# Identity Management Overview

Anthony Nadalin

Geneva, 19 September 2007

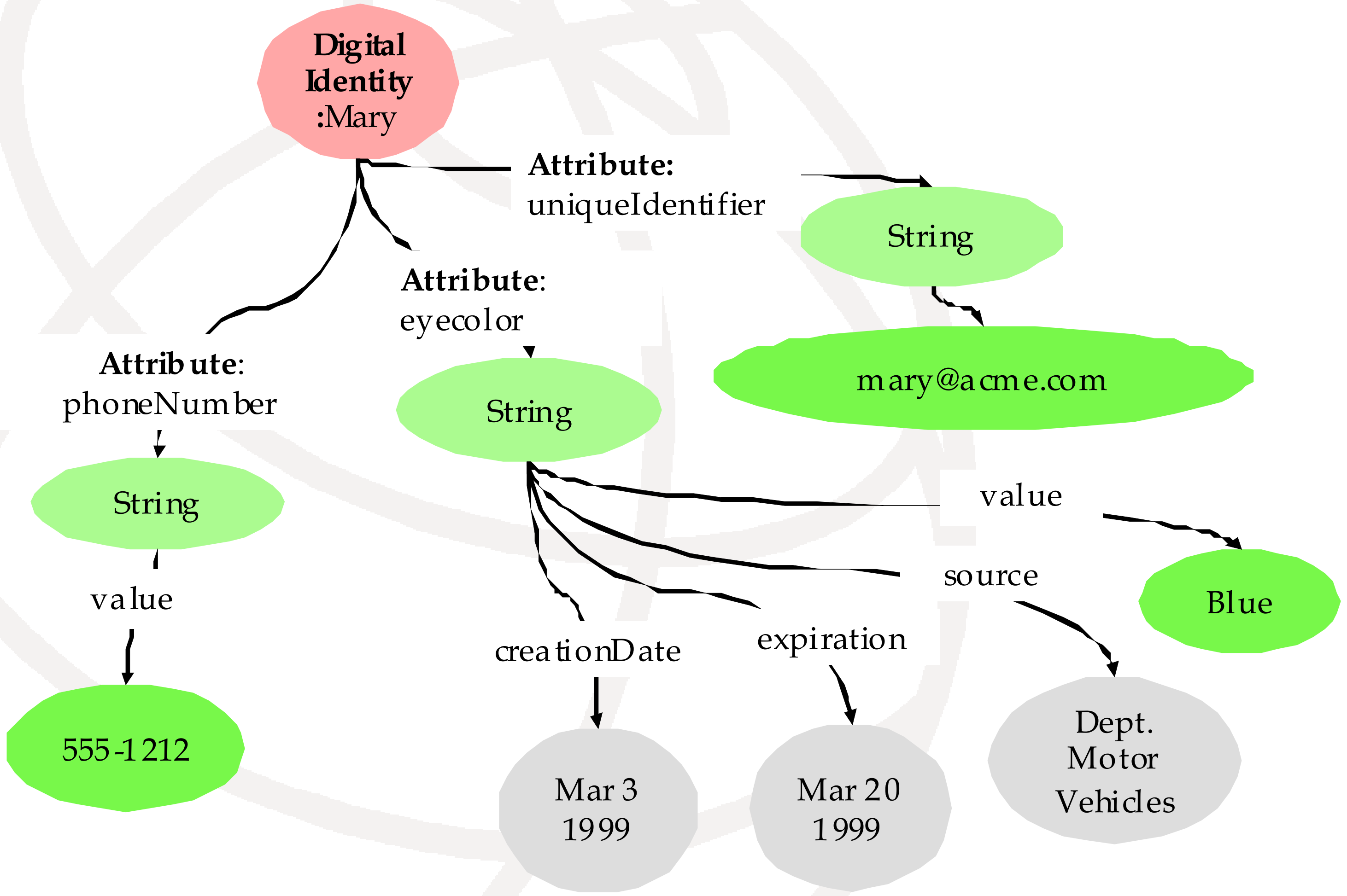
V1.0, 19Sep 2007

# Identity

# What is Identity

- Identity is both a “real-world” concept and a digital artifact;
  - The term “digital identity” or “identity” is preferred to refer to what technologists in the field of IdM conceive of as “a digital representation of a set of claims made by one party about itself or another data subject.”
  - Similar to the real world, a person may have any number of different identities in the electronic world. In the electronic realm, however, an identity can be a very simple set of identity information (e.g., an address), rather than the real-world concept that identity, which is fuller and much more closely tied with a person’s sense of who they are.

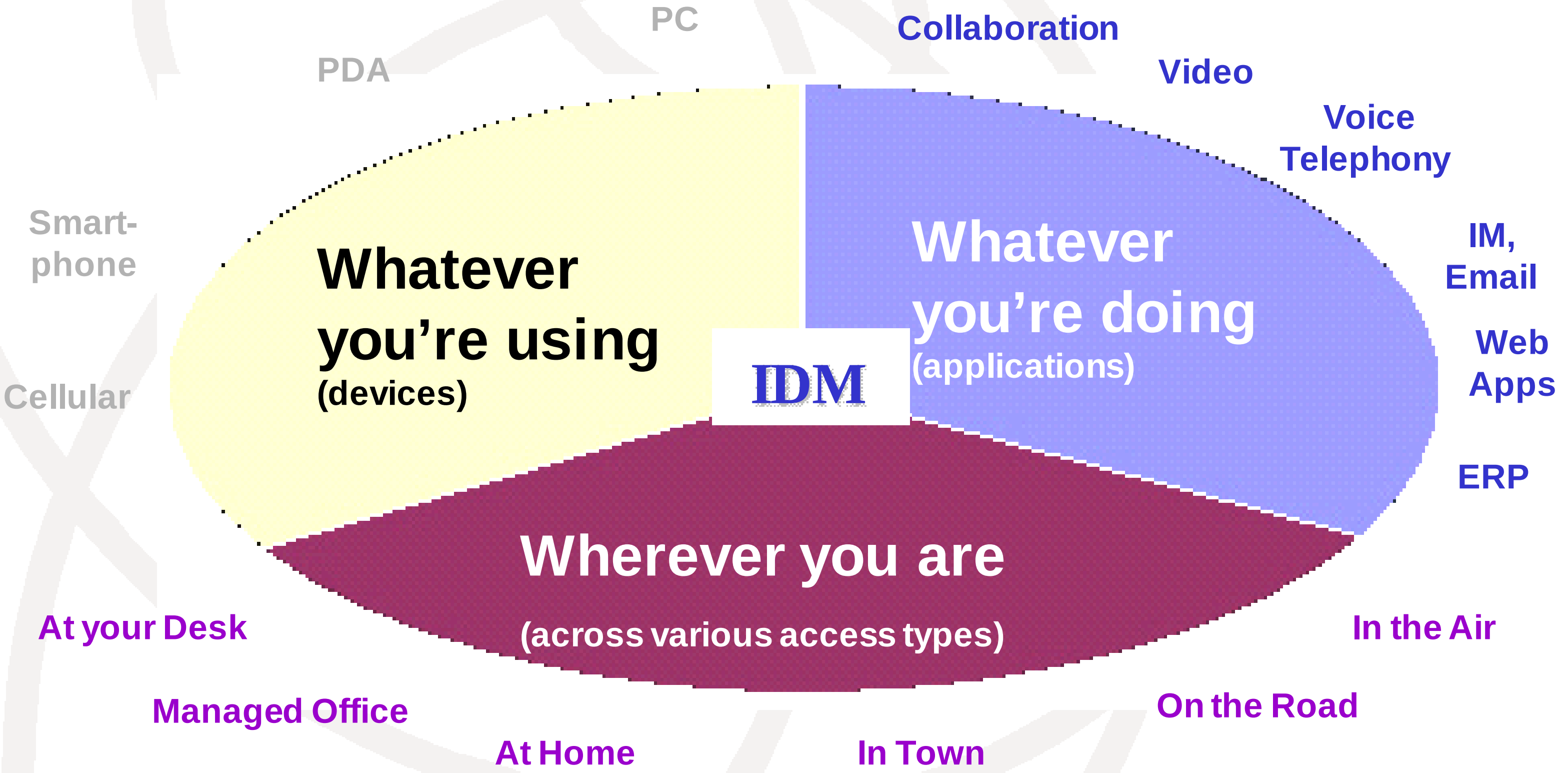
# Digital Identity



# Identities Exist in Many Places

**People have multiple "identities"**

- Work – me@company.com
- Family – me@smith.family
- Hobby – me@icedevils.team
- Volunteer – me@association.org

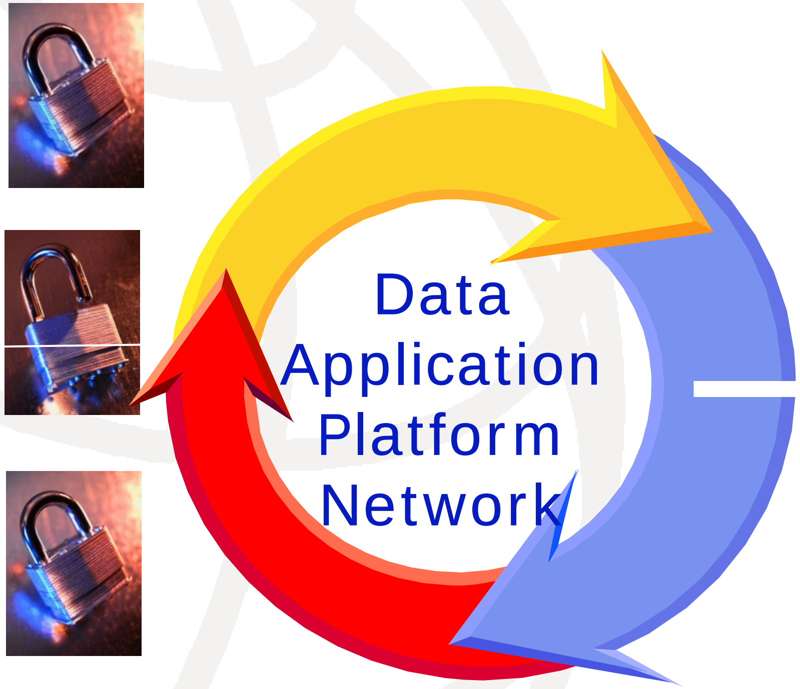


**IdM as underpinning for a secure and trusted hyper-connected ecosystems**

# Perimeter-less security demands strong Identity

***Can the right business system, person, or device can join, transact and terminate a desired business process***

Rapidly expanding Identity Types



Compliance Tools & Measurements

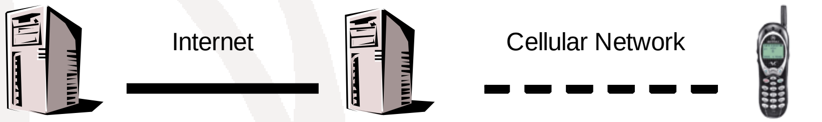
Risk Management Methodology

# Integrated relationship of Identities and Transactions

1. Manage end to end policy complexity of users, customers, resources & BPs
2. Drive cost efficiency today….now!!!
3. Create *dynamic* security of occasionally connected users, businesses & resources

## High integrity e-commerce transactions

Telco, Government, Financial



Internet

Cellular Network

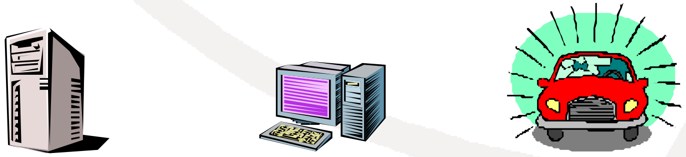
Web Server

Cellular SP Corporate Server

Handset Vendor

## Device personalization and corporate liability

Automotive, Telco, Financial



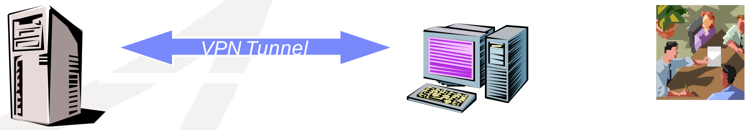
Vendor Corporate Server

Vendor Distributor Server

Vendor Consumer

## Brand image, privacy and Identity validation

Financial, Healthcare



VPN Tunnel

Credit Card Vendor Corporate Server

Member Bank

Local Validation Service or Customer

# Identity Management

# What is Identity Management

- Relative to information systems, **identity management (IdM)** is the management of the identity life cycle of entities (subjects or objects) during which:
  - the identity is established
  - the identity is described and defined
  - the identity is destroyed.
- This involves
  - both technology and process
  - managing unique IDs, attributes, credentials, entitlements
  - the ability to enable enterprises to create manageable lifecycles
  - the ability to scale from internally facing systems to externally facing applications and processes

# Goals of Identity Management

- To consistently enforce business and security policies, regardless of network entry point by employees, partners, and customers.

# Why Identity Management ?

- Reduced risk of improper use of systems, devices, etc
- Reduce risk of privacy or other regulatory violations
- Substantial administration cost savings by reducing redundant security administration

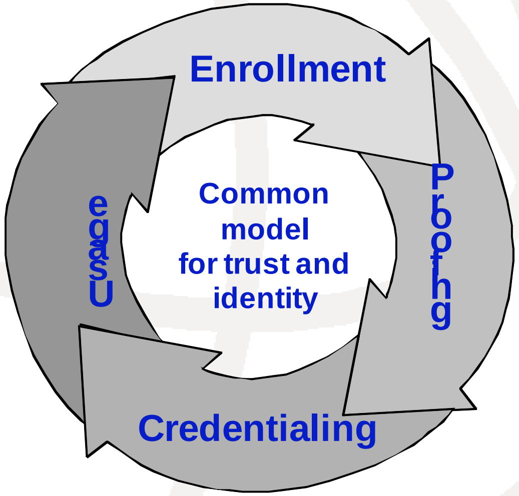
# Why Identity Life Cycle ?

- Elimination of the potential for errors, omissions and redundancies in identity data across systems
- Accuracy and completeness of identity information
- Better management of identity lifecycle
- Dissemination of assets, services and accounts
- The right resources to the right people at the right time
- Logging and audit capabilities of company assets and resources
- Connect ID access with device, application access

# Identity Life Cycle

- Biographics, demographics
- Reputation, portability
- Biometrics
- Drivers License Passports, etc

- Authentication
- Trust and reputation
- Logical access control
- Physical access control
- Enterprise identity mgt
- User-centric identity mgt
- Fraud detection
- Identity monitoring



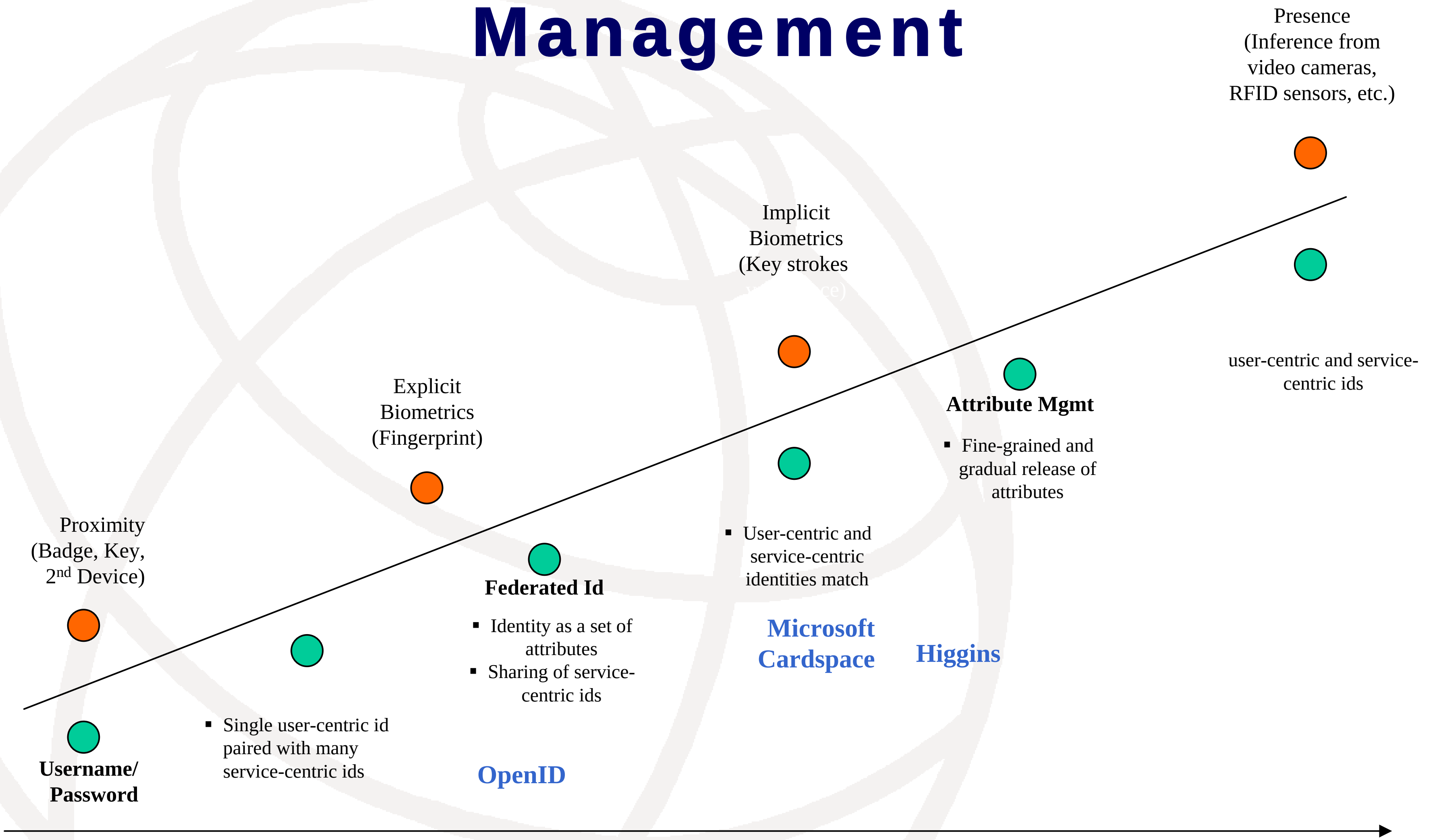
- Background identity and reputation checks
- Document security
- Identity Analytics
- Biometrics

- Logical credentials (e.g., OTP, public key certificates)
- Physical tokens (e.g., id cards w/ chip)
- Smartcards

# Current Identity Management Status

- Today’s identity management systems are ad hocracies, built one application or system at a time
  - Apps, databases, OSes lack a scalable, holistic means of managing identity, credentials, policy across boundaries
  - Fragmented identity infrastructure: Overlapping repositories, inconsistent policy frameworks, process discontinuities
  - Error prone, creates security loopholes, expensive to manage
  - The disappearing perimeter has put identity on the front burner
  - No interoperability between these ad hocracies
- Infrastructure requirements: extend reach and range
  - Increased scalability, lower costs
  - Balance of centralized and distributed management
  - Infrastructure must become more general-purpose and re-usable

# Evolution of Identity Management



Presence
(Inference from
video cameras,
RFID sensors, etc.)

Implicit
Biometrics
(Key strokes
Voice)

Explicit
Biometrics
(Fingerprint)

Proximity
(Badge, Key,
2nd Device)

**Username/ Password**

- Single user-centric id paired with many service-centric ids

**Federated Id**

- Identity as a set of attributes
- Sharing of service-centric ids

**OpenID**

- User-centric and service-centric identities match

**Microsoft Cardspace**

**Attribute Mgmt**

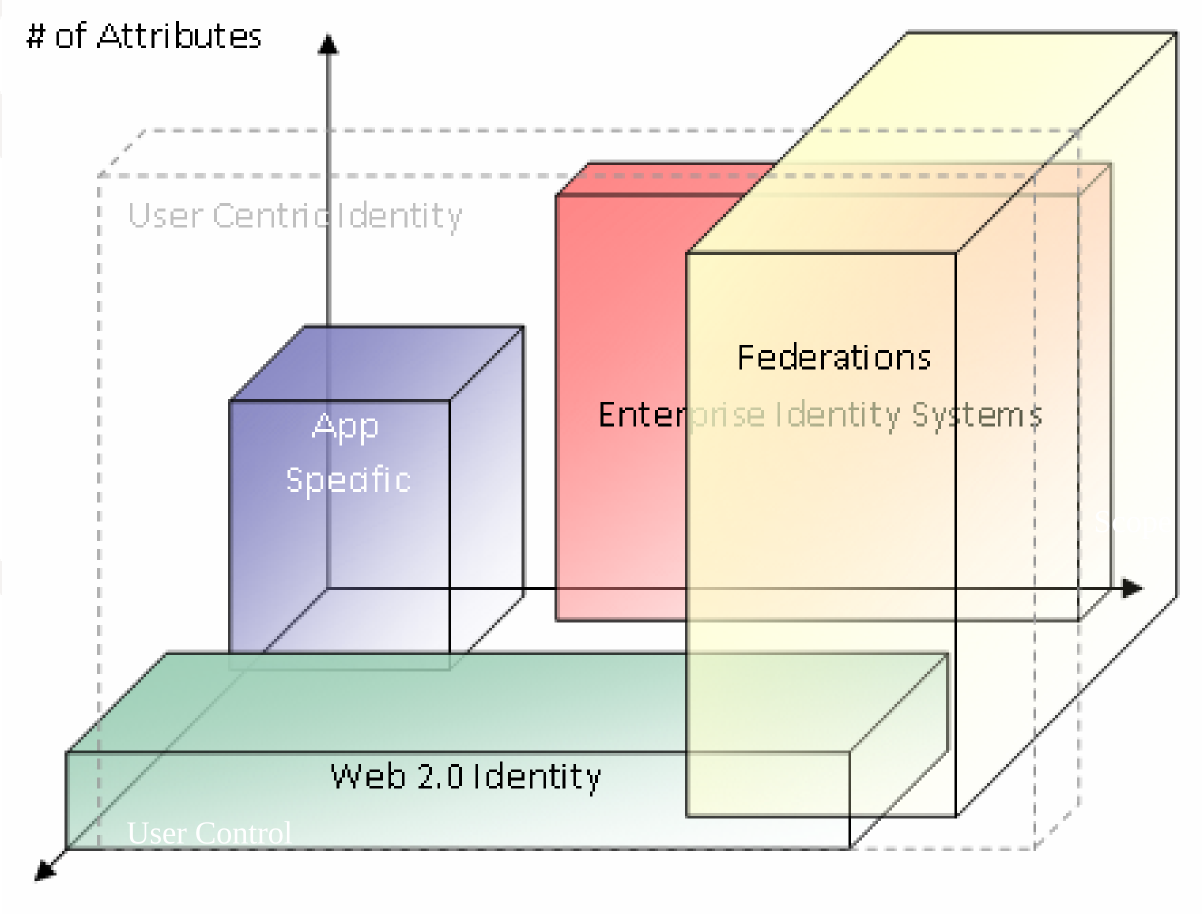
- Fine-grained and gradual release of attributes

**Higgins**

user-centric and service-centric ids

# Technology Eco System: Identity Domains

Based on their different aspects, identity systems are useful or typically used in certain types of applications. E.g. in Web 2.0 applications (like blogs, wikis, etc.) identity systems have typically only a very limited number of attributes (often only an email address), but a very high degree of user control. On the other hand, federation systems have a large variety of user control and contained attribute information, but usage only makes sense on a fairly global scale.



# Typical identity domains that are quite common

- **Application Centric Identity**
  - Applications have (and probably always will) maintain their own identity system or authentication database. (such as e.g. eBay, Amazon, etc.)To a certain extent, even operating system user databases can be considered application specific identity systems – their usefulness obviously depends on how the contained identity information can be used elsewhere. Isolated Identity When the extensibility is low or non-existent in a given application centric identity system, it is effectively isolated from all other applications.
- **Enterprise Identity**
  - As soon as computers obtained the ability to network – i.e. essentially with the advent of IBM's S/360 class mainframes – enterprises and large organizations started to create their own identity systems. At first, the number of attributes was quite limited. But with directory technology starting to become a reality in the early 1980s, organizations extended the amount of information immensely. Today, enterprise identity systems are typically large and complex federations of different attribute sources that contain a huge number of attributes on employees, business partners, customers, and inventory. Managing such extensive federation systems often requires a lot of effort and resources, particularly since stricter guidelines on identity auditing are being mandated by regulatory bodies. Problems
    - different regulations regarding accounting, auditing and privacy across the world
    - proper backup and disaster recovery
    - integration of users other identities, e.g. in private life etc.
- **User Centric Identity**
  - User centric identity systems (such as e.g. Windows CardSpace) and Higgins are aiming at enabling the user to take a larger control of their digital identities. As such, user control has to be very high, by definition. User centric identity system can have a broad variety of scope and the contained information. The Web 2.0 centric OpenID system has typically a fairly small number of attributes, but is used best across simple, "low profile" web applications**.**
- **Social Networks**
  - User centric identity systems have the potential to allow the accurate modeling of social networks of users in real time. To enable this, the system must allow the user to edit their own identity information – specifically all information on how he relates to other users in the system. This can be achieved e.g. by maintaining lists of links and related meta data about these links.
- **Network Identity**
  - All previous identity systems play a crucial role in their respective domains. But without a high degree of extensibility, there are doomed to stay fairly isolated from each other. Network identity systems are explicitly designed to be able to bridge the gap between existing and emerging identity systems.

# Identity Domains Technologies

**Higgins -** an extensible, platform-independent, identity protocol-independent, software framework to support existing and new applications that give users more convenience, privacy and control over their identity information.

**Cardspace –** is a system in the Windows Communications Foundation (WCF) of WinFX allows users to manage their digital identities from various identity providers, and employ them in different contexts where they are accepted to access online services.

**Liberty -** allows consumers and users of Internet-based services and e-commerce applications to authenticate and sign-on to a network or domain once from any device and then visit or take part in services from multiple Web sites.

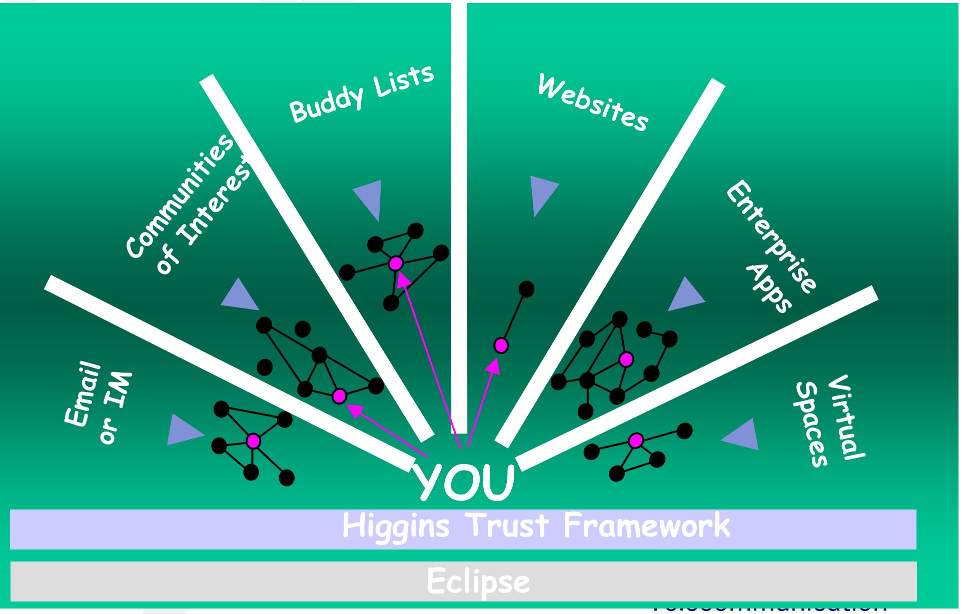
**OpenID -** is a decentralized single sign-on system. On OpenID-enabled sites, Internet users do not need to register and manage a new account for every site before being granted access. Instead, they only need to be previously registered on a website with an OpenID "identity

# Higgins

## Higgins Trust Framework will boost productivity by integrating identity, profile and relationship data across lex ent pr

An Eclipse open source project supported by IBM, Novell and Parity that will:

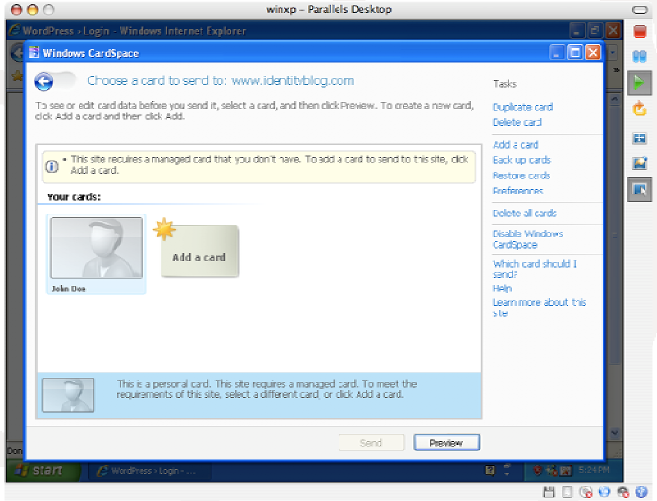
- Enable dynamic, automatic capture of people information from disparate information repositories
- Facilitate integration with diverse identity management systems
- Ease management of identity, profile, reputation and relationship data across repositories



# Cardspace

- Replaces Username and Passwords with cryptographically strong tokens containing identity claims
  - Collaborated with Trusted 3rd party Identity Provider
- Centres around simple to use Identity selector
  - Identity represented by a card metafore

- Easier
  - No passwords to remember
  - Consistent login



Choose a card to send to: www.identityblog.com

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

- This site requires a managed card that you don't have. To add a card to send to this site, click Add a card.

This is a personal card. This site requires a managed card. To meet the requirements of this site, select a different card, or click Add a card.

- Safer
  - Avoid phishing
  - Multi factor Authentication

# OpenID

- Decenterlized system for Single Signon
  - Single global Identifier used for all systems (simplifies number of user accounts)
  - User choice of where your identity is hosted
  - Providers and consumers of OpenID
  - Low barrier to entry
    - Works with static HTML pages
    - Understandable identity (a URL)
    - No public keys (key revocation, etc...)
    - No SSL required
    - No browser plugins
  - Largest user base is LiveJournal

# Liberty

Establish an op

network identity through open technical specifications that will:

- Support a broad range of identity-based products and services
- Allow for consumer choice of identity provider(s) and the ability to link accounts through account federation
- Provide the convenience of simplified sign-on, when using any network of connected services and
- Enable organizations to realize new revenue and cost saving opportunities
- Allow organizations to economically leverage relationships with customers, business partners, and employees
- Improve ease of use for e-commerce

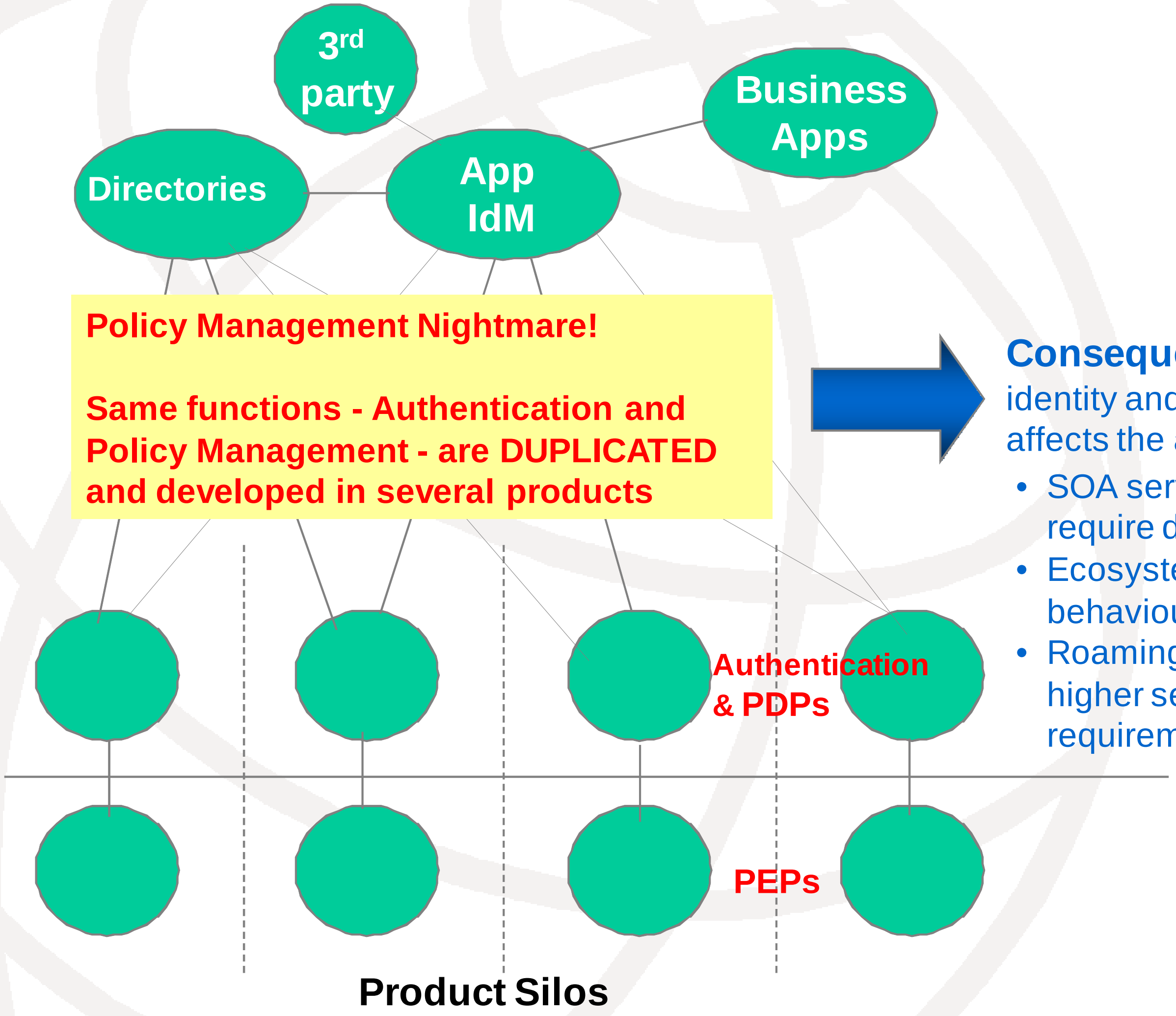
# ITU-T IdMFG

Geneva, 19 September 2007

# Why a ITU-T Focus Group ?

- Common global needs for interoperability
  - Platforms, discovery, practices, and trust models
  - Very diverse activities and stakeholders worldwide
  - Autonomous networks for nomadic always-on, anytime, anywhere services
  - Essential for network/cyber security
  - One of the most important development areas in industry today
- An open ITU-T Focus Group enjoys a unique value proposition
  - Outreach and bringing all IdM perspectives and communities together
  - Analyzing use cases, platforms, gaps
  - Providing initial requirements, framework(s), reference information
  - Follow-up actions remain with ITU and other industry forums

# Typical Service Provider Today



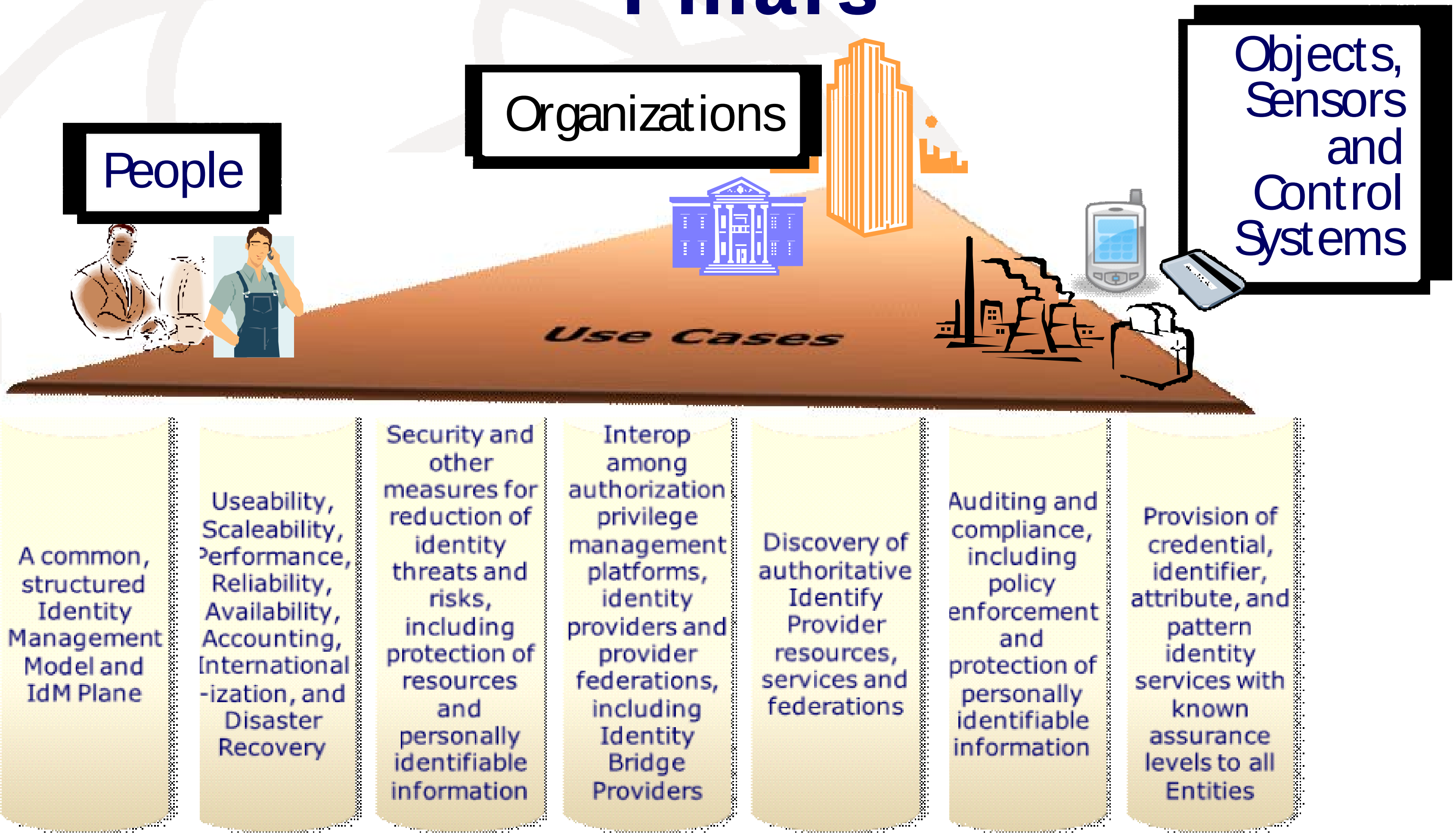
**Policy Management Nightmare!**

**Same functions - Authentication and Policy Management - are DUPLICATED and developed in several products**

**Consequences:** Complex identity and policy management affects the ability to support:

- SOA service components that require decoupling & autonomy
- Ecosystem autonomic behaviours
- Roaming and mobility under higher security and trust requirements

# Requirements for Global Interoperable IdM: the Seven Pillars



People

Organizations

Objects, Sensors and Control Systems

Use Cases

A common, structured Identity Management Model and IdM Plane

Useability, Scaleability, Performance, Reliability, Availability, Accounting, Internationalization, and Disaster Recovery

Security and other measures for reduction of identity threats and risks, including protection of resources and personally identifiable information

Interop among authorization privilege management platforms, identity providers and provider federations, including Identity Bridge Providers

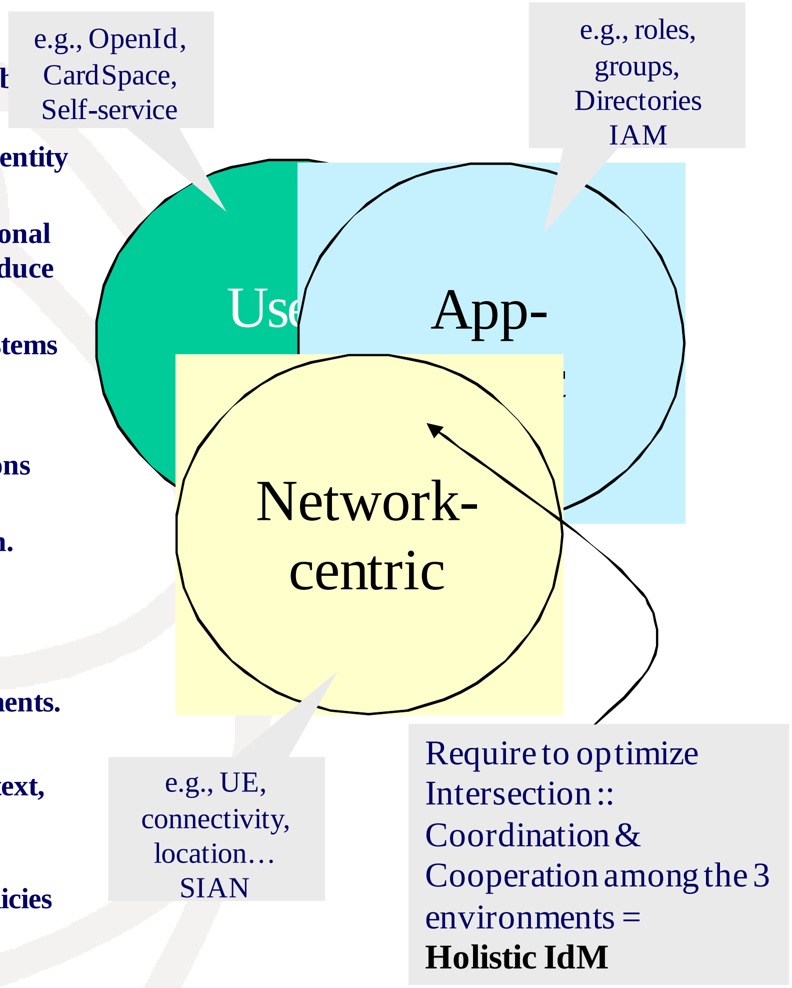
Discovery of authoritative Identify Provider resources, services and federations

Auditing and compliance, including policy enforcement and protection of personally identifiable information

Provision of credential, identifier, attribute, and pattern identity services with known assurance levels to all Entities

# Interoperable Framework Goals

- meet requirements as specified in the Report on Requirements for Glob Interoperable Identity Management
- support user-centric, application-centric and network-centric based identity management systems.
- assist entities/users in protecting privacy, and limit the amount of personal information exposed to the minimum required by any party to help reduce the amount of correlation that may occur.
- promote interworking with diversity to allow identity management systems to interact with scalability and performance for public networks.
- support and promote open standards and specifications.
- support the identity lifecycle management functions as well as operations that facilitate the run-time of request/query based transactions.
- address high priority issues such as identity theft, identity proliferation.
- be forward looking, providing a target for existing systems to migrate towards.
- enable appropriate access and use of resources based on identity.
- assist the implementations that meet the legal and regulatory requirements.
- provide usability (e.g. SSO).
- enable the creation, update and discovery of meta-attributes (e.g., context, location, connectivity, roles, cards…) associated with an entity's meta-identifier (e.g., XRI).
- enable the distributed and dynamic (i.e., on the fly) enforcement of policies within and across federations
- enable the auditing of framework functionality and transactions



e.g., OpenId, CardSpace, Self-service

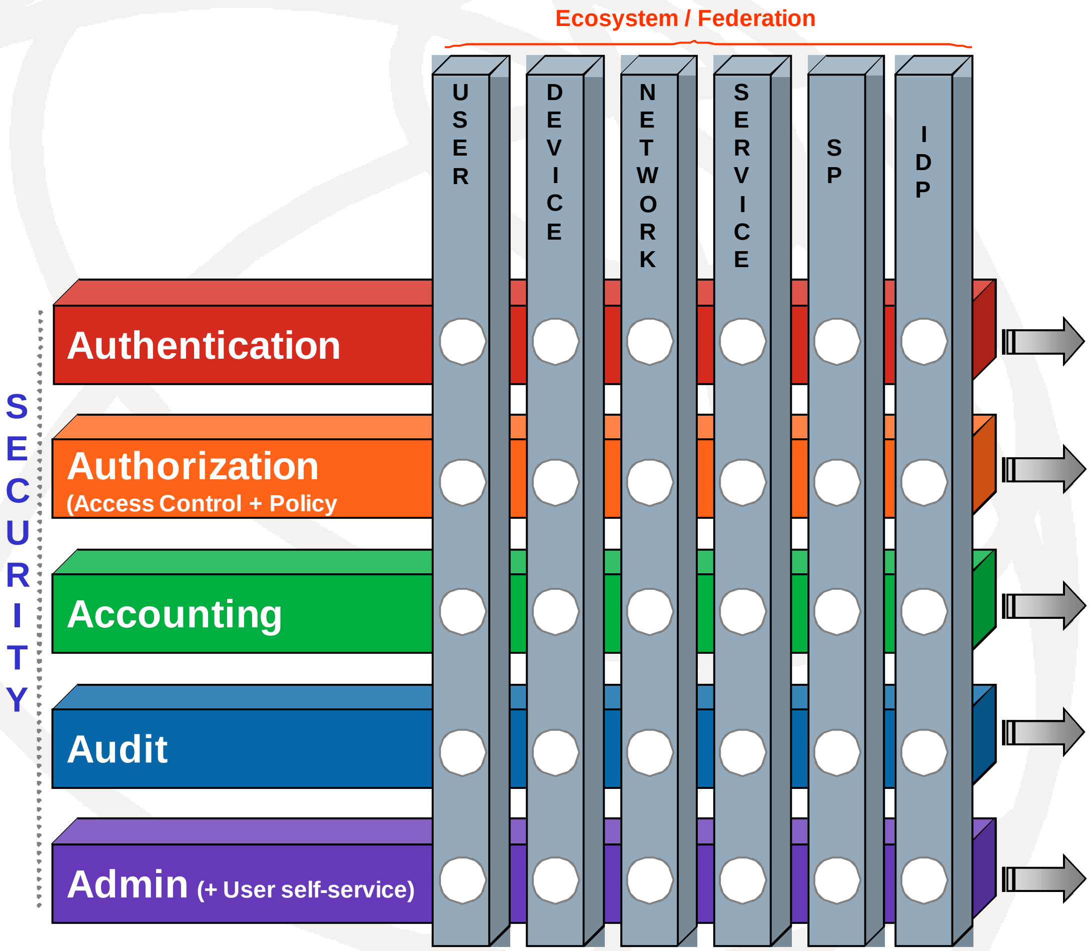
e.g., roles, groups, Directories IAM

e.g., UE, connectivity, location… SIAN

Require to optimize Intersection :: Coordination & Cooperation among the 3 environments = **Holistic IdM**

QoE = Quality of Experience
SOA = Service Oriented Architecture
IAM = Identity Access Management

# A IdM Perspective



- Validate users for the network & service
- Heightened levels of security

- Grant users a specific set of services and access to information
- Safeguard Privacy

- Enables charging &
- billing

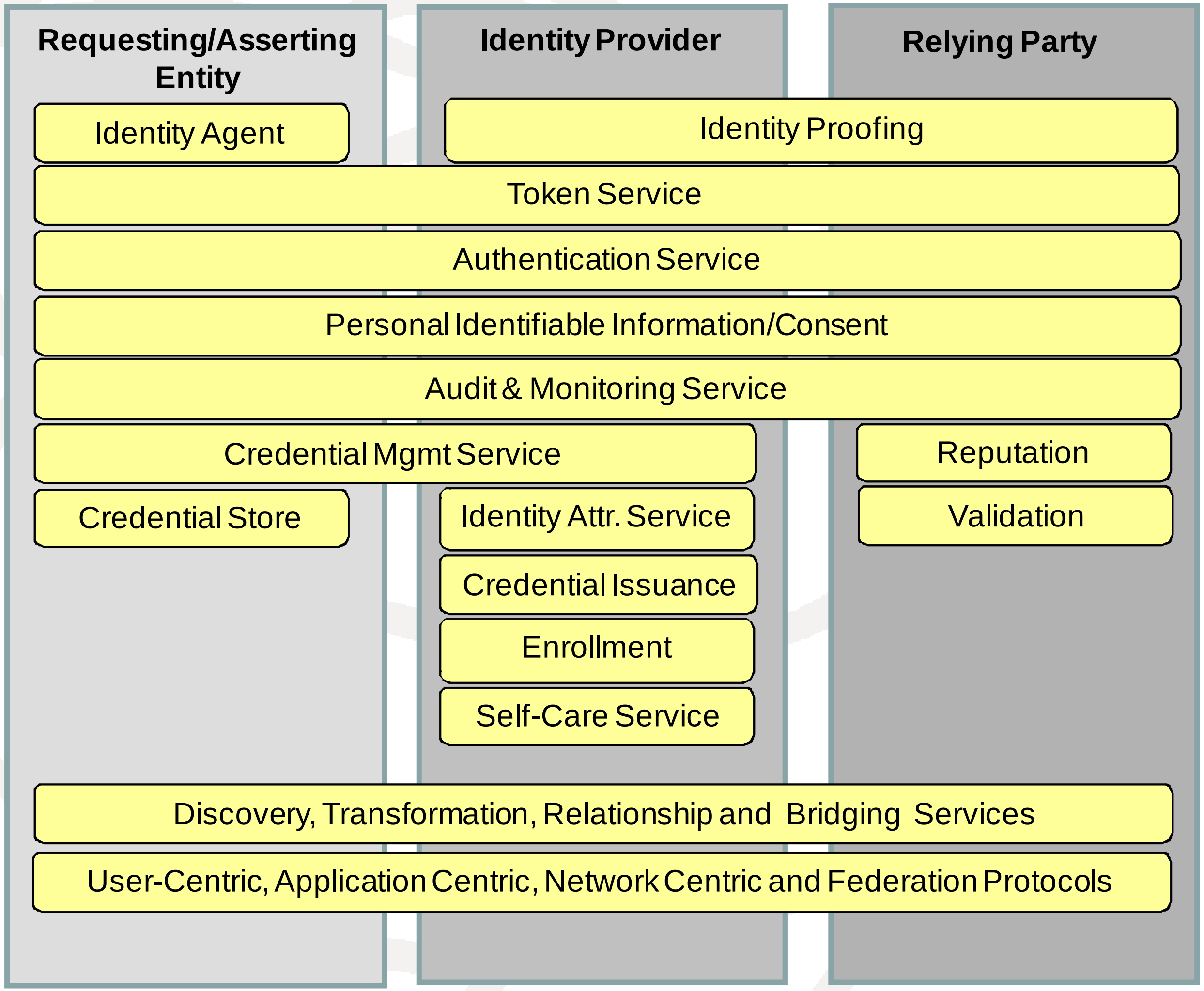
- Simplified audit and regulatory compliance

- Simplifies Policy Management
- Enhanced customer service levels
- Self service

6

Geneva, 19 September 2007

# Interoperable Framework



Requesting/Asserting Entity

Identity Provider

Relying Party

Identity Agent

Identity Proofing

Token Service

Authentication Service

Personal Identifiable Information/Consent

Audit & Monitoring Service

Credential Mgmt Service

Reputation

Credential Store

Identity Attr. Service

Validation

Credential Issuance

Enrollment

Self-Care Service

Discovery, Transformation, Relationship and Bridging Services

User-Centric, Application Centric, Network Centric and Federation Protocols