

ITU-T Joint Meeting on the IdM Focus Group Reports

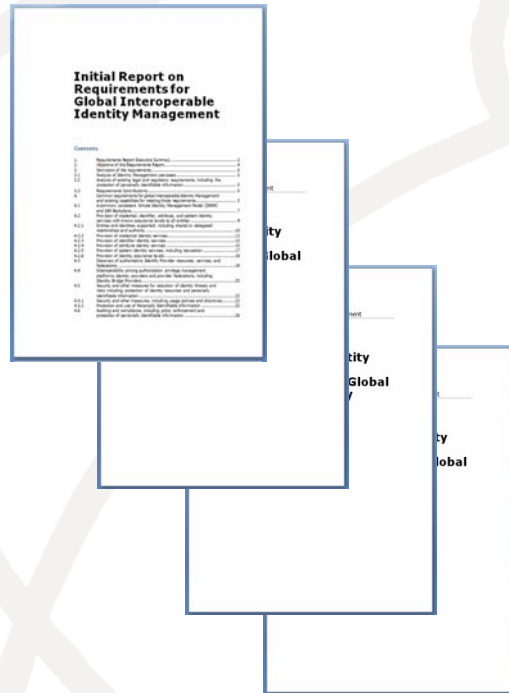
Toward global Interoperable Identity Management

Anthony-Michael Rutkowski

Vice-President, VeriSign

Chair, ITU-T IdM FG Requirements WG

Focus Group Products



- Reference materials
 - Ecosystem
 - Lexicon
 - **Existing legal & regulatory compendium, including privacy**
- Use cases, platforms, gaps
- **Requirements structure and provisions, including privacy related deliverables**
- Draft framework(s)

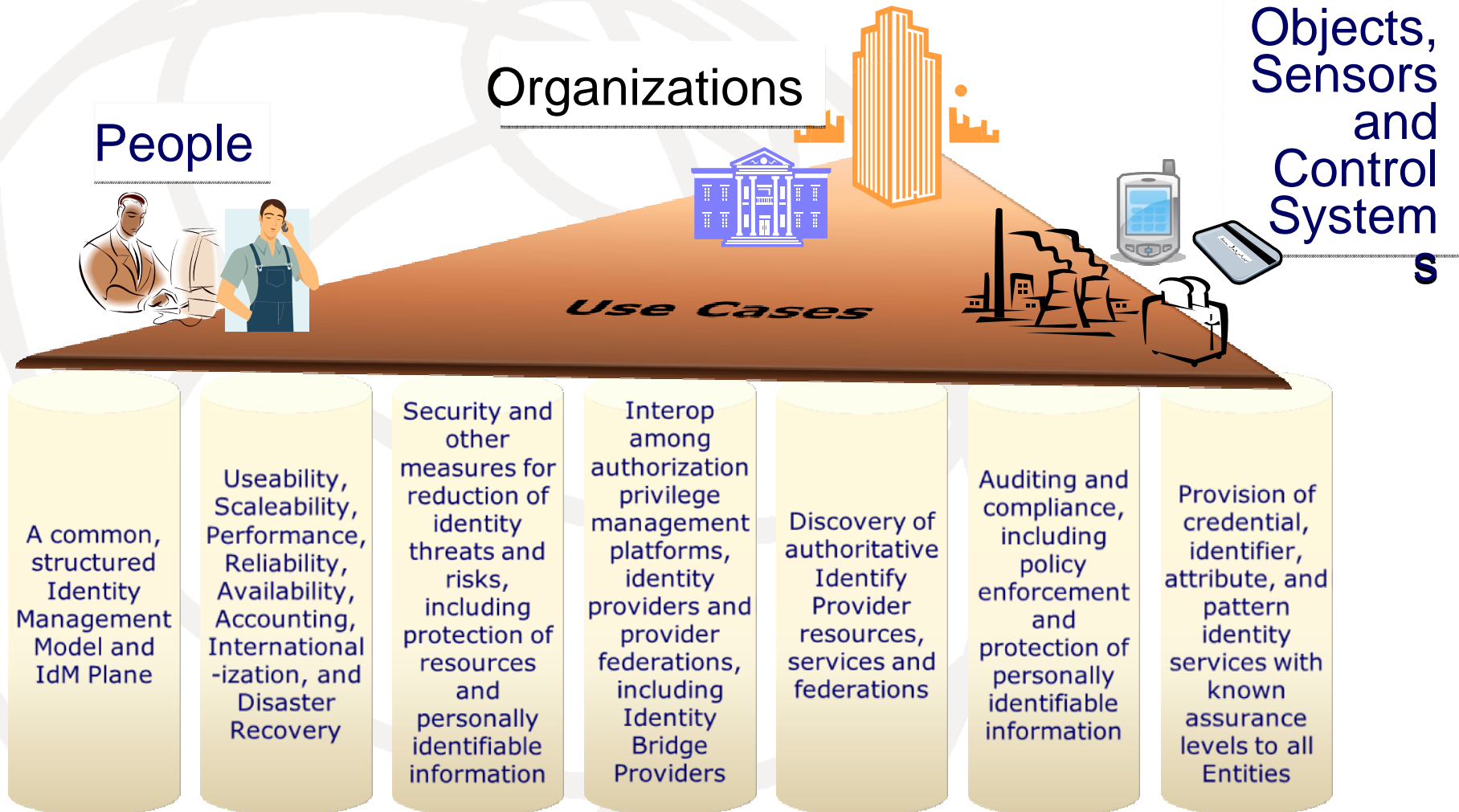
Largely Network Centric

Initial Report on Requirements for Global Interoperable Identity Management

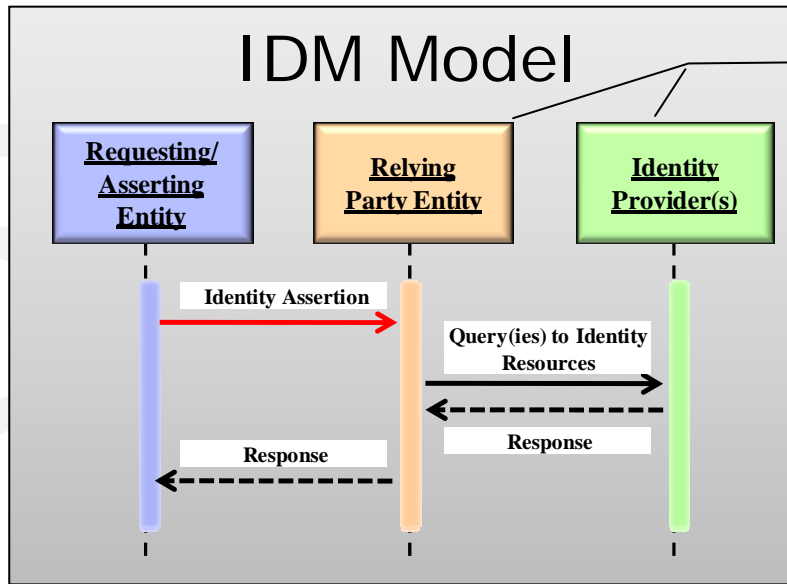
Contents

1.	Requirements Report Executive Summary	2
2.	Objective of this 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 Contributions.....	5
4.	Common requirements for global interoperable Identity Management and existing capabilities for meeting those requirements.....	5
4.1	A common, consistent Simple Identity Management Model (SIMM) and IdM Backplane.....	7
4.2	Provision of credential, identifier, attribute, and pattern identity services with known assurance levels to all entities	9
4.2.1	Entities and identities supported, including shared or delegated relationships and authority	10
4.2.2	Provision of credential identity services.....	13
4.2.3	Provision of identifier identity services	15
4.2.4	Provision of attribute identity services	15
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 Bridge Providers	20
4.5	Security and other measures for reduction of identity threats and risks, including protection of identity resources and personally identifiable information	22
4.5.1	Security and other measures, including usage policies and directives.....	22
4.5.2	Protection and use of Personally Identifiable Information	25
4.6	Auditing and compliance, including policy enforcement and protection of personally identifiable information	26

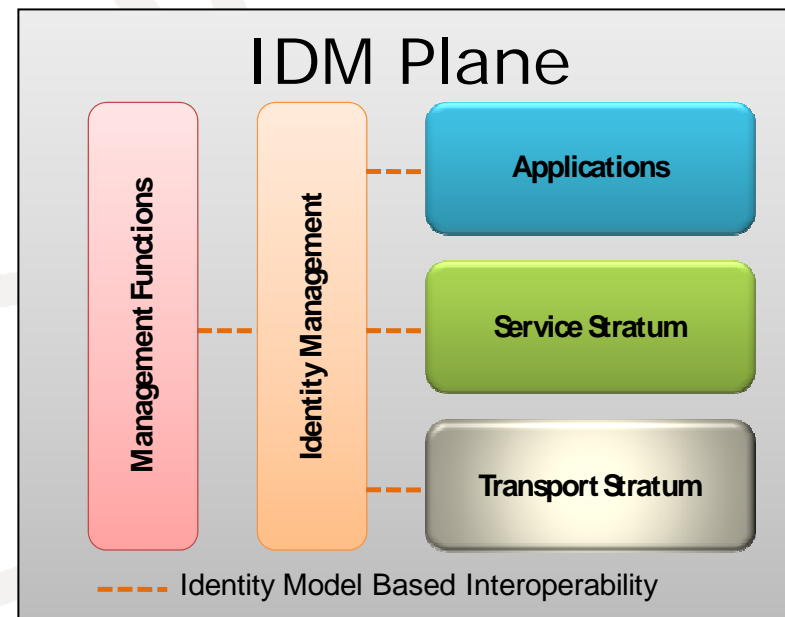
Requirements for Global Interoperable IdM: the Seven Pillars



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



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

- 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)

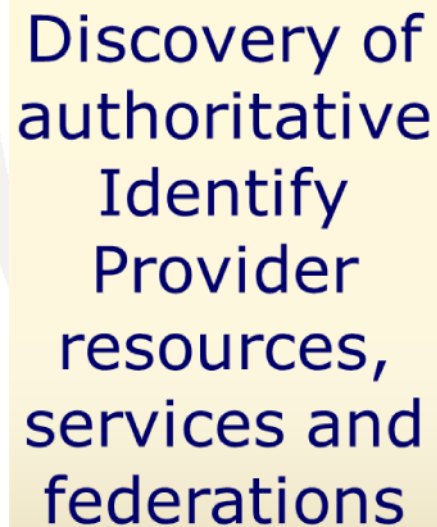
- Real persons
- Legal persons
 - Institutions
 - Organizations
 - Guardians/agents
 - Group
- Objects
 - Physical
 - Terminal devices
 - Network equipment
 - SIM or Smart Card
 - Virtual
 - Software
 - Geospatial
 - Content

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



Discovery of authoritative
Identify
Provider
resources,
services and
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



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

- 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



Auditing and compliance, including policy enforcement and 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



Useability,
Scaleability,
Performance,
Reliability,
Availability,
Accounting,
International-
ization, and
Disaster
Recovery

- 3 recommendations applicable to Useability, Scaleability, Performance, Reliability, Availability, Accounting, Internationalization, and Disaster Recovery
- Important recommendation include support for accounting mechanisms
- Area where more work would occur in Phase II of the Focus Group

Implications for NGN and other developments

- Almost every ITU-T Study Group has new Identity Management action items arising from the requirements
 - Unclear how to coordinate
 - Significant WTSA 2008 implications
- Requirements are 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
- Requirements produce numerous new and evolved
 - Opportunities for business
 - Actions for government
- Residual work on IdM aimed at
 - Transitioning the work into all ITU-T Study Groups and ITU-D
 - Dealing with objects and new NGN services