



INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION
STANDARDIZATION SECTOR**

STUDY PERIOD 2005-2008

COM 17 – LS 265 – E

English only

Original: English

Question(s): 2/17

Geneva, 7-18 April 2008

Ref. : TD 1438

Source: ITU-T SG 17 (Geneva, 7-18 April 2008)

Title: LS to OASIS Security Services (SAML) TC on X.500 attribute profile in SAML 2

LIAISON STATEMENT

To: OASIS Security Services (SAML) TC

Approval: Agreed to at SG 17 meeting

For: Information

Deadline:

Contact: Erik Andersen
Rapporteur, Q.2/17

Tel: +45 2097 1490
Email: era@x500.eu

The document SAML V2.0 X.500/LDAP Attribute Profile was considered during the joint meeting of ITU-T Study Group 17 Question 2 and ISO/IEC JTC 1/SC 6/WG 8. Our comments are as follows.

The notation for attribute type using the URN oid namespace gives an unambiguous notation for all the attributes defined in X.520 or defined using any other object identifier values.

The comparison of attribute names presented in 2.3.1 using names derived from object identifiers is also correct.

According to 2.5, SAML attribute values can be encoded in two forms:

- for attributes having a LDAP-specific encoding producing an UTF8String value, an UTF8String is used with xsi:type set to xsd:string;
- for other attributes, a base64 string is used with xsi:type set to xsd:base64Binary.

If the usage of base64 encoding of the octet string content resulting from the BER encoding can be effectively used, it produces unreadable strings.

The Directory group considers that an XER encoding of the ASN.1 value could produce a more readable string and suggests that XER encoding should be considered.

Attention: Some or all of the material attached to this liaison statement may be subject to ITU copyright. In such a case this will be indicated in the individual document.

Such a copyright does not prevent the use of the material for its intended purpose, but it prevents the reproduction of all or part of it in a publication without the authorization of ITU.

For example, an algorithm used in an X.509 certificate (algorithm identifier and parameter) can be encoded as:

<algorithm>

<algorithm>1.2.840.113549.1.1.1</algorithm>

<parameters>

<NULL/>

</parameters>

</algorithm>
