

TAS³ Architecture

Sampo Kellomäki (sampo@symlabs.com), Symlabs
23.11.2009, ServiceWave, Stockholm

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 216287 (TAS3 - Trusted Architecture for Securely Shared Services - www.tas3.eu)

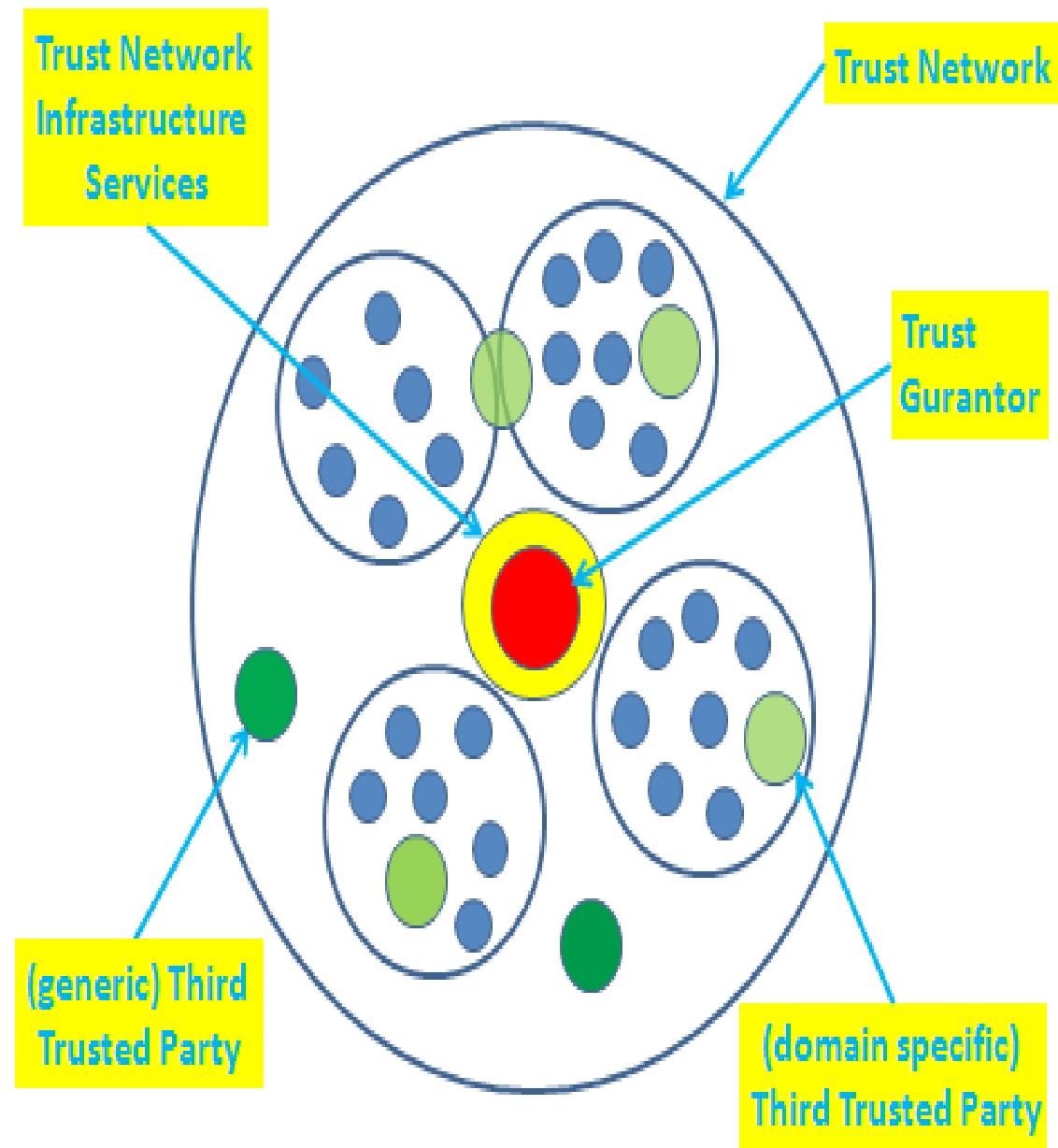
TAS3 Project (48 months, 2008-2011)

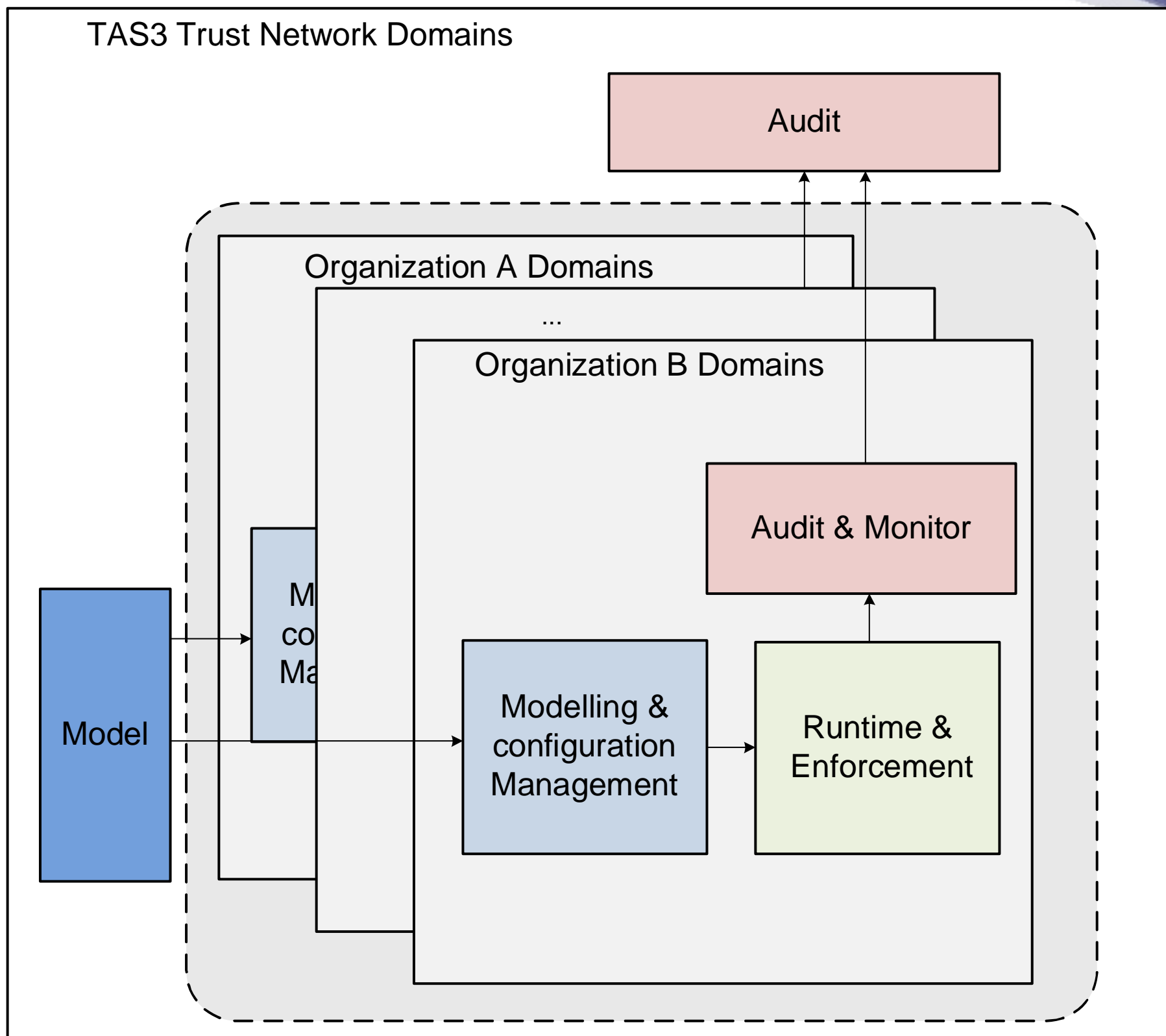
- Goals

- Trusted Architecture for Securely Shareable Services
- Web Services made secure, *privacy friendly*, and shareable
- Dashboard for user's privacy settings and self audit
- Full audiability, leverage digital signatures
- Advanced Trust and Privacy Negotiation and Trust Scoring
- Business and legal model

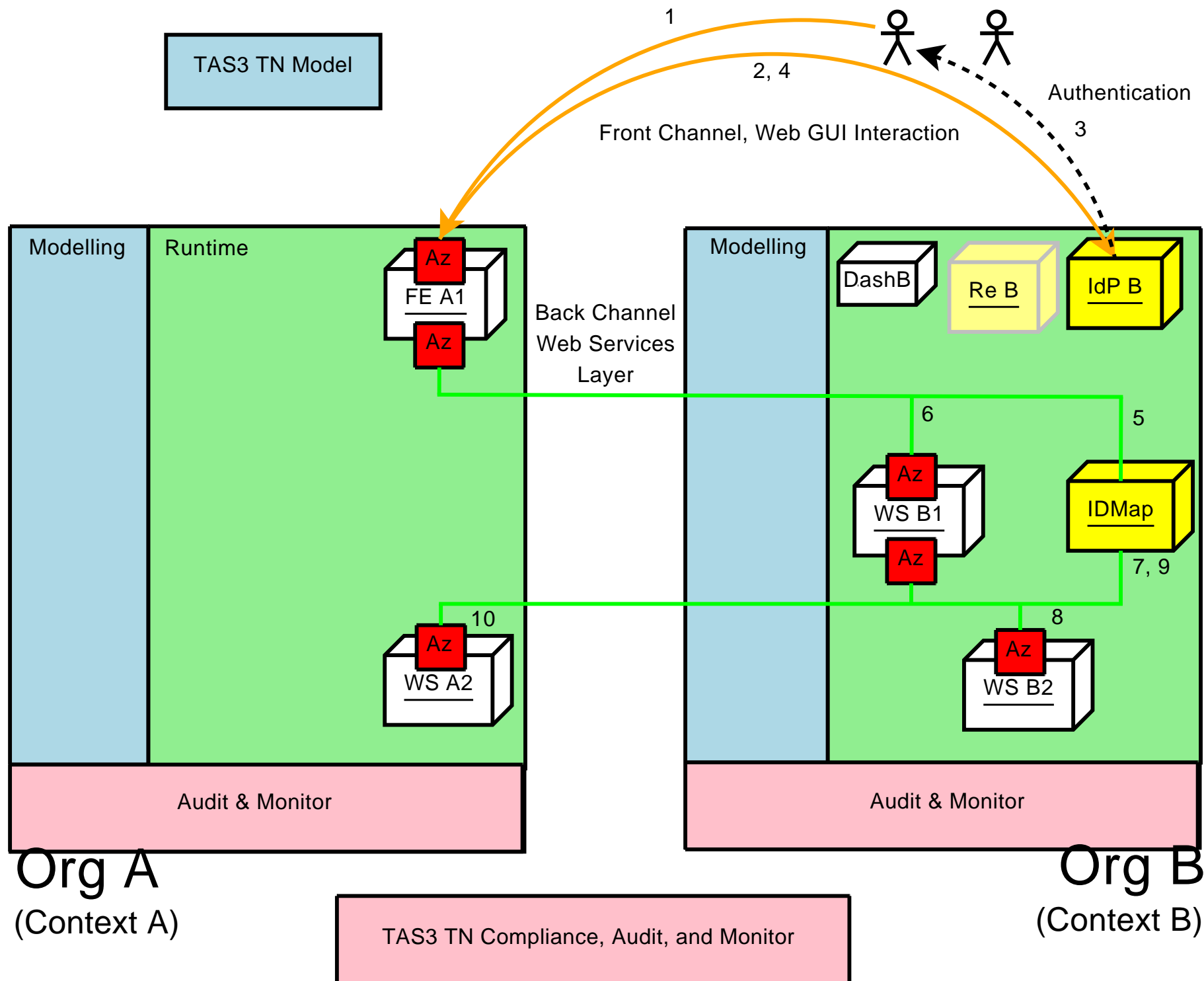
- Practical

- Standards based (SAML, ID-WSF, XACML) *interoperable* wirespecs
- API (Java, C#, PHP, Perl, C/C++)
- Reference implementation (zxid.org)
- Pilots
- Exploitation: buy TAS3 enabled components from vendors such as Symlabs, Risaris, Custodix, and Synergetics

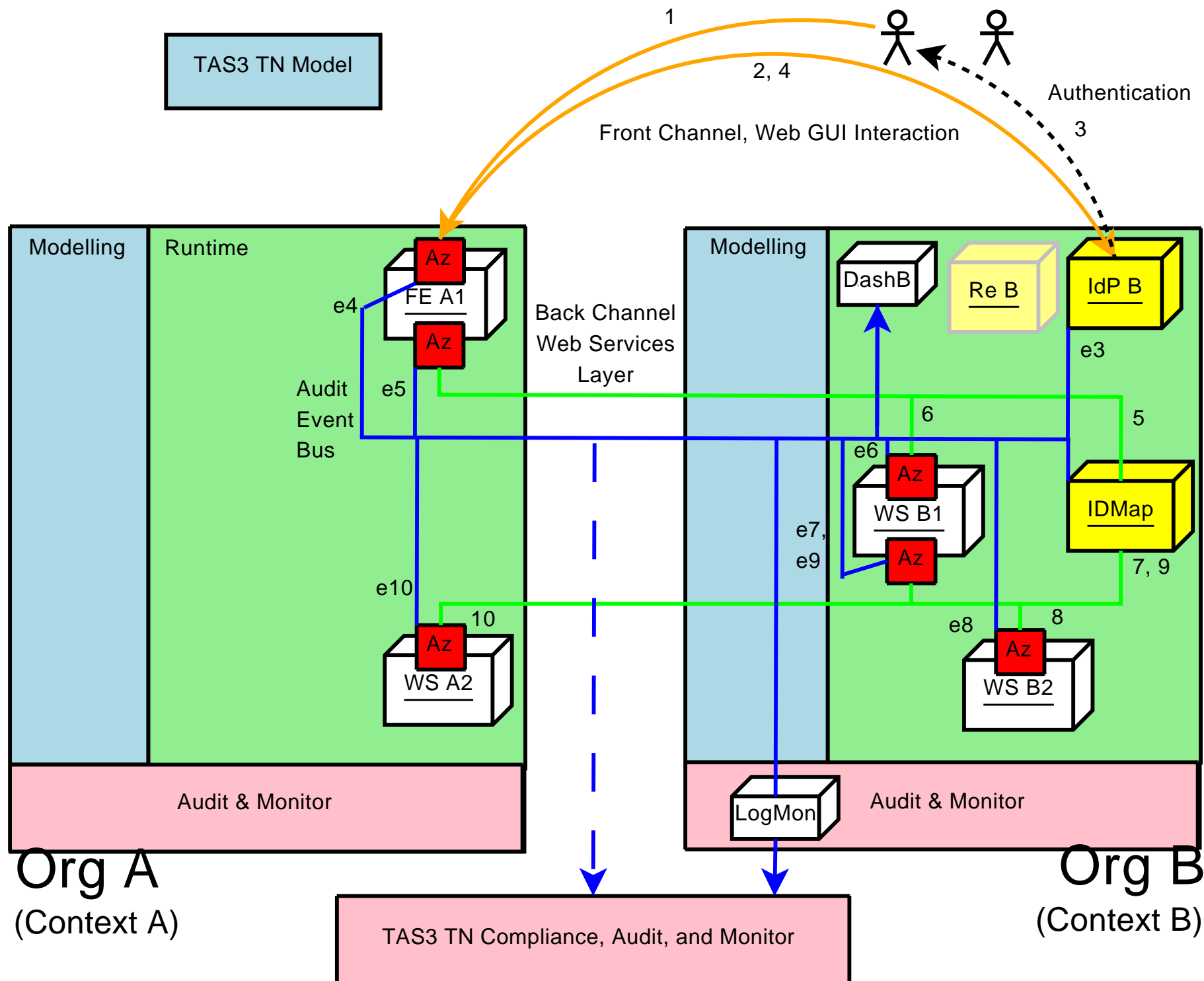




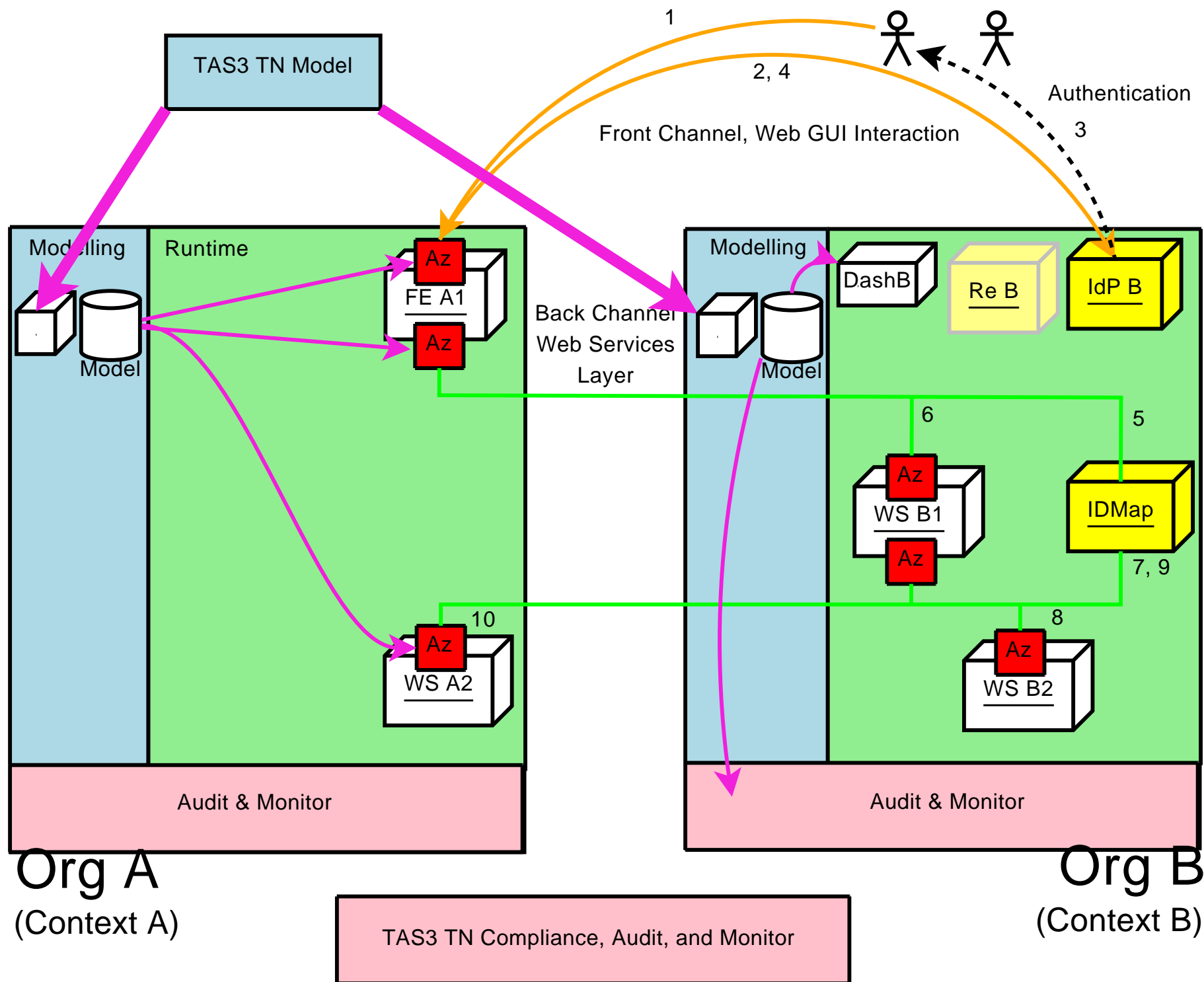
Front channel and back channel interaction



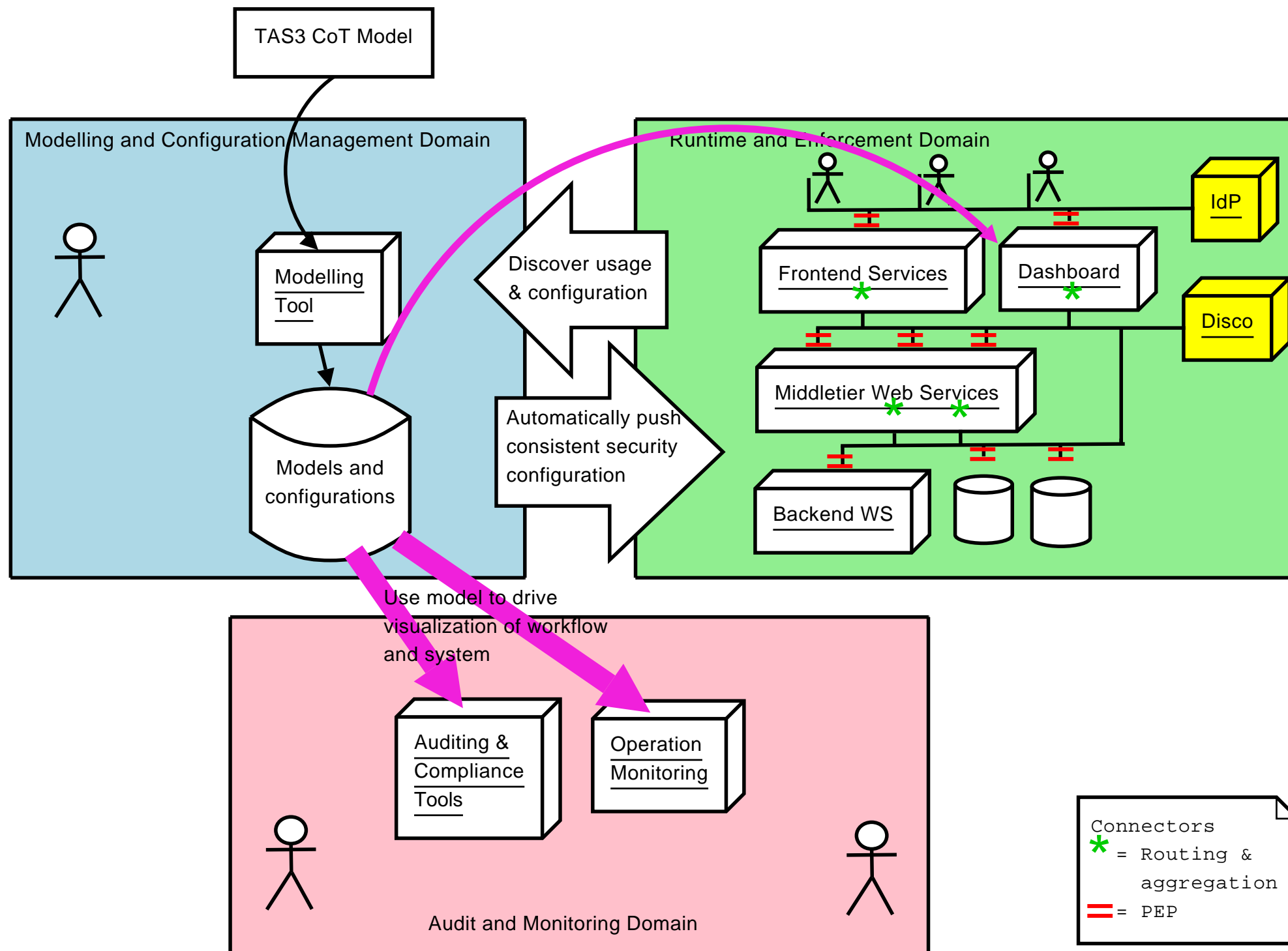
Audit Channel

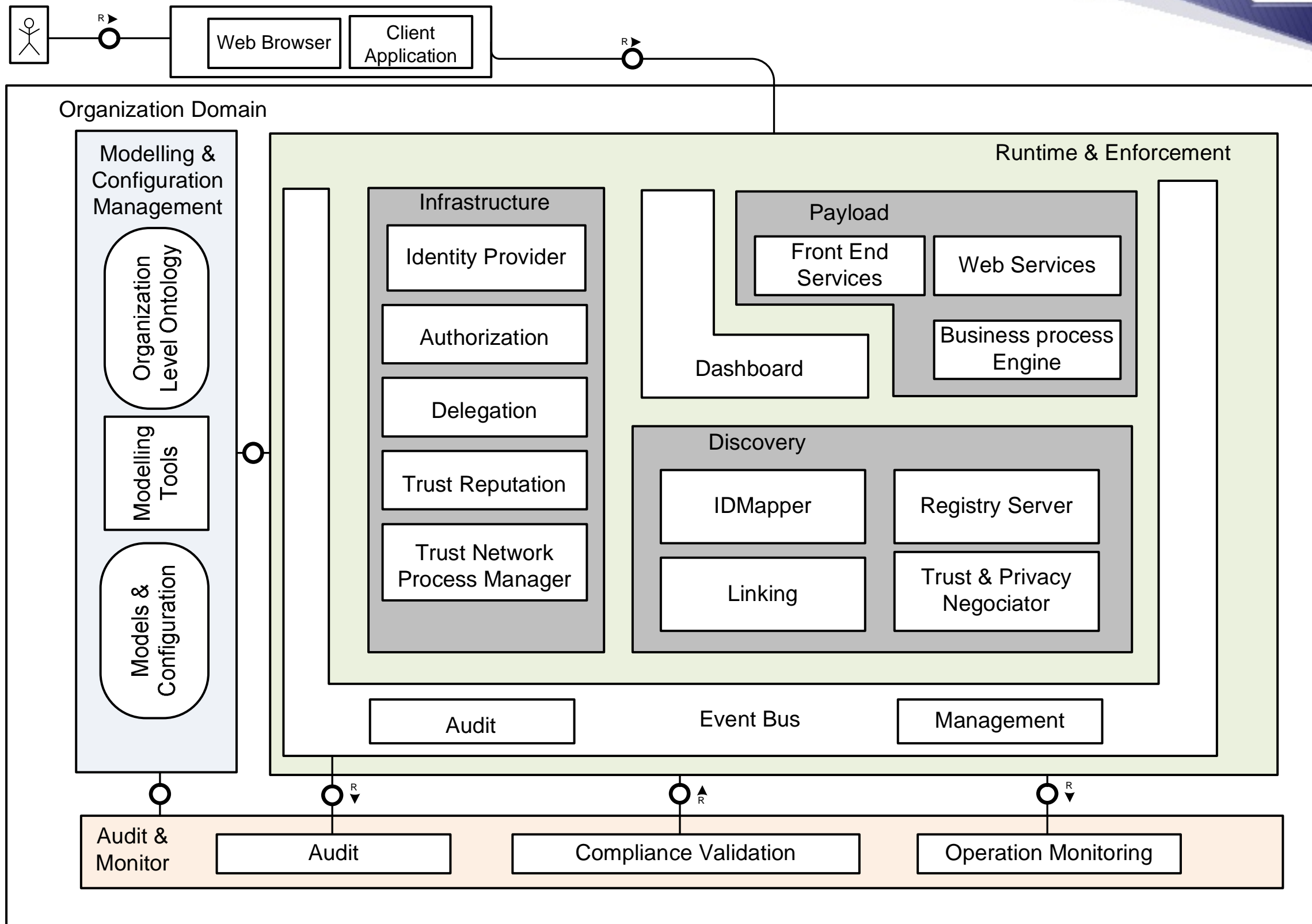


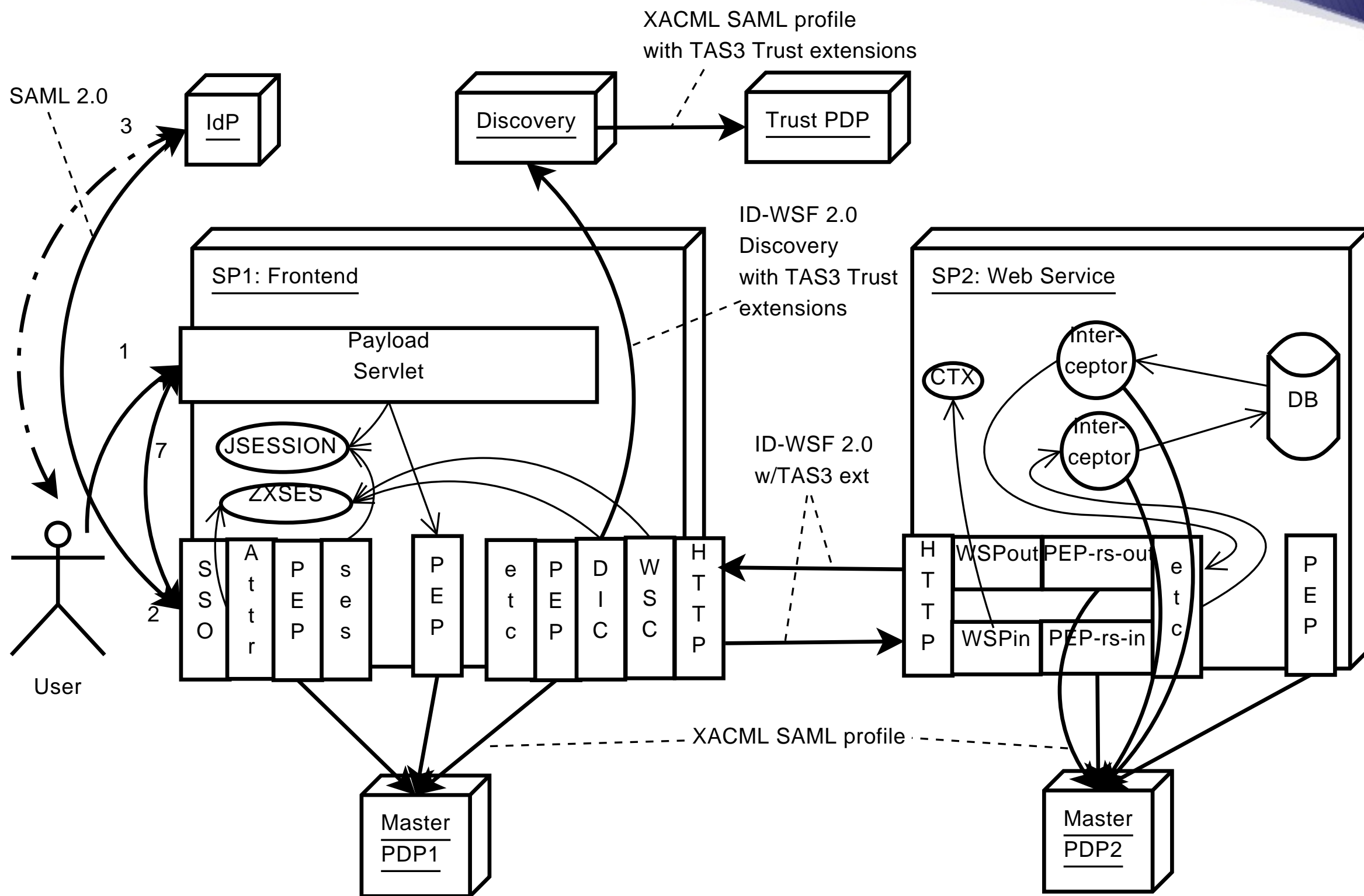
Model driven configuration



Model driven audit







Prior Art and Reference Architectures

- TAS³ Architecture draws from and is compatible with
 - Nessi's NexofRA
 - Master's concept of audit bus and Awareness Cockpit
 - Access-eGov Platform Architecture
 - Liberty Alliance's ID Web Services Framework (ID-WSF)
 - Hafner & Breu's Security Engineering for Service-Oriented Architectures
- TAS³ Architecture is not as abstract as a reference architecture
 - Goal is to drive real interoperable implementations

Novelty of the Architecture Itself (1/2)

- TAS³ Architecture is novel as a blueprint that brings together
 - Identity management
 - Attribute based access control
 - Business process modelling
 - Dynamic trust
 - Distributed auditing
 - Legal & Policy
 - Support for multiple policies in different languages
 - Annex A in combination with D2.2, acts as an interoperability profile for standards based protocols covering these areas
- User transparency features
 - Dashboard
 - User accessible audit trail
 - Automated compliance validation

Novelty of the Architecture Itself (2/2)

- Privacy protection using sticky policies
- Marriage of Trust and Privacy Negotiation with discovery and trust scoring
- Secure dynamic business processes
- Built-in first class support for delegation
- Architecture needs to be instantiated in context of a *business model* and legal / contractual framework
 - Leave many decisions to be decided in that context
 - Many business models are possible (the one currently in annex will become a document of its own)

Wire interoperability, many software implementations possible

- Any implementation that speaks wire protocols and flows correctly is valid, irrespective of the software architecture
- Software architecture of the entities specified by the TAS³ Architecture is up to implementers of those entities (some of the implementer's are TAS³ work packages)
- The architecture includes a legacy integration strategy to illustrate some feasible ways to TAS³ enable existing applications (but which way is chosen, or if a totally different software architecture is used, is an implementer's choice)

Trustworthy and Secure (1/2)

- Operational, legal, and business model to ensure trustworthiness
 - Responsible entity, Trust Guarantor, ensures "buck stops here"
 - Legal framework developed hand-in-hand with architecture
 - Certification of software and deployments
 - Automated Compliance Validation keeps SPs in line
 - Manual audits complement automated approaches
 - Modeling network and its members provide consistent security configuration
- Legal concerns are built-in from the ground up
- Threat analysis to understand what we are defending against

Trustworthy and Secure (2/2)

- Technical

- Fully encrypted, fully digitally signed
- Fully pseudonymous design ensures maximum privacy
- Fully cross organizational federation model
- Explicit tokens based audit trail at all layers
- Explicit authorization at all layers
- Advanced trust and reputation management
- Model and ontology driven to ensure accurate implementation

Deploying TAS³ Architecture

- Set up Trust Network
 - Draft legal
 - Run some services, like audit bus and compliance validation
 - Outsource or run other services like discovery and IdP
- Join a Trust Network
 - Much of the infrastructure shared or already provided
 - Application integration
 - Buy and deploy TAS³ proxy or connector product, or
 - Adapt your application using TAS³ Standard API.
 - Outsource or buy/run some infrastructure services like IdP or PDP

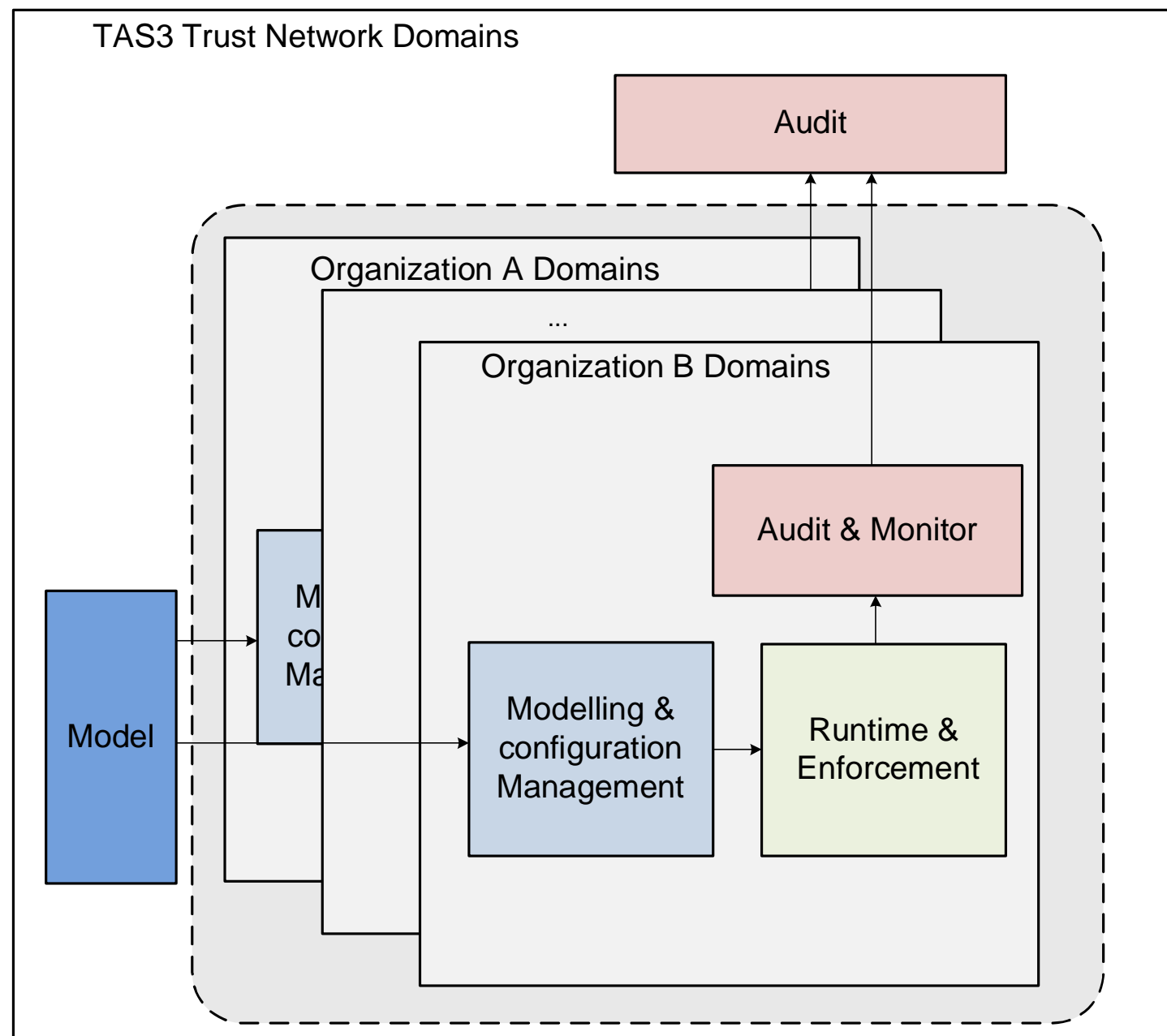
Thank You, Questions?

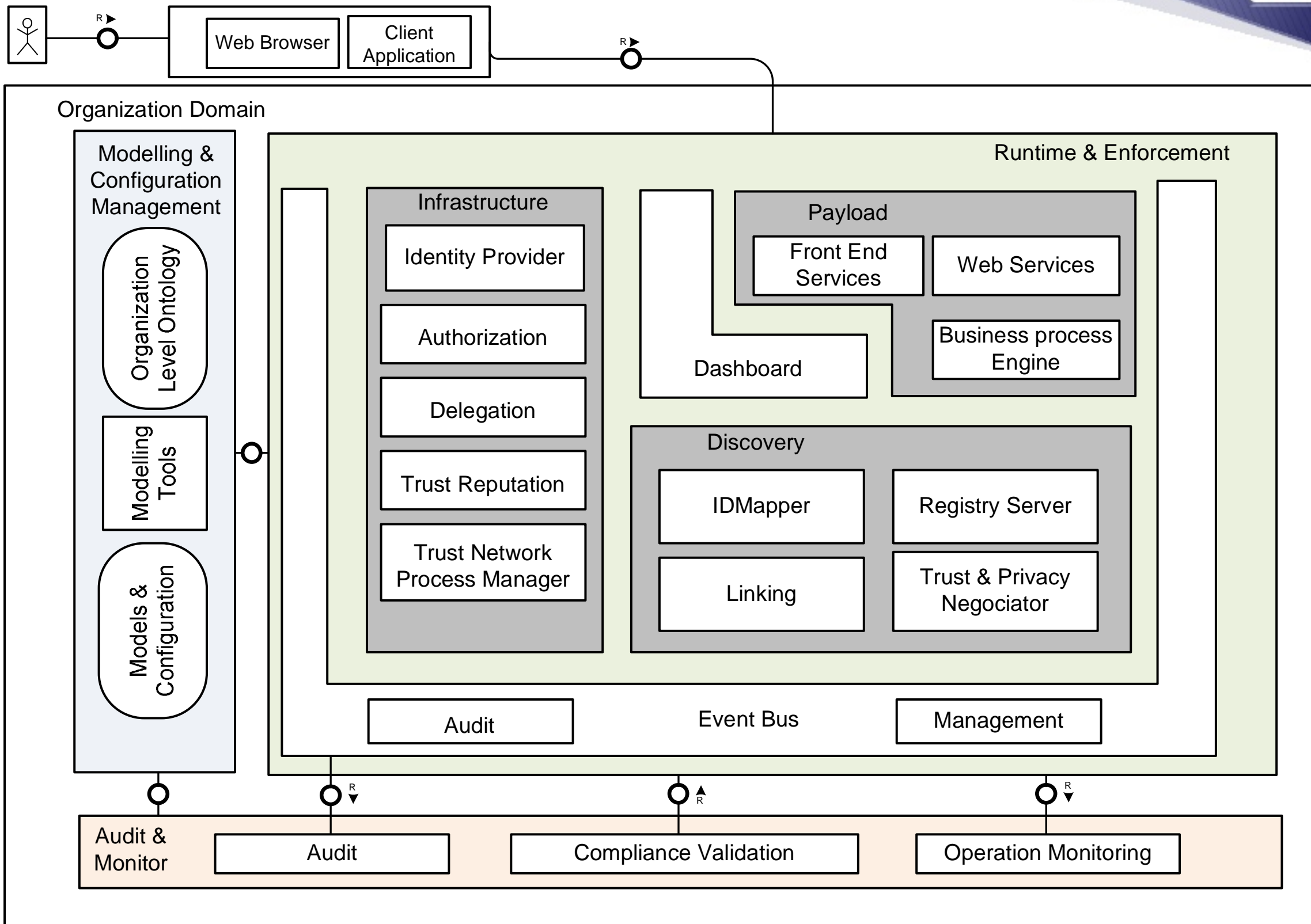
Sampo Kellomäki (sampo@symlabs.com)

+351-918.731.007

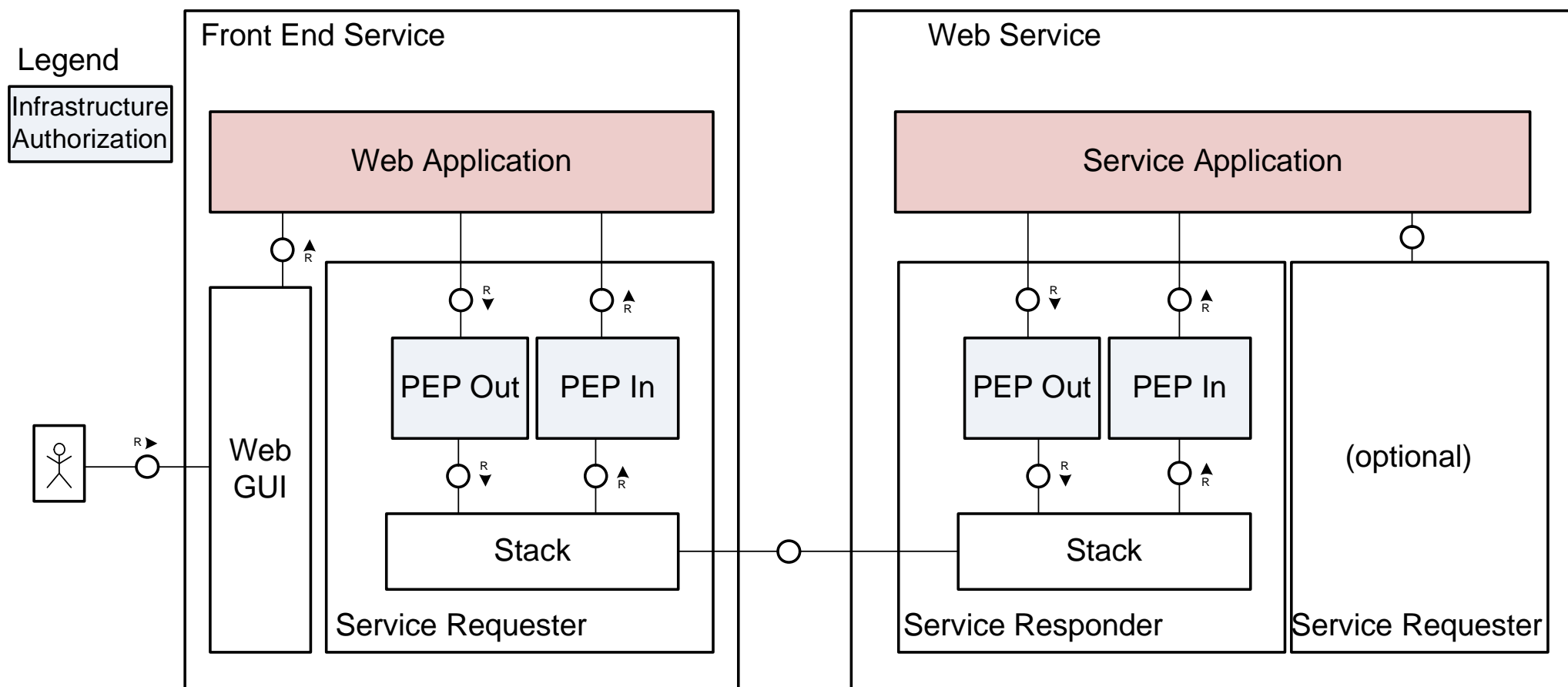
- www.tas3.org
 - Official dissemination website
- <http://zxid.org/>
 - Reference implementation of TAS³ Core Security Architecture
- <http://zxid.org/tas3/>
 - ZXID specific TAS³ news
- http://zxid.org/tas3/arch/tas3-deliv-2_1-arch-v17_2.pdf
 - TAS³ Architecture Document
- <http://zxid.org/tas3/arch/tas3-proto-v06.pdf>
 - Revised TAS³ API and protocol profiles

Architecture Drilldown

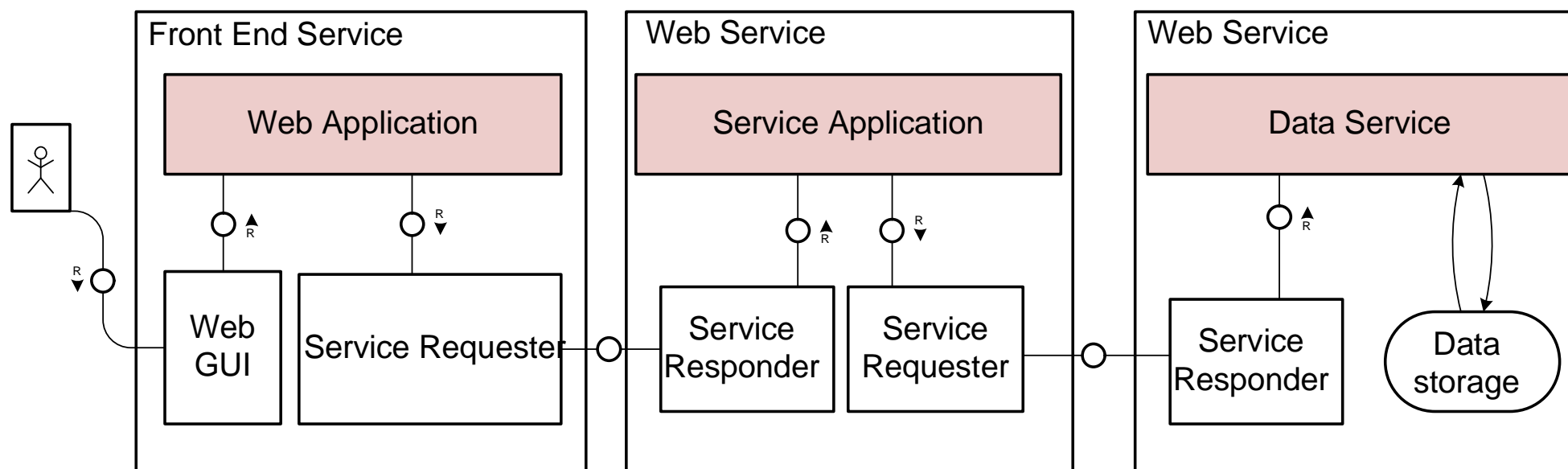




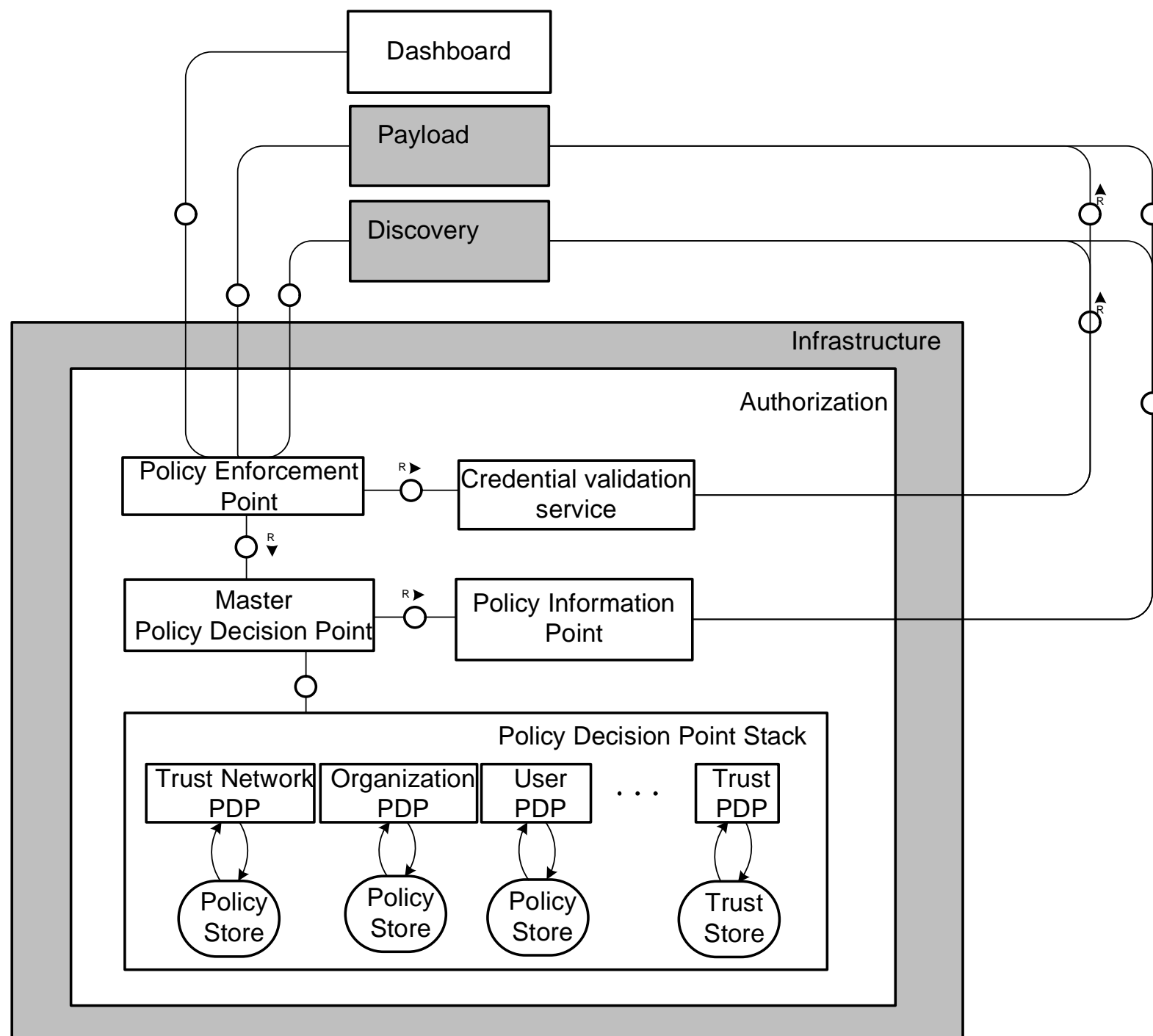
Web Service Authorization



Multi-tier Web Service Call



Details of Authorization



Legacy Integration

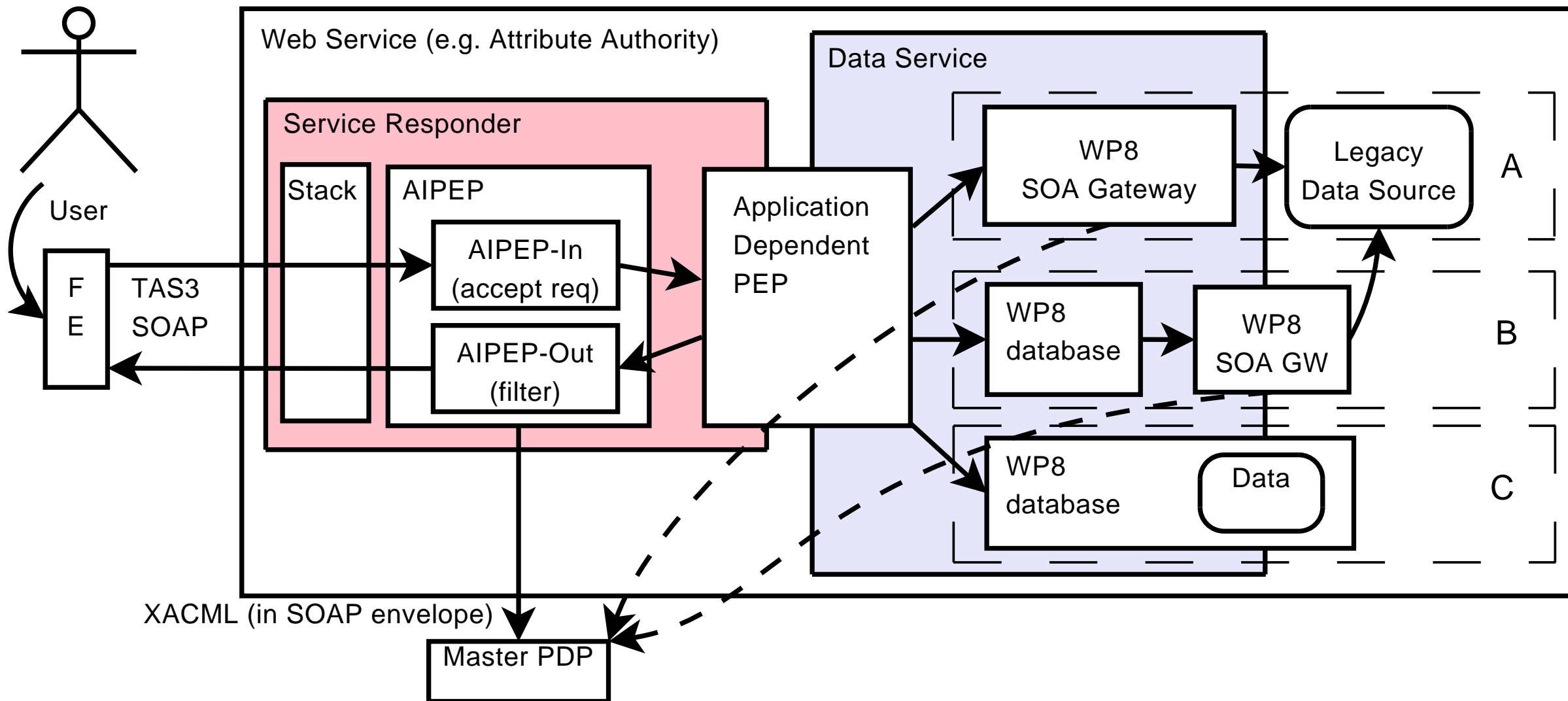


Figure 1: Application Integration using ADPEP and (A) WP8 SOA Gateway, (B) WP8 as frontend to WP8 SOA GW, (C) WP8 database.

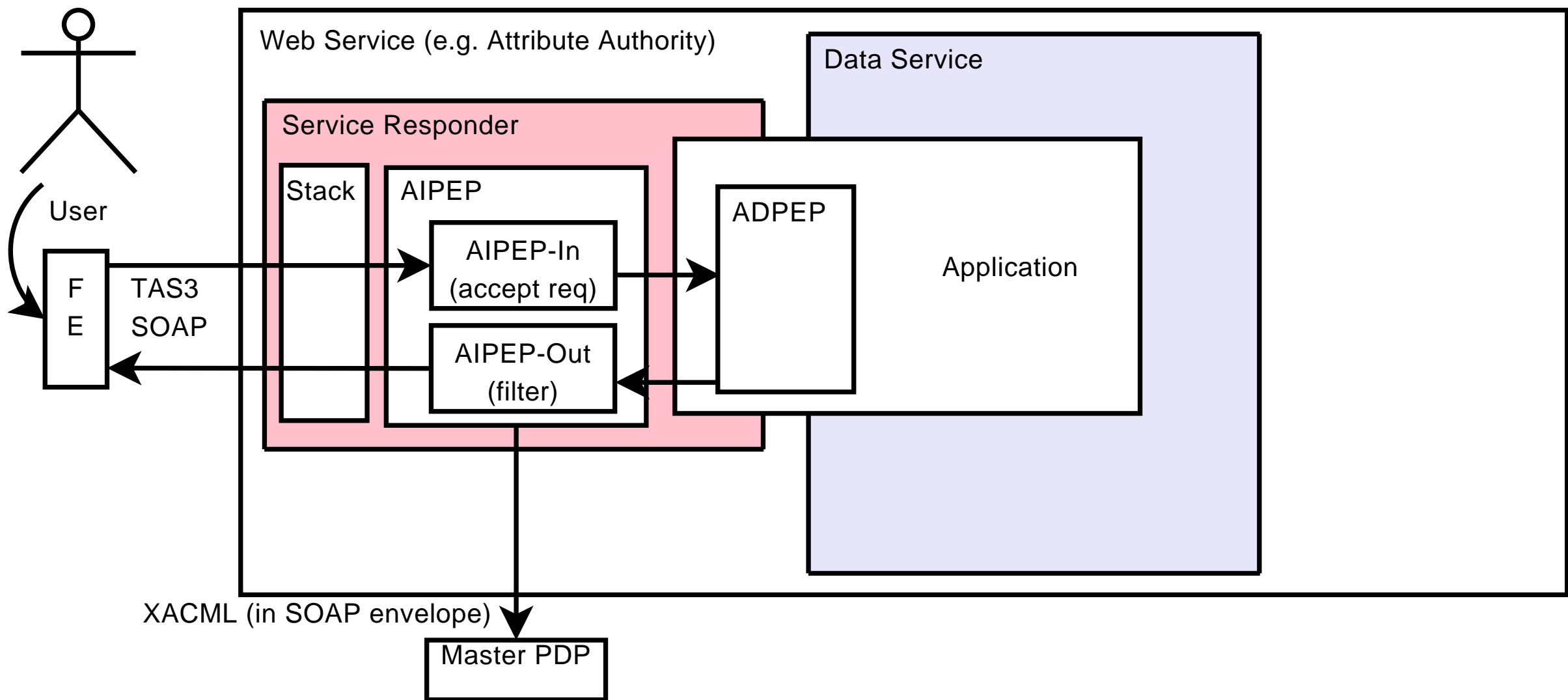


Figure 2: Application Integration: ADPEP implemented in application itself.

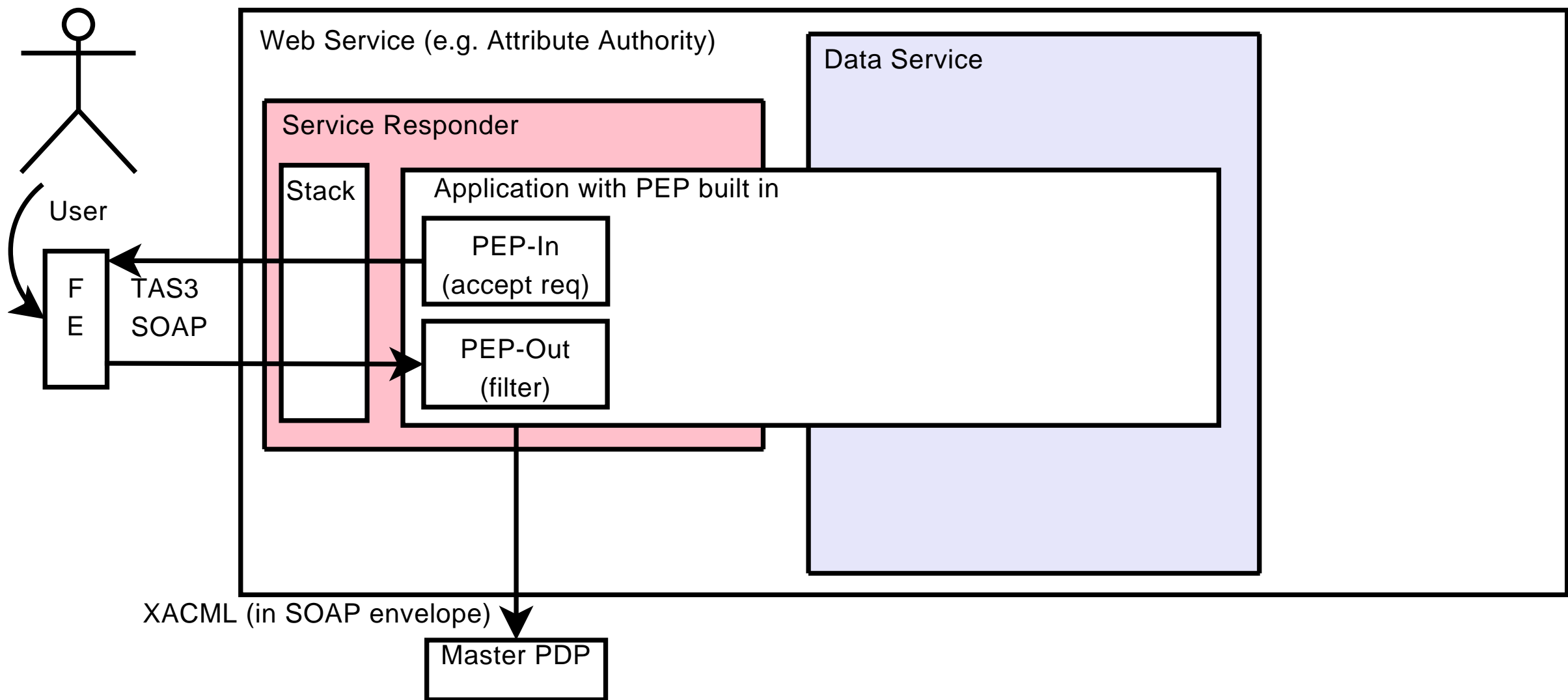
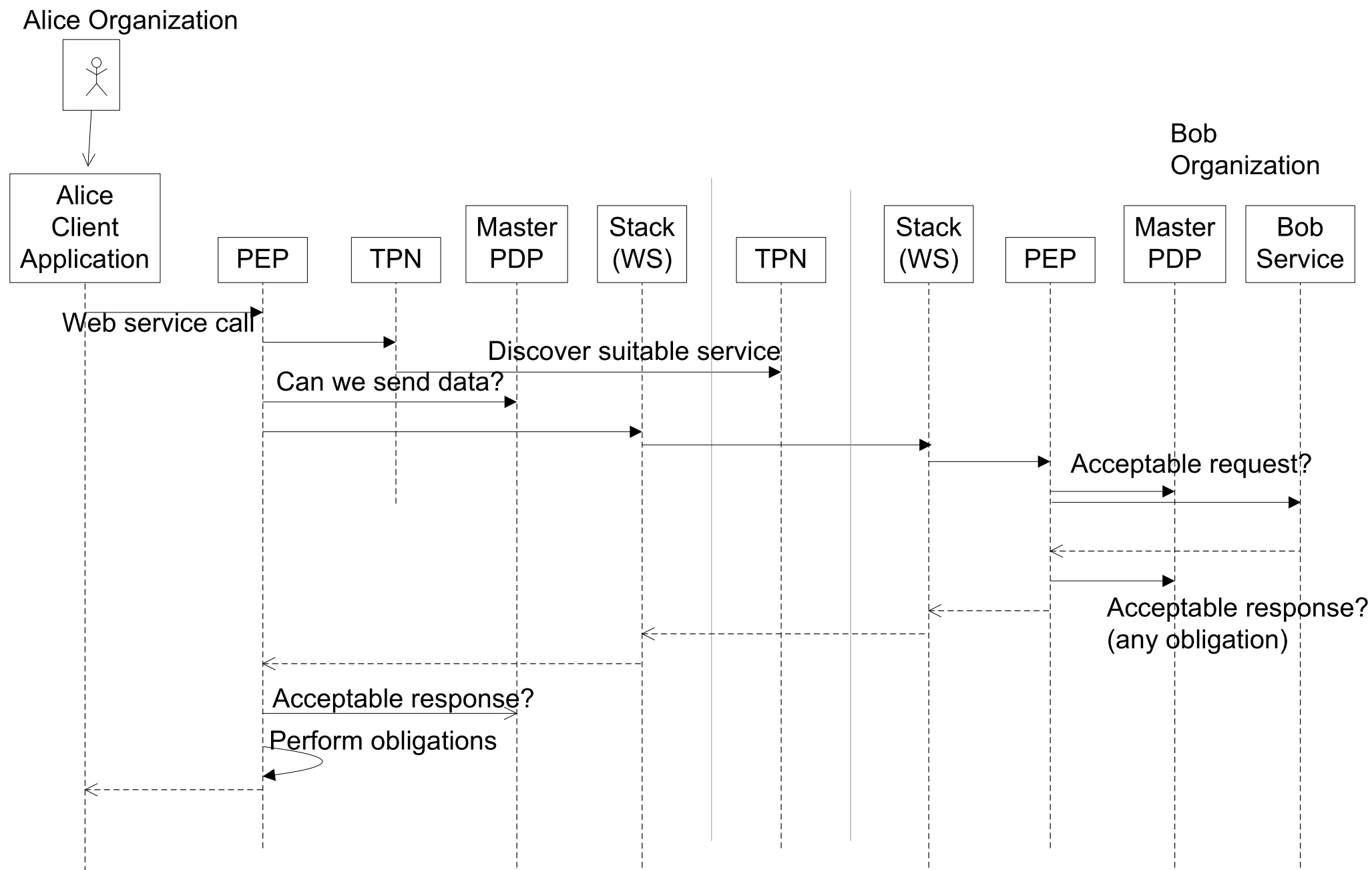
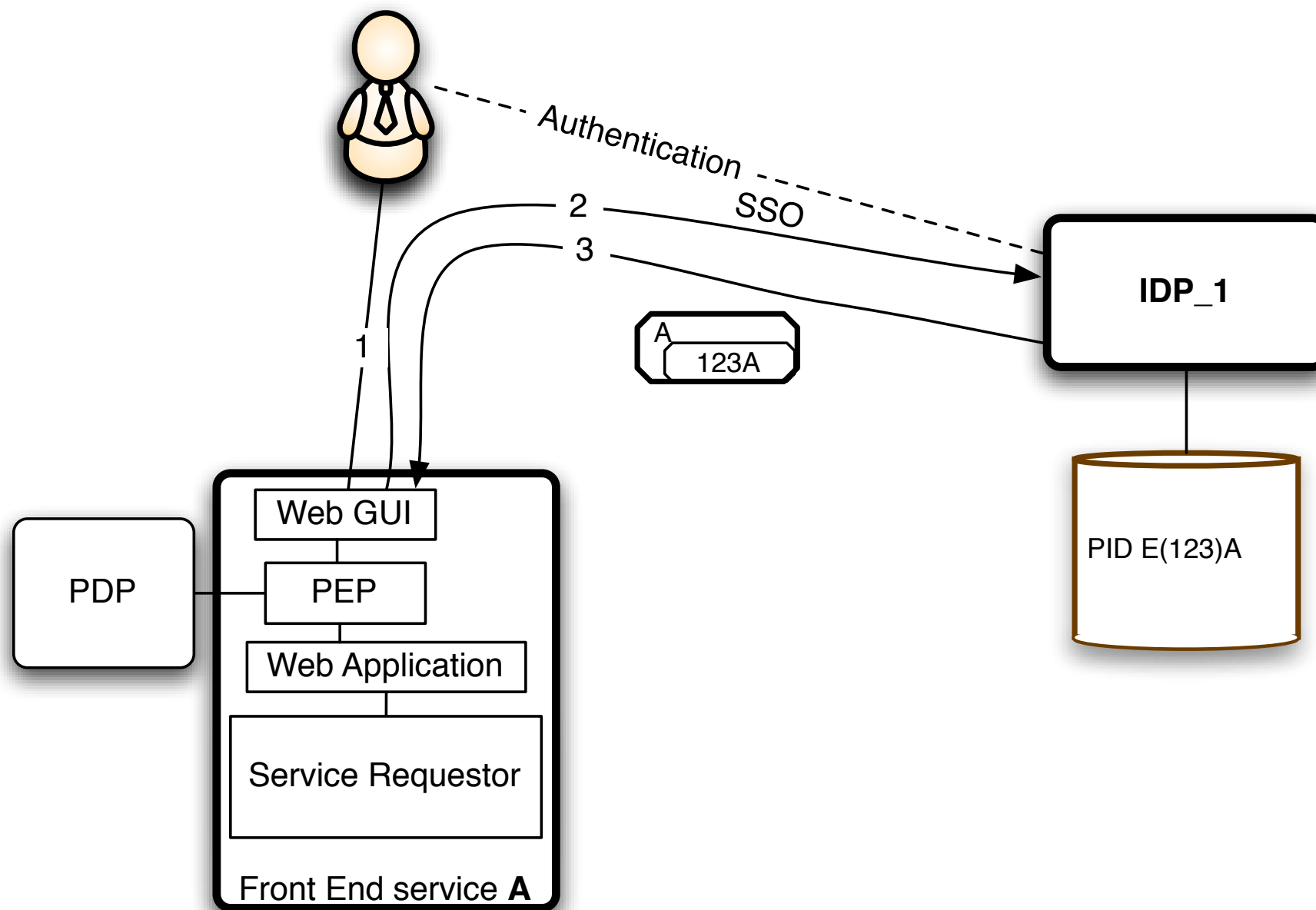


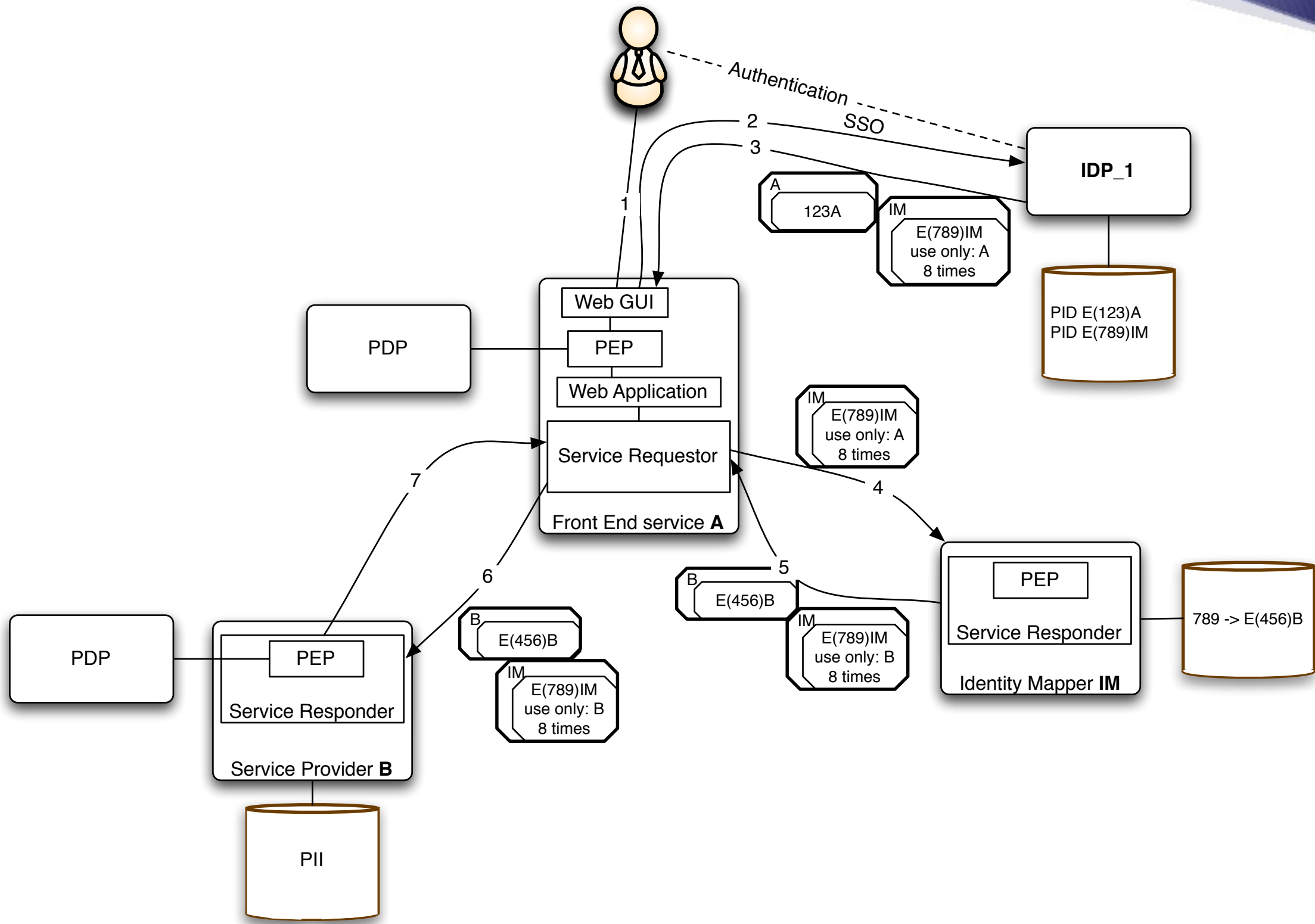
Figure 3: Application Integration: PEP implemented directly in application.

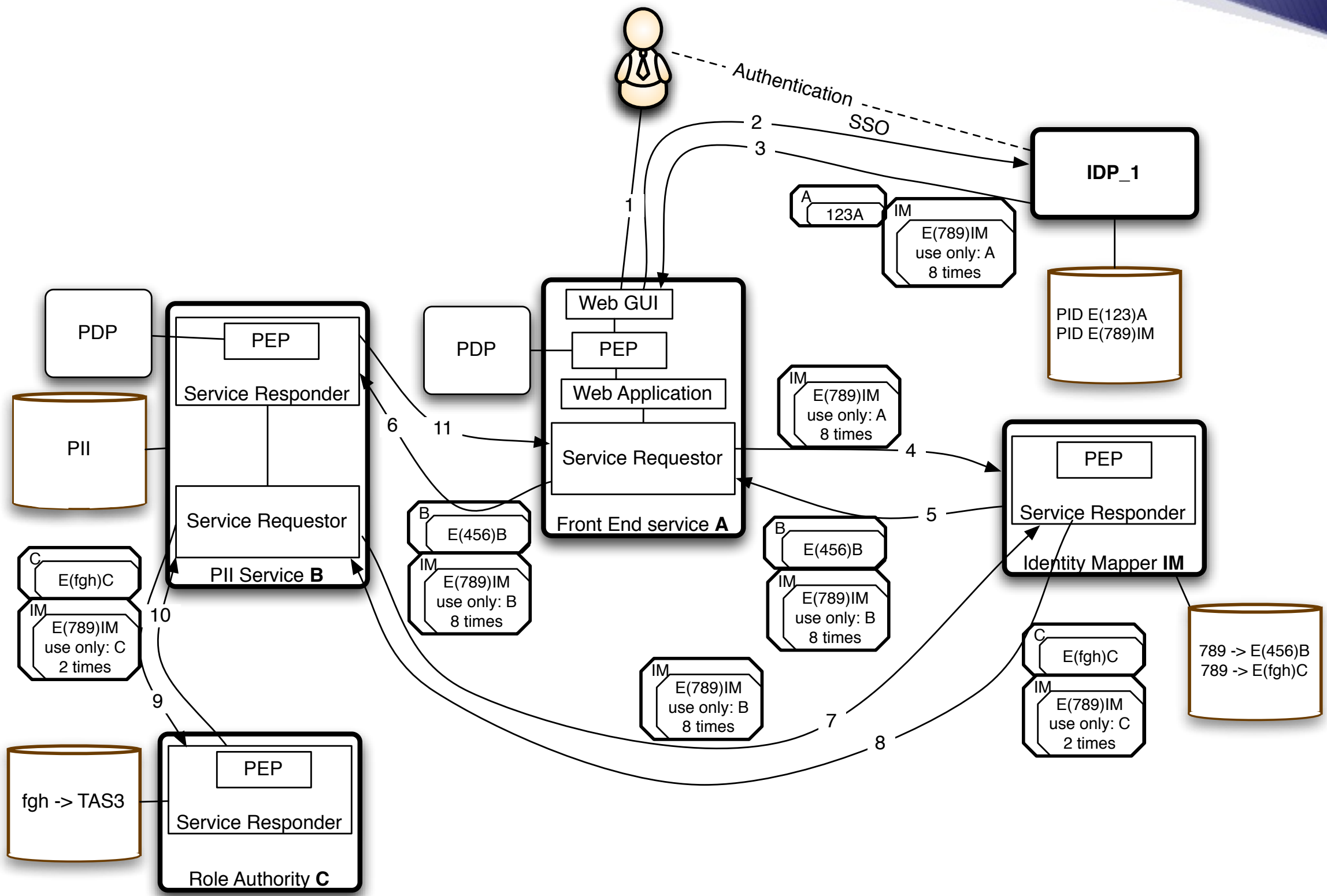
Steps of a Web Service Call



Core Security Architecture Flows







Acronym Expansion

TG Trust Guarantor, the organization that operates TN ("Summit")

TN Trust Network

IdP Identity Provider (SAML role, aka authentication authority)

SP Service Provider: a member organization of TN that operates Frontend and/or Web Services

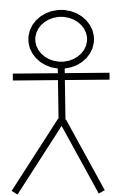
Disco Service discovery, sometimes specifically identity enabled service discovery such as Liberty ID-WSF Discovery Service.

DB Dashboard, a web GUI for viewing audit records, work flow status, and/or viewing and editing privacy settings and permissions.

FE Frontend, here means web site, i.e. SP

WS Web Service, SOAP based machine to machine communication. Sometimes specifically Identity enabled web service, e.g. Liberty ID-WSF based WS.

Summit



TAS3 CoT Model

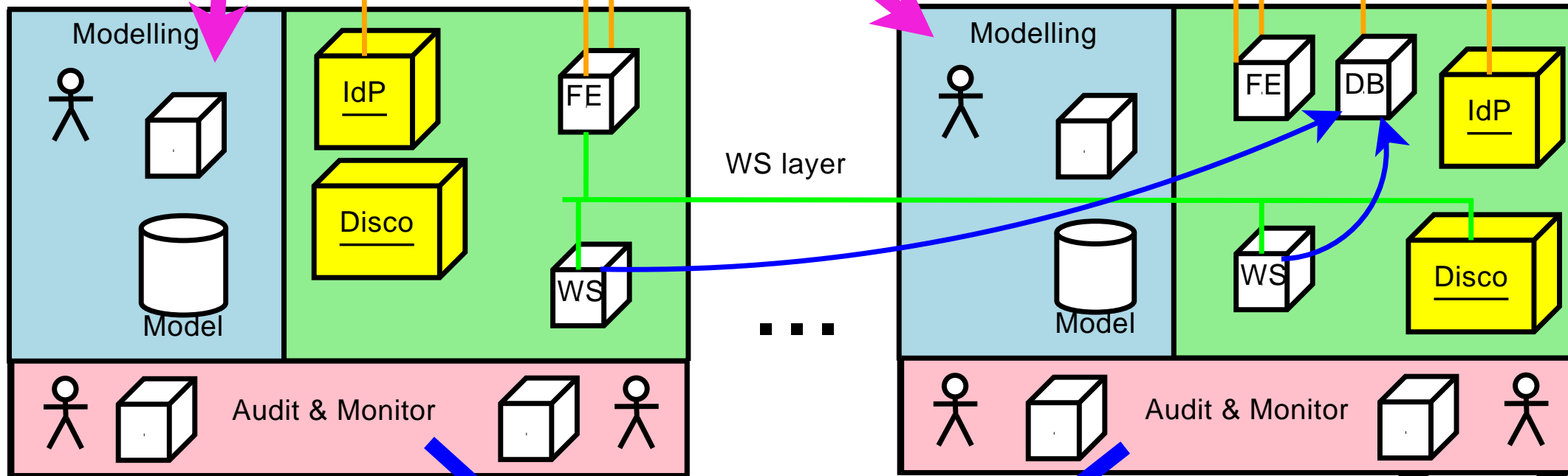
SSO sub CoT B



SSO sub CoT A

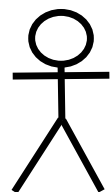


Core



Org A
(Context A)

Org B
(Context B)



TAS3 CoT Audit

