3GPP TSG SA WG3 Security — S3#26
25 - 28 February 2003
Sophia Antipolis, France

S3-030116

Title:	**SA3 response on the "Additional Release 5 work needed for Policy Control and Subscription Control of Media"**
Source:	**3GPP TSG SA WG3**
To:	**3GPP TSG SA, SA1, SA2, SA4, CN, CN1, CN4**
Cc:	
Work Item:	**IMS-ASEC**
Document for:	**Decision**

Contact Person:

Name:	**Vesa Torvinen**
E-mail Address:	Vesa.Torvinen@lmf.ericsson.se

Attachments: **S3-030013**

1. Overall Description:

SA3 thanks SA TSG for the liaison statement on "Additional Release 5 work needed for Policy Control and Subscription Control of Media". SA requested SA3 to investigate the security attacks and confidentiality problems with the 488 message when used as a rejection mechanism for SDP request with media disallowed by a CSCF.

SA3 WG has discussed the LS in SA3 meeting #27.

The following is SA3 opinion on the issues identified by the LS:

The use of 488 message may be seen to open a door for denial of service attacks because a malicious UE is able to initiate INVITE and/or re-INVITE messages with media descriptions that are known to be rejected by a CSCF. In this way, the assumed attacker would be able to cause some additional load to the network, and create state in the CSCFs. However, this issue should rather be seen as a feature of SIP as a protocol. There are other similar features in SIP. For example, SIP UA is able to send OPTION method to any CSCF in the IMS network, and cause similar load. Furthermore, 488 is an error message that does not require the CSCF to keep any state after the response message has been sent.

Because the 488 response message includes policy information of the entity that rejected the message, the mechanism can be used to acquire information about the operator local policies. However, this cannot be avoided because the UAC needs this information to generate a new media description. SA3 is not aware of any mechanism that could be used to avoid revealing the policy descriptions to the UAC.

SA3 would also like to point out that the real source of the 488 response is not necessarily revealed to the UAC because the same error message can be used between the UE and various CSCFs, and between two Ues. The UAC (or the adjacent CSCFs) may not know which entity is responsible for the response. However, this is a question related to the SIP as a protocol rather than to the security of the system.

SA3 is not currently planning to introduce new security requirements related to the above issue.

2. Actions:

None.

3. Date of Next TSG SA WG3 Meetings:

Meeting	Date	Location	Host
S3#28	06 - 09 May 2003	Berlin	European 'Friends of 3GPP'
S3#29	15-18 July 2003	San Francisco (tbc)	NA 'Friends of 3GPP' (tbc)
S3#30	7-10 October 2003	Italy (tbc) ??	tbd

Technical Specification Group Services and System Aspects **TSGS#18(02)0839**
Meeting #18, New Orleans, USA, 9-12 December 2002

Title:	**Additional Release 5 work needed for Policy Control and Subscription Control of Media**
Source:	**TSG SA**
To:	**SA1, SA2, SA3, SA4, CN1**
Cc:	**CN, CN4**
Release:	**Release 5**
Work Item:	**IMS-CCR**
Agenda item:	
Document for:	**Decision**

Contact Persons:
Name: Stephen Hayes
Tel. Number: +1 469 360 8500
E-mail Address: stephen.hayes@ericsson.com

Attachments: None

1. Overall Description:

At CN#18 and SA#18 CRs were approved which implemented the use of the 488 message as a rejection mechanism for SDP requests with media disallowed by a CSCF. These CRs can be found in NP-020668 and SP-020838 respectively. This solution was selected as an alternative to the previous solution in which CSCFs directly edited the SDP.

The adoption of this solution, while solving the IETF interworking issue has introduced new issues and hilited issues already present which need to be resolved in order to have a complete acceptable solution.

This liaison requests that the addressed working groups investigate the following issues and provide appropriate Release 5 CRs to the CN#19 and SA#19 meetings as appropriate to close these holes.

The following issues should be addressed:

1. Definition of default Codecs to be supported by IMS entities (CSCF and UE) – In both the original and new policy control solutions there is the possibility that different network policies for supported codecs could lead to a situation where no suitable codec is available; the session cannot therefore be supported and must be rejected. In addition, with no common dependable set of codecs, it may be difficult for the UE to find an acceptable codec that will not be rejected by the other UE or elsewhere in the network. SA therefore asks SA4 to develop guidelines as a minimum set of media parameters (e.g. codecs, bandwidth…) that IMS UEs and CSCF should support. SA4 is requested to provide guidance or CRs as appropriate.

2. With the new solution, there is the possibility that the UE could have to retry several times to find an acceptable codec. This could lead to an unacceptable session setup delay. SA requests that CN1 investigate optimizations in either the CSCF (P and S) or UE that will minimize this delay.
This could also investigate optimisations exploiting intelligent behaviour by the UE or CSCF such as “remembering” previous successful codec selections by the UE. CN1 is requested to provide CRs as appropriate.

3. Error handling in the case that UE violates procedures

There was a concern that under the new solution, there is a need for network based error-handling solutions in the case that the UE keeps retrying the same unacceptable request. CN1 is requested to investigate the appropriate error handling and provide CRs as appropriate.

4. Handling of 488 by non-IMS UEs.
CN1 should investigate any compatibility issues that may arise due to fixed terminals receiving 488 messages. CN1 is requested to provide CRs as appropriate.

5. Security attacks and confidentiality problems with the 488 message
SA3 is requested to investigate attacks that may be possible based upon the 488 message such as denial of service attacks or the use of the 488 message as a tool to deduce an operator's policies and subscriber's profile. SA3 is requested to provide CRs as appropriate.

6. Set of media parameters sent in the 488 message
When sending the 488 message, the CSCF shall insert either all the allowed media parameters, according to local policy and users profile (for S-CSCF), or only a subset of them, based on operator configuration. CN1 is requested to provide CRs as appropriate on stage 3.

In addition, the IETF has acknowledged that there is a general requirement that SIP and SDP be extended to allow a UE to understand the policies of the various networks involved in a dialog. This is an area of future work in the IETF and should be addressed in the planned IETF/3GPP workshop on Release 6 requirements.

2. Actions

SA1:

Provide input on Release 6 user and network requirements to the IETF/3GPP workshop

SA2:

Provide input on Release 6 architectural requirements to the IETF/3GPP workshop

SA3:

Investigate the relevant issues listed above and provide information and CRs as appropriate to the SA#19

SA4:

Investigate the relevant issues listed above and provide information and CRs as appropriate to the SA#19

CN1:

Investigate the relevant issues listed above and provide information and CRs as appropriate to the CN#19

3. Date of Next TSG-SA Meetings:

SA#19	17th – 20th March 2003	Birmingham UK