

# Sustainable Identity Framework for the Future Internet

Amardeo Sarma, NEC

# Background & Motivation

- Interaction between players getting increasingly messy
  - Access complicated by conflicting technical and business solutions
  - Identity management solutions are fragmented
  - Paid and free use need to be technology-independent and easy
- Privacy and enterprise data protection are major issues
  - Privacy can be a key selling point in Europe
  - Marketing of European privacy protection even beyond Europe – e.g. in the US that has none → data storage and Id management in Europe
- Identity Management Framework as an all-layer enabler
  - Leverage results of EU FP6/FP7 projects for immediate deployment in the PPP → Primcluster has provided a base for an Identity Framework as a generic enabler of the PPP core platform

# What is Needed: Issues

- Use of Identities is to serve users, business and society:  
Independence from specific technology solutions: bridges
- Support user intentions without knowing the architecture →  
next generation of *single-sign-on* and *cross-layer security*
- Use of multiple (also public) devices, possibly simultaneously
- More controlled privacy than today: Not letting technology dictate level of privacy (IP addresses in the network)
- The capability to establish zones of privacy as in real life
- Controlled linkability and identity disclosure for accountability
- Capability of “limited identities” for minors
- Mere conduit, ignorance of content to protect enterprises:  
knowing content: law suits for allowing illegal content

# Privacy: Follow OECD guidelines

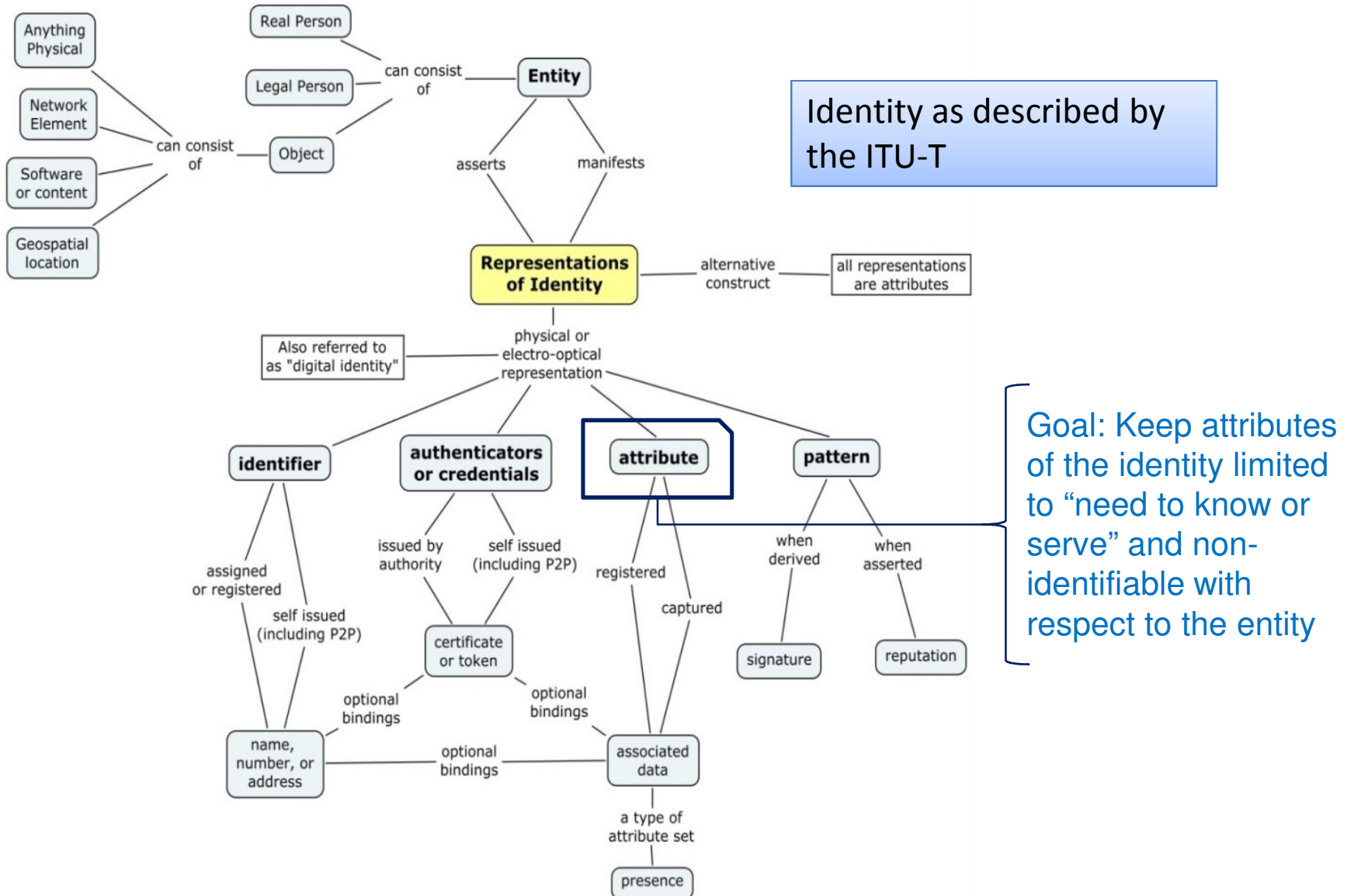
- Goal: Protection of personal data
  - Personal data: any information relating to an identified or identifiable individual (data subject): “Personally Identifiable Information” (PIM)
- OECD privacy guidelines (relevant principles)
  - Collection Limitation Principle
  - Data Quality Principle
  - Security Safeguards Principle
  - Openness Principle
  - Individual Participation Principle
  - Purpose Specification Principle (Limitation Principle)

# Identity Definition

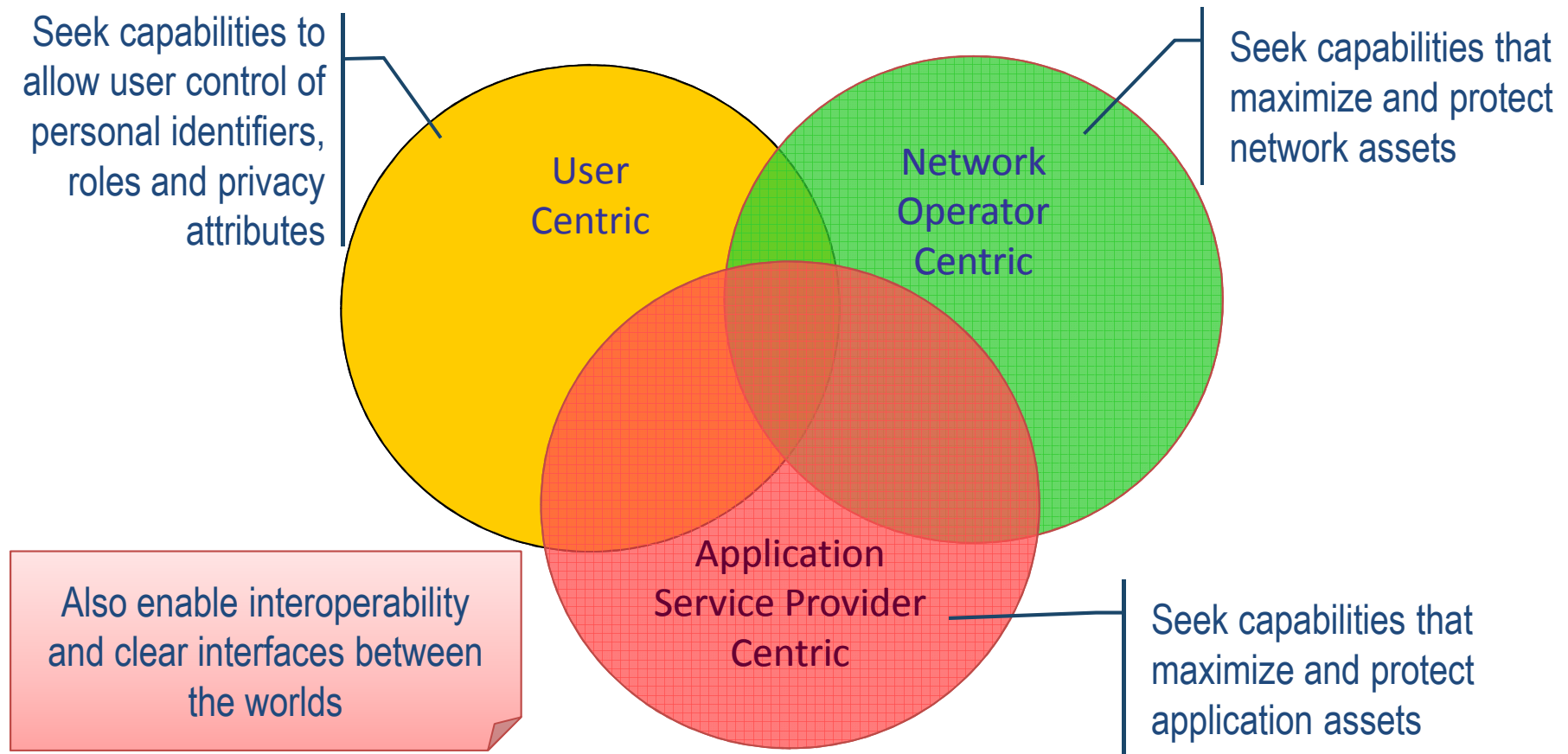
## → Identity

- ❑ The attributes by which an entity is described, recognized or known (ITU-T)
- ❑ The fundamental concept of uniquely identifying an object (person, computer, etc.) within a context. (OpenGroup)
- ❑ A set of claims made by one party about another party. Claims are typically conveyed in Signed Security Tokens (Microsoft)
- ❑ The essence of an entity. One's identity is often described by one's characteristics, among which may be any number of identifiers [Liberty & OASIS]

# Privacy of Identity data (attributes)



# Tradeoff between different Worlds



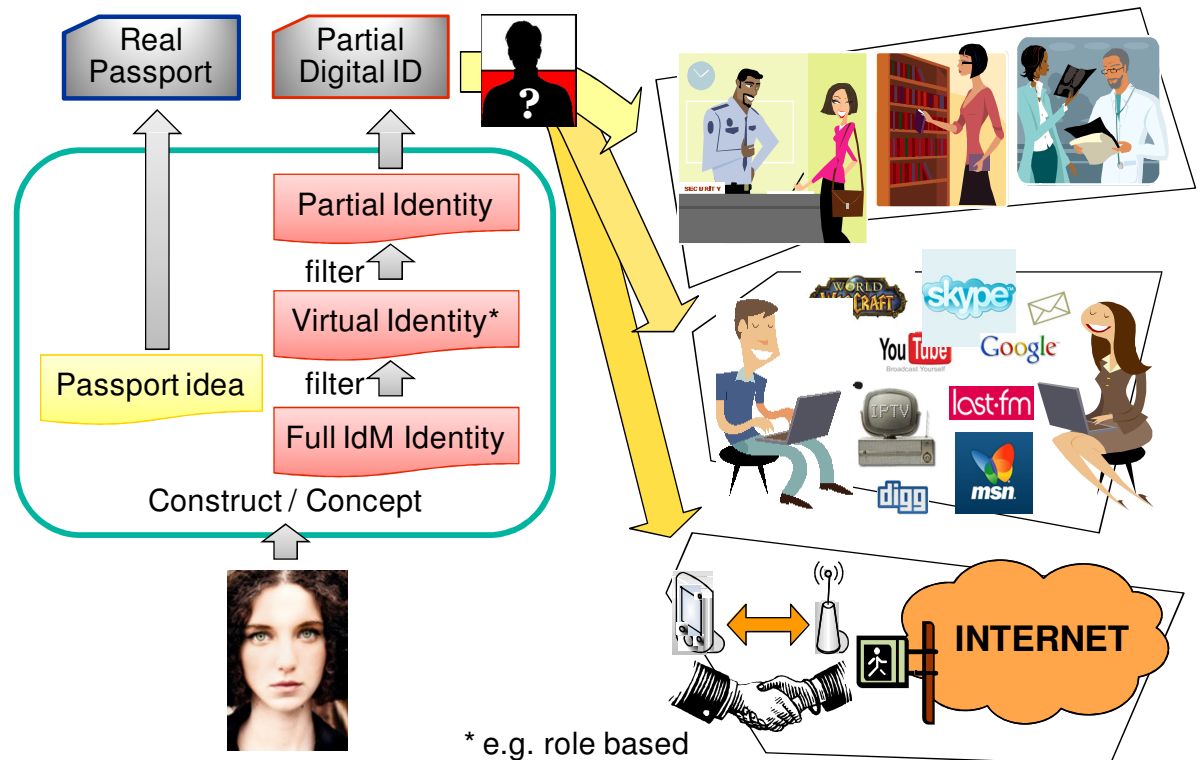
Source : Report on Identity Management Use Cases and Gap Analysis, ITU-T FG IdM

# Needed Privacy Approach



## Best of two worlds

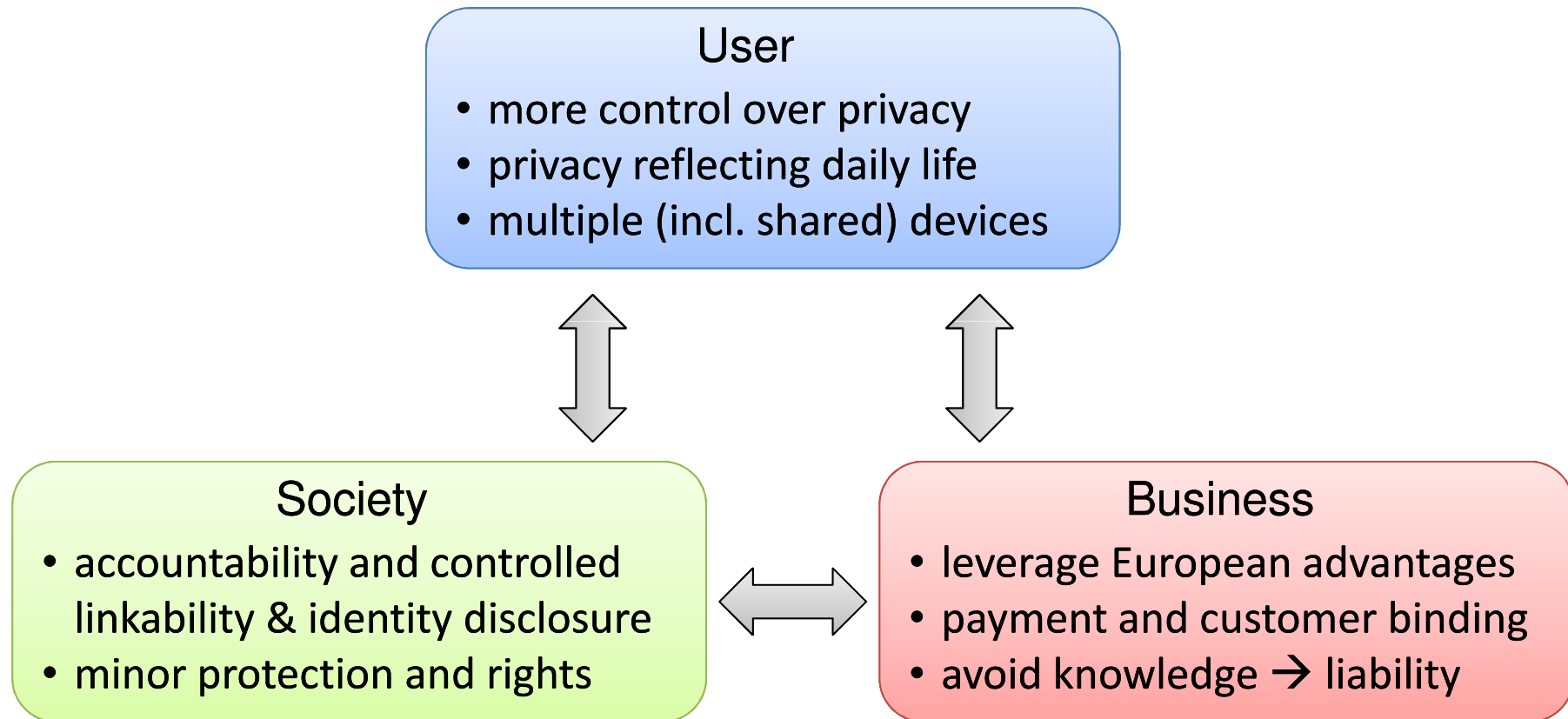
- Make it impossible (difficult) to link partial ID to entity → privacy
- Maximize ability of partial ID to support functions & operations → functionality



# PPP

- *"The proposed Public Private Partnership (PPP) will enable Europe to consider supporting the sector driven requirements, such as identity management, scale and user acceptability, by using known and emerging technologies (...) to providing entire solutions for societal challenges" (White paper on the Future Internet PPP Definition, January 2010.)*
- Core platform should include *"Trust and Identity capabilities enabling end users and service providers to be identified globally in a trusted manner including lawful interception."*

# Supporting needs of stakeholders



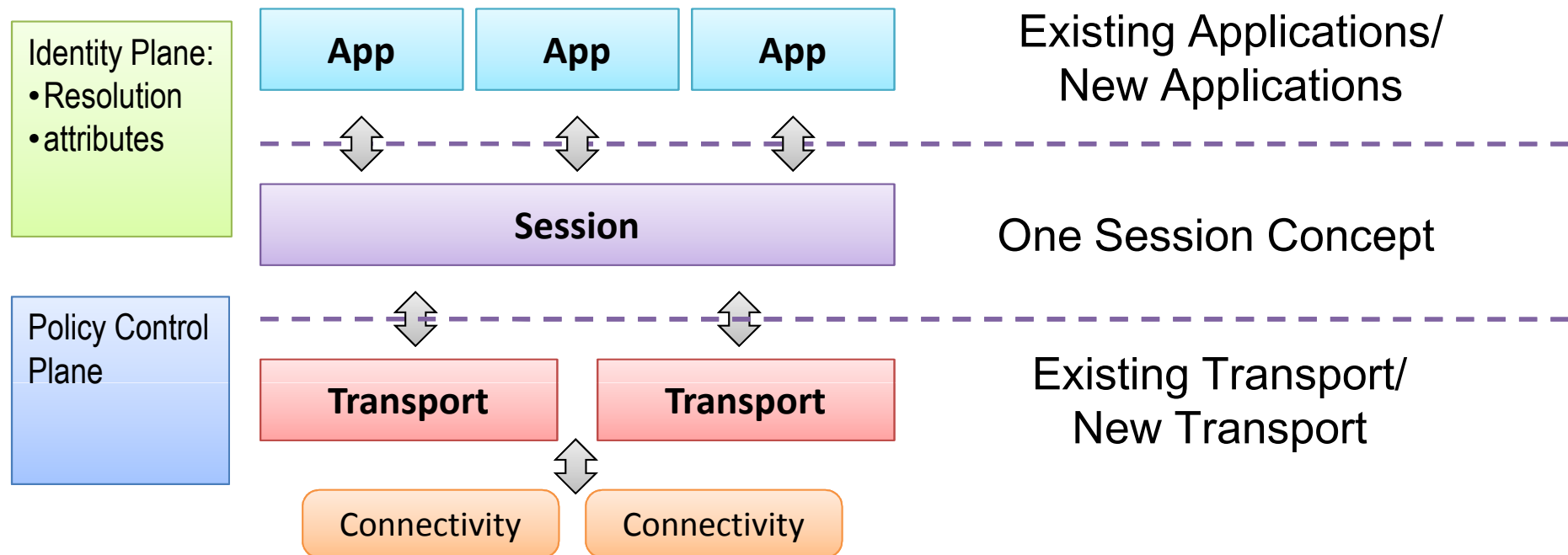
# FP6/FP7 possible Project Inputs

- PRIME and PRIMELIFE can control and minimise the identity-related information at **application-layer** entities: Available technologies are Idemix and anonymous credentials
- SWIFT deals with this from the **cross-layer** perspective: Available technologies are ID Aggregator and a conceptual framework for virtual identities and virtual terminals
- TAS3 has provided a **linking service** which links short lived credentials from different issuers using a random identifier;

# PPP: Identity as Generic Enabler

- Leverage existing privacy solutions of PrimeLife, TAS3 and SWIFT towards privacy enabled systems and infrastructures
- Create a platform bringing to life an Identity Framework that bridges existing Identity silos and provides the base for applications and scenarios
- Enable new business offerings taking advantage of European privacy protection norms and laws in Europe and beyond Europe's borders
- Identity, Privacy and Trust as a generic enabler of a Citizen Living Use Case in the Future Internet

# Beyond SWIFT: Long-term Goal



- Replace Transport layer by session aware transport, e.g. a new switching layer mapping sessions to labels
- Overlay connectivity aware Identity-based routing
- Identity can be locally mapped and policies applied to provide the conditions

# Beyond FP7: Future Research Direction

- Network, service, content and end-point entities should be aware of relevant identity *attributes* for:
  - Support of network, service and content functions not necessarily making players (users) identifiable
  - Stakeholders must not be forced to reveal more than is needed
- Dynamic trust management and solutions that provide a trade-off between divergent stakeholders with different and conflicting interest
- Enable privacy, accountability, minor protection and new business opportunities while minimizing unnecessary risks
- User in the center of the control of its data and where they are stored and who use/access it
- **Goal: better privacy and security than available today and make privacy a European seller of the 21st century!**

# Good collaborative effort

- Fine example of cross clustering in FIA between Trust and Identity caretakers as well as MANA caretakers
- Several events
  - preparation workshop for FIA Stockholm
  - FIA Stockholm
  - Interim workshop March 2010 (see attendees list)
- More Info:  
[http://security.future-internet.eu/index.php/FIA\\_Valencia](http://security.future-internet.eu/index.php/FIA_Valencia)

# Attendees of Preparatory Workshop

First name	Family name	Affiliation
James	Clarke	Waterford Institute of Technology -TSSG
Nick	Wainwright	HP
Keith	Howker	WIT-TSSG
Jacques	Bus	EC, DG INFSO, F5
Gustav	Kalbe	EC, DG INFSO, F5
Bart	Van Caenegem	EC, DG INFSO, F5
Wout	Van Wijk	EC, DG INFSO, F5
Amardeo	Sarma	NEC Europe Ltd.
Fabio	Massacci	University of Trento
Jan	Camenisch	IBM Zurich
Joao	Girao	NEC Europe Ltd.
Antonio	Skarmeta	Murcia University
Giuseppe	Bianchi	University of Roma
Kai	Rannenber	Goethe University Frankfurt
David	Chadwick	Univ. of Kent
Christian	Weber	Goethe University Frankfurt
Martin	Kuppinger	Kuppinger Cole
Lefteris	Leontaridis	IKED

# Sustainable Identity Framework for the Future Internet

Amardeo Sarma, NEC