INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 13 – LS 115 – E

English only

Original: English

Question(s):	15/13	Geneva, 17-28 July 2006

Ref. : TD 191 Rev.1 (WP 2/13)

Source:	ITU-T Study Group 13 (Geneva, 17-28 July 2006)
Title:	ITU-T studies on security aspects of NGN Identity Management (NGN/IdM)

LIAISON STATEMENT

To:	ATIS (PTSC), ETSI TISPAN (WG7), ISO/JTC 1/SC 27/WG 5, IETF, IEEE, Liberty Alliance, NIST (CSRC), OASIS (SSTC), Open Mobile Alliance, TTC (Networked RFID-SAG), TTA (RFID-PG), CCSA
Approval:	**Agreed to at ITU-T SG 13 meeting**
For:	**Information and Action**
Deadline:	**15 October 2006**

Contact: Mr. Chae-Sub Lee E-mail: chae-sub.lee@ties.itu.int

We would like to share with you two recent ITU-T SG13 outcomes of the Q.15/13 meeting.

First, Mr. Richard Brackney (rcbrackney@earthlink.net) has been appointed the ITU-T SG13 Q15 (Q13/15) liaison to ISO/IEC JTC 1/SC 27 for matters concerning our IdM study activities.

Second, ITU-T Study Group 13 (Next Generation Networks) Question 15/13 (Q.15/13) is studying some of the technical elements of the service commonly referred to as IdM, focusing on IdM security aspects of the NGN. This liaison describes these elements and indicates the Q.15/13 plans to relate them more closely to IdM and to work already underway in other venues. We understand that you are also active in this field and would appreciate sharing relevant work between us, as well as your comment on our project.

BACKGROUND

The NGN is a converged open network that provides wireline and wireless access to a broad array of services for fixed and mobile users. Access to the NGN network and services will require authentication/authorization by the user, the terminal, and the network. Nomadicity of NGN users adds further complexity to the service providers' authentication/authorization process. In a worldwide mobile environment based on multiple service providers, this authentication/authorization process requires a technically sophisticated and flexible mechanism, commonly referred to as IdM, to maintain a trust relationship between users, devices and service providers.

An IdM capability offers the possibility of providing mobile users with a single authentication/authorization mechanism applicable to any access point in the NGN. Achievement of this complex capability is the reason for studying technical aspects of IdM as it relates to the NGN.

SCOPE OF WORK

Q.15/13 on "Next Generation Network Security" recognizes the need to study and harmonize approaches to IdM. In particular, Q.15/13 is primarily interested in the security aspects of IdM. To this end, Q.15/13 intends to study the existing NGN security aspects of IdM and address further security mechanisms required to support IdM.

Q15/13 will:

- Refine the following Q.15/13 working definition

  "IdM ("Identity Management"). A working definition of IdM is "management by NGN providers of trusted attributes of an entity such as: a subscriber, a device or a provider". This is not intended to indicate positive validation of a person.

- Determine IdM security requirements
- Define a framework and architecture(s) for IdM
- Identify IdM secuirty mechanisms that need to be addressed
- Assess security threats and vulnerabilities associated with the IdM.

OUTPUT

Q.15/13 intends to develop ITU-T Recommendations addressing IdM Security Requirements, a security architecture, technical procedures, and eventually a best practices document.