**3GPP TSG SA WG3 Security — S3#20** **S3-010511**

**16 - 19 October, 2001**

**Sydney, Australia**

**3GPP TSG SA WG3 Security — IMS Security ad-hoc**

**14 September, 2001**

**Sophia Antipolis, France**

**Source:** **TSG-SA WG3**

**To:** **TSG-CN WG1**
**Cc:** **TSG-SA WG2**

**Title:** **Network initiated re-registration in the IMS**

**Contact person:** **Guenther Horn**
Guenther.horn@mchp.siemens.de
phone: +49 89 636 41494

**Attachments:** **S3z010092**

SA3 would like to inform CN1 and SA2 that SA3 sees a requirement for network initiated authentication in the IMS. This is needed to give operators the kind of flexibility in their authentication policy which they have in GSM and UMTS Rel'99. The means to achieve this in IMS would be (authenticated) network initiated re-registrations.

It is a desirable feature of GSM and UMTS Rel'99 that the network can flexibly decide when to authenticate a user. A network operator may e.g. want to authenticate when chargeable events occur, and not only when the registration period nears expiry. A typical policy employed in today's networks is to authenticate a user for 1 out of n calls where n is a small number (n= 1, ... ,5). Operators have asked for this kind of flexible authentication policy also for the IMS, cf. e.g. TD S3-010205. However, it did not seem possible to realize such a policy with the current working assumption of SA3 that authentication is only required for registration and re-registration and the currently specified procedures.

With this working assumption and the currently specified procedures, a network operator can influence the points in time when authentications occur only by his choice of the expiry date of the registration.
The network operator basically has three choices all of which seem unsatisfactory:

- He sets the duration of the registration period to a relatively low value to ensure that the user cannot incur a high amount of charges between two authentications. This is undesirable as it may create a lot of unnecessary authentications of users which have remained largely inactive.
- He sets the duration of the registration period to a relatively high value to avoid unnecessary authentications. Then he runs the risk that some users may incur high charges between two authentications.
- He de-registers the user when a certain threshold for charges (or number or duration of sessions) is reached without giving the user a chance to re-authenticate and remain registered, even if a valid registration is ongoing. This seems clearly unacceptable from a service point of view.

Network initiated authenticated re-registrations in the IMS would seem to give the desired kind of flexibility in the authentication policy as they would allow the network operator to authenticate whenever he chooses to. (It should be noted here that, as far as SA3 understands, it is possible to have authenticated re-registrations also during ongoing SIP sessions.) Also, the current working assumption of SA3 that authentication is only required for registrations and re-registrations would remain valid. In this context, it was noted with interest that CN1 recently accepted a procedure for network-initiated DE-registration based on the SUBSCRIBE method of SIP. As network initiated re-registration appears to be a problem which is very similar to network initiated de-registration, SA3 would like to ask CN1 to study also the problem of (authenticated) network initiated re-registration and propose a solution. Once a solution is available SA3 would like to review it from a security point of view.

A contribution to the SA3 ad hoc meeting on IMS security on 14 September (S3z010092) proposed a stage 2 solution for the problem. It should be noted, however, that, due to lack of time, the proposed solution could not be discussed at the SA3 ad hoc meeting and, therefore, does not reflect an agreed SA3 view.

This LS was approved by SA3 by email after the SA3 ad hoc meeting on 14 September.

**Actions:**

- CN1 is kindly asked to study the problem of  (authenticated) network initiated re-registrations and propose a solution.
- This solution should be such that network-initiated re-registration can be initiated by the S-CSCF at which the user is registered. It is for further study if the P-CSCF where the user is roaming is also required to be able to initiate re-registrations.
- CN1 should also note that, in order for the measure to be effective, the feature cannot remain optional, i.e. it cannot be left to the user’s choice whether the network can initiate an authentication of the user.
- CN1 is kindly asked to send an LS to SA3 once a solution is available so that SA3 can review it from a security point of view.
- In the meantime, SA3 would be happy to provide any further information on the subject as required by CN1.