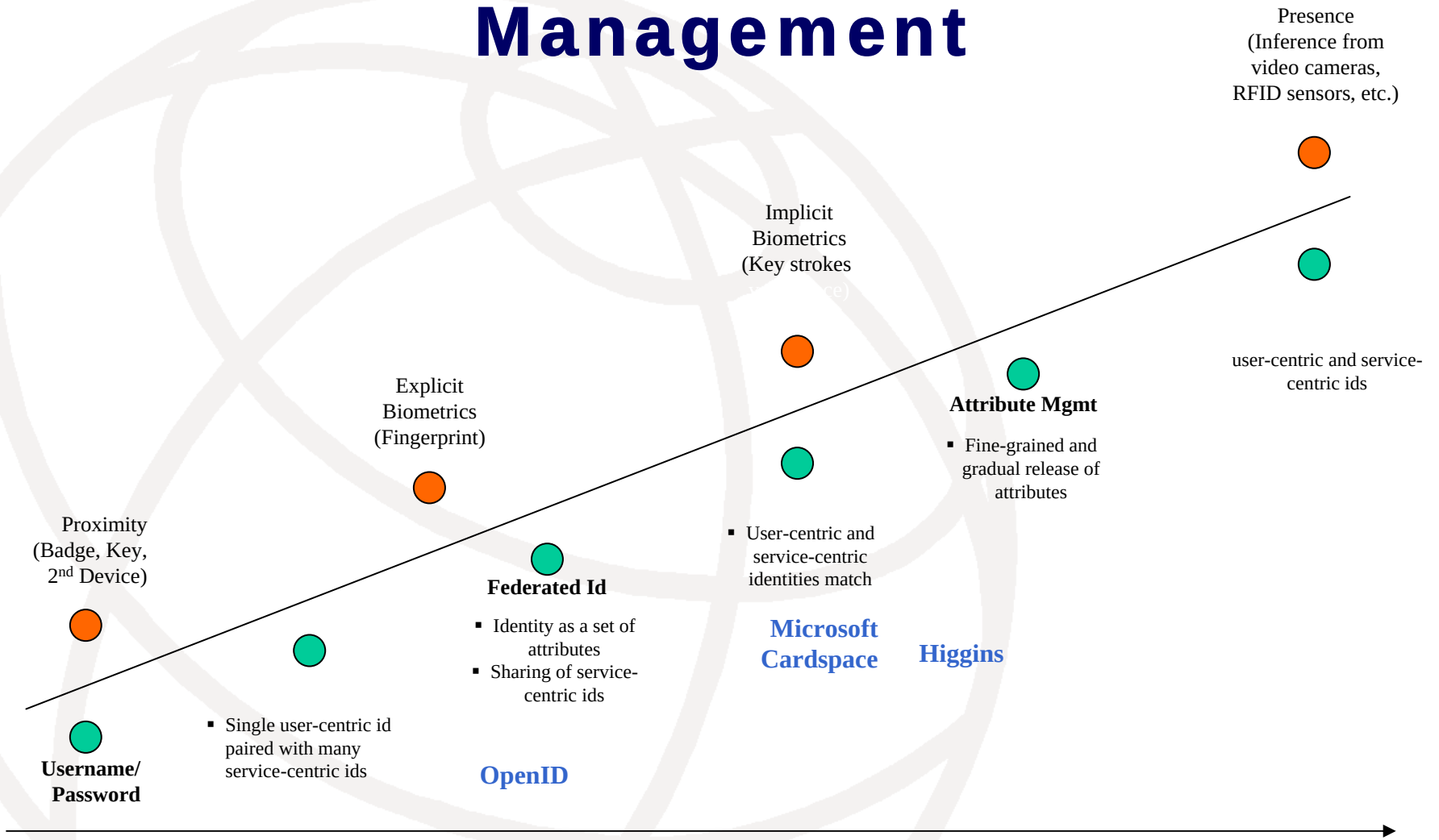
ITU-T IdMFG
Framework Work Group

Geneva, 19 September 2007

Evolution of Identity Management



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

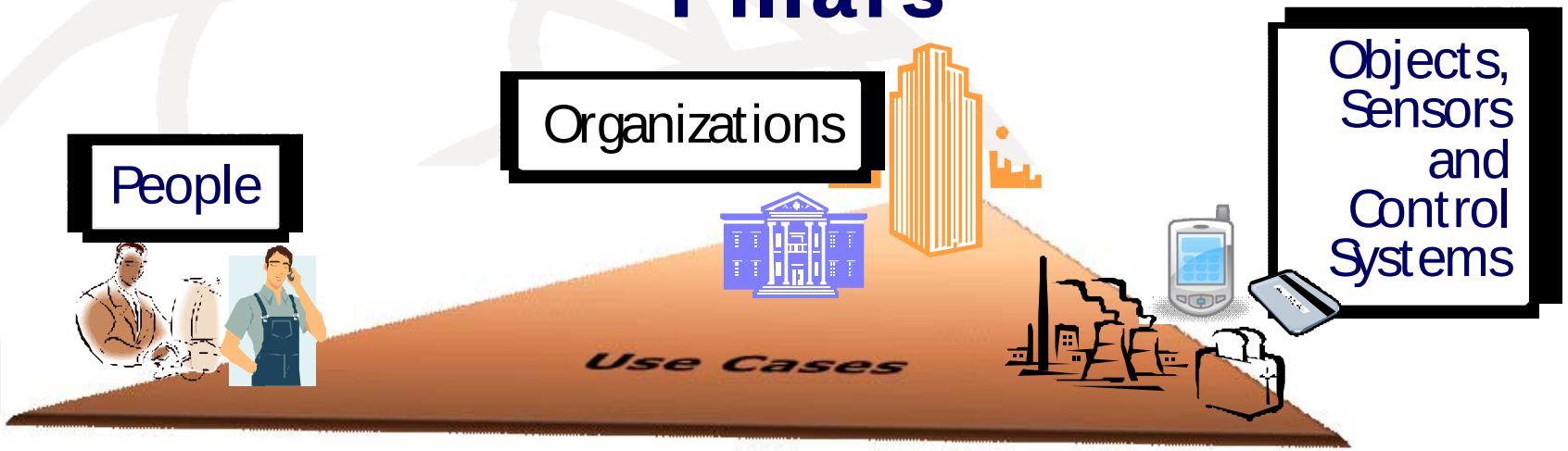
Higgins - an extensible, platform-independent, identity protocol-independent, software framework to support existing and new applications that give users more convenience, privacy and control over their identity information.

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

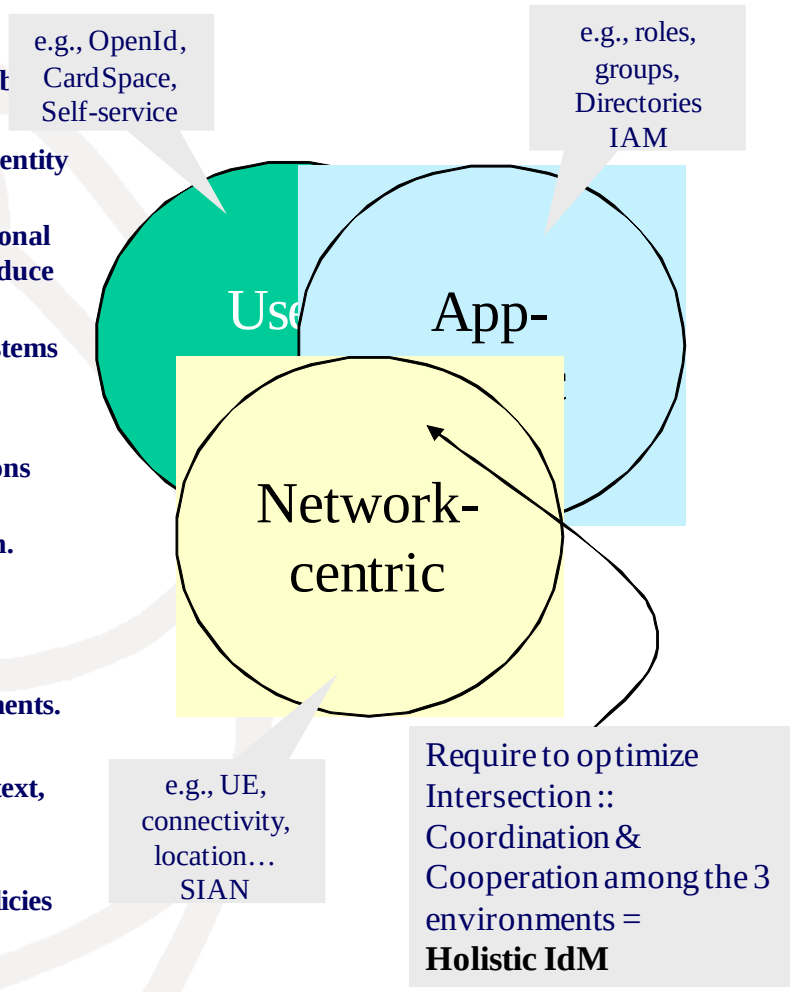
Requirements for Global Interoperable IdM: the Seven Pillars



A common, structured Identity Management Model and IdM Plane	Useability, Scaleability, Performance, Reliability, Availability, Accounting, International -ization, 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

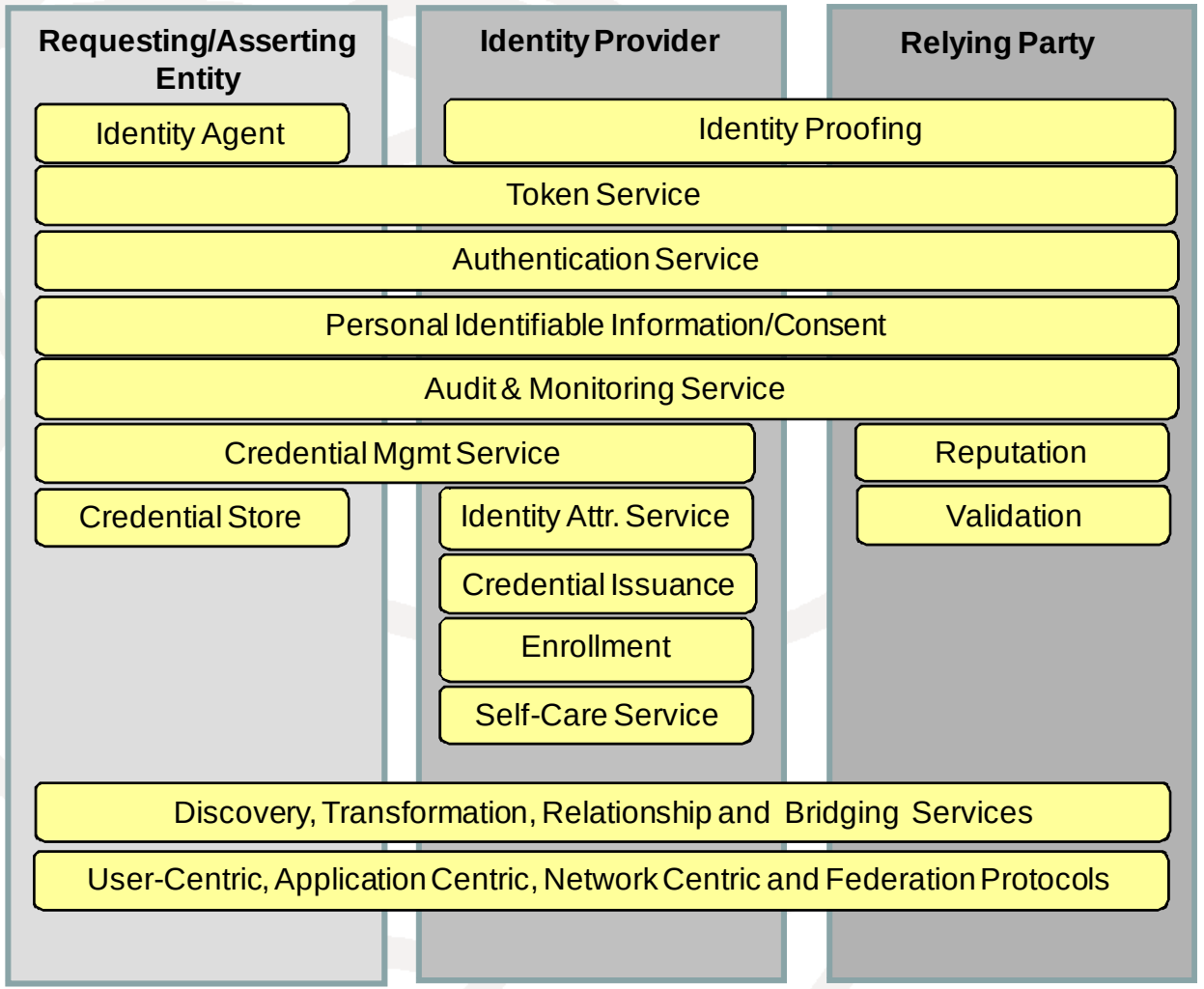
Interoperable Framework Goals

- 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



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

Interoperable Framework



Identity Transformation and Bridging