Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13981
Date:	2009-06-10
Replaces:	
Document Type:	Outgoing Liaison Statement
Document Title:	Liaison Statement from JTC 1/SC 6/WG 8 to ITU-T SG 17 on the Draft New Recommendation ITU-T X.1250, Baseline capabilities for enhanced global identity management trust and interoperability
Document Source:	SC 6/WG 8 Tokyo meeting
Project Number:	
Document Status:	As per the SC 6 Tokyo resolution 6.8.2, this document is forwarded to ITU-T SG 17.
Action ID:	FYI
Due Date:	
No. of Pages:	2

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

6N 13981 Liaison Statement from ISO/IEC JTC 1/SC 6 to ITU-T SG 17 (Q10/17)

Subject: Comments on COM 17 – R 5 – E, DRAFT NEW RECOMMENDATION ITU-T X.1250 (X.idmreq), Baseline capabilities for enhanced global identity management trust and interoperability.

The comments are generally related to the use of Directory as specified in the ITU-T X.500 | ISO/IEC 9594, but in particular to ITU-T X.509 | ISO/IEC 9594-8.

SC 6 has studied the above mentioned document and can offer the following comments:

7.3.2 (Credential capabilities) mentions X.509. It gives a rather weak description of X.509.. If the first edition of X.509 was developed two decades ago, it is under continuous development to keep up with current requirements. The sixth edition of X.509 was completed late 2008 and the seventh edition is under development. Many groups have based their work on X.509, such as the IETF PKIX group (http://www.ietf.org/html.charters/pkix-charter.html), CA/Browser Forum (http://www.cabforum.org/), ETSI ESI (http://portal.etsi.org/Portal_Common/lite/TBDETAILS.asp?tb_id=607), etc. X.509 is clearly a key component within IdM and should have a more prominent treatment in the document.

7.3.2 also mentions OCSP (IETF RFC 2560, Online Certificate Status Protocol). As written, it gives the impression that OCSP may be used for validating different kinds of credentials, while its scope is "limited" to check the status of an X.509 digital certificate. OCSP is developed by the IETF PKIX group. A tutorial on OCSP may be found on http://www.x500standard.com/index.php?n=X509W.OCSP.

The document has some considerations on protection, control and use of identifiable information (PII). According to a study by the Butler group, in all the Identity Management they have studied, directories are used for storing identifiable information. Storage of identifiable information should be treated in the document. In addition, how such information storage might be protected (access control, authentication, authorisation, etc.) should also be considered.

The document talks a lot about trust. The document could benefit from the work that has been done within X.509 and within PKIX (e.g. IETF RFC 5280).