3GPP TSG SA WG3 Security — S3#25   **S3-020578**
8 - 11 October 2002
Munich, Germany

Title:	Liaison statement on Interoperability Issues and SIP in IMS
Response to:	LS S3-020480 (N1-022160) and LS S3-020485 (SP-020627) on Liaison Statement on Interoperability Issues and SIP in IMS
Release:	Release 5
Work Item:	IMS-ASEC

Source:	SA3
To:	CN1, SA1, SA2, CN, SA
Cc:	SA4, SA5, CN2,CN3, CN4,CN5

Contact Person:

Name:	Tao Haukka
Company:	Nokia Corporation
Tel. Number:	+358 40 5170079
E-mail Address:	**tao.haukka@nokia.com**

Attachments: None

---

1. Overall Description:

SA3 would like to thank CN1 and SA for communicating their Liaison statement on Interoperability Issues and SIP in IMS. As requested, SA3 have discussed all issues listed and agreed with CN1's opinion. Furthermore, SA3 would like to point out a couple of matters related to security below.

The usage of S/MIME from UA to UA mentioned in issue 3 and 7, would sacrifice current 3GPP requirements as pointed by CN1 in their Liaison statement. When tunnelling SIP messages inside S/MIME, requirements pointed out in issue 2 would be prohibited as well. An alternative may be investigated whether S/MIME usage could be exercised between one 3GPP network element and aSIP User Agent outside of IMS. Due to the stringent timetable, however, SA3 do not believe the investigation could be concluded in R5.

Issue 1 discusses P-CSCF initiating BYE request on behalf of IMS-compatible terminal. Other than CN1's answer, SA3 observe another scenario when a SIP User Agent outside of IMS would like to authenticate BYE request from IMS P-CSCF. In this case, the external User Agent is a valid one instead of an attacker. Still, SA3 agree CN1's conclusion that forged BYE from external network is the Internet interoperability issue as well as the scenario pointed in this Liaison statement.

Regarding to P-CSCF performing identity checks (issue 5), SA3 confirm that no claim has been raised up in SA3 to change security requirements for IMS. It is seen an essential thing that operator's network must be able to verify the identity has an association with private ID to be charged, and the association should be established before usage. This however, does not impose restriction to services provided by any third party as explained by CN1 in their Liaison statement.

2. Actions To SA1, SA2, CN1:

SA3 kindly ask SA1, SA2 and CN1 to give comments on SA3's opinion (if necessary), and communicate to SA3 if any changes arise in the future.

3. Date of Next SA3 Meetings:

SA3 #26   19 – 22 Nov. 2002   Oxford, UK.

SA3#27   25 - 28 Feb. 2003   TBC