Identity Management as An Application Enabler

Laurence Feijt,
Solution Architecture, Director APAC, Alcatel-Lucent
Outline

- Identity Management as an Application Enabler
- Definition & Standardization Status
  - Standardization of the new services in Question 16
  - Questions that Question 16 of SG 13 studies
  - Collaboration on IdM and security with other Standards Development Organizations (SDO)
- New Business Models and Use Cases
- Key Take Aways
Section 1: Identity Management as an Application Enabler
Internet companies are creating increasingly complex offers

- Connect users to businesses
- Using speech recognition
- Others: Free411, TellMe

- Location-based service platform
- Makes IM and SMS interchangable
- Presence-enabled address book (for example, IMS/RCS)

- Single personal phone number
- Visual voice mail
- Conference calling
- Personalized greetings
- For free

Web offers are rapidly getting richer
Relationship between Internet and network-based service providers

Service is about experience

Service is about access and connection

The current business model is unstable
Enabling a trusted web experience

OPEN INNOVATION
- Ecosystem
- App developers
- New services

BETTER EXPERIENCE
= More Customers

TRUST
- Security
- Reliability
- Billing
- Privacy
The full scope of service innovation

- Few high volume services (typically service provider branded)
- Medium number of medium volume services (for example, co-branded)
- Huge number of third-party services serving few customers

Enabled by an open mesh structure of application/content providers, service providers and developers

Result: Internet scale for telco innovation

Yogyakarta, Indonesia, 27-29 July 2009
Service providers own assets to enhance end-user applications

- Presence, network address book
- Location
- Content
- Reliable, global, fixed and mobile voice services, SMS
- Service-aware IP network
- Trusted payment channel
- Subscriber profiles
- Secure identification, authentication
- Home service gateway
- 1 800-252-2835

Yogyakarta, Indonesia, 27-29 July 2009
Zoom-in: Service provider API/asset base monetization flow

#1. Capture increased share of content and application revenues (spend) through direct and indirect users
#2. Increase demand for SP-branded applications and data usage/access

- **Service provider**
  - API
  - Revenue Share
  - API usage-based fee/revenue share
  - Incremental revenue based on application usage (such as an increase in data and voice minutes)

- **SPs app developers**
  - API
  - Revenue Share
  - API usage-based fee/revenue share

- **SPs app store**
  - App
  - Voice mail, voice calls
  - SMS, speech-to-text

- **End user**
  - Monthly subscription

- **Third-party app developers**
  - API

- **Third-party app store**
  - App
  - Notification app
  - Broadcast SMS app
  - Profiling app

- **End user**
  - License/subscription

- **Enterprise app portal**
  - App
  - Voice mail, voice calls
  - SMS, speech-to-text

- **End user**
  - License/subscription

- **Third-party app developers**
  - App

- **End user**
  - License/subscription

- **Service provider**
  - API
  - Revenue Share
Section 2: Identity Management
Definition and Standardization
Security and Identity Management work in ITU-T Study Group 13 (SG 13)

ITU-T SG 13 (Future networks including mobile and NGN) is an ITU-T Lead Study Group
- For future networks and NGN
- On mobility management and fixed-mobile convergence

Within SG 13 Working Party 4 (QoS and Security) leads standardization on security and IdM

<table>
<thead>
<tr>
<th>Question</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q.4/13</td>
<td>Requirements and frameworks for QoS enablement in the NGN</td>
</tr>
<tr>
<td>Q.16/13</td>
<td>Security and Identity Management</td>
</tr>
<tr>
<td>Q.17/13</td>
<td>Packet forwarding and deep packet inspection for multiple services in packet-based networks and NGN environment</td>
</tr>
</tbody>
</table>

Q.16/13 of WP 4 is dedicated to studies of security and identity management

Yogyakarta, Indonesia, 27-29 July 2009
Identity Management as an Application Enabler

- IdM deals with the life cycle and correlation of identifiers.
- It enables the emerging applications that rely on integration of the IMS-based authentication with the
  - PKI-
  - OpenID-
  - Kerberos-based authentication mechanisms
- These integration mechanisms are being standardized in ITU-T SG 13.
- IdM is an enabler of the Mobile Payment applications – work item of SG 13.
Identity Management (After ITU-T Recommendation Y.2720)

IdM Capabilities
- Identity Lifecycle Management
- Correlation and Binding of Identity Information
- Authentication, Assurance, and Assertion of Identity Information
- Discovery and Exchange of Identity Information

Identity Information
- Identifiers (e.g., User ID, email address, telephone number, URI, IP address)
- Credentials (e.g., digital certificates, tokens, and biometrics)
- Attributes (e.g., roles, claims, context, privileges, location)

Entities
- Organizations, Business Enterprises, Government Enterprises
- Users & Subscribers
- Network and Service Providers
- User Devices
- Network Elements and Objects

Business and Security Applications
- Federated Services
- Application Access Control (e.g., Multimedia and IPTV)
- Single Sign-on/Sign-off
- Role-based Access to Resources
- Protection of Personally Identifiable Information
- Security Protection of Information and Network Infrastructure
Standardization of the new services in Question 16 (1/3)

Mechanism for integration of the PKI-based authentication with IMS

- IMS security is based on the AKA mechanism, while security of certain NGN services (e.g., IPTV) is based on PKI certificates.

The integration mechanism:

- Enables blending of the NGN services and IMS services
- Leverages the strength of IMS security
Standardization of the new services in Question 16 (2/3)

- Mechanism for integration of the OpenID-based authentication with IMS
  - Enables the network operators to provide identity services to the users accessing the Web applications
  - Provides users with a SSO across the IMS and web services with an existing ISIM application
  - Allows users to control their public identifiers on the Web as specified by OpenID
  - Improves user security by engaging a user-trusted network operator in the access control to the Web applications
Standardization of the new services in Question 16 (3/3)

Mechanism for integration of the Kerberos-based authentication with IMS

- Allows a network provider to offer a range of authentication and authorization services based on a 3G handset. Particularly it can support the following use cases:
  - Access of the services of the enterprise network by a user with a 3G handset
  - Access of the Video-on-Demand (VOD) services offered by a Kerberos-enabled VOD server by a user with a 3G handset
Work items of Question 16 (Security and Identity Management)

- **Y.2701** Security Requirements for NGN Release 1
- **Y.2702** NGN Authentication and Authorization Requirements
- **Y.2703** NGN AAA
- **NGN Certificate Management**
- **NGN Security Mechanisms**
- **Architecture for Secure Mobile Financial Transactions in NGN**
- **Y.2720 NGN IdM Framework** (starts new series)
- **NGN IdM Requirements** (includes IdM Use Cases)
- **NGN IdM Mechanisms**

- **IdM Framework** defines the concepts of the IdM
- **IdM Use Cases** is a base for deriving the IdM requirements
- **IdM Mechanisms** provide support for the requirements
Leadership of the IdM and Security work in SG 13 (1/2)

- Hui-Lan Lu (Alcatel-Lucent, USA) – Chairman of WP 4/13
- Igor Faynberg (Alcatel-Lucent, USA) – Rapporteur of Q.16/13
- Igor Milashevskiy (Intervale, Russian Federation) – Associate Rapporteur of Q.16/13

The table below lists Editors of the Q.16/13 documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Editors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Y.2701 Security Requirements for NGN Release</strong></td>
<td>Martin Dolly (AT&amp;T, USA) Takashi Egawa (NEC, Japan)</td>
</tr>
<tr>
<td><strong>Y.2702 NGN Authentication and authorization Requirements</strong></td>
<td>Martin Dolly AT&amp;T, USA Ray Singh (Telcordia, USA)</td>
</tr>
<tr>
<td><strong>Y.2703 The application of AAA service in NGN</strong></td>
<td>Michael Hird (UK) Heang-Suk Oh (ETRI, Korea)</td>
</tr>
<tr>
<td>NGN Security Mechanisms</td>
<td>Martin Dolly (AT&amp;T, USA) Takashi Egawa (NEC, Japan)</td>
</tr>
<tr>
<td>NGN Certificate Management</td>
<td>Martin Dolly (AT&amp;T, USA) Ray Singh (Telcordia, USA)</td>
</tr>
<tr>
<td>Architecture for Mobile Financial Transactions in NGN</td>
<td>Igor Milashevskiy (Intervale, Russian Federation)</td>
</tr>
</tbody>
</table>
Leadership of the IdM and Security work in SG 13 (2/2)

<table>
<thead>
<tr>
<th>Document</th>
<th>Editors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Requirements for Mobile Financial Transactions in NGN</td>
<td>Igor Milashevskiy (Intervale, Russian Federation)</td>
</tr>
<tr>
<td>Mobility Security Framework in NGN</td>
<td>Yinxing Wei, (ZTE, PR of China)</td>
</tr>
<tr>
<td>Mobility Security Framework in NGN</td>
<td>Terry Wang (ZTE, PR of China)</td>
</tr>
<tr>
<td><strong>Y.2720 NGN IdM Framework</strong> (starts new series of Recommendations)</td>
<td>Richard Brackney (DoD, USA)</td>
</tr>
<tr>
<td><strong>Y.2720 NGN IdM Framework</strong> (starts new series of Recommendations)</td>
<td>Takashi Egawa (NEC, Japan)</td>
</tr>
<tr>
<td>NGN IdM Requirements (includes IdM Use Cases for NGN)</td>
<td>Martin Dolly (AT&amp;T, USA)</td>
</tr>
<tr>
<td>NGN IdM Requirements (includes IdM Use Cases for NGN)</td>
<td>Enhui Liu (Huawei, China)</td>
</tr>
<tr>
<td>NGN IdM Requirements (includes IdM Use Cases for NGN)</td>
<td>Anthony Rutkowski (Verisign, USA)</td>
</tr>
<tr>
<td>NGN IdM Requirements (includes IdM Use Cases for NGN)</td>
<td>Ray Singh (Telcordia, USA)</td>
</tr>
<tr>
<td><strong>NGN IdM Mechanisms</strong></td>
<td>Takashi Egawa (NEC, Japan)</td>
</tr>
<tr>
<td><strong>NGN IdM Mechanisms</strong></td>
<td>Zachary Zeltsan (Alcatel-Lucent, USA)</td>
</tr>
<tr>
<td>NGN Requirements and Use Cases for Trusted Service Provider Identity</td>
<td>Martin Dolly AT&amp;T, USA</td>
</tr>
<tr>
<td>NGN Requirements and Use Cases for Trusted Service Provider Identity</td>
<td>Ray Singh (Telcordia, USA)</td>
</tr>
</tbody>
</table>
Questions that Question 16 of SG 13 studies (from the Q.16/13 description)

- Recommendations, enhancements needed to standardize identification and cataloguing NGN threats and vulnerabilities?
- Security requirements of NGN to effectively counter these threats? Which of these requirements should be included in all NGN and which could be offered as an optional service?
- Recommendations or guidance for comprehensive, E2E security in NGN that span across multiple heterogeneous administrative domains?
- Recommendations or guidance for enabling attachment of terminals securely to NGN?
Questions that Question 16 of SG 13 studies (from the Q.16/13 description)

- How to define security architecture of identity management in next generation networks?
- What are security requirements to identity management in NGN?
- What new Recommendations are needed for supporting security requirements of identity management in NGN?
- What new Recommendations are needed for supporting secure interoperability among different circles of trusts (CoT) in NGN?
Questions that Question 16 of SG 13 studies (from the Q.16/13 description)

- What are security requirements of IPTV as its study evolves?
- What new NGN Recommendations are needed for supporting security requirements of IPTV?
- What new NGN Recommendations are needed for supporting security of financial transactions?
- What enhancements are required to provide energy savings directly or indirectly in information and communication technologies (ICTs) or in other industries? What enhancements to developing or new Recommendations are required to provide such energy savings?
Section 3: New Business Models and Use Cases
New Potential Business Models

Enhanced Loyalty Mgt:
End-user trade usage credits with frequent flier miles / other loyalty points

Targeted Advertising:
“Free” minutes, reduced content with receipt of advertising / coupons

Tiered Pricing:
Identity Management / Zero-Sign-on with pricing based on bandwidth usage

Third-Party Applications:
Enabling Revenue Acceleration with 3rd-party application developers

Privacy / Preferences:
End-user defines application behavior, conforms service to their needs

Policy Mgt

User Centric Personalized
Loyalty rewards
Determined by subscriber preferences

Welcome Bob to your concierge service

You have XXX points that can be instantly redeemed for your personal reward choices:

- **Book your next vacation and pick up your ticket at the counter**
- **Shop for gifts and pick up at the local store or have it delivered to friends and family**
- **Purchase sports memorabilia and pick it up at the next game**

**Single Sign-on / Identity Federation**
Link to page where transaction with 3rd party actually takes place

**Immediate, real-time results based on redemption / exchange of points**
Loyalty rewards
Determined by subscriber preferences

Welcome Bob to your concierge service

You have XXX points that can be instantly redeemed for your personal reward choices:

- Book your next vacation and pick up your ticket at the counter
- Shop for gifts and pick up it delivered to friends and family
- Purchase sports memorabilia and pick it up at the next game

Redeem

Identity federation through Data Grid provides single sign-on across domains

Bob clicks on United
With Federated Identity, no add'l “sign-on / password” required

Or – decides to go shopping and clicks on Amazon.com – again, no add'l “sign-on / password” required

Bob clicks on United
With Federated Identity, no add'l “sign-on / password” required

Identity federation through Data Grid provides single sign-on across domains
Multi-Screen Content store front
Personalization at it’s finest

- Personalized discovery
  - Stores targeted to specific subscriber market segments, devices, bearer’s location, and preferences
  - Personalized portal with specific theme, content offers and promotions
  - Dynamic, branded portals and subscriber storefronts
  - Customizable templates and reusable components for mobile and Web subscriber portals

Tailor the storefront based on Identity-based preferences
ITU-D Regional Development Forum for the Asia Pacific Region
“NGN and Broadband, Opportunities and Challenges”
Yogyakarta, Indonesia, 27 – 29 July 2009

Section 4: Conclusions
Identity As A Service: Network personalization Will Lead

Market Share Trends

- Personalization will lead to changes in market dynamics
- Personalized services will increase take rate from “generic” services – dropping competitors market share
- Personalized services will reduce churn – too difficult & inconvenient to transition/move “personalized” attributes to other providers

Yogyakarta, Indonesia, 27-29 July 2009
Collaboration on IdM and security with Standards Development Organizations (SDO)

Question 16/13 works with the following SDOs:

- ITU-T Study Group 17 (SG 17)
- The Joint Technical Committee 1 of the Organization for International Standardization and the International Electrotechnical Commission (ISO/IEC JTC1)
- The 3Rd Generation Partnership Project (3GPP)
- Open Mobile Alliance (OMA)
- Liberty Alliance
- Internet Engineering Task Force (IETF)
ITU-D Regional Development Forum for the Asia Pacific Region
“NGN and Broadband, Opportunities and Challenges”
Yogyakarta, Indonesia, 27 – 29 July 2009

Q&A