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

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.

Contact: Amardeo Sarma
Rapporteur
NEC Europe Ltd.
Germany
Tel: +49 6221 43421-44
Fax: +49 6221 43421-55
Email: Sarma@netlab.nec.de

Contact: Herbert Bertine
Lucent Technologies
Tel: +1 732 949 4022
Fax: +1 732 949 1196
Email: hbertine@lucent.com

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.

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.

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.

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.