



Trusted Architecture for Securely Shared Services

Information Protection & User Consent

Danny De Cock
K.U.Leuven ESAT/COSIC

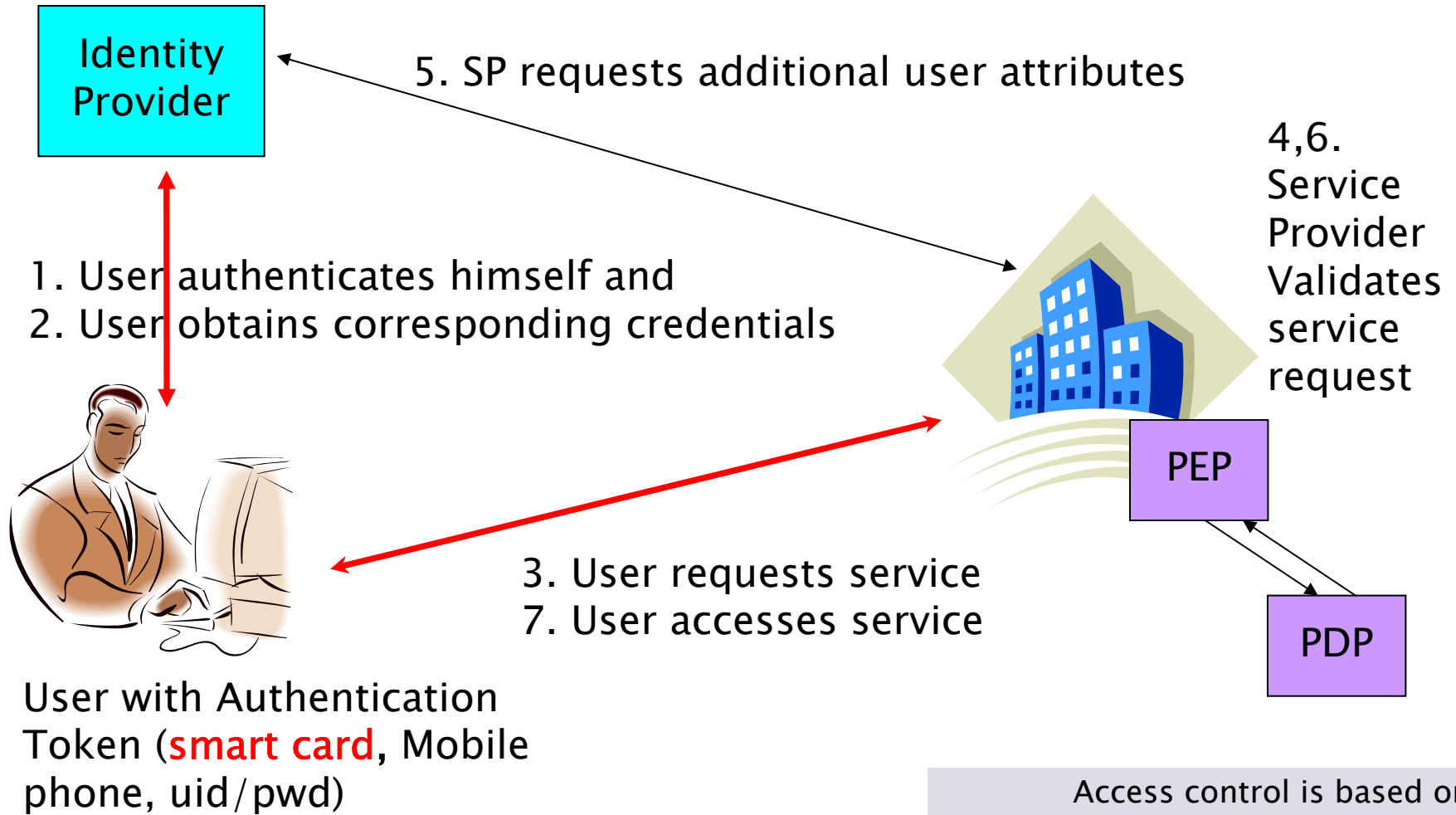
Danny.DeCock@esat.kuleuven.be



What is TAS³ About?

- ▶ TAS³ is an FP7 Integrated Project focusing identity management
- ▶ Consolidating **scattered research** in
 - Security, Trust, Privacy, Digital identities, Authorization, Authentication...
- ▶ Integrating adaptive business-driven **end2end** Trust Services based on personal information:
 - Semantic integration of Security, Trust, Privacy components
- ▶ Application-level **end2end** exchange of personal data
 - *... "a dynamic view on distributed data" ...*

TAS³ High-level Process Flow



TAS³'s – 4 Layers

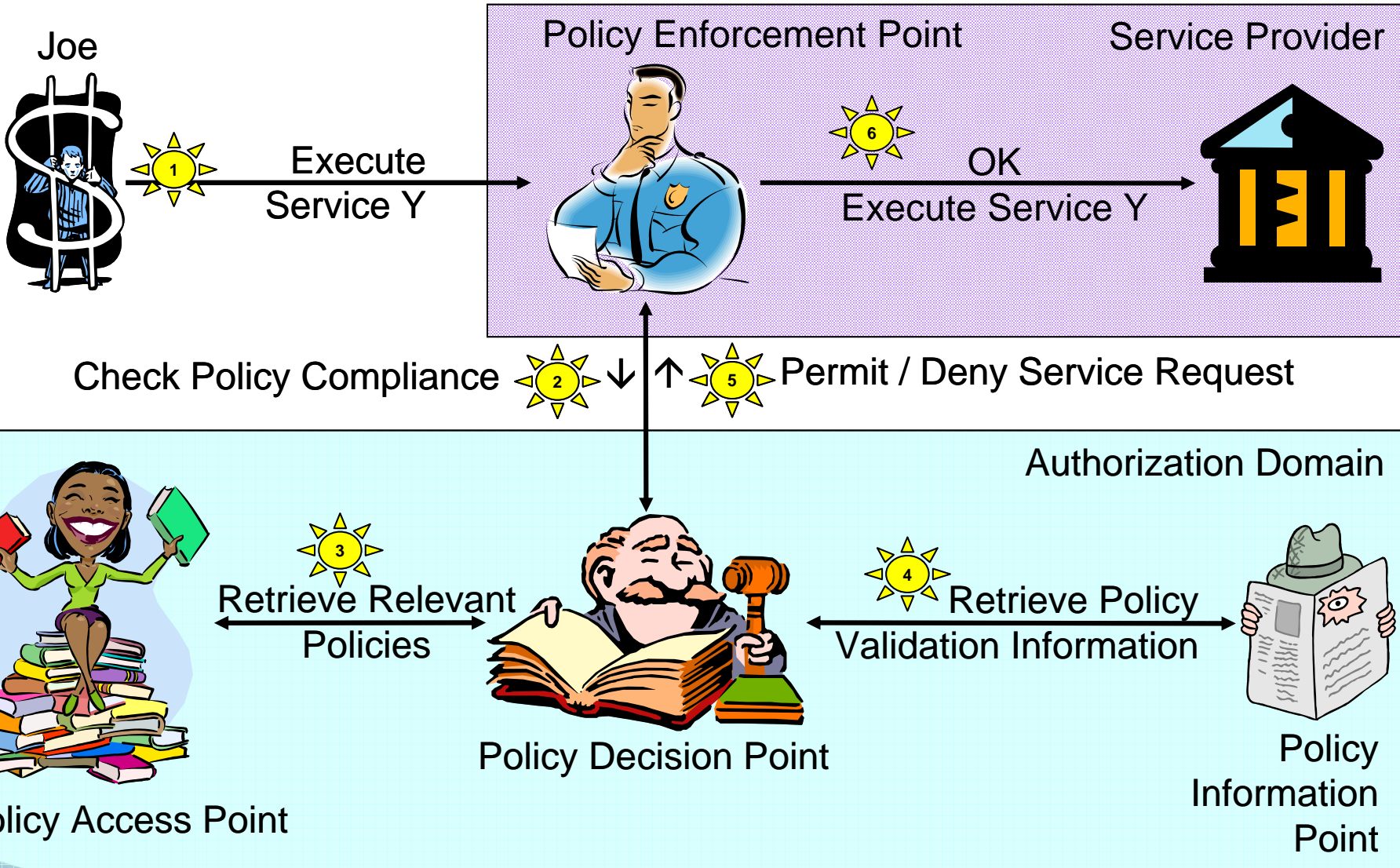
- ▶ Layer 1 – Authentication
 - Federated identities
- ▶ Layer 2 – Authorization
 - Federated attributes
- ▶ Layer 3 – Trustworthiness & Reputation score
 - End-user controlled
 - Fine-grained role-based
- ▶ Layer 4 – Data-protection policy enforcement

Layer 1 – Authentication & Level of Assurance (LoA)

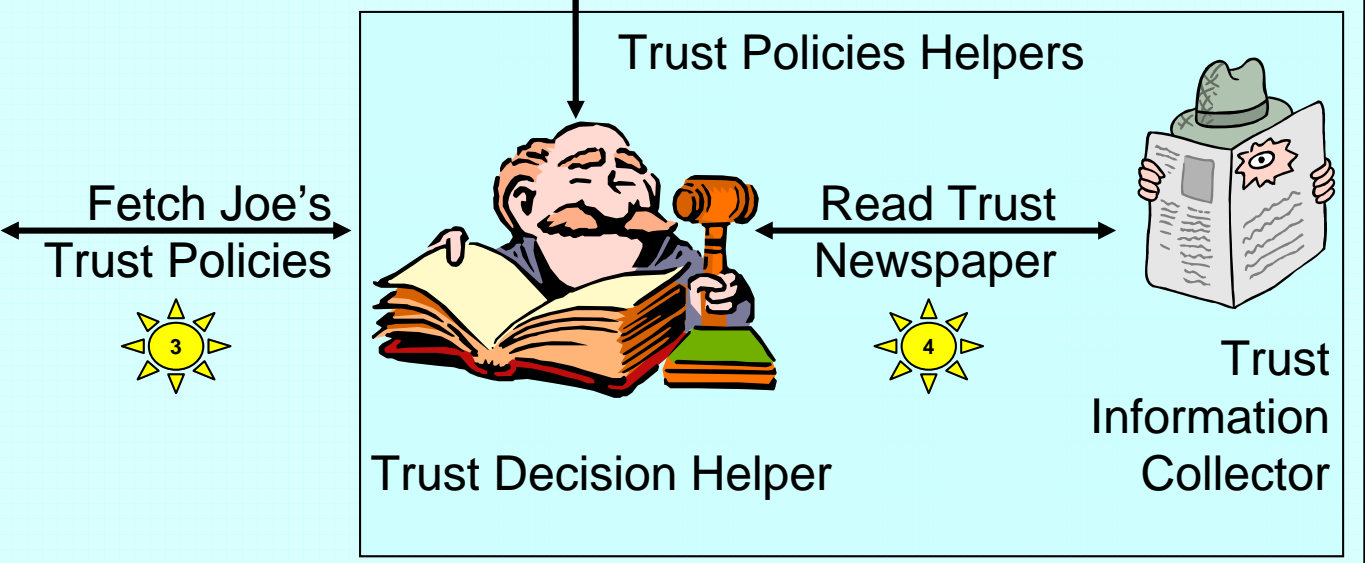
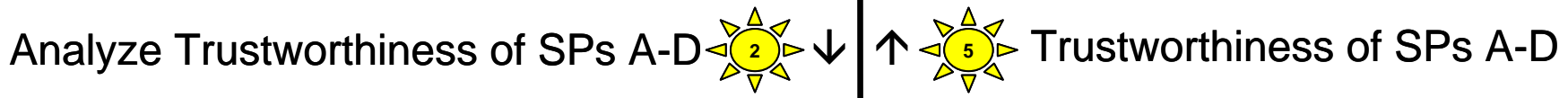
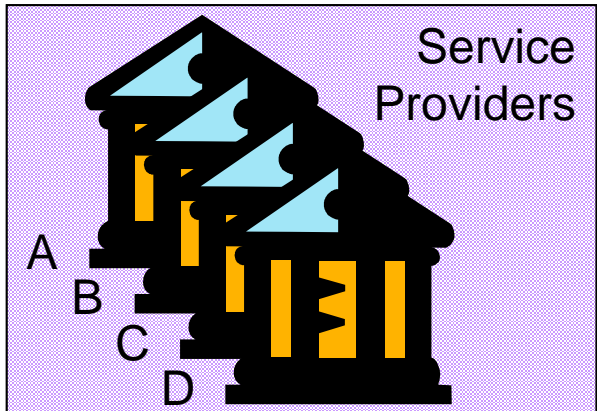
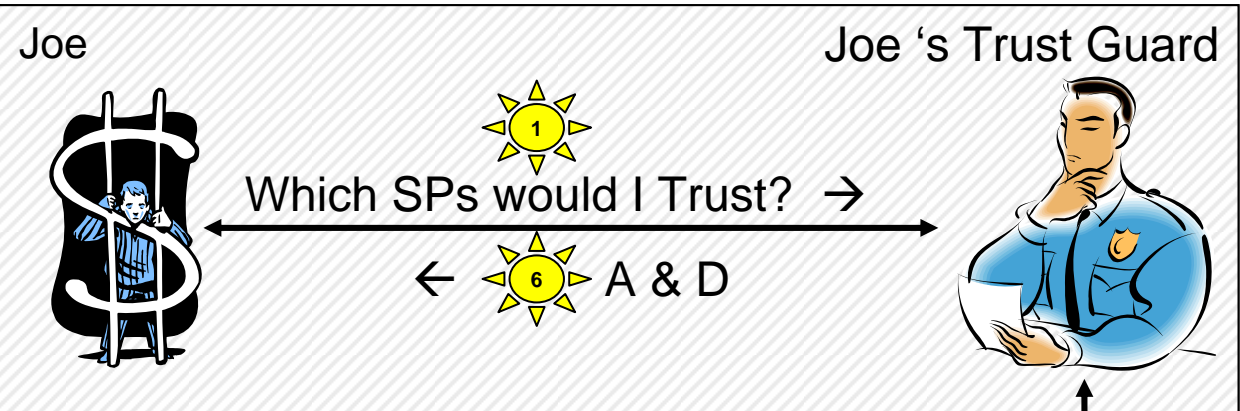
- ▶ Federated identity management model
 - E.g., Shibboleth, Liberty Alliance, CardSpace...

LoA 4+ (qualified plus biometric)	Setting access policies
LoA 4 (qualified cert with smart card EAL4+)	Sensitive medical records (e.g. HIV), Consultant notes containing opinions. Ability to Break the Glass. Bank to bank transfers
LoA 3 (2-factor authentication, non-qualified cert, EAL4 smart card)	Patient confidential records (non-sensitive)
LoA 2 (one time password)	Some Internet banking applications System administration
LoA 1 (uid/password, Verisign Class 1 cert)	Retrieve degree certificate. Completing public service employment application
LoA 0 (no authentication)	Public data

Layer 2 – Authorization

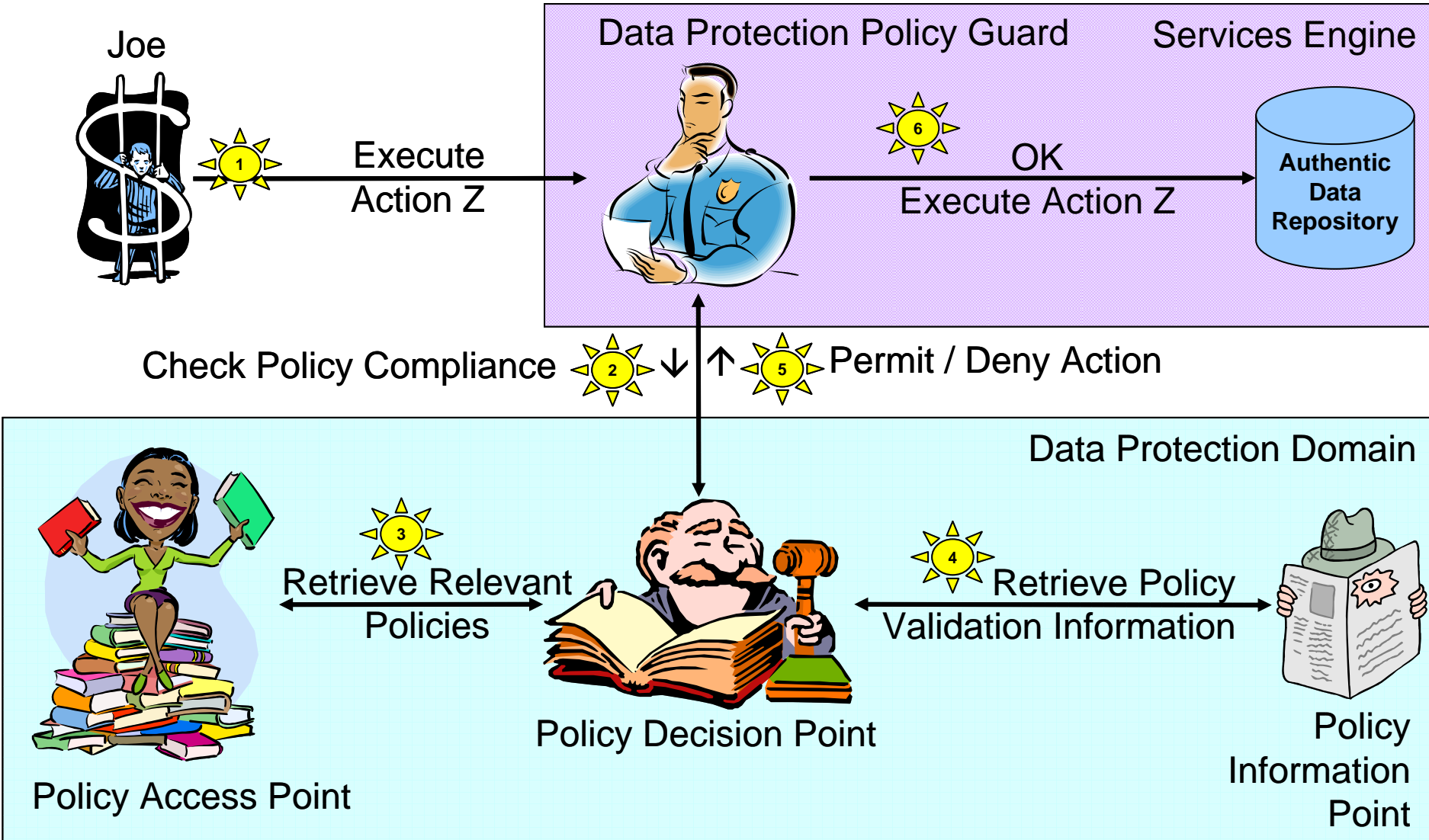


Level 3 – Trustworthiness & Reputation

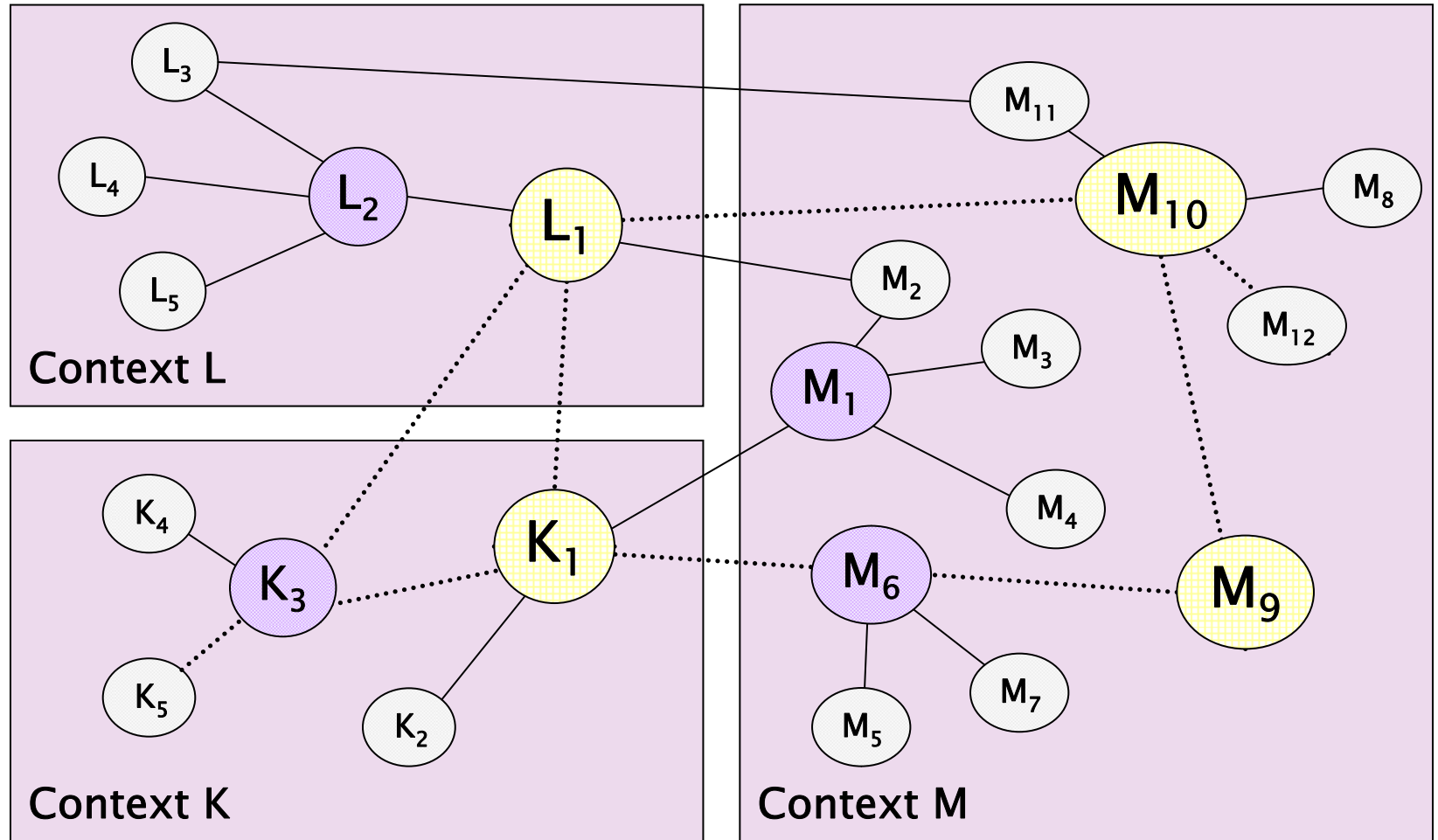


Trust Domain

Level 4 - Data Protection Policy Enforcement



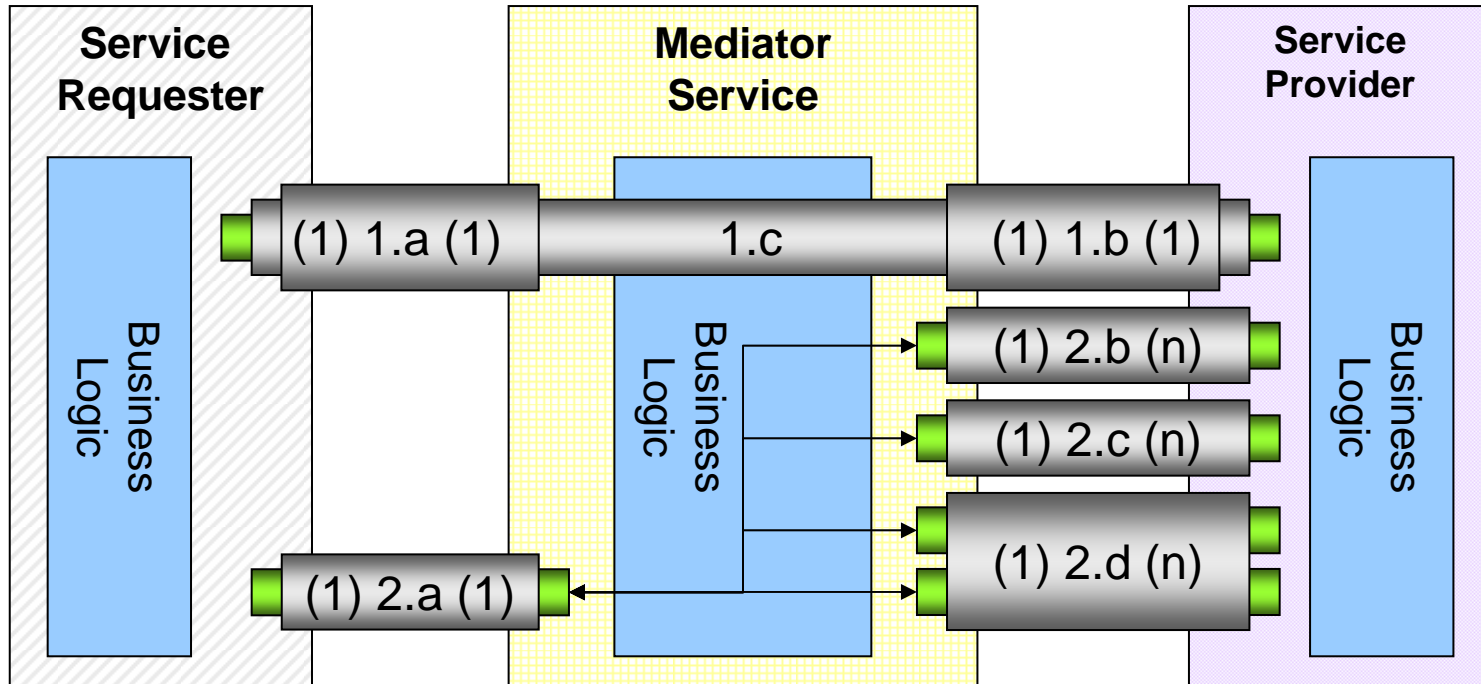
Support for Cross-Context Processes



Sticky Policies

- ▶ Authentic data repositories store information containers
- ▶ Information container consists of:
 - The information itself (data + semantics)
 - Data Blob
 - Identification:
 - Unique identifier of this information
 - Unique within the scope of the service provider
 - Finality policy:
 - Reference to role-based context in which container was collected
 - Reference to role-based purpose for which the container was collected
 - Sticky access policy:
 - Reference to role-based context in which container can be used
 - Sticky trust & reputation policy:
 - Reference to trust & reputation policies to be enforced to access the container
 - Integrity protection field
 - Guarantees that container cannot be changed without being detected
- ▶ Audit trail logs information container processing

Secure Communication Pipes



Application Data

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

Communications Tunnel

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

Questions?

- ▶ Email:

- Danny.DeCock@esat.kuleuven.be

- ▶ Web:

- <http://tas3.eu>

- ▶ Slides:

- <http://godot.be/slides>