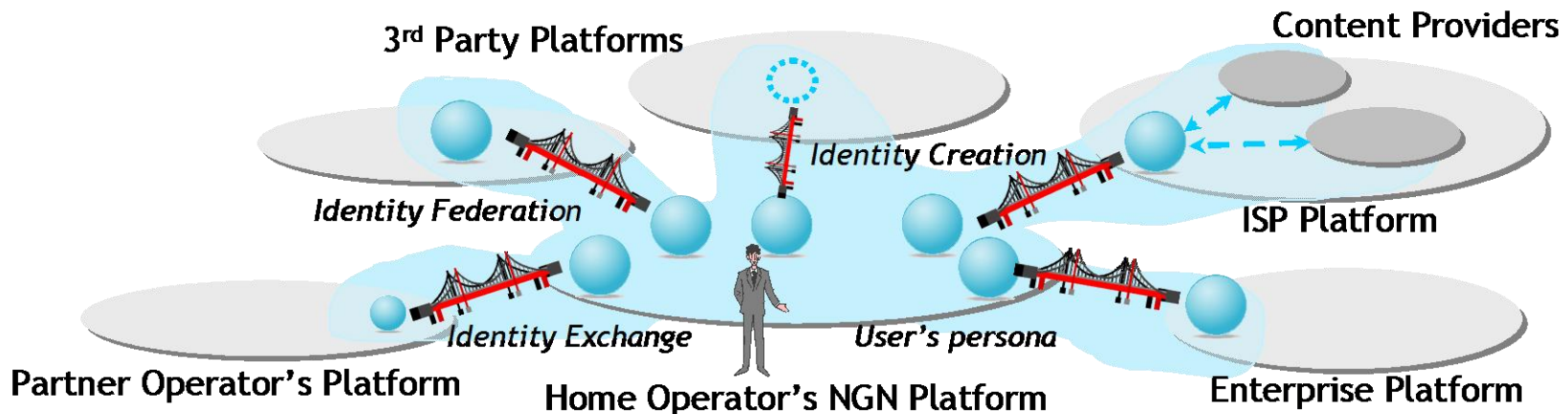




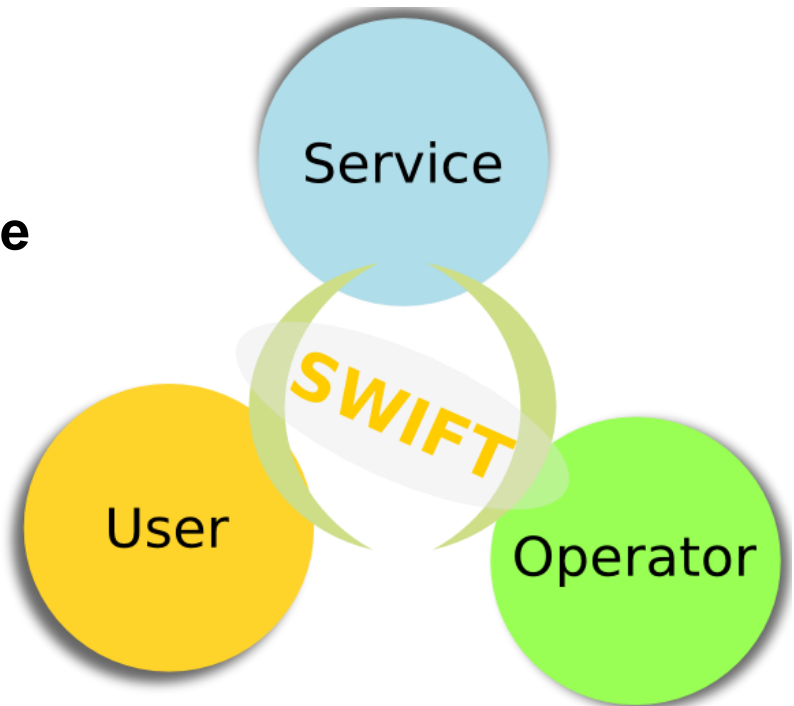
A cross-layer approach to Identity Management solution in networking: The SWIFT approach

Antonio F. Gómez Skarmeta
skarmeta@um.es
University of Murcia

- ▶ Identity Management (IdM) solutions are still limited in scope.
- ▶ Users need:
 - **ubiquitous access** to the digital world.
 - **simple** and **privacy enable access** with a minimum number of separate service contracts.
 - simplify the multiple **IDs** and **authentication methods**
- ▶ Build a cross-layer identity framework with emphasis on networks and services → identity becomes a key convergence enabler & bridge for various platforms



- ▶ SWIFT leverages Digital Identities to:
 - **Solve** identity fragmentation
 - **Extend IdM systems** for **multiple services** at **different network layers** using **the same ID**
 - **Bridge platforms** and **layers**
 - **Converge** networks, services, applications and content
 - **Connect** operators, service providers, micro-operators, even **users as providers**



Identity Management Systems

Stratum

Today

Future – i2010/eldM

Societal/
legal

Several IdM
concepts

Several eldM-
based concepts

Service

Several digital
IdM-based
concepts

Several
eldM-based
concepts

Transport

Some digital
IdM-based
concepts

Several
eldM-based
concepts



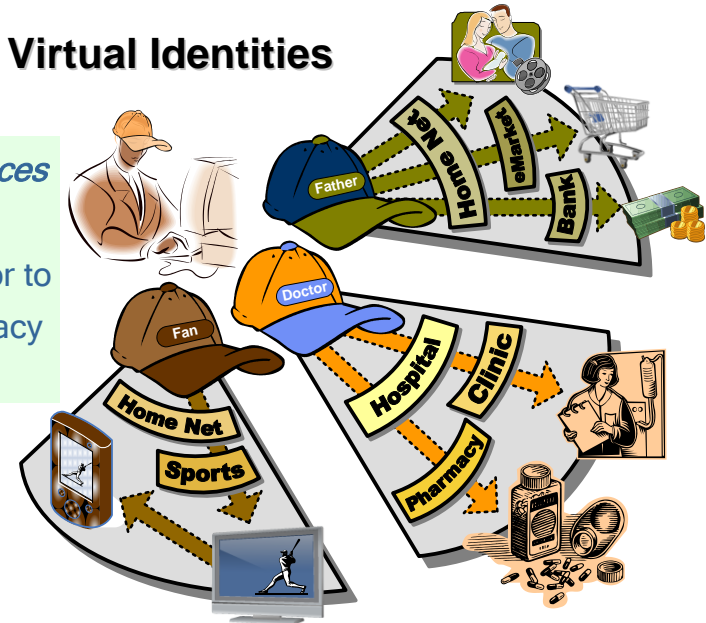
- ▶ Vertical integration of identity, privacy, trust and security across layers
- ▶ New identity-centric user schemes supporting different levels of information access control.
- ▶ Methods and techniques on how users are identified but preserve privacy
- ▶ Identity-based mobility solution: Adaptation across devices, services and networks.
- ▶ Semantic interoperability of eIdM systems – of legacy and possibly different instances.

Virtual Identity Concept

- ▶ multiple personae
- ▶ identity-based privacy across layers
- ▶ data model for new & dynamic business
- ▶ Cross-layer usability features
 - ubiquitous connectivity
 - user-centred mobility
 - SSO based on vertical & horizontal federation principles
- ▶ Separate management from resolution of identities at all layers

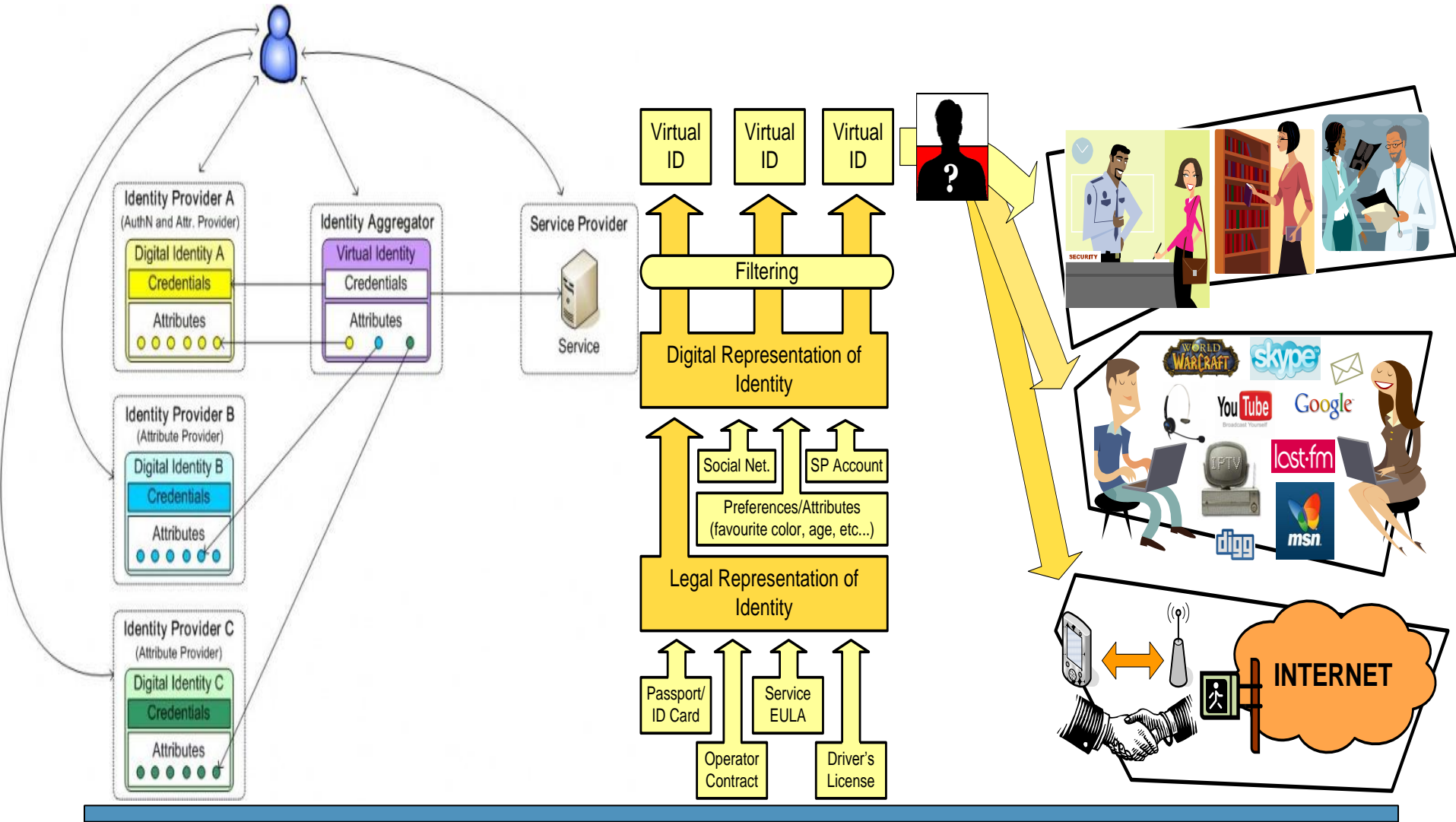
SWIFT: Virtual Identities

One person has many *faces* to the digital world in different usage contexts or to separate roles or for privacy or billing reasons



These faces are people's avatars or Virtual Identities (VIDs) → these must be unlinkable even if some attributes are shared between them

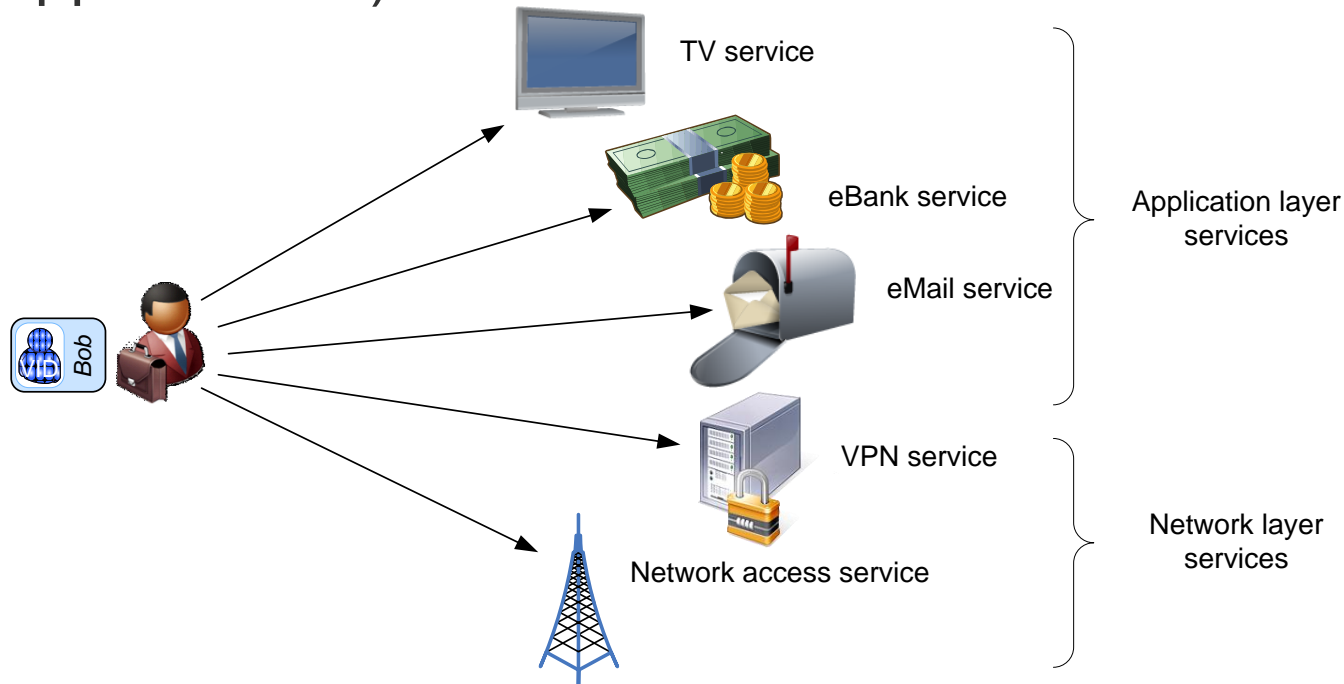
The Vertical Axis



- ▶ The main SWIFT objectives are:
 - Cross-layer Identity management in scenarios where network access requires authentication
 - **Also provides cross-layer SSO**
 - Virtual identities allowing the aggregation of attributes from heterogeneous sources
 - **i.e. using different technologies**
 - Advanced access control policies for privacy management
 - **Distributed policies**
 - **Deductive policies**

Cross-layer approach

- ▶ SWIFT addresses identity management across layers (vertical approach)
 - Virtual identities are managed homogeneously among different services on different layers (network, application...)



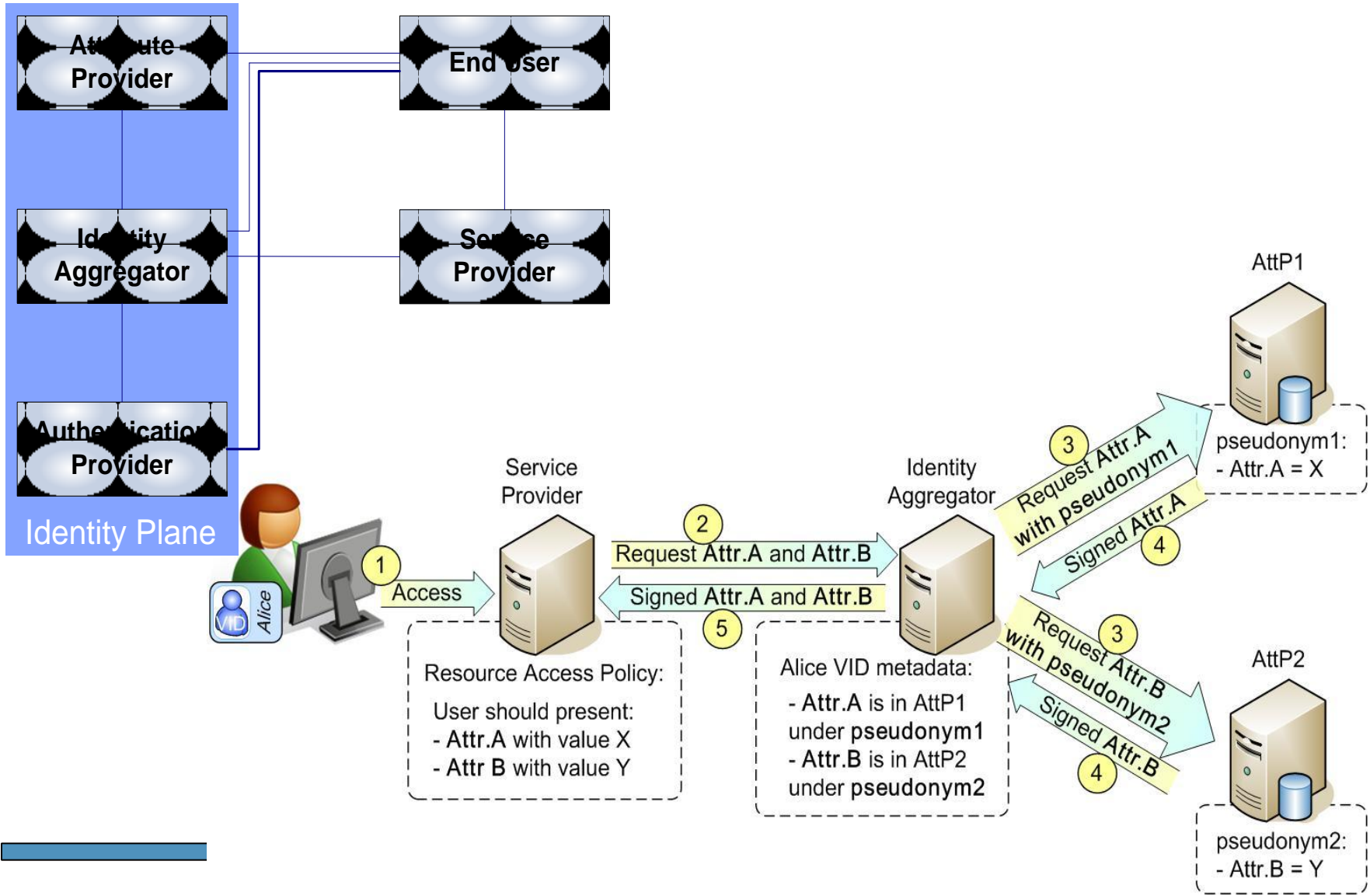
- ▶ Additionally, SWIFT also includes the following “add-ons”
 - LoA management
 - Card-based model
 - Virtual terminal support
 - **Identity moves among user’s devices**
 - Service bound access
 - **The service can pay for the user's network access**

▶ **SWIFT defines an IdM architecture that:**

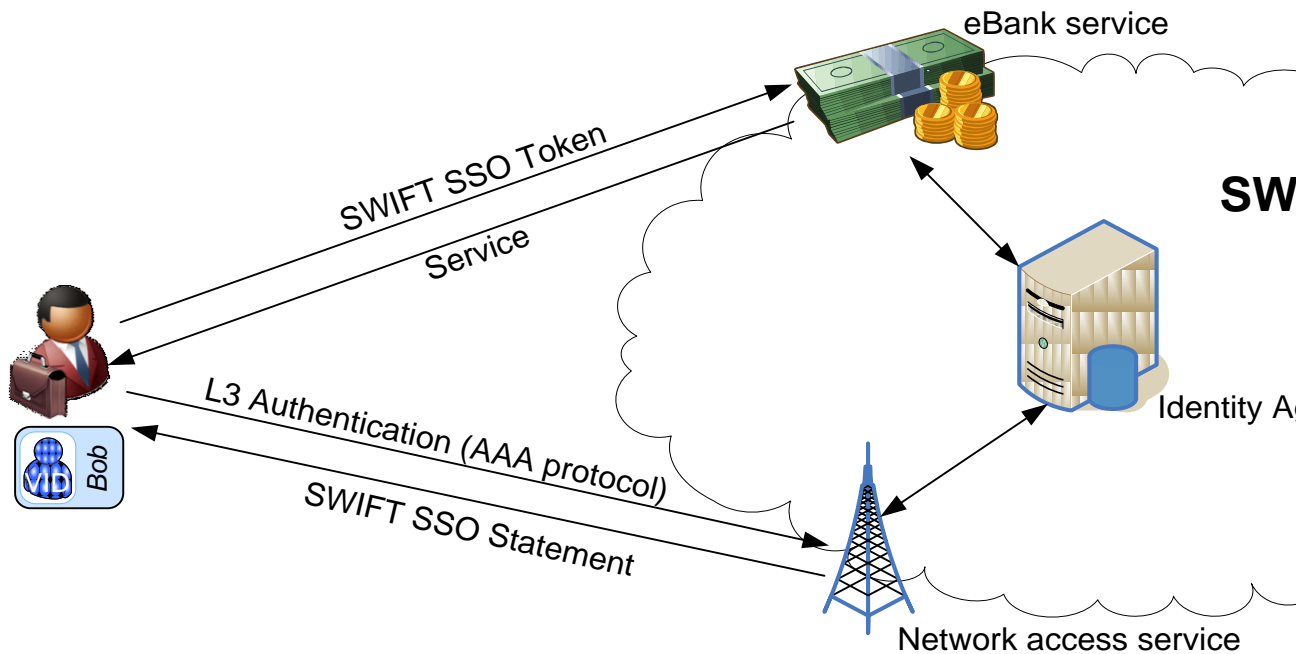
- Allows full distribution of Identity information and functions keeping a hierarchical control
 - **Distribution includes attribute provisioning, authorization and policy management, authentication and billing**
- Manages interoperability among different existing IdM technologies
- Provides a distributed access control framework
 - **Distributed policy management and actuation framework, which includes the distributed processing of policies.**

- ▶ **Identity Aggregator (IdAgg)**
 - The Identity Aggregator is responsible for the management of User Profiles, Virtual Identities, SSO mechanisms and statements, etc.
- ▶ **Authentication Provider (AuthNP)**
 - An AuthNP provides methods to verify the EU's authenticity.
- ▶ **Attribute Provider (AttP)**
 - An AttP manages information of the EU in terms of attributes, which can be related to specific services or for general purpose.
- ▶ **Service Provider (SP)**
 - A SP provides some kind of service to the EU. This role also includes the network service provider.
- ▶ **End User (EU)**
 - The EU makes use of the services provided by the IdM system (IdAgg, AuthNP, AttP) to get access to the services offered by SPs.

SWIFT roles



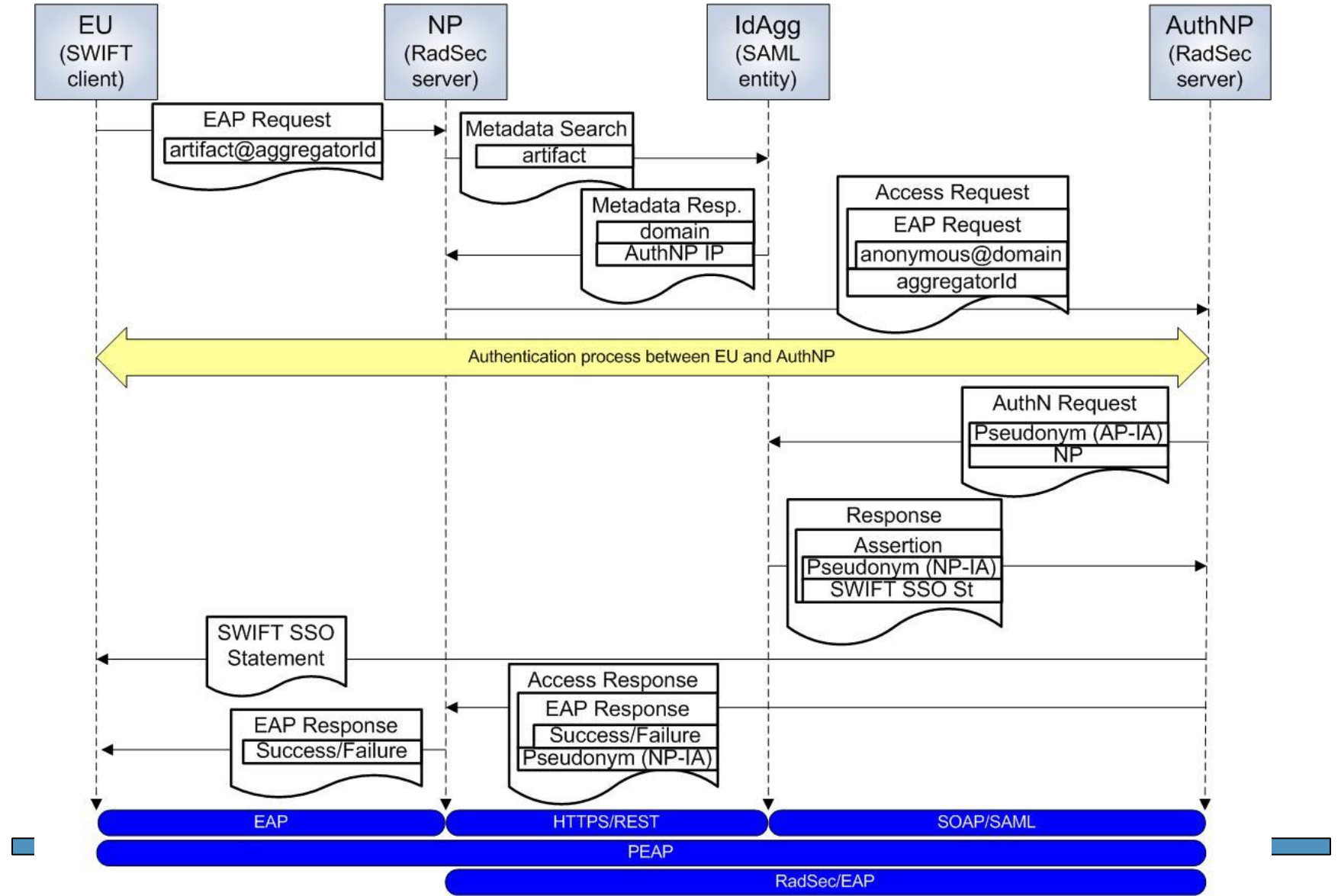
- ▶ SWIFT addresses identity management across layers (vertical approach)
 - The idea is, for example, to use the same virtual identity to access a network service than to access a web service
 - **Benefits from the SSO mechanisms**



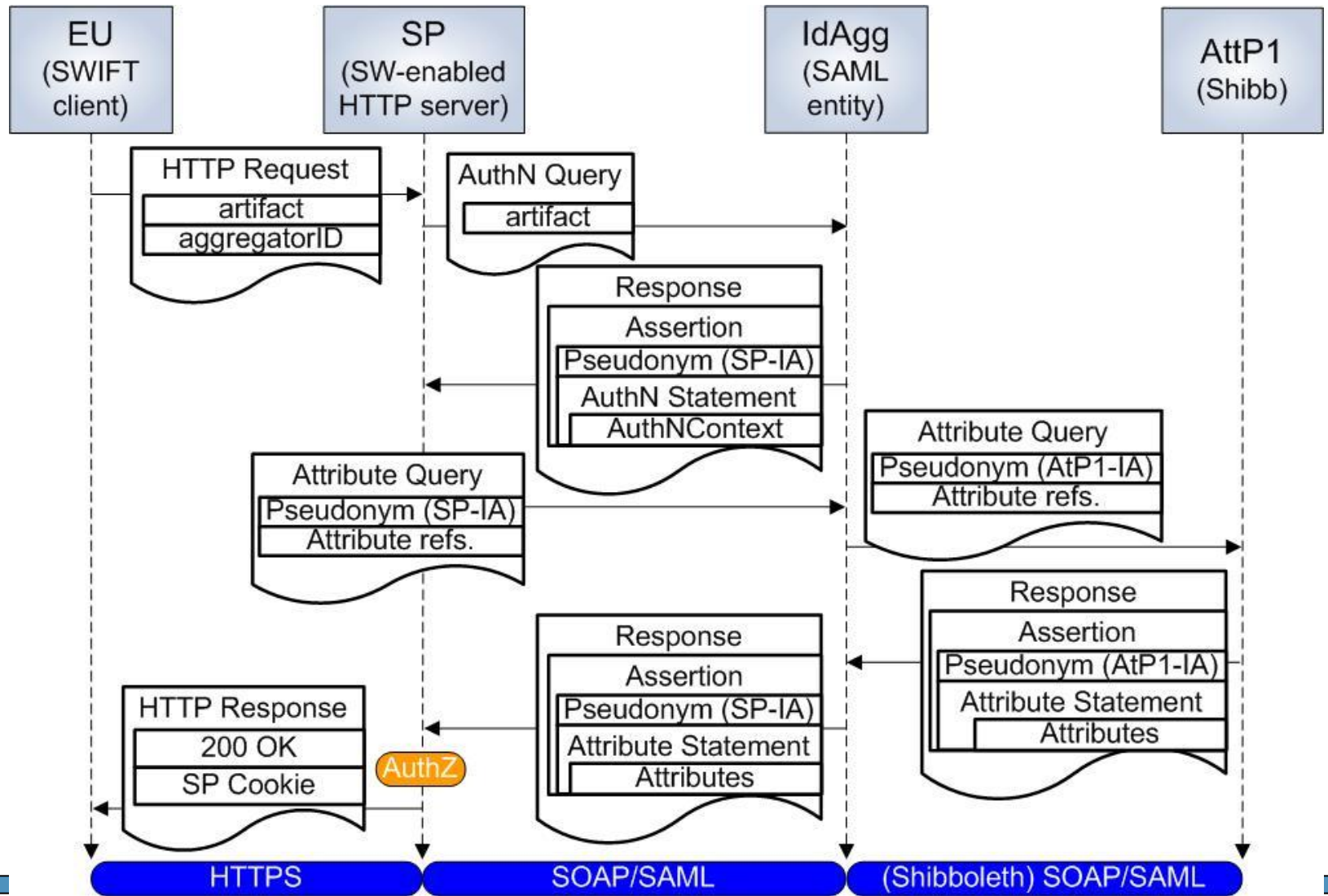
SWIFT instantiation

- ▶ The functionality of the SWIFT framework can be incorporated into the already existing architectures and protocols
- ▶ Sometimes the existing elements can be used to provide the SWIFT functionality:
 - Network authentication using current AAA deployments
 - **Using RadSec, Diameter...**
 - Web layer authentication based on current IdM solutions
 - **Using Shibboleth, OpenID...**
 - Attribute management based on solutions at different layers
 - **Using Shibboleth, SAML, Diameter...**
- ▶ Sometimes the SWIFT functionality can not be incorporated into any existing element
 - New elements should be included to provide the missing functionality (e.g. the IdAggr)
- ▶ SWIFT serves as intermediary or *glue* to perform cross-layer and federated identity management, using the different already existing identity *silos*
 - E.g. It is possible to use RadSec to authenticate at network layer and after that access a web service, obtaining some needed attributes from a Shibboleth IdP and some others from an OpenID IdP

Example of instantiation

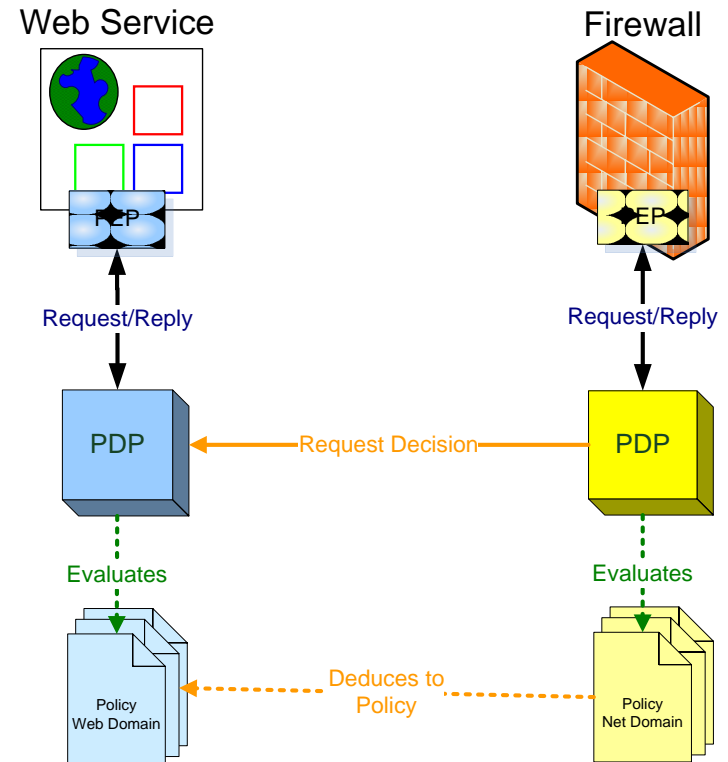


Example of instantiation

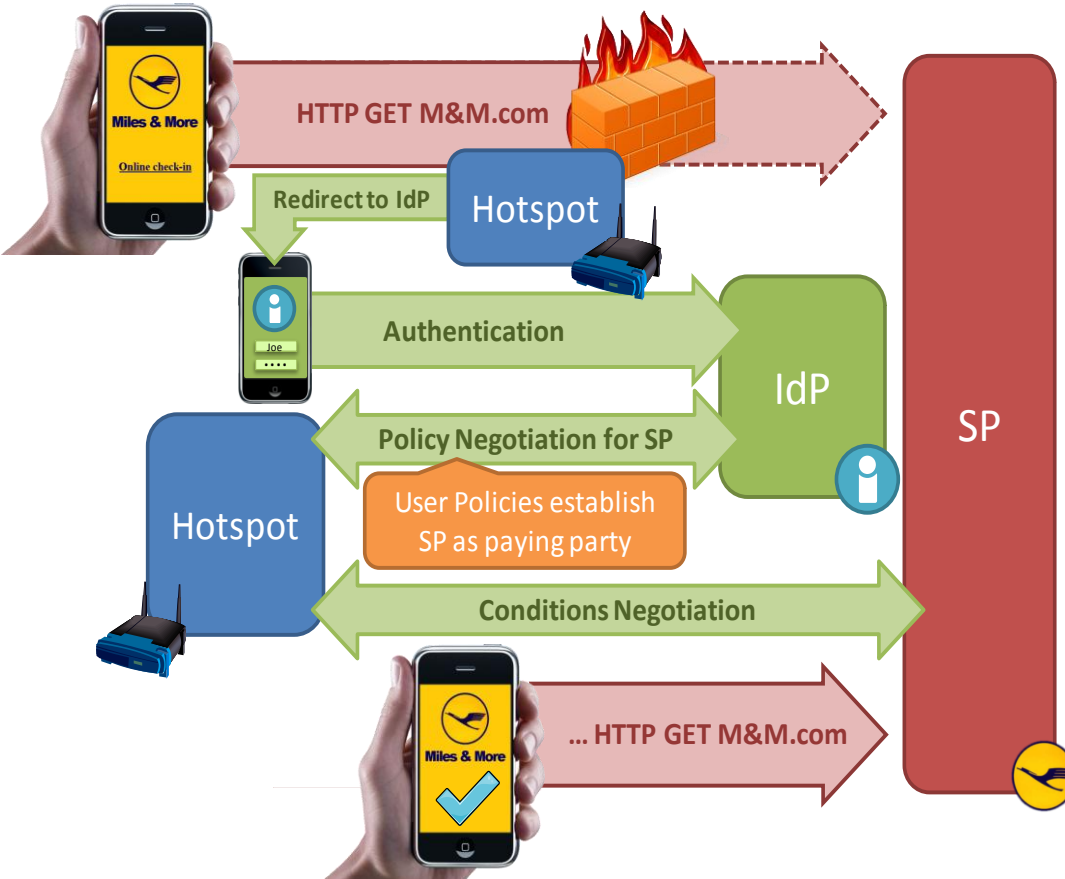
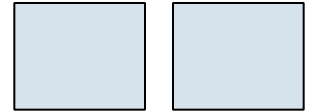


Deductive Policies

- ▶ Several distributed PDPs can coordinate to take a whole authorization decision
 - Using rules defined for one domain to deduce decisions that are valid in other domains
- ▶ Example: A network operator can deduce an access control decision based on an authorization decision from another domain/service
- ▶ XACML extensions defined to support deductive policies



New business: Service Bound Access



- User picks M&M bookmark and selects nearby Hotspot (could be automatic)
- IdP knows SP's identity through the Hotspot's policy query
- IdP knows the user has a subscription with the SP

SP is charged for the user's network access based on policies supplied by the IdP

- Concept benefits:
 - **Profit:** Hotspot is accessed by more customers
 - **Increase customer base:** SP gains more users; value-added service
 - **Trust:** Users get a consistent, simple view of the service

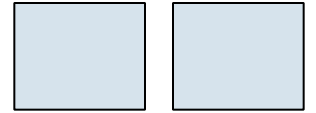
- ▶ Goal is to bring Identity Management to the network and services in a common approach
 - Enable access and reachability across domains
 - Make Identities of people, services, things, software modules a part of the future Internet architecture
- ▶ The Future Internet could
 - *Identity* as the *end point* of communication
 - whether user, service, thing, device or software module
 - *Identity* as the *convergence* layer
 - Privacy can be dealt with vertically thus reducing the danger of conflicting policies and mechanisms
 - *Identity* as an enabler for Intent-based communication
 - Support access, (non-) reachability, ubiquity

ICT Trust & Security FP7-ICT-2007-1 ICT-1-1.4

Secure Widespread Identities for Federated Telecommunications

Grant agreement no.: 215832

<http://www.ist-swift.eu>



Thanks