Submission Date:	2015-04-2
Title:	Response to Liaison on Cryptographic Message Syntax
From:	Security Area Directors (sec-ads@tools.ietf.org)
To:	ITU-T SG 17 (tsbsg17@itu.int)
Cc:	martin.euchner@icn.siemens.de stephen.farrell@cs.tcd.ie Kathleen.Moriarty.ietf@gmail.com The IESG
Response Contact:	scott.mansfield@ericsson.com
Technical Contact:	scott.mansfield@ericsson.com
Purpose:	For Action
Referenced liaison:	Liaison Statement: Response to liaison on Cryptographic Message Syntax
Attachments:	(none)

Body:

We have previously submitted a liaison [1] in reference to the Cryptographic Message Syntax (CMS) [RFC5652] in which we recommended that if new work on CMS is felt to be needed, the best place to do that is in the IETF. This ensures interaction with the active community of editors, developers, and users of that technology.

We have very recently seen [2] sent to an IETF mailing list and which has as an attachment, a document that significantly overlaps with and apparently incompatibly extends RFC5652. Such a development could significantly damage security and interoperability if it affected any implementations.

We note that the particular change proposed by [2] ("signcryption") could be done in a backwards compatible and interoperable manner and also seems to overlap with ISO 29150:2011 [3], though we have not analyzed whether or not there may additionally be some conflict between the new text in [2] and that ISO standard.

We do not have a formal view on the document that is up for consent at the next SG17 plenary meeting in April 2015, as the document was not formally liaised. However, we would ask that ITU-T not undertake such duplicative and damaging work without first having a real dialog with those who implement, deploy and depend upon CMS.

The place for such a dialog is on the IETF S/MIME mailing list [4], which remains open and active and could be used to re-activate the S/MIME working group, should new work in that area be required.

The normal IETF process remains available should anyone wish to extend CMS, as has been done numerous times,(e.g. [5]) and we (as security area directors) are happy to discuss how best to approach any such proposed work within the IETF.

Regards,

Stephen Farrell/Kathleen Moriarty

IETF Security Area Directors

References:

[RFC5652] https://tools.ietf.org/html/rfc5652

[1] https://datatracker.ietf.org/liaison/1294/

[2] https://www.ietf.org/mail-archive/web/pkix/current/msg33206.html

[3] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45173

[4] https://www.ietf.org/mail-archive/web/smime/current/maillist.html

[5] https://datatracker.ietf.org/doc/rfc4073/