INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

February 2007

English only

Original: English

Question(s):

ITU-T- FG IdM – REPORT 1

Source: FG IdM Chairmanship

Title: Report of ITU-T FG IdM meeting, Geneva, Switzerland, 13-16 February 2007

This is the report of the first face-to-face (F2F) meeting of the ITU-T Focus Group on Identity Management (FG IdM) that was held 13-16, February 2007 in Geneva Switzerland.

Executive Summary

There is currently a continuing rapid expansion of IdM work among many forums, coupled with the increasing need for some manner of dialogue and convergence among those forums. Identity Management is emerging as a core Cybersecurity and infrastructure protection capability. Identity Management has also appeared as an important technical area in the overall NGN studies. To address these needs, the December 2006 meeting of SG 17 discussed and then approved establishing the Focus Group on Identity Management (FG IdM) with SG 17 as its parent Study Group. This was announced in TSB Circular 130. The FG IdM allows the ITU-T to play a high level coordinating role in bringing together for the first time, the many different forums, platforms, and experts in the Identity Management field. Such a need had already been identified at the ITU-T Workshop on *Digital Identity for Next Generation Networks* held on 5 December 2006, see http://www.itu.int/ITU-T/worksem/ngn/200612/index.html.

The first face-to-face (F2F) meeting of the Focus Group on Identity Management was held from 13-16 February 2007 in Geneva. The welcome address was delivered by Malcolm Johnson, Director of TSB´, who welcomed participants and asserted his support for the work of this FG. The meeting was well attended (55 participants) and represented key players in the IdM field. Participation was wide in scope including key Standardization Organizations (SDO), consortia, alliances, vendors, operators, academia and developers of solutions in the IdM space.

By almost any measure, the 1st FG IdM meeting was successful in addressing the need for a global IdM. After an initial day of traditional introduction of contributions and an evening of new platform demonstrations, two days of highly innovative "Silicon Valley" like Open Space meetings were conducted, during which all participants could collectively construct their own topic and meeting spaces. This allowed the participants to share their views, experiences towards constructive future solutions. A tool supporting this activity was an open, private "Wiki" used by the participants to collectively express and draft their own structure and text for IdM work going forward (See www.ituwiki.com). This was followed by more traditional meetings and activities to produce a Focus Group structure, meeting report, and calendar of future activities. The pioneering process turned out to be useful and can potentially be used by other ITU groups to institute new working methods common in today's ICT development community.

One of the key objectives of the Focus Group's work at its first meeting, i.e. to identify and bring together the many IdM groups and experts, was fully met. It has already served to both reinforce the collective work, as well as to identify how to minimize duplication among existing Study Groups and SDOs through collaboration and re-use of specifications. This remains the basic purpose of the IdM FG. A primary focus of FG IdM is on "assertions of identity" and means for enhancing trusted exchange and authoritative verification of those assertions, not the authentication process for creating an identity. As such the meeting refined the scope of the FG IdM and created various working groups. The current structure includes the following working groups:

- *Framework Coordination* with the four subgroups *Requirements, Use-Cases, Data model* and *Architecture*
- *Discovery*
- *Legal and Regulatory*
- *Lexicon and Ecosystem* including terminology

- *Liaison and Coordination*

Action plans and list of deliverables for all working groups were developed in the meeting.

In addition to the presentations on the 1st day, there were a set of demos presented by Microsoft, Verisign, OpenId, AmSoft and Higgins.

In conclusion, this F2F meeting illustrated the value add that this FG can bring to the ITU-T and to the IdM community in general. This is the first time where an activity of such scope was able to bring together experts who would not otherwise have collaborated and converged on this subject. This clearly demonstrates the substantial value of the FG IdM.

Table of contents

1. Introduction

ITU-T SG 17 at its 9-15 December 2006 meeting in Geneva established a Focus Group (FG) on Identity Management (IdM) (See TSB Circular 130). The creation of the FG came as a result of the of the ITU-T Workshop on Digital Identity for Next Generation Networks that was held in Geneva, 5 December 2006 and the support expressed by ITU-T Members and non-members on the subject. The results of the workshop (see COM 17-TD 0227 Rev. 5) depicted the inadequate coverage of network aspects in current approaches and the fragmentation of existing IdM solutions. It was evident that there is an immediate need for a gap analysis and harmonization effort among existing approaches.

The FG IdM held its first face-to-face (F2F) meeting from 13-16 February 2007 in Geneva. The welcome address was delivered by Malcolm Johnson (Director of TSB), who welcomed participants and asserted his support for the work of this FG. The meeting was well attended (55 participants) and represented key players in this field. Participation was wide in scope including key Standardization Organizations (SDO), consortia, alliances, vendors, operators, academia and developers of solutions in the IdM space. The attendance break down is depicted in Figure 1.1. From the Figure, 72% of the participants came from members, 11% from the academic field, 9% non-members, 6% experts in the field, and 2% from the press, Many countries participated in the event. The highest percentage of participants came from the USA (27%) followed by the United Kingdom (UK) at 15% and Germany at 13%. Participation from companies, SDOs, operators etc. is given in Figure 1.2.

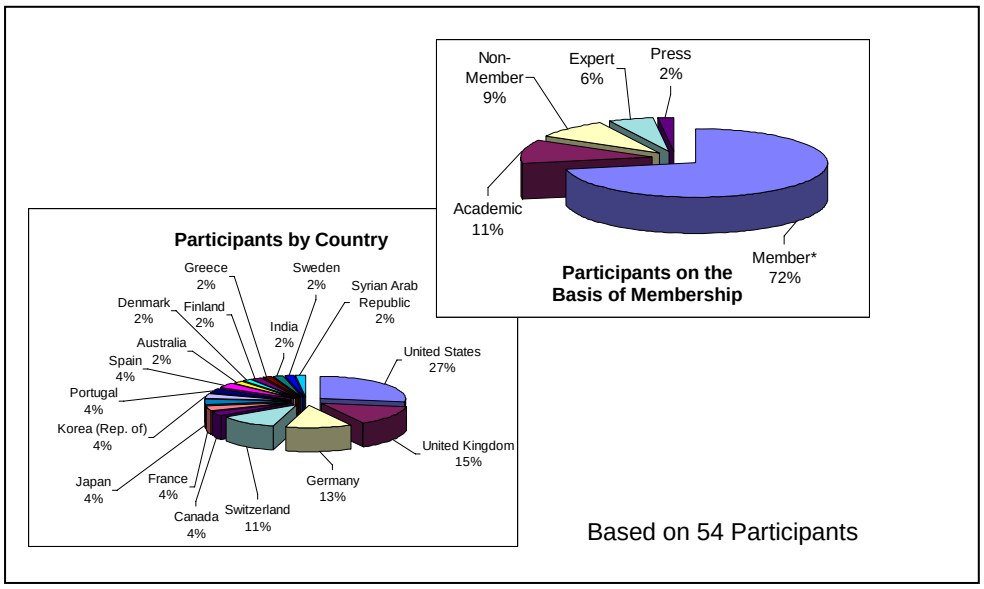

Figure 1.1 Attendance Breakdowns

- Alcatel-Lucent
- AmSoft Systems
- Australia - DCITA
- British Telecom
- Cadzow (ETSI IdM STC)
- Deutsche Telekom
- ENISA
- ERO
- ETRI
- France Télécom
- Harvard University
- Iamdentity
- IBM
- Identity Trust
- Identity Woman
- Independent Accessiblity Consultant
- Instituto Telecomunicações Aveiro
- Japan - NICT
- Microsoft
- Motorola
- NEC
- Netnod Internet Exchange Ab
- Neustar
- Nokia
- Nortel Networks
- OFCOM
- Parity Communications
- Siemens Networks
- Sun Microsystems
- Switzerland - BAKOM
- Syrian Arab Republic
- Telcordia Technologies
- Telefónica
- TeliaSonera
- Tertius
- UK - CESG
- Universidad Carlos III
- University College of London
- University of Stuttgart
- US - DoD
- Verisign
- Warren Communications News
- WIPO

Figure 1.2 Participants Affiliation

Currently, there are various players in the development of IdM solutions that range from application centric with central control of identifiers to user centric approaches to card based solutions. At this time, the identity management landscape can be described as a triangle with three pillars (see Figure 2.1.1). From the Figure, there are essentially three approaches for IDM, those that are based on Liberty/SAML, those that are based on user centric principles (such as OpenID) and the Microsoft approach that is based on Card Space. All of these solutions are application centric with little emphasis on network-based identifiers. Network-based identity approaches are not adequately covered in current application centric solutions. As such, one objective of the first F2F meeting was to get the three communities talking to each other to help them agree on the existence of gaps in the current solutions and to set a framework for cooperation. The meeting used Open Space concepts (see http://en.wikipedia.org/wiki/Open_Space_Technology) to help achieve good results in terms of getting the various communities to interact and help define the scope and deliverables of the FG. In order to facilitate collaboration between participants, the meeting used a private wiki tool as a real time scratch pad to allow participants to share information (see www.ituwiki.com). The wiki will be used as a collaboration tool between meetings and can be accessed to view the latest discussion of the FG.

2. F2F meeting working methods

Currently there are many organization and groups working in the IdM space. One of the objectives of the first F2F meeting of the FG IdM was to agree on the terms of reference as specified in TSB Circular 130. As such, the agenda of the meeting included a list of topics that were deemed important for the discussions (see Annex A). Furthermore, a list of presentations was designed to set context for the participants during the first day of the meeting. The presentations covered a wide scope of topics and were delivered by participants from various SDOs, vendors and operators. The list of presentations is given in Table 2.1.

Table 2.1: Presentations

Topic	Presenter	Affiliation
Welcome	Mr. Malcolm Johnson	Director TSB
Mission, Scope and Deliverables	Abbie Barbir	Nortel
ITU-T SG13, SG17 IdM Activities	Tony Rutkowski	VeriSign
ISO/IEC JTC 1/SC 27 IdM Activities	Dick Brackney	USA
ETSI IdM Activities	Scott Cadzow	ETSI
Content Industry Standard Identifier Activities	Norman Paskin	AmSoft
NGN Overview	Tony Rutkowski	VeriSign
Liberty Alliance	Fulup Ar Foll	Liberty Alliance
3 GPP IdM Related Activities	Martin Euchner, Frederick Hirsch	Siemens, Nokia
CardSpace and Identity Metasystem	Mike Jones	Microsoft
OpenID	David Recordon	OpenID
XRI (i-names) and XDI	Ajay Madock	Amsoft
Higgins Project	Paul Trevithick	Higgins
JCA-NID	Pierre-Andre Probst	JCA-NID
OID	Oliver Dubuisson	France Telecom
Handles Systems	Norman Paskin	Handel.org
Secure Identity Aware Networks	Sergio Fiszman	Nortel
3 GPP IdM Related Work and Identities	Martin Euchner, Frederick Hirsch	Martin Euchner, Frederick Hirsch
Identity Commons	Kaliya Hamlin	Kaliya Hamlin

2.1 Focus on minimizing overlap

In the meeting presentations from SG 17, SG 13, JCA-NID, and ISO/IEC JTC 1/SC 27 were used to set context for the meeting in two ways. The first objective was to focus on minimizing overlap within and with ITU-T activities and the second objective was aiming towards identifying the gaps in current solutions when it comes to network identifiers. There was an understating among participants to emphasize gaps in current solutions. The FG also agreed on the minimization of duplication of work among existing Study Groups and SDOs as a primary objective of the FG IdM through collaboration and re-use of standards. It was also agreed that the primary focus of FG IdM is on "assertions of identity" and means for enhancing trusted exchange and authoritative verification of those assertions as opposed to the authentication process for creating an identity. Such work has long been treated by SG 17 (and its predecessor SG 7).

Figure 2.1.1 depicts the current identity management solution space. There are three solutions in the market space. Those that are based on Liberty/SAML, those that are based on user centric approach (OpenID) and the WS-Trust (Cardspace) approach. Other identity efforts are being carried out in SG 13, SG 17 and JCA-NID. These solutions are application centric and generally do not use network based identifiers. However, as was apparent from the 5 December 2006 Workshop on Identity management that was held by the ITU-T (COM 17-TD 0230, December 2006 - see Annex D), these solutions are incomplete and there is a common understating that these solutions need to interoperate.

The FG IdM is developing a logical global IdM framework that provides interoperability among the current diverse identity silos that either use an identity provider centric identity, a card based solution or a user centric based identity solution (see Figure 2.1.1).

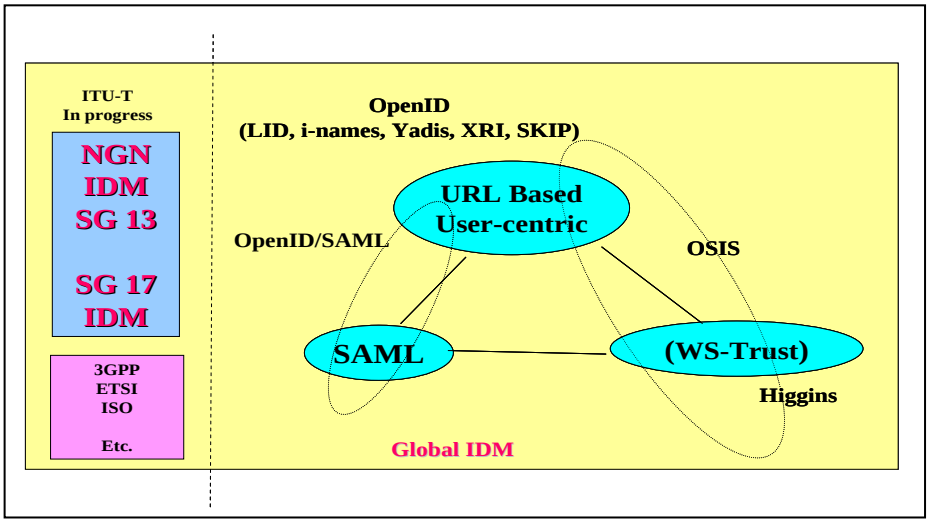

Figure 2.1.1 Identity solutions landscape

In order to achieve a global IdM infrastructure, current and future networks will require additional identity related capabilities (discovery of identity attributes, advertisement of identity attributes, etc.). In other cases, gateways or new protocols will be needed to achieve seamless identity interoperability among the identity capabilities that are embedded in networks, especially those in legacy systems where the opportunity to add additional identity capabilities will be limited.

Given this scope of IdM work, the Focus Group will support the development of global IdM framework principles and guidelines for its parent Study Group, SG 17. The group will identify requirements for specific infrastructures that will then be the specific responsibility of groups or SDOs responsible for that particular infrastructure, such as ITU-T SG 13 for NGN. This would, for example, include requirements on additional functionality needed within the NGN to achieve a global IdM framework. Brokering identities or bridging the identity capabilities in different networks is however an overarching issue, which will require an input from ITU-T SG17, which is the main ITU-T SG responsible for IdM guideline and principles versus specific network IdM solutions like those for the NGN.

This division of work is similar to ITU-T X.805 Recommendation developed by SG 17. This Recommendation defines network security architecture for providing end-to-end network security. The X.805 security architecture can be applied to various kinds of networks where end-to-end security is a concern and can be applied independently of the network's underlying technology. X.805 defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of X.805 is to serve as a foundation for developing the detailed

recommendations for the end-to-end network security. For example X.805 is the basis for developing the WiFi security standards. This is analogous to the IdM work underway by the FG IdM/SG 17.

Furthermore, the work in the FG is broader than that which is occurring in JCA-NID. The work in JCA-NID evolved from the ongoing RFID and sensor network studies in the ITU-T, remains focussed on this subject, and useful collaboration in this area has been maintained, including related liaison with other organizations. The FG IdM will look to the JCA-NID for RFID and sensor network identifier expertise and assist in the integration of its work into the overall identifier assertion, discovery, and interoperability framework.

One of the tasks of the FG IdM will be to do a gap analysis (see Figure 2.1.2). From the figure the following can be said:

- There are gaps related to the exchange, correlation and linkage of the identity related information between the different planes (user, application/service and network) that needs to be investigated. Example gaps are:
    - Data model for exchange (pull and push) of identity related information between the network and application/service (e.g., application requesting and the network providing location or network address information as generic objects)
    - Architectural model to allow correlation of the identity related functions in the different planes (e.g., user control process, application process and network functions) to allow interoperability (i.e., bridging of existing functions and capabilities) and adherence to policy controls
    - Model to support user control of certain network related preferences (e.g., user control of network/service provider preferences and privacy attributes)

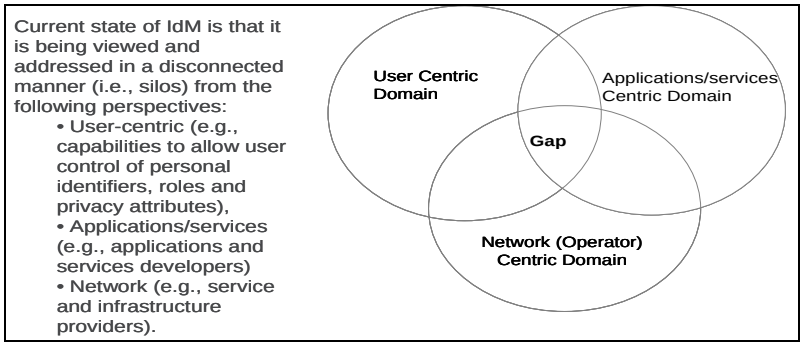

Figure 2.1.2 Gap analysis

2.2 Proposed scope

The scope of the Focus Group is Identity Management (IdM) for telecommunications/ICT in general; and specifically to facilitate and advance the development of a generic IdM framework that:

- includes the means of contextualized discovery of resources (e.g. person, device, application, access point, service, process, network, object, providers, content resources) and attributes and policies (for interaction, quality, security and privacy) about them
- includes the means to provide and optionally use claims (verifiable or not) to gain access to interact with these resources
- doesn't preclude the use of comprehensible, consistent user interfaces
- seeks to minimize the disclosure of personal information
- works towards interconnected, interoperable entities (network, services, users, applications)

2.3 Benefits

- Making possible entirely new user experiences and new business opportunities based on the emergence of a global identity/social layer
- Unlocking or leveraging the often latent value of social/identity infrastructure

- Making the user's life easier, privacy-respecting, and more secure in the digital world
- The ability to communicate securely, and exchange information across domains
- Reduce cost through the reuse of existing infrastructure
- Mitigate security risks for the network infrastructure, end users, governmental authorities and operators

2.4 Working assumptions

- Entities may have several digital identities
- Digital identities are contextual
- Focus on reuse rather than reinvention
    - Delegate items better done in specific Study Group or other SDOs to those groups
    - Work on bridging existing architectures and on gaps not addressed by others
    - FG Covers the whole ID space to bridge the approaches
- The FG will focus on the minimization of duplication among existing Study Groups and SDOs. This will be achieved through collaboration and re-use of specifications. If the FG determines that any specification of another Study Group or SDO needs modification, the need will be communicated to the affected body and a request made for that body to do the work. The FG group will not attempt to pursue such work on its own.

2.5 Working principles

The FG developed several principles that are listed in the next sub-clauses.

2.5.1 General

- social networking applications are valuable space to be engineered towards
- phone is a social networking tool
- identity anchorage is valuable
- Operators have opportunity to be identity anchor
- operators/vendors have a role to play in the emerging social networking space
- The area of reputation is of value
- reputation is contextual
- identity is contextual

2.5.2 Overall observations

- There was / is a communication gap between those working at the web services / network levels
    - Some inroads were made on bridging the gap
- The refined scope now differentiates the Focus Group from both ITU-T SGs and other fora
    - Identify functions / issues to be addressed from a global perspective
    - Pass on items relevant to those concerned
    - Work on items will be done in the FG only if it cannot be delegated
- A key item is to identify the gaps that open the door to new real business opportunities
- After some initial surprise, the working method in the FG (open spaces, ..) was well taken

2.5.3 Key problem areas

- Advertisement of attributes

- Discovery of attributes
- Insertion of strongly authenticated attributes (MSISDN, telephone number, address, name, billing address)

2.5.4 Common understanding

- There is a great opportunity in leveraging identity that already exists
  - Bridging the gap and addressing the missing pieces will make this even more powerful
- Need to discover and combine the attributes of three domains network centric / user centric / application centric
  - Policies should be understandable across domains
- We need to have an overview of existing architectures by 3Q 2007
  - This is the starting point to identify gaps and bridges
  - Identify missing functions, protocols, etc.
- A Metadata model is needed
- Controlled release and transmission of context data must be supported
  - Privacy of the user always at the centre
- Disruptions are arising
  - Identity can leverage such disruptions towards new business
  - Operators can become identity providers and leverage such new business

2.5.5 Operator can add value in these spaces

- Geographic location attribute assertion (cell ID, City, x Street)
- Contact identifier/s attribute assertion
- Identity anchorage (MSISDN on SIM card, telephone number, IMS HSS identities)
- Deriving user's context (home, work)
- Deriving user's task (from handset velocity etc.)
- Social relationship ("buddy list") storage/advertisement geographic location attribute assertion (cell ID, City, x Street)

2.5.6 General observations

- Social networking applications are valuable space to be engineered towards
- Identity anchorage is valuable
  - operators have opportunity to be identity anchor
- Operators/vendors have a role to play in the emerging social networking space
- The area of reputation is of value
- Reputation is contextual
- Identity is contextual

3. FG IdM organization

3.1 Leadership positions

- Chairman: Abbie Barbir, Nortel Networks

- Vice-Chairman, Richard (Dick) Brackney, USA
- Vice-Chairman, Tony Nadalin, IBM

3.2 Working groups

The discussion and collaboration among participants led to the creation of four continuing working groups.

1. *Framework Coordination* including (Leaders Tony Nadalin (IBM, USA) and Scott Cadzow (Cadzow, UK)) :
   - *Requirements* subgroup (Leader: Amardeo Sarma (NEC, Germany), Piotr Pacyna (Universidad Carlos III, Spain))
   - *Use Case* subgroup (Leaders: Sergio Fiszman (Nortel, Canada), Mike Jones (Microsoft, USA), Lee Dryburgh (University Collage of London, UK))
   - *Data model* subgroup (Leaders: Tony Nadalin (IBM, USA), Paul Trevithick (Parity, USA))
   - *Architecture* subgroup (Leaders: Sergio Fiszman (Nortel, Canada), Zachary Zeltsan (Alcatel-Lucent, USA), "OP"tdb)
2. *Discovery* (Leader: Tony Rutkowski (Verisign, USA), Lee Dryburgh University Collage of London, UK))
3. *Legal and Regulatory* including privacy protection (Leaders Tony Rutkowski (Verisign, USA))
4. *Lexicon and Ecosystem* including terminology, definitions, and links to other IdM forums, activities, and developments (Leaders , Michael Hird (UK), Kaliya Hamlin (Identity Woman, USA))
5. *Liaison and Coordination* including collaboration within the ITU. Current liaison officers:
   - Dick Brackney (DoD, USA), FG Vice Chairman liaison to SG 13;
   - Scott Cadzow (Cadzow, UK), liaison to ETSI TISPAN;
   - Jae Young Ahn (ETRI, Korea), liaison to JCA-NID and SG 2.

3.3 Current WG and subgroups scopes

1. Terms of Reference of Framework Coordination Working Group. Scope of WG:
   - Develop a functional architecture for IdM taking into account discovery issues, satisfying the requirements and use cases, and leveraging an abstract data model.
2. Terms of Reference of Requirements subgroup. Scope of subgroup:
   - Capture IdM-related requirements for the subgroups within the WG
   - Derive requirements from use cases.
   - Identify requirements from various planes of perspective (e.g. user, network, application…).
3. Terms of Reference of Use Case subgroup. Scope of subgroup:
   - Production of example use cases (user, operator).
4. Terms of Reference of Data model subgroup. Scope of subgroup:
   - Developing an abstract, generic data model interconnecting interoperable entities (e.g. networks, devices, content resources, people, applications etc...).
5. Architecture subgroup. Scope of subgroup:
   - Identity suitable architectures for IdM in telecommunications
   - Analyze candidate architectures from the viewpoint of IdM
   - Define functional entities in the IdM architecture
   - Identify (exposed) interfaces in IdM architecture
   - Identity security functions for IdM in the architecture entities

- Show mapping/relationship of IdM architecture with Telecommunications architecture(s)
- Identify and close gaps.

6. Terms of Reference of Discovery Working Group. Scope of WG:
   - The means of contextualized discovery of resources (e.g. person, device, application, access point, service, process, network, object, providers, content resources) and attributes and policies (for interaction, quality, security and privacy) about them.

3.4 Action plan

This section provides current work scope of each working group and current list of deliverables.

3.4.1 Action plan of the Discovery working group

Compile and produce a Technical Report “Contextualized discovery of resources”

Editors: Tony Rutkowski (Verisign, USA)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

3.4.2 Action plan of the Requirements subgroup

Compile and produce a Technical Report ”IdM Requirements”

Editors: Piotr Pacyna (Universidad Carlos III, Spain), Paul Trevithick (Parity, USA)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

3.4.3 Action plan of the Use Cases subgroup

Compile and produce a Technical Report “IdM Use cases”

Editors: Mike Jones (Microsoft, USA), Sergio Fiszman (Nortel, Canada), Lee Dryburgh (University College of London, UK)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

3.4.4 Action plan of the Data Model subgroup

Compile and produce a Technical Report “Data Model for IdM”

Editors: Tony Nadalin (IBM, USA), Paul Trevithick (Parity, USA), Joao Girao (NEC, Germany)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

3.4.5 Action plan of the Architecture subgroup

Compile and produce Technical Report “IdM Architecture for Telecommunications”

Editors: Joao Girao (NEC, Germany), Sergio Fiszman (Nortel, Canada), Martin Euchner (Siemens-Networks, Germany)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

- Inspect input contributions from 1st F2F meeting for architecture aspects
- Check consistency with IdM-related activities in NGN

3.4.6 Legal, Regulatory and Privacy Requirements

Draft Requirement document

Editor: Tony Rutkowski (Verisign, USA)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

3.4.7 Lexicon, and Ecosystem

Lexicon, Glossary, Living List: Mike Hird (UK), Abbie Barbir (Nortel, Canada)

Editor: Kaliya Hamlin (Identity Woman, USA)

Milestones: Stable draft available in Q3/2007, 1st draft available in April 2007

4. Meeting results

Several documents were generated in the meeting as a result of the breakout sessions that occurred during the meeting. These documents are available in the ITU-T FTP site of the FG IdM. Liaison statements were sent to various Study Groups and SDOs.

4.1 List of input documents

Number	Source	Title
DOC-000	TSB	Live list of documents
DOC-001	ITU-TQ.15/13 Rapporteur Group	Liaison statement on proposal for the joint work on Identity Management
DOC-002	ITU-T SG 17	Liaison statement on report from Lead Study Group on telecommunication security
DOC-003	AmSoft Systems	Role of Identity in NNA
DOC-004	Chairman, FG IdM	Draft Agenda for FG IdM Meeting
DOC-004r1	Chairman, FG IdM	Draft Agenda for FG IdM Meeting – v2
DOC-004r2	Chairman, FG IdM	Draft Agenda for FG IdM Meeting – v2
DOC-004r3	Chairman, FG IdM	Draft Agenda for FG IdM Meeting – v2
DOC-005	Iamdentity Ltd	Case study for identity management
DOC-006	Tertius Ltd: Dr. Norman Paskin	Content Industry Standards Activities
DOC-006r1	Tertius Ltd: Dr. Norman Paskin	Content Industry Standards Activities
DOC-007	Tertius Ltd: Dr. Norman Paskin	The Handle System®
DOC-007r1	Tertius Ltd: Dr. Norman Paskin	The Handle System®
DOC-008	Olli Jussila, TeliaSonera	Evaluation reports of the Eureka/Celtic/FIDELITY -project
DOC-009	Telcordia Technologies	IdM discussion items
DOC-010	Telcordia Technologies	IdM example use case – eGovernment Services
DOC-011	Telcordia Technologies	IdM example use case – operational response to cyber attacks
DOC-012	Siemens-Networks GmbH & Co KG	ETSI TS 184 002 “NGN Identifiers” - An Overview
DOC-013	Nokia, Siemens-Networks GmbH & Co KG	Identity Management in 3GPP - An Overview
DOC-013r1	Nokia, Siemens-Networks GmbH & Co KG	Identity Management in 3GPP - An Overview
DOC-014	Members of EU IST FP6 Daidalos Project	Mapping a Virtual Identity Framework to the A4C
DOC-015	ITU-T ASN.1 Project leader	Object identifiers (OIDs) and Registration Authorities
DOC-016	VeriSign	IdM Forums, Platforms, and Protocols – a Mapping to Topics
DOC-017	VeriSign	CardSpace Implementation Use Case
DOC-018	VeriSign	Discussion Framework for Identity Management Assurance Metrics
DOC-019	ATIS	ITU-T Focus Group on Identity Management meeting
DOC-020	JCA-NID Convener	ITU-T JCA-NID Overview
DOC-020r1	JCA-NID Convener	ITU-T JCA-NID Overview
DOC-021	ETSI TISPAN	Identity management in ETSI – Security
DOC-022	VeriSign	A NGN Overview: from an IdM perspective

Number	Source	Title
DOC-023	AmSoft Systems	Interoperable Identifiers in Next Generation Networks
DOC-024	ITU-T SG4	Liaison on "Identity Management Focus Group
DOC-025	Sergio Fiszman, NORTEL	Secure Identity Aware Networks
DOC-026	Chairman, FG IdM	FG IdM Overview
DOC-027	Siemens-Networks GmbH & Co KG	Proposed FG-IdM Working Group "IdM Architecture"
DOC-028	Scott Cadzow, ETSI, TISPAN	NGN identity
DOC-029	TSB	List of participants-15-02-2007
DOC-045	Liberty Alliance	Identity Federation and Web Services
DOC-046	OPEN ID	Making the Web Less cumbersome!
DOC-047	Paul Trevithick	Higgins Summary

4.2 List of output documents

Output documents are on the ITU FG FTP site.

Number	Source	Title
DOC-030	Chairman, FG IdM	RESULT: Summary of Discovery discussion session
DOC-031	Chairman, FG IdM	RESULT: Summary of Handle and XRI session
DOC-032	Chairman, FG IdM	RESULT: Summary of HIGGINS discussion session
DOC-033	Chairman, FG IdM	RESULT: IDMFG Scope
DOC-034	Chairman, FG IdM	RESULT: Summary of IDM Framework discussion session
DOC-035	Chairman, FG IdM	RESULT: Summary of Law enforcement in Identity space (NGN) discussion session
DOC-036	Chairman, FG IdM	RESULT: Summary of Legal & Privacy IDM Working Group discussion session
DOC-037	Chairman, FG IdM	RESULT: IDMFG Means and Mechanisms
DOC-038	Chairman, FG IdM	RESULT: Summary of Terminology & Living List discussion session
DOC-039	Chairman, FG IdM	RESULT: Summary of NGN and Identity discussion session
DOC-040	Chairman, FG IdM	RESULT: Summary of Principles and Requirements discussion session
DOC-041	Chairman, FG IdM	RESULT: Summary of Resolution discussion session
DOC-042	Chairman, FG IdM	RESULT: Session allocation
DOC-043	Chairman, FG IdM	RESULT: Summary of Identity & Government Requirements discussion session
DOC-044	Siemens-Networks GmbH & Co KG	RESULT: Proposed FG-IdM Working Group "IdM Framework Architecture"
DOC-048	Chairman, FG IdM	RESULT: FG IdM Research Topics
DOC-049	Chairman, FG IdM	RESULT: Identifiers in ITU-T NGN
DOC-050	Chairman, FG IdM	RESULT: FG IdM Summary

4.3 List of liaison statements

1. A liaison statement was sent to Liberty Alliance, OASIS, IEC/ISO JTC 1, 3GPP, 3GPP2, ETSI, ATIS, W3C, OPenID Foundation, Identity Commons, TCG, IETF, ISO TC46/SC9, ITU-T SGs 2, 4, 11, 13, (17), ITU-T FG IPTV, ITU-T JCA-NID
2. A specific liaison statement was sent to ITU-T SG 13
3. A response liaison statement was sent to ATIS

Liaison statements are in Annex B.

4.4 List of attendees

See Annex C.

4.5 Future meetings of ITU-T Focus Group IdM

- 23-25 April 2007 (Geneva, colocated with NGN-GSI event), Host ITU/TSB
- 16-18 May 2007 (Mountain View, USA), Host VeriSign
- 18-20 July 2007 (Tokyo, Japan), Host NEC

Annex A Topics for discussions

1. **Identity and authentication, authentication management**
   - Authentication management communities, federations, and technical platforms (how it relates to NGN identity management)
   - Is interoperability possible?
   - Which authentication platforms have the broadest buy-in and should open-platform and/or user-centric platforms given preference.
   - Do we need an "identity layer"
   - Is it possible to develop common global assurance measurements?
   - Is authentication assurance limited only to user/device-provider interactions, or does value proposition also extend to provider-provider interactions.
   - What are the comparative advantages of transaction-based, risk-based and role-based models for assurance management?
   - What exists in the way of establishment and maintenance of authentication policies within and among federations that provide for assurance measurements.

2. Identity and authentication, identities
   - What NGN "identities" should be identified as part of a framework?
   - What variances exist within the industry as to the definition and treatment of "identity?"
   - Is the public-private dichotomy is the primary distinguishing feature for identities?
   - When are private identities acceptable and should they be discoverable?
   - What constitutes "open identity?" How should it be implemented?

3. Identity and authentication, authorization privilege management
   - What is IdM authorization privilege management, and is this something more than the use of the third party to manage user authentication relationships as an identity provider.
   - What platforms are under development or being trialed for authorization privilege management, and what standards are being used to support these services?
   - What are the significance of privilege management service in an IdM environment, and the importance of open platforms for allowing the service?

4. Infrastructure provisions and operations, entity identifiers
   - What kinds of identifiers are or should be or should note be within the scope of the IdM management framework? Is machine readability a primary criterion?
   - Are identifiers such as geospatial, radio channelization, and similar object descriptive identifiers within the IdM framework.
   - What is the usefulness and importance of a public vs. private identifier dichotomy?
   - Are public providers are completely encompassed by the two categories: public identifier creation, bindings, and maintenance, and public Identifier availability and use, and whether these actions should incur IdM capability support responsibilities.
   - Should parties other than the providers of identifiers should regarded as "authoritative" sources of identifier information, e.g., trusted third parties. What specific Identifier Systems that should be specified for NGN IdM use and what is the basis for inclusion?
   - What obligations should be applied to identifier providers, including support for validation and repudiation, applicable protocols, capture of what minimal information about the assignee, support for discovery and availability of [SAML-based] authoritative response interfaces concerning identifiers, maintenance of audit trails for what actions and for how long.
   - What public requirements should apply to the management of private identifiers?

5. Infrastructure provision and operations, entity credential management
   - Higgins, Authentication Assurance, TBD
   - What is credential management in the context of NGN IdM?
   - What credential management policies, practices, and standards exist?
   - To whom are they applied, including the sharing and notification of federation credential management policies? What federations exist?
   - What happens outside the federation?
   - How does entity credentialing differ from authentication assurance?
   - Should open credential platforms, e.g., X.509 or ECC based be required?

6. Identifier information attributes and bindings

- What specific “access permissions and routing bindings” systems, especially for NGN, must be supported for which identifiers, including the criteria, bases and protocols?
- What specific NGN profile/database systems must be supported for which identifiers, including the criteria, bases and protocols?
- What presence and availability systems must be supported for which identifiers, including the criteria, bases and protocols?

7. Discovery in a generic framework IdM framework

- What discovery platforms and protocols have been developed for IP-enabled entity credentials, identifiers, and systems of associated information attributes?
- What discovery policies, practices, and specifications for IdM entity credentials, identifiers, and systems of associated information attributes should be required?
- How do you provide for interoperability with legacy discovery systems?
- What is the usefulness of sets of “well-known” rules for discovery of IdM resources?

8. Infrastructure provision and operations, common data models and schema

- Data models, Higgins,
- Identify generic data model and structures for IdM functional architecture and services, including schemas for data exchange and interpretation among different entities and system for IdM.
- Identify OAM functions associated with IdM functional architectures and services for configuration, fault and performance management and measurements.

9. Identity and authentication, management of identity patterns

- What identity patterns technologies and deployments exist, how should different, kinds of pattern systems, should be supported, and the criteria, bases and protocols?
- Specifically, what implementations exist for exchanging identity patterns for single sign-on capabilities, NGN needs for authentication supplementing, identity theft, profile and fraud detection and management, digital brand management, intellectual property rights protection, WWW search service interoperability, network security analysis, and law enforcement assistance give rise to the management of identity patterns, and other possible needs?

10. IdM Integrity, threats and risks security objectives and requirements

- Secure IdM, presentation, Sergio Fiszman (Nortel)
- Discussion points, moderator Tony Nadalin
- Threats and risks that underlie the implementation of IdM platforms, including the risks to the platforms.
- NGN specific threats and risks. What security objectives should be established, and what steps can be taken to minimize the risks, whether trusted out-of-band signalling planes for IdM would mitigate the risks, whether the risks be compartmentalized, possible IdM vulnerability detection systems, and what operational mechanisms can be established to diminish discovered vulnerabilities.

11. Identity and authentication, access across multiple service/network provider boundaries

- What kinds of IdM federation schema been described or created?
- How these federations relate to users/subscribers, service providers/operators, and objects?
- How federation policies are or can be discovered?
- What happens if parties are not part of federations?

12. IdM integrity, framework

- The concept of “identity service providers,” and whether they should be explicitly recognized in an NGN IdM framework, and reflected in the NGN architecture.
- Adequacy of the present definition of the “framework” (capabilities associated with the creation and use of identifiers and related identity).
- The basis for the framework capabilities, including whether they should be “based on existing and anticipated industry models and practices manifested in identity management for a and SDOs and specifications applicable to NGN infrastructure and services“”
- "Transitioning capabilities” and their deployment.
- Relationship of the NGN IdM Framework in the context of NGN functional reference architecture (FRA), 1) whether the FRA needs to be changed, especially to provide for an “out of band” trusted backplane and whether it should be physical or virtual, and 2) the usefulness or detriments of an explicit division in the present FRA between application and transport “profile information.”

Annex B. Liaison statements

B.1 General liaison statement

ITU - Telecommunication Standardization Sector

Focus Group on Identity Management: Geneva 13-16 February 2007

Source:	ITU-T Focus Group on Identity Management (Geneva, 13-16 February 2007)
Title:	Liaison statement concerning results of the first face-to-face meeting,
Sent to	Liberty Alliance , OASIS, IEC/ISO JTC 1, 3GPP, 3GPP2, ETSI, ATIS, W3C, OPenID Foundation, Identity Commons, TCG, , IETF, ITU-T SGs 2, 4, 13, (17), ITU-T JCA-NID, and ITU-T FG IPTV
Purpose:	For information and discussion

ITU-T recently established an Identity Management (IdM) Focus Group. The first of a series of meetings was held in Geneva from 13 -16 February 2007. The objective of the Focus Group is to facilitate the development of a generic Identity Management framework, by fostering participation of all telecommunications and ICT experts on Identity Management. The FG IdM is open to ITU Member States, Sector Members and Associates as well as any individual from a country which is a member of ITU willing to contribute to the work; this includes individuals who are also members or representatives of interested Standards Development Organizations.

Attached is the report from the first meeting of the FG for your review and comment. Key members from the IdM community attended this February 2007 meeting and we encourage members of your organization to participate in the next meeting which will be held in Geneva, 23-25 April 2007.

B.2 Liaison statement to SG 13

Source:	ITU-T Focus Group on Identity Management (Geneva, 13-16 February 2007)
Title:	Liaison statement concerning results of the first face-to-face meeting,
Sent to	SG 13
Purpose:	For information and discussion

ITU-T Focus Group IdM thanks SG13 for the liaison statement informing on its NGN Identity Management Framework.

We recognize the need to minimize duplication and to leverage the work being done within your organization and others.

We agree with your suggestion concerning scheduling our next Focus Group IdM meeting at a time when SG 13 is scheduled to meet. Consequently, we have scheduled our next meeting for 23-25 April 2007 (Geneva, colocated with NGN-GSI event), host ITU/TSB and we encourage your participation in this second meeting.

A lot of time during this February 2007 meeting was devoted to refinement of the Focus Group scope and the working group structure. As a result, it was difficult to provide specific feedback on the NGN IdM framework (Y.IdMsec draft Recommendation) at this time. However, the working groups will be developing material between now and the next Focus Group meeting which coincides with the next SG 13 meeting.. We plan to provide SG 13 with a status of the effort and materials that are relevant to NGN prior to the April 2007 SG 13 meeting. You can also find additional information about the Focus Group IdM on the following web site: http://www.ituwiki.com/index.php?title=Main_Page.

B.3 Liaison statement to ATIS

Source:	ITU-T Focus Group on Identity Management, Geneva, 13-16, February 2007
Title:	Liaison statement concerning results of the first face-to-face meeting,
Sent to	ATIS
Purpose:	For information and discussion

ITU-T Focus Group IdM thanks ATIS for the Letter dated 2 February 2007, Subject: Re: ITU-T Focus Group on Identity Management.

We recognize the need to minimize duplication and to leverage the work being done within your organization and others.

We agree with your suggestion concerning scheduling our Focus Group IdM meetings not at a time when ATIS/PTSC is scheduled to meet. Consequently, the schedule for the next three Focus Group meetings is: 23-25 April 2007 (Geneva, Switzerland), 16-18 May 2007 (Mountain View, CA, USA), and 18-20 July 2007 (Tokyo, Japan). We value and encourage ATIS/PTSC participation in these meetings.

Annex C List of participants

Family name	Given name	Affiliation	Country	emailcontact
Aguiar	Rui L.	Instituto Telecomunicações Aveiro	Portugal	ruilaa@det.ua.pt
Ahn	Jae Young	ETRI	Korea (Rep. of)	ahnjy@etri.re.kr
Ar Foll	Fulup	Sun Microsystems	France	fulup@sun.com
Barbir	Abbie	Nortel Networks	Canada	abbieb@nortel.com
Barisch	Marc	University of Stuttgart	Germany	barisch@ikr.uni-stuttgart.de
Billquist	Scott	Warren Communications News	Switzerland	scott.billquist@mac.com
Boll	Berend	Deutsche Telekom	Germany	berend.boll@t-systems.com
Brackney	Richard	US DoD	United States	rcbrack@verizon.net
Buttar	Alistair	Motorola	United Kingdom	alistair.buttar@motorola.com
Cadzow	Scott	Cadzow Communications Consulting	United Kingdom	scott@cadzow.com
Dryburgh	Lee	University College of London	United Kingdom	dryburghl@gmail.com
Dubuisson	Olivier	France Télécom	France	olivier.dubuisson@orange-ftgroup.com
Egawa	Takashi	NEC	Japan	t-egawa@ct.jp.nec.com
Euchner	Martin	Siemens Networks	Germany	martin.euchner@siemens.com
Fiszman	Sergio	Nortel	Canada	sergio@nortel.com
García López	Miguel A.	Telefónica	Spain	magl223@tid.es
Girao	Joao	NEC	Germany	joao.girao@netlab.nec.de
Gross	Thomas	IBM Research	Switzerland	tgr@zurich.ibm.com
Hamlin	Kaliya	Identity Woman		kaliya@mac.com
Hird	Michael		United Kingdom	mikehird@onetel.com
Hirsch	Frederick	Nokia	United States	frederick.hirsch@nokia.com
Hogben	Giles	ENISA	Greece	giles.hogben@enisa.europa.eu
Jeffrey	Mark	Microsoft	Switzerland	mark.jeffrey@microsoft.com
Jenny	Christian		Switzerland	christian.jenny@bakom.admin.ch
Jones	James	BT	United Kingdom	james.e.jones@bt.com
Jones	Michael	Microsoft	United States	mbj@microsoft.com
Jussila	Olli	TeliaSonera	Finland	olli.jussila@teliasonera.com
Kisrawi	Nabil		Syrian Arab Republic	nabil.kisrawi@ties.itu.int
Krueger	Dietmar	Deutsche Telekom	Germany	dietmar.krueger@t-systems.com
Lee	Chaesub	ETRI	Korea (Rep. of)	chae-sub.lee@ties.itu.int
Lesnewich	Robert	Telcordia Technologies	United States	rlesnewi@telcordia.com
Lindqvist	Kurt Erik	Netnod Internet Exchange Ab	Sweden	kurtis@netnod.se
Lizar	Mark	Identity Trust	United Kingdom	mark@identity-trust.org
Madhok	Ajay	AmSoft Systems	India	ajay.madhok@amsoft.net
Malan	Philip	Iamdentity	United Kingdom	philip@iamdentity.com
Matos	Alfredo	Instituto Telecomunicações Aveiro	Portugal	alfredo.matos@av.it.pt
Mc Intosh	Michael	IBM	United States	mikemci@us.ibm.com
Moriyama	Eimatsu	NICT	Japan	moriyama@nict.go.jp
Mulberry	Karen	Neustar	United States	karen.mulberry@neustar.biz
Nadalin	Anthony	IBM	United States	drsecure@us.ibm.com

Oliver	Colin	DCITA	Australia	colin.oliver@dcita.gov.au
Pacyna	Piotr	Universidad Carlos III	Spain	ppacyna@it.uc3m.es
Paskin	Norman	Tertius	United Kingdom	n.paskin@tertius.ltd.uk
Probst	Pierre-André	OFCOM	Switzerland	probst-pa@bluewin.ch
Rakkolainen	Jukka	ERO	Denmark	rakkolainen@ero.dk
Recordon	David	Verisign	United States	drecordon@verisign.com
Rundle	Mary	Harvard University	United States	mrundle@cyber.law.harvard.edu
Rutkowski	Anthony	VeriSign	United States	trutkowski@verisign.com
Saks	Andrea	Independent Accessiblity Consultant	United States	asaks@waitrose.com
Sarma	Amardeo	NEC	Germany	sarma@netlab.nec.de
Singh	Ray	Telcordia Technologies	United States	rsingh@telcordia.com
Trevithick	Paul	Parity Communications, Inc.	United States	paul@socialphysics.org
Vazquez	Victor	WIPO	Switzerland	victor.vazquez_lopez@wipo.int
Zeltsan	Zachary	Alcatel-Lucent	United States	Zeltsan@alcatel-lucent.com

Annex D Report on 5 December 2006 ITU-T Workshop on Digital Idetity for NGN

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

STUDY GROUP 17

TD 0230

English only

Original: English

Question(s): 2, 6, 9, 10/17 Geneva, 6-15 December 2006

TEMPORARY DOCUMENT

Source: Rapporteur for the Workshop on Digital Identity for NGN

Title: Summary of the Workshop on Digital Identity for Next Generation Networks

1. The Workshop Programme

The workshop on Digital Identity for Next Generation Networks was held on 5 December 2006 in Geneva and attracted about 70 participants. 22 presentations in 7 sessions addressed various aspects of the topic. It was organised by ITU-T SG17 and the EU IST Daidalos project and hosted by the ITU-T.

After the welcome by Herbert Bertine, SG17 Chairman, and the introduction to the workshop topic by Amardeo Sarma (NEC), the workshop began with the first Session on *Why do Operators need Digital Identities.* These included presentations by Aude Pichelin (France Télécom Group), Susumu Yoneda (Softbank Telecom Corp.) and SangRae Cho (ETRI), who gave some insight on plans and activities by operators, as well as some expected trends. The second session on Approaches to Digital Identities in NGN showed how telecom vendors plan to deal with digital identities. Presentations were give by Hidehito Gomi (NEC), Sergio Fiszman and Ed Koehler Jr (Nortel) and Wei Jiwei (Huawei). Issues covered were Identity Convergence, Context awareness and security. The third session featured IBM (Anthony Nadalin) and Verisign (Hemma Prafullchandra), and they focused on enabling productivity, providing new user experiences and what needs of youth should be addressed.

Two sessions focused on what is going on in research projects world-wide (but mainly Europe) with presentations from the Ambient Networks project (Göran Selander), PRIME (Jan Camenisch), Daidalos (Joao Girao), University of Purdue (Elisa Bertino), FIDIS (David-Olivier Jaquet-Chiffelle) and MAGNET (Dimitris M. Kyriazanos).

Another two sessions dealt with the approach and status of standardisation related to digital identities. Presentations were given by Mike Pluke (TISPAN WG4 STF 302), Hal Lockhart (OASIS), Richard Brackney (ISO/IEC), Hellmuth Broda (Liberty Alliance), Pierre André Probst (ITU-T JCA-NID), Marco Carugi (ITU-T SG13) and Abbie Barbir (ITU-T SG17).

A summary and open debate concluded the workshop. The workshop presentations and detailed programme are available on the ITU-T web site.

2. Workshop results

The immediate feedback on the workshop was positive. The following is a summary of some general observations:

- Several companies, projects and standardization bodies are addressing similar questions, and it would be useful to have a map of which projects and in particular which standardization bodies address are addressing specific issues.
- Roadmaps of standardization bodies on digital identity would also be very useful information.
- The network level and in general lower layers have not been addressed sufficiently with regard to digital identity, and this remains a weak point in standardization and research. In particular, NGN standardization needs to take this up.

- Some similar approaches are being developed, and there is a need to exchange information and harmonize views. Even terminology needs to be synchronized.
- Privacy is an overriding concern, but it seems that this has a large dependency on international consensus and agreements.
- The role of directory was not touched on sufficiently at this event and must be included in future discussions and workshops

There was considerable discussion on the need and rationale of frameworks for digital identity. The consensus was that we need interoperability of frameworks with techniques to bridge the gap between different frameworks. Harmonization should target consistency, as a danger was seen in early industry deployment that could in some cases lead to future needlessly inconsistent scenario, that would be hard to sort out later.

Several questions and requirements were raised in the presentations and during discussions that need to be dealt with and answered. One was which entities digital identities need to be tied to, from users via networks, services, applications, content etc. to "things" in general. The need was also mentioned to support roles and partial identities targeted to specific roles or usage contexts. Furthermore, there was a requirement to support both roles that represent real persons as well as the construction of virtual persons with fictitious roles. How do we deal with real vs. virtual persons in practice and how do they need to be differentiated?

Some overall considerations were addressed with respect to requirements. Is X.800 attacker model sufficient? Do we need an overarching namespace that connects specific name spaces? Or do we rather need to delimit name spaces such that they do not collide? How do we protect youth without "imposing" on them, but still make them sensitive to predators? As the presentations mentioned different identifier standards, such as UCI (TISPAN) and NUI (ITU-T), the question of their scope and harmonization was raised. Are identifiers even needed for software and software modules?

Regarding the impact of existing standards, one question raised was whether SAML 2.0 is sufficient for all layers including the network in view of NGN, which needs to be looked into.

As a result of the questions raised, some specific gaps were identified. There is a need to define a usable "metaphor" for identity that people understand (and accept), as this will play a big role in the acceptance of any digital identity scheme. This includes items, such as:

- What does it contain?
- Defining what groups are?
- Defining how to process privacy policies

Also, the role of network Identities needs to be clarified in this context, more specifically how such concepts support dynamically changing networks, their co-operation and perhaps composition and any resulting network identities of composed networks.

3. Data and data structures for identities

The workshop showed that the definition of data to be linked to digital identities will be a critical item. Operators, service providers and even Amazon / Google maintain data that may need to be linked via digital identities. Specific questions in this connection are:

- Which data do we need to model?
- Who owns or can modify data?
- Where is that data stored?
- Who owns and has to keep that data?
- Who is liable by the content?
- Is most data in heads of people and may not be modelled at all?
- How is data handled and exchanged between domains?

The following types of data elements were identified (initial list, to be extended):

- Classify according to duration: forever, assigned, acquired
- Classify as whether related to identification or not

It was consensus that data structures will be needed to cope with the storing and in particular exchange of data. Further, we need to have data structures as seen and used by users / devices. This required the capability and modelling of data that is linked to user digital identities. What is needed is a unified (standardized) personal identity data model including its parts (context, profile, preferences etc.). Context management needs to include schemes to blur context or information in general to improve privacy.

4. Consensus achieved on some issues

The following was widely agreed as consensus:

- Dissemination of user information needs to generally be under user control, but some user data may be such that it cannot be modified by user, such as age or tarif
- The use of digital identities must be simple and at the same time react in real-time
- Social networking must be supported
- Digital identities must be usable across layers and support multi-layer privacy
- Well-defined requirements for digital identities are needed, which includes usability, security and privacy
- The legal framework generally lags behind the developed technology. Users often become victims, such as for malicious Personal ID reading, but at the same time the technology often makes it easy for law breakers to exploit. What is important is that it must be made difficult to fake identities.

5. Outlook

The workshop was considered as timely and useful, which resulted in the request for an early follow-up meeting to answer some of the questions raised. A workshop alongside SG17 WP2 in April, which will be held at the same time as the SG13/SG19 meeting was proposed, which will be discussed further at the SG17 closing plenary. Later meetings could be linked to the ISO/IEC JTC1 SC27 proposal for a workshop in 2008.

The need for a co-ordination mechanism was seen as necessary. Pierre-Andre Probst pointed out that the JCA NID could be used for issues related to network identities. But discussions that continued after the workshop showed that there were further proposals to set up an additional JCA with wider scope as well as a proposal for Focus Group on digital identities.

Since it was widely agreed that the exchange of information and co-ordination of efforts should continue, it will be up to the SG 17 closing plenary to decide on the next concrete steps, in particular on a follow-up workshop including its dates, as well as on setting up a Focus Group or JCA.

_____