ITU-T Focus Group on Identity Management (FG IdM): Report on IdM Use Cases and Gap Analysis

Ray P. Singh
Telcordia Technologies
732-699-6105
rsingh@telcordia.com

ITU-T

Outline

- Scope
- Meaning of Gap
- Current View of IdM Landscape
- General IdM Architectural Model
- Use Cases Addressed in Report

ITU-T

Scope

- Documents the Use Cases and Gap Analysis findings of the ITU-T Focus Group on Identity Management (FG IdM).
- It includes a gap analysis that identifies areas where there are gaps among the various IdM islands, documented in the form of use case examples and scenarios.
- These gaps represent the lack of (or lack of adoption of) end-to-end solutions, taking into consideration
  - the distributed autonomous infrastructure, and
  - the common need for global interoperability among
    service providers, network providers,
    government / regulatory agencies,
    countries / regional bodies, and
    the end users / subscribers.

ITU-T

Meaning of Gap

- A gap is
  - the lack of (or lack of adoption of) a solution based on open standards or specifications to support a specific industry need or requirement,
  - the lack of a specific feature, or
  - an incomplete capability.
- A gap can arise from the lack of
  - a technical mechanism or protocol,
  - a best practice or guidelines specification, or
  - a performance specification.
- A gap can also arise from the lack of a specification describing the application of a defined technology to address specific network architectures (e.g., NGN and IMS), business models, and assumptions (e.g., scalability).
- A gap can also arise from the lack of a sufficient administrative mechanism or national mandate.

ITU-T

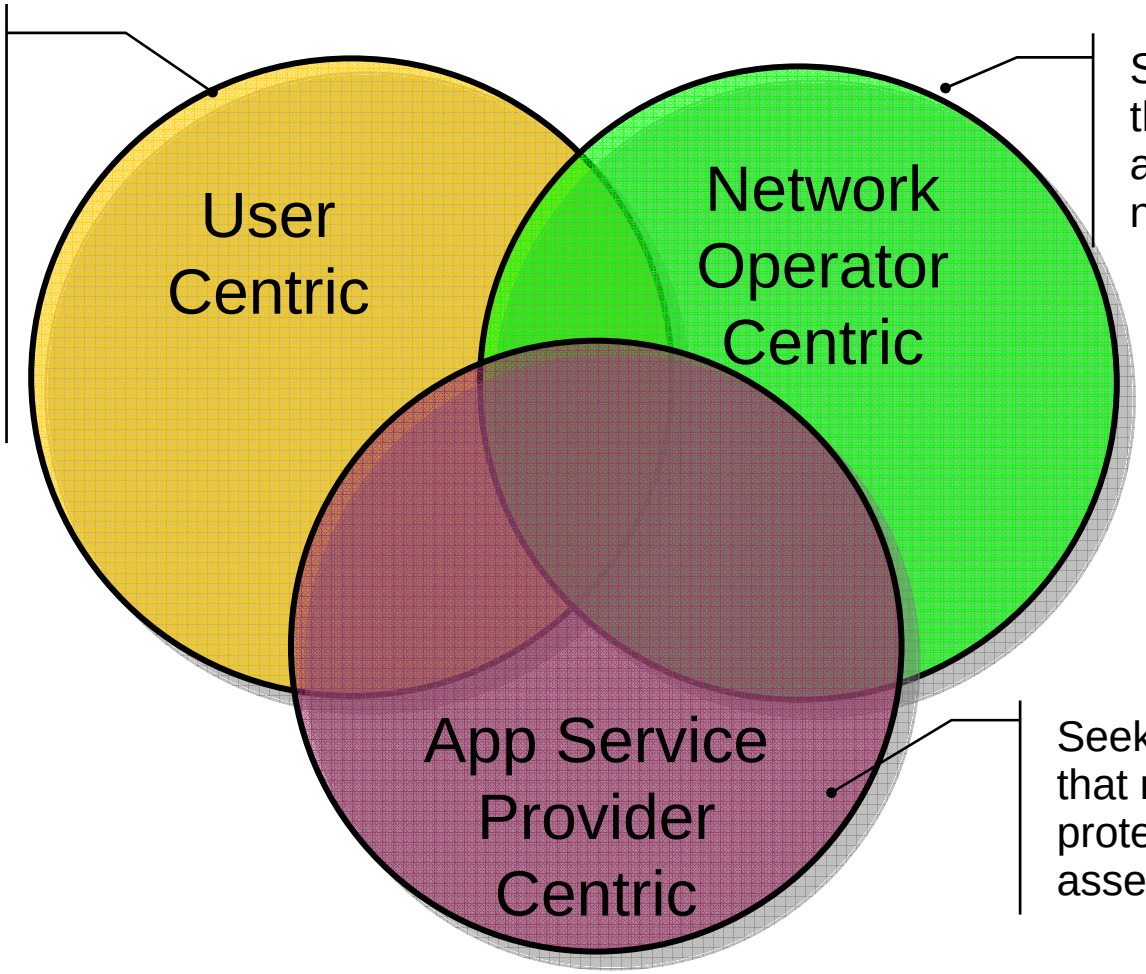
Current View of IdM Landscape

- A variety of IdM specifications have been developed and deployed
  - E.g., Security Assertion Mark-up Language (SAML), Liberty Alliance, Web Services – Federation, OpenID
  - In the future these may converge, but in order to provide a global cohesive IdM Framework, they must be compatible.
  - Convergence of IdM initiatives has been recognized by recent developments within the IdM community
- These standards may not meet the needs of certain industry segments, or may assume specific architectures and infrastructures. As a result, new standards may be developed.
- Therefore, the IdM infrastructure must support the coexistence of both current and newer standards, and must support a graceful transition from one solution to another.

ITU-T

Current View of IdM Landscape

Seek capabilities to allow user control of personal identifiers, roles and privacy attributes



Seek capabilities that maximize and protect network assets

Seek capabilities that maximize and protect application assets

ITU-T

Current View of IdM Landscape

- User-centric
  - A model of IdM developed primarily from the perspective of end-users, and optimized for the interests of those end-users.
- Application-centric
  - A model of IdM optimized for the requirements of applications, e.g., protecting access to application resources.
  - Historically, IdM implementations driven by enterprise use cases (e.g., SAML, Shibboleth, WS-Federation) focused on federated access to applications and services.
  - However, these implementations can be leveraged and customized for other broader use.

ITU-T

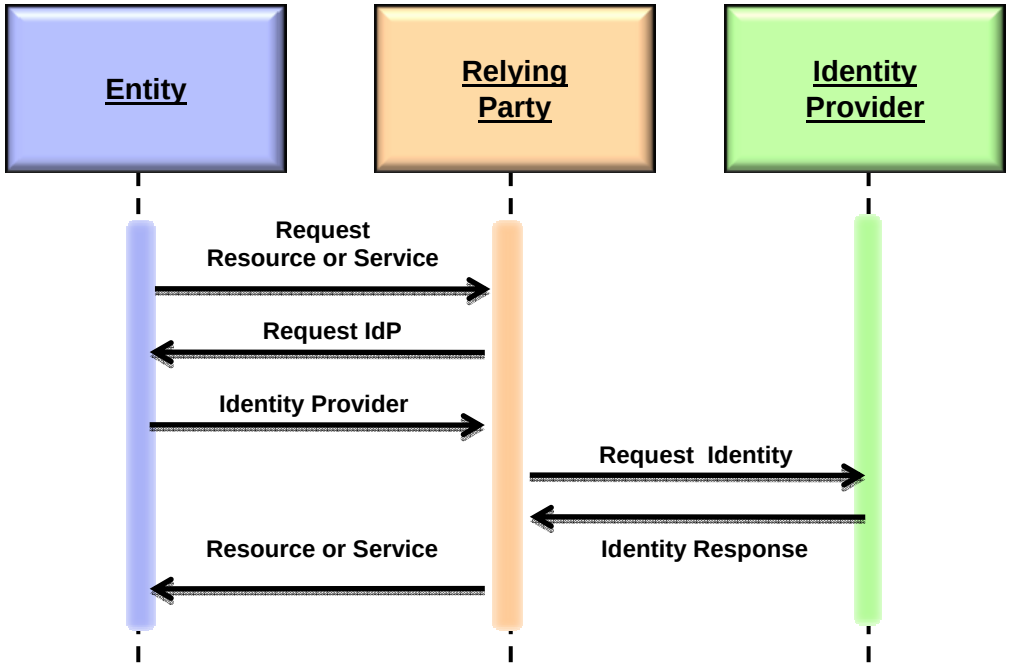
Current View of IdM Landscape

- Network-centric
  - A model of IdM optimized for networks and network providers (e.g., NGN providers and operators)
  - Focused on network- and device-centric interests for NGN. Network-centric interests include preventing fraud and theft of service.
- The boundaries between the three models are blurred. In general:
  - Any IdM deployment will typically include aspects of all three models (user, application, network)
  - Any of the existing IdM implementations can be deployed consistent with the three different models.

General IdM Architectural Model

ITU-T

- **Entity** - a User or a Requestor, who seeks Service from a Relying Party, and provides a claimed Identity to that Party.
- **Relying Party (RP)** - Needs to have this Identity authenticated before providing the Service. Queries Entity for the name of the Identity Provider for the claimed Identity. Queries Identity Provider for validation of the claimed Identity (and for the attributes of that Identity).
- **Identity Provider (IdP)** - Authenticates the claimed Identity, and may return attributes of the Identity to the RP. Uses trust mechanisms and security policy to process Identity requests from the RP.



- IdM Query-response mechanisms should be "well-structured", with syntaxes and profiles that are known or potentially obtainable by each of the parties involved

ITU-T

Use Cases Addressed in Report

- Integration of IdM in NGN Architecture
- Discovery of Identity Resources
- Inter-Federation/Inter-CoT Interoperability
- Interoperability of Mechanisms Used to Exchange Identity Information
- Identity Assurance
- Transparency, Notice, Access, and Privacy
- Integration of Object Management
- IdM Security and Identity Patterns
- IdM Time-Stamp Accuracy
- Token Transformation
- Delegation