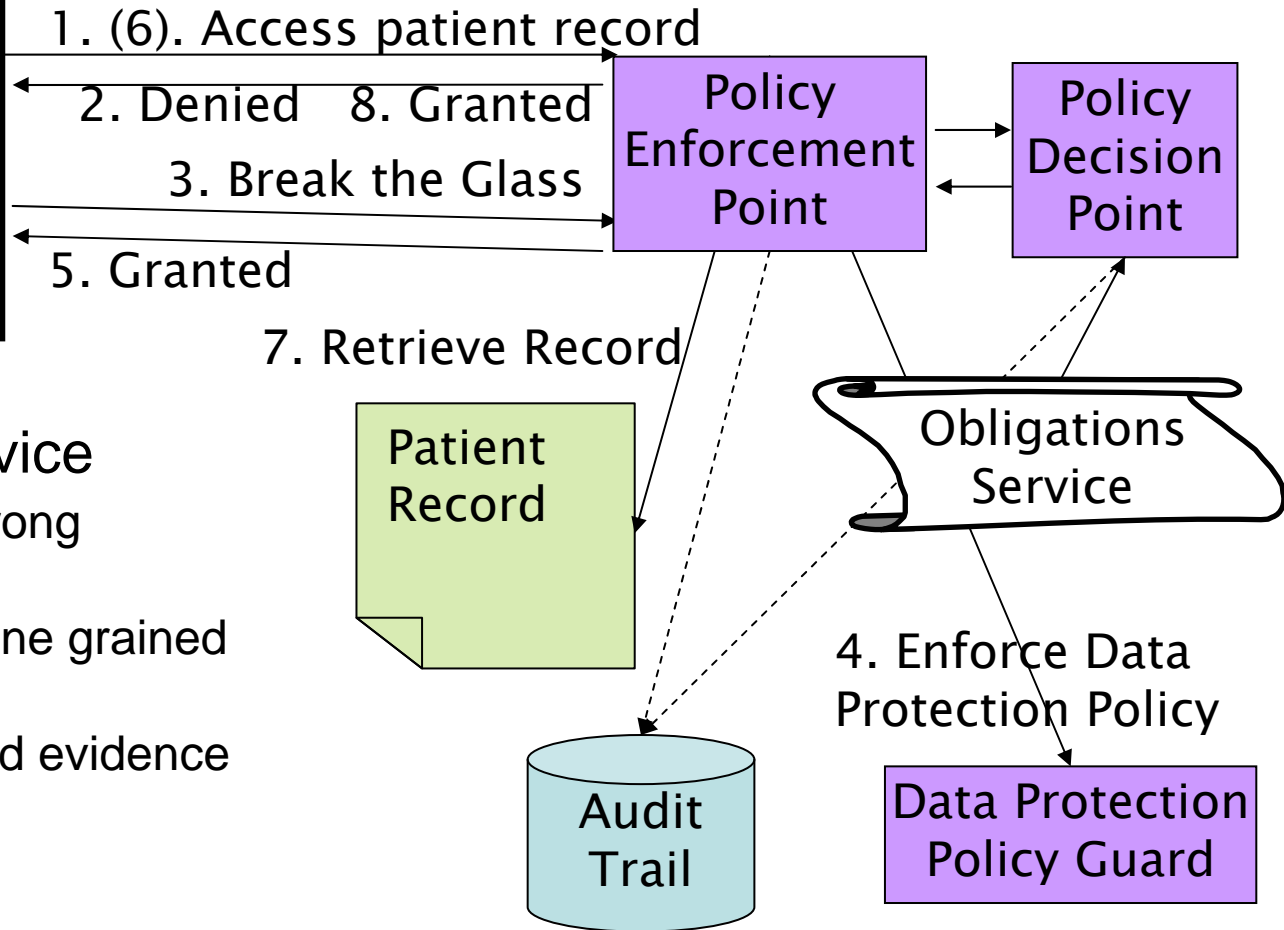
Trusted Employability Platform



Healthcare Demonstrator Platform



eHealth – Break the Glass Service



- Break-the-Glass service
 - Only activated after strong authentication
 - Triggers advanced & fine grained monitoring
 - Audit trail provides hard evidence

Extreme Instantiation ☺

- Why limit ourselves to healthcare and employability use cases?
 - Generic architecture
 - Service providers can be physical gate keepers or other guards
- When trustworthiness becomes user-unfriendliness
 - Granularity of policy specifications & validations
 - Automating Big Brother through obligations

Contact Information

- Web: <http://tas3.eu>
- Email: tas3@ls.kuleuven.be