INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 17 – LS 073 Rev.1 – E

English only

Original: English

Question(s): 11/17

LIAISON STATEMENT

Source: ITU-T SG17

Title: LS/o on Cryptographic Message Syntax [to ISO/IEC JTC 1/SC27/WG2, ISO/TC 68/SC2, IESG]

LIAISON STATEMENT Rev.1

For action to: -

For comment to: -

For information to: ISO/IEC JTC 1/SC27/WG2

ISO/TC 68/SC2

IESG

Approval: ITU-T SG17 meeting (Geneva, 26 August – 4 September 2013)

Deadline: -

Contact: Erik Andersen
Rapporteur of ITU-T SG17 Question 11/17
Tel: +45 2097 1490
E-mail: era@x500.eu

Contact: Jean-Paul Lemaire
Associate Rapporteur of ITU-T SG17 Question 11/17
Tel: +33 618473756
E-mail: jean-paul.lemaire@univ-paris-diderot.fr

ITU-T SG 17 has established a new work item to update the Cryptographic Message Syntax (CMS) to eliminate all obsolete ASN.1 features and make it usable with all ASN.1 standardized encoding rules, and possibly extend its capabilities. CMS is being used to protect information of any type or format from the threats of accidental or deliberate disclosure, alteration, destruction, or substitution, while the information is at rest or during transfer across interconnected network.

The summary of this new Recommendation is given below:

Summary:
The purpose of this Recommendation is to update the Cryptographic Message Syntax (CMS) to eliminate all obsolete ASN.1 features and make it usable with all ASN.1 standardized encoding rules. CMS is being used to protect information of any type or format from the threats of accidental or deliberate disclosure, alteration, destruction, or substitution, while the information is at rest or during transfer across interconnected networks. The Recommendation will continue to support the existing CMS features of data integrity, confidentiality, origin authenticity, and non-repudiation services needed for reliable information exchange and for strong authentication.

The Recommendation will bring together a set of cryptographic key management techniques to support flexible key establishment mechanisms, such as constructive key management, key agreement, key exchange, and password-based encryption. These techniques can be used to prevent fraud, and to protect personally identifiable and other sensitive information from the threats outlined above. The CMS will support digital signature, encryption, and signcryption techniques based on the public-key technology defined in the X.500 series of Recommendations.

The Recommendation will be independent of cryptographic algorithms so that the syntax supports any set of algorithms required by any community. All of the encoding rules defined in the ASN.1 Recommendations will be supported to enable efficient transfer in environments constrained by mobility, limited battery life, or bandwidth (e.g., wireless communications using hand held and personal devices), high volumes of transactions (e.g., mobile internet commerce), or limited storage capacity (e.g., common access (CAC), personal identity verification (PIV), and other smart cards). The flexibility of the extensible markup language (XML) will be provided through support for the ASN.1 XML Encoding Rules.