INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 13 – LS 127 – E

English only

Original: English

Question(s): 16/13 Geneva, 6-16 September 2010

Ref. : TD 551 (NGN-GSI) - Annex 1

Source: Q.16/13 Rapporteur Group (NGN-GSI event, Geneva, September 2010)

Title: Response to the liaison statement from 3GPP SA 3 Reply to Integration of the OpenID-based authentication with IMS

LIAISON STATEMENT

For action to: **3GPP SA 3**

For comment to:

For information to:

Approval: **Agreed at Q.16/13 meeting**

Deadline: **31 December 2010**

Contact: Igor Faynberg
Alcatel-Lucent
USA

Tel: +1 908 582 2626
Email: Igor.Faynberg@alcatel-lucent.com

Question 16 of Study Group 13 thanks SA 3 for its liaison statement *Reply to Integration of the OpenID-based authentication with IMS*. Q.16/13 supports alignment of the work on identity management between the two groups.

The table below addresses comments provided in the liaison statement of SA 3.

N	Comment of SA 3	Response from Q.16/13
1	It was noted that in the current ITU OpenID-IMS integration chapter in 6.2.7 the exact nature of the interfaces for the flows are not visible (e.g. if the HSS (S-5) would need to support a new interface or if an existing one would be extended). Also, the access and trust management for such an interface is not clear.	The chapter has now an explicit statement that there are no additional requirements to the interface between A-2 and S-5 (HSS). There is no need for HSS in supporting any new or extending an existing interface. The access and trust management do not require any changes.
2	The A-2 seems to have a similar functionality then the current GBA-BSF, but from the current description it can not be determined if 3GPP functionality can be re-used and if a common backend can be used.	The interface between A-2 and S-5 uses the Diameter protocol in the same manner as GBA does.

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.

3	It is not clear, if the A-2 abides to the security principle of key separation, that would prevent that one compromised application server endangers the security of the entire system.	There is no need for key separation because the mechanism does not deal with key distribution at all.
4	SA3 noted the issues pointed out in the editor's note in 6.2.7, and hence based on the description and the points above, at this time it is not possible to fully assess the impact on core network and further study is needed. SA3 favors interworking arrangements that have minimal or no impact on the core network. Optimally, SA3 would like to see solutions outlined in the attached TR 33.924 as the base for a common framework for security.	The editor's note has been removed. Q.16/13 agrees that TR 33.924 provides a workable solution for the interworking in the environments where GBA has been deployed. To this end, Q.16/13 has developed several GBA-based mechanisms for Identity Management. The purpose of the mechanism under discussion is to support OpenID in the absence of the fully-deployed GBA. GBA is not essential for supporting OpenID.