ITU-T Workshop on Multimedia in NGN

Toward global Interoperable Identity Management

Anthony-Michael Rutkowski
Vice-President, VeriSign
Chair, ITU-T IdM FG Requirements WG
Outline

- What is Identity Management and why was a Focus Group created?
- Significant recent IdM industry development examples
- Success of the Initial FG IdM work
- Timeline Context
- Focus Group Products
  - Requirements structure and summary
- IdM for object communications
- Implications for NGN and other developments
What is Identity Management
Why an ITU-T Focus Group

- Management of digital identity
  - All trusted ICT and network capabilities and resources for
    - Authentication (e.g., certificates)
    - Identifiers (e.g., E.164 nos., URIs, OIDs, IP addresses, domain names)
    - Attributes (e.g., names, location)
    - Patterns and reputation
  - For entities of any kind
    - People
    - Organizations
    - Objects (e.g., devices, SIMs, RFIDs, content..)

- 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/cybersecurity
  - 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
  - Analysing use cases, platforms, gaps
  - Providing initial requirements, framework(s), reference information
  - Followup actions remain with ITU and other industry forums
Shift to Identity Providers

Legacy Identity Management

Next Generation Identity Management
Significant recent IdM industry development examples

OpenID emerged as a large-scale, open, non-proprietary means to implement IdM as
• a fully decentralized system.
• a much lighter cost structure

InfoCard emerged as a large-scale, open, proprietary (Microsoft) means to implement IdM on a large-scale with ubiquitous computer/commercial wireless operating systems
Identity Management Focus Group Basics

- Participants and their diversity
  - 139 different people, 88 different organizations in 22 countries
- Meeting location diversity
  - Geneva (2), Mountain View, Tokyo, Boston
- Contributions and their diversity
  - 114 input contributions from 41 different companies and organizations
- Outreach diversity
  - Discovered, analyzed, and in many cases contacted more than 100 different IdM forums within more than 60 different organizations
  - Made use of unofficial IdM Focus Group Wiki; extensive teleconferencing for meetings

Four Major Reports
- Requirements for Global Interoperability: structure & provisions
  - 73 Requirements and Recommendations in seven sectors
- Identity Management Use Cases, Platforms, Gaps
  - Scores of Use Cases
- Identity Management Framework(s)
  - Initial draft framework
- Identity Management Ecosystem and Lexicon

Three IdM Reference Compendiums/Living Lists
- Ecosystem (60 organizations)
- Lexicon
- Legal & regulatory (35 IdM requirements in 9 topical groupings)

Multimedia in NGN
Geneva, 10-11 September 2007
IdM Focus Group Timeline Context

Identity Management Focus Group

- Created Dec 2006
- 1 - Geneva 13-16 Feb 2007
- 4 - Tokyo 17-20 Jul 2007

Phases:
- Phase 1
- Phase 2

TSAG
SG17 Q.6 X.Idmf Draft Group
SG13 Q.15 Rec. Y.IdMsec Draft Group
WTSA

Multimedia in NGN
Geneva, 10-11 September 2007
Focus Group Products

- Requirements structure and provisions
- Use cases, platforms, gaps
- Draft framework(s)
- Reference materials
  - Ecosystem
  - Lexicon
  - Legal & regulatory compendium
Initial Report on Requirements for Global Interoperable Identity Management

Contents

1. Requirements Report Executive Summary .............................................. 3
2. Objective of the Requirements Report ...................................................... 4
3. Derivation of the requirements ................................................................ 5
3.1 Analysis of Identity Management use cases ......................................... 5
3.2 Analysis of existing legal and regulatory requirements, including the protection of personally identifiable information .............................................. 5
3.3 Requirements Contribution ................................................................. 5
4. Common requirements for global interoperable Identity Management and existing standards for meeting these requirements .................................................. 5
4.1 A common, consistent Simple Identity Management Model (SIMM) and IDM Backbone ............................................................. 7
4.2 Provision of credential identifiers, attribute, and pattern identity services with unique attributes tied to all entities ................................................. 7
4.2.1 Types and identities supported, including shared or delegated relationships and authority .................................................... 9
4.2.2 Provision of credential identity services .......................................... 10
4.2.3 Provision of identity services ........................................................ 12
4.2.4 Provision of attribute identity services ........................................ 13
4.2.5 Provision of pattern identity services, including reputation ........ 17
4.2.6 Provision of identity assurance levels ............................................. 18
4.3 Discovery of authoritative Identity Provider resources, services, and federations ................................................................. 18
4.4 Interoperability among authorization, privilege management, platforms, identity providers, and provider federations, including Identity Trust Providers ...................................................... 20
4.5 Security and other measures for reduction of identity threats and risks, including protection of identity resources and personally identifiable information ........................................ 20
4.5.1 Security, and other measures, including usage policies and directives .......................................................... 22
4.5.2 Protection and use of Personally Identifiable Information ........... 23
4.6 Auditing and compliance, including policy enforcement and protection of personally identifiable information .................................................. 26
Requirements for Global Interoperable IdM: the Seven Pillars

People

A common, structured Identity Management Model and IdM Plane

Useability, Scaleability, Performance, Reliability, Availability, Accounting, International-Cization, 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

Objects, Sensors and Control Systems

Use Cases

Organizations

Multimedia in NGN
Geneva, 10-11 September 2007
A common, structured Identity Management Model and IdM Plane

Relying Party is most often the service provider or network operator – which may also be an Identity Provider

Multimedia in NGN
Geneva, 10-11 September 2007
16 requirements/recommendations concerning support for identified entities below

21 requirements/recommendations applicable to IdPs for credential, identifier, attribute, pattern and assurance services

Especially important
- Interoperable protocols, including objects
- Assurance/confidence metrics
- Delegation
- Lifecycle management
- Improved identity proofing and discovery for public network identifiers in hierarchical assignment identifier structures

---

**End-User Entities** (Requesting/Asserting Identities)
- Real persons
- Legal persons
- Institutions
- Organizations
- Guardians/agents
- Groups
- Objects
  - Physical
  - Terminal devices
  - Network equipment
  - SIM or Smart Card
- Virtual
  - Software
  - Geospatial
  - Content

**Relying Parties** (Using asserted identities)
- Service or resource provider
- Alliances

**Identity Providers** (to End-Users)
- Credential provider
- Identifier provider
- Attribute provider
- Pattern/reputation provider
- Discovery provider
- Identity Bridge provider
- Auditing or Policy Enforcement provider
- Federations
3 requirements and recommendations

Especially important

- Global mechanisms for discovery of asserted forms of identity
- Determining source for "authoritative" identities
- Interfederation bridging capabilities
  - Should include characteristics and policies of the interfaces, dynamic registration and de-registration of federation relationships, authentication, permissions, and attributes
- Provider business agreements and federation based policies
7 recommendations concerning platform interoperability
Includes the use of federations and Identity Bridge providers by end users

Important recommendations
- Support for authentication domains within alliances and federations
Security and other measures for reduction of identity threats and risks, including protection of resources and personally identifiable information

- 13 recommendations applicable to IdPs
- Security of identity resources, including 4 specifically related to protection of personally identifiable information

Important recommendations

- Support for non-repudiation of assertions
- Consider adopted global standards in ITU, ISO and other bodies for Identity Assurance and Authentication
- Dynamic establishment of time-limited trust mechanisms for transient and changed relationships
- Support for terminal device objects (e.g., SIM cards)
- Notification of compromised identity resources to affected parties
- Support for multi-factor authentication
- IdM identity proofing matching different authentication contexts, especially when requested
- Provide levels of identity protection, including support for relevant OECD privacy guidelines
- Provide end user transparency and notification capabilities relevant to protection of personally identifiable information
3 requirements/recommendations for auditing and compliance

Especially important

- Support for use of auditing mechanisms and exchange of information about those mechanisms
- Recommended time-stamp accuracy
- Area where more work would occur in Phase II of the Focus Group
3 recommendations applicable to Useability, Scaleability, Performance, Reliability, Availability, Accounting, Internationalization, and Disaster Recovery

- Important recommendation includes support for accounting mechanisms
- Area where more work would occur in Phase II of the Focus Group
Object Communications

- Most Identity Management capabilities apply equally to all object communications
- Some objects that are terminal based (e.g., SIM cards, physical credential readers, geospatial units, and sensors readers) both support and require significant IdM capabilities
- Support for autonomous networked object IdM interoperability requires further study together with JCA-NID, SG4 (OA&M), and other object-oriented bodies
  - How will competing object demands for network resources be prioritized and managed, especially during emergency conditions or network failures
  - What legal responsibilities and rights are associated with objects and how they expressed globally and discovered
  - This work is an important part of proposed FG IdM Phase II remit
Implications for NGN and other developments

- Almost every ITU-T Study Group has new Identity Management action items
  - Unclear how to coordinate
  - Significant WTSA 2008 implications
- Actions also essential network/cyber security
- Requirements include changes to IdM administrative practices
- TSB IdM responsibilities and ITU organs are similarly implicated including responding to global IdM needs at WTSA and other venues
  - How is global discovery of authoritative identifiers and other identity resources going to occur
- GSC-12 resolution calls for an ITU global coordinating role across array of standards bodies
- Numerous new and evolved
  - Opportunities for business
  - Actions for government
- Second Phase of Focus Group IdM aimed at
  - Completing framework
  - Assisting implication assessment
  - Dealing with objects
  - Facilitating transfer of work to Study Groups and other forums