3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010129**

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.

3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010092**

14 September, 2001

Sophia Antipolis, France

Source: **Siemens AG**

Title: **Network initiated re-registration**

Document for: **Discussion / Decision**

Agenda Item: **7.3, IP multimedia subsystem security**

Abstract

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. Some operators have asked for this kind of flexible authentication policy also for the IMS, cf. e.g. TD S3-010205. However, it seemed difficult to provide this in IMS without introducing unwarranted complexity. This contribution proposes a mechanism which is designed to provide the desired flexibility in a way which is compatible with the current working assumption of SA WG3 that authentication is only required for registration and re-registration. It uses the SUBSCRIBE method of SIP which has also been used in a proposal recently accepted by CN1 to provide network-initiated DE-registration. Network-initiated re-registration may be initiated by the S-CSCF at which the user is registered as well as by the P-CSCF where the user is roaming. The proposal also includes the appropriate information flows for both cases.

1 Introduction

At S3#19 (London, UK, 4 - 6 July, 2001) the information flows for authenticated registrations and re-registrations including various failure cases were accepted in principle for inclusion in [TS 33.203].

It was already agreed in 3G SA3, that a mechanism to enforce re-authentication is required. It was discussed if this may be facilitated by specifying an authenticated *Invite*. [S3-010205] widened the discussion and stated that (analogously to UMTS release 99) "the ability to authenticate a UE at any time in the IMS needs to be fully considered".

This contribution shows how a UE may be forced by the network to authenticate itself at any time. Otherwise the UE would be automatically de-registered. The proposal makes use of the Subscribe/Notify method specified in [IETF Draft].

For the sake of clarity the information flows for a successful registration will not be shown in full detail here. Instead only a simplified version will be used, indicating only the (in our context) relevant parts of a registration procedure. The complete flows can be found in [S3-010355].

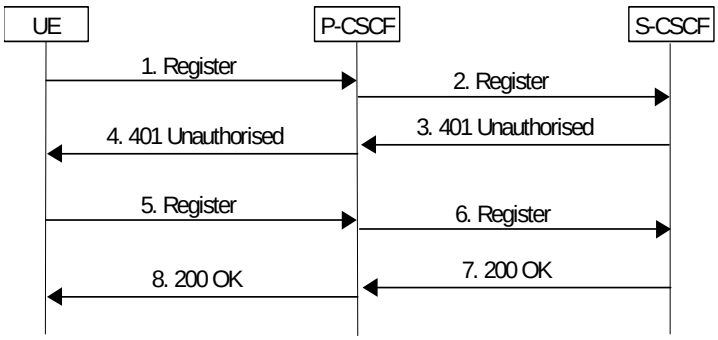

Figure 1: Successful (re-)registration with authentication(simplified)

Section 2 shows a proposal for network-initiated re-registration triggered by the S-CSCF. In section 3 it is described how the P-CSCF may additionally also trigger this event. Section 4 discusses technical aspects of the proposals which are relevant for S-CSCF as well as for P-CSCF initiated re-registration.

2 S-CSCF initiated re-registration

Figure 3 shows the information flow for a registration with subsequent subscription to network initiated re-registration which can only be triggered by the S-CSCF.

Messages 1 - 8 are part of one successfully authenticated registration procedure. Immediately after completion of registration the UE shall subscribe to the *network-initiated re-registration* event. To that the UE sends a *Subscribe* (message 9) to the P-CSCF which forwards it in message 10 to the S-CSCF. The S-CSCF subsequently responds with a *200 OK* message to the P-CSCF.

Note, that the subscription to the *network-initiated re-registration* event shall be mandatory after completion of a successful registration. I.e. the S-CSCF does not receive a subscription to this event within a certain time the user will be automatically de-registered by a *network-initiated de-registration* procedure (cf. [N1-011xxx]).

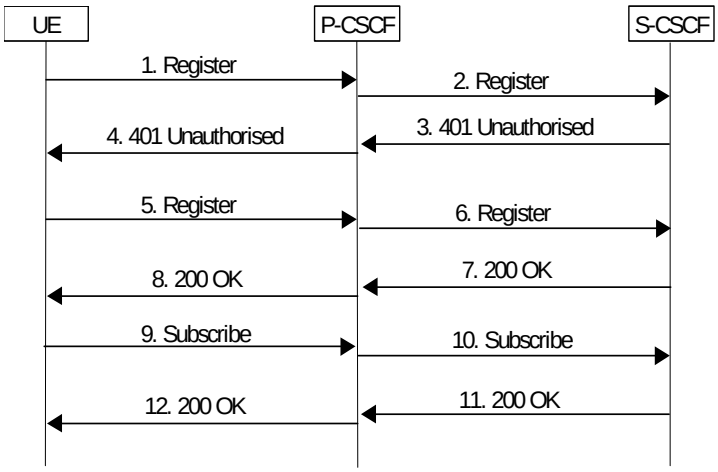

Figure 2: UE subscribes to the network- initiated re-registration event triggered by the S-CSCF

The S-CSCF might at any time request the UE for (an authenticated) re-registration, e.g. for security reasons. Figure 3 shows how this can be achieved.

In order to request (an authenticated) re-registration from the UE the S-CSCF sends a *Notify* for the event *network-initiated re-registration* to the UE. The UE responds with a *200 OK* message. Subsequently, the UE re-registers itself at the S-CSCF (messages 5 - 12 of Figure 3).

The messages with the broken lines are only needed in the case that not only the first registration of a UE but also each subsequent re-registration has to be followed by a new subscription to network-initiated re-registration. This however depends on the setting of the expire-header for the subscription, which is discussed in section 4 below. Due to discussions held at the last CN1 meeting, the timer for

Subscription is very likely to be much higher then the one for registration, i.e. it is not needed to re-subscribe with every re-register.

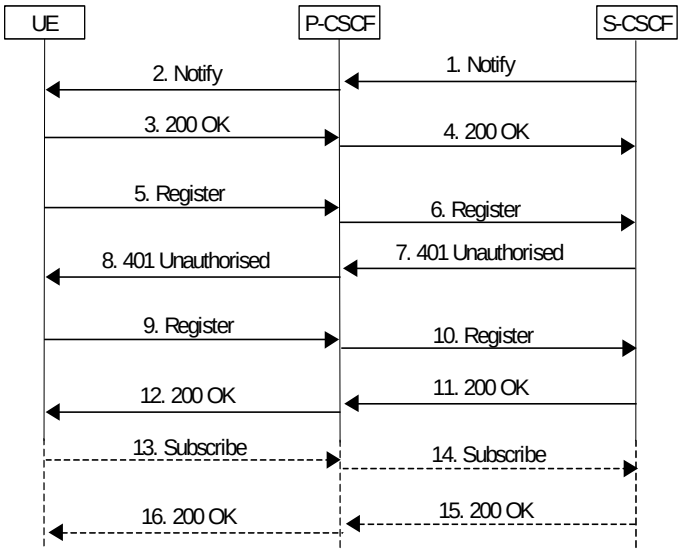

Figure 3: S-CSCF initiated re-registration

If the S-CSCF does not receive a re-registration attempt from the user within a certain timeframe then the S-CSCF automatically triggers a network-initiated de-registration (cf. [N1-011xxx]).

3 P-CSCF initiated re-registration

The solution presented here for a P-CSCF initiated re-registration automatically includes the case of an S-CSCF initiated re-registration described in section 2 above.

The flow presented in Figure 4 is very similar to the one shown in Figure 2 above. Compared to Figure 2 there are only two additional messages needed. In message 13 the S-CSCF sends a *Subscribe* for *network-initiated re-registration*. The P-CSCF responds with a *200 OK* message. By these two additional messages the S-CSCF subscribes to network-initiated re-registration at the P-CSCF.

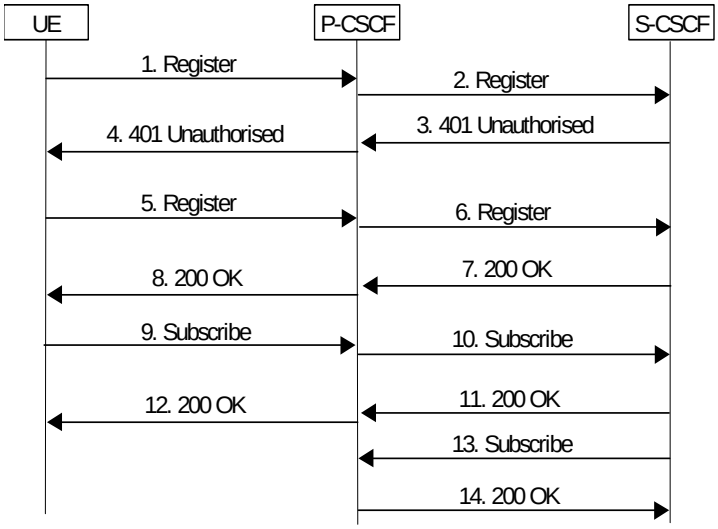

Figure 4: Subscription to the network initiated re-registration event triggered by the P-CSCF

The P-CSCF might at any time request the UE for (an authenticated) re-registration, e.g. for security reasons. Figure 5 shows how this can be achieved.

In order to request (an authenticated) re-registration from the UE the P-CSCF sends a *Notify* for the event *network-initiated re-registration* to the S-CSCF. The S-CSCF responds with a *200 OK* message. (The subsequent messages are identical to the ones for an S-CSCF initiated re-registration shown in

Figure 3 of section 2.) In order to request (an authenticated) re-registration from the UE the S-CSCF sends a *Notify* for the event *network-initiated re-registration* to the UE. The UE responds with a *200 OK* message. Subsequently, the UE re-registers itself at the S-CSCF (messages 7 - 14 of Figure 5).

The messages with the broken lines are only needed in the case that not only the first registration of a UE but also each subsequent re-registration has to be followed by a new subscription to network-initiated re-registration. This however depends on the setting of the expire-header for the subscription, which is discussed in section 4 below.

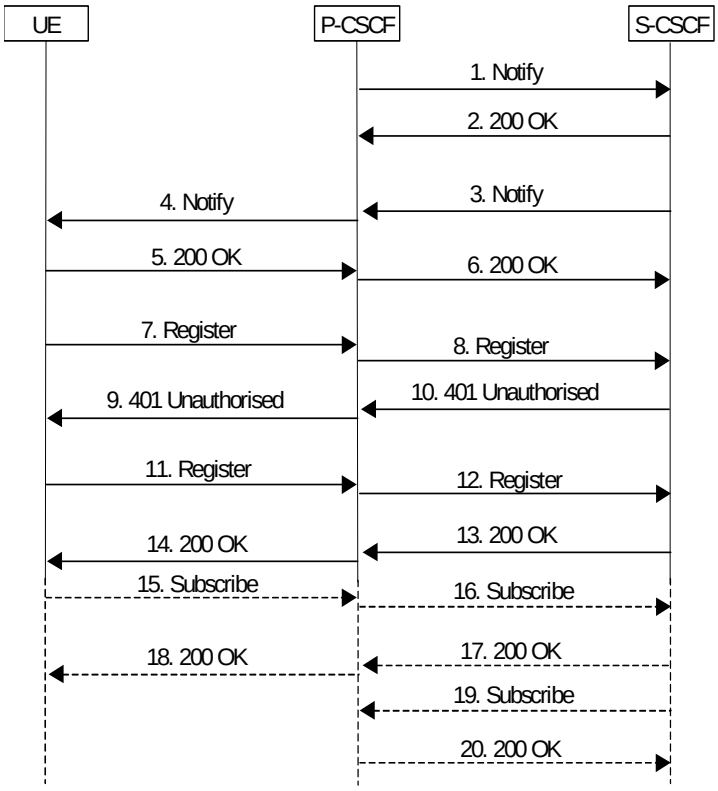

Figure 5: P-CSCF initiated re-registration

If the S-CSCF does not receive a re-registration attempt from the user within a certain timeframe then the S-CSCF automatically triggers a network-initiated de-registration (cf. [N1-011xxx]).

4 Discussion

The *Subscribe* message includes an expire-header. This expire-header is set by the entity which originates the *Subscribe* message. It may be reset by the recipient of the *Subscribe* message. The expire-header (with a possibly different value) is then sent back for information to the originator of the *Subscribe* message in the subsequent *200 OK* message.

The question not discussed in the sections above: Which values for the expire-header are acceptable for the appropriate network node?

It is obvious that an expire-header for subscription to network-initiated re-registration which would be lower than the expire-header for the last successful registration procedure is not sensible.

It is therefore proposed that the expire-header of the *Subscribe* message (Figure 2) sent from the UE to the S-CSCF should at least be as large as the expire-header of the last successful registration procedure. Otherwise the S-CSCF should set the expire-header for *Subscribe* at least to this value. However, the decision on this should be left to CN1 as it is a general question.

For the *Subscribe* message sent from the S-CSCF to the P-CSCF (Figure 4) it is proposed that the S-CSCF should at least be as large as the expire-header of the last successful registration procedure. Otherwise the P-CSCF should set the expire-header for *Subscribe* at least to this value.

If the timer is set to the value of the last successful (re-) registration, then as a consequence, a new subscription to network-initiated re-registration would be necessary after each re-registration attempt.

This may be avoided, if the S-CSCF would set the expire-header to the maximum value allowed, i.e. 2^{32}-1 seconds (about 136 years) [RFC 2543-bis-04, section 10.24]. Then a *Subscribe* to network-initiated re-registration would only be needed immediately after initial registration. It would be valid until the user is de-registered. This would save load on the IMS.

If the first alternative is chosen then in Figure 3 and Figure 5 the complete information flow for a network initiated re-registration includes the messages in the broken lines, otherwise these messages would not be needed.

From the security perspective both alternatives are considered to be equivalent.

5 Proposal

It is proposed to use the features of this contribution to provide network-initiated re-authentication of a UE in the IMS.

As the alternatives for the setting of the expire-header for the subscription to network-initiated re-registration discussed in section 4 are considered to be equivalent from the security perspective, it is proposed that N1 should decide on the alternative to be chosen. This decision shall be forwarded to S3 in a liaison statement.

It should be clarified if the information flows are to be integrated into [TS 33.203] or if they will be part of a technical standards document of S2 or N1.

The solution proposed should be sent in an LS to CN1.

6 References

[3G TS 33.203] 3GPP TSG SA WG3 Security, TS 33.203: *Access security for IP-based services;* v. 0.3.0, May 2001.

[S3-010355] 3GPP TSG SA WG3 Security, S3-010355: *Information flows for IMS authentication and key agreement;* Source: Siemens, S3#19, 4 - 6 July 2001, London (UK).

[S3-010205] 3GPP TSG SA WG3 Security, S3-010205: *Authentication aspects in IM;* Source: BT, S3#18, 21 - 24 May 2001, Phoenix (USA).

[N1-011xxx] 3GPP TSG CN1 WG1, N1-011xxx: *Network-initiated de-registration;* Source: Siemens, 27 - 30 August 2001, Helsinki.

[IETF Draft] IETF Internet Draft: *Event Notification in SIP;* February 2001.

[RFC 2543-bis-04] IETF RFC 2543-bis04: *SIP Session Initiation Protocol;* July 20, 2001.