3GPP TSG SA3 IMS ad hoc TDoc **S3z020011**
January 31st, 2002
Antwerp, Belgium

Source: **Nokia**
Title: Unprotected re-registration during SA lifetime
Document for: Approval/Discussion
Agenda: **6.1,** SIP signalling protection, Integrity

1. Introduction

In 33.203 1.0.0 version re-registration procedure, It is FFS if old SA shall protect the first two messages of the authenticated re-registration, i.e. SM1(register) and SM4 (authentication-challenge). The message chart is copied in Figure 1.

In this Tdoc, we discuss whether unprotected re-registration messages should be allowed. The effort is aimed consist S3 stage 2 with CN1's work together. The conclusion brings proposed CR which is attached at the end of this document. Toward to the attacks may relevant to that, a couple of basic anti-attack solutions are discussed and proposed.

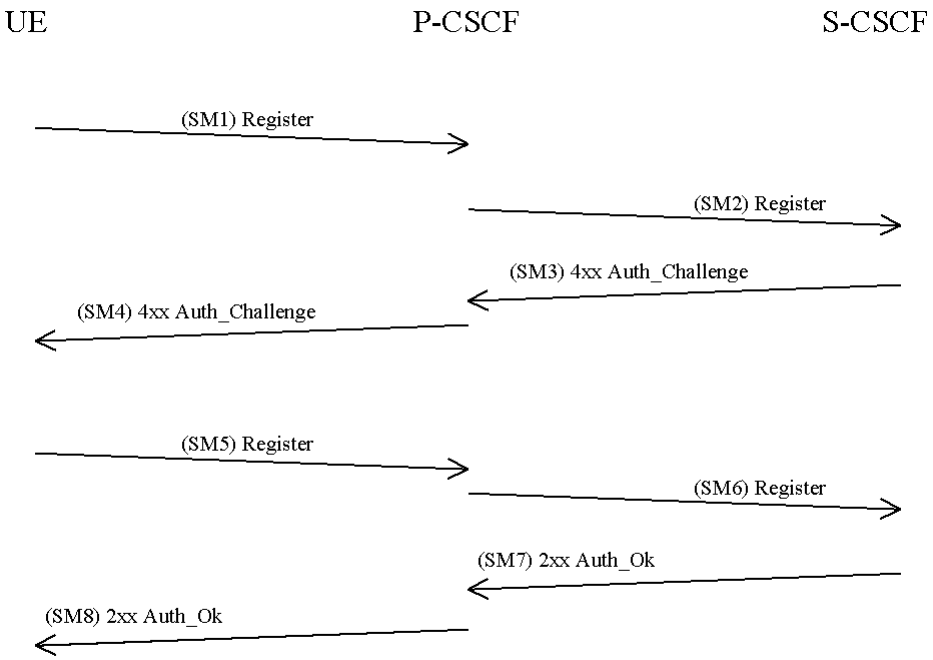

Figure 1: Security association set up

2. Discussion and conclusion

2.1 Unprotected re-registration requirements

When a re-registration takes place, the old SA is still valid, since re-registration timer is set a bit shorter than SA lifetime. Theoretically it is possible to send first 2 messages under old SA's protection. This is shown in section 7.3.3.1.

On the other hand, if S3 mandate the protection of old SA, the following scenarios are not permitted:

Case 1: When mobile battery is removed instantly, mobile does not have chance to acknowledge the network. So when mobile does power-on again (should the timer saved to UICC), it shall re-register in unprotected format since last session's keys and parameters are lost. Therefore the network should allow unprotected re-registration message though last agreed SA may not be expired.

Case 2: During the first registration, the last successful acknowledge, 200 OK message (SM8) is lost due to transmission error and not received by the UE. So UE waits time-out and declares re-registration without protection, though P-CSCF has last valid SA stored.

To satisfy the requirement from both cases, CN1 made their decision that re-registration is allowed without protection during their ad hoc meeting last week (14-18 Jan 02). To compliant with that, S3 should not prohibit these scenarios taking place either. It is proposed to editor's notes in TS 33.203 section 7.3.3, that it is not mandatory to use the agreed SA to re-register procedure messages, namely, SM1 and SM4.

2.2 The attacks relevant to re-registration

2.2.1 Change the registration status

The both cases show an inconsistency of statuses stored in network side and in UE. It opens a chance to abuse user as described in TS 33.203 v1.0, section 6.1.1: *"The UE initiated re-registration opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber unprotected and respond with the wrong RES and the HN could then de-register the subscriber. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered."*

If the abuse permits the registration flag set as unregistered, it's possible that every time UE starts a session, it finds out the status is un-registered. Therefore network must challenge it, which leads to challenge every INVITE. Or the other way round, when S-CSCF receives an INVITE, it checks the status of the UE is un-registered, and does not divert the mobile terminated call. Both cases would cause reachability problems.

To prevent the abuse above happening, the CR below is proposed to TS 33.203 text. The idea is to allow the IMS subscriber remaining registered after unsuccessful re-authentication as long as timer set for re-registration is not expired. In this case the registration flag is kept in the HSS to the value *registered* even if the latest authentication was unsuccessful. The S-CSCF does not remove the data about subscriber's registration, it's path and it's contact IP address. On the other hand, if the true user does not "fresh" registration before timer expiration of the next re-registration, the SA will be expired and status is set to unregistered.

2.2.2 Challenge the re-registration request

This section may not necessarily affect to S3's architecture. Yet provided for discussion and approval if needed.

It is working assumption that the network should not challenge every re-registration message. Many of the re-registration can be sent by protection of old SA, the re-authentication may happen much rare than the re-registration messages. Therefore, the network needs to differentiate true user (due to inability of remembering last session's SA in case 1 or case 2), and the attackers who keeps sending bad-RESs to pester the network. For the true user, the P-CSCF will forward the message to S-CSCF, with information that the previous agreed SA is not in use. The S-CSCF shall challenge the user, the same manner as initial registration. This part is compliant to CN1's working assumption. We fear that simply shortening SA lifetime does not help to avoid user abuse either. First of all, it shall increase a lot of registration traffic; yet attacker can still send those messages, make those problems mentioned above valid. Therefore it is seen the necessity to specify basic anti-abuse behave as proposed below.

Toward to the behave that keeps sending bad-RES to pester network, the network should not answer every message due to the heavy load to server and network traffic. The network side must implement such functions to detect intensive registrations burst. The network can send 403 Forbidden response to that site. This is from CN1's approved Tdoc N1-020158 that S3 should reflect to TS 33.203. It is also

IETF SIP people's consensus. The verification of the site should be based on both IP datagram address and contact header to avoid IP spoofing attack.

Finally it is proposed that a 100 trying response is used during registration procedure, for P-CSCF rejecting DoS registration messages from attacker or too frequent repeat of same requests. In other words, P-CSCF sends 100 trying to acknowledge the receive of SM1 and SM5. if UE keeps sending SM1 or SM5 before P-CSCF responses SM4 or SM8, P-CSCF simply discards all.

2.3 Network initiated re-authentication

This subsection discusses network initiated re-authentication. Though currently it is not specified in TS 33.203, it is worth of taking a look at whether the proposal in the Tdoc conflicts to network initiated re-authentication procedure that will be contained in R6. The procedure is specified in TS 24.228 section 6.8 for no hiding case. The procedure is copied in Figure 2. The notification of a user in figure is about the re-authentication event that occurs at the S-CSCF assigned to that user.

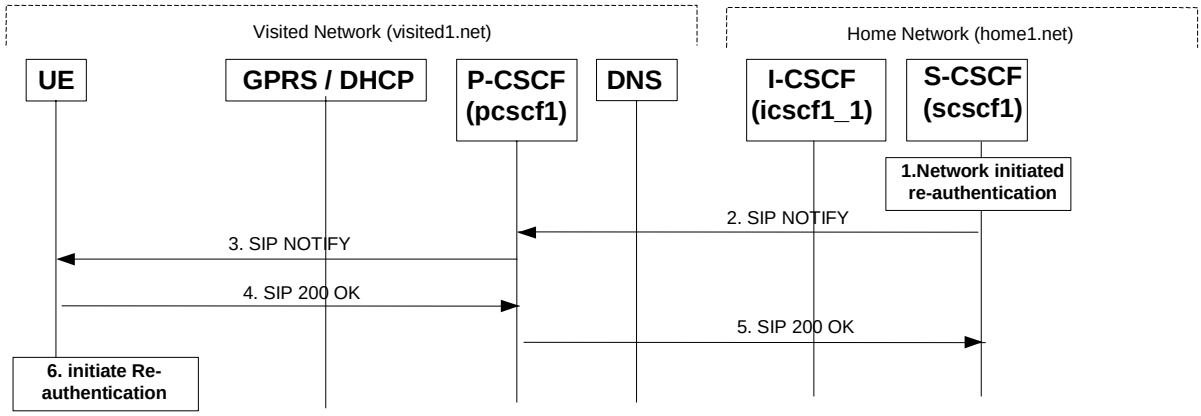

Figure 2: Network initiated re-authentication

It is compliant to our current architecture, that UE initiates re-authentication as shown in step 6. In this case, since S-CSCF initiates the procedure, the SA's validation is set to be updated. It can be both protected or unprotected message, and both cases should be challenged. If the user fails to be authenticated, the registration will be set as un-registered since timer for next registration is expired, instead of failure of RES match.

3 Summary

In this document, it is proposed:

- to reflect the acceptance of unprotected re-registration messages, namely, SM1 and SM4 in TS 33.203 due to the facts;
- to disallow the change of registration status other than re-registration timer;
- that P-CSCF informs S-CSCF whether the agreed and valid SA is used for that REGISTER message. This is compliant to CN1's stage 3 work;
- to reject re-registration abusing true subscribers, the network can use 403 Forbidden response.
- to reject DoS attack during registration, the network can apply 100 trying to bound back them.

⌘	33.203 CR		⌘	ev	-	⌘	Current version:	1.0.0	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Unprotected re-registration during SA lifetime
Source:	⌘	Nokia
Work item code:	⌘	***Date:*** ⌘
Category:	⌘	**B**

Release: ⌘ REL-5

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	To accept unprotected re-registration message.
Summary of change:	⌘	Remove text to allow de-registration of unsuccessful re-registration.
Consequences if not approved:	⌘	Inconsequent definitions of UICC leading to misunderstandings.

Clauses affected:	⌘	6.1.1
Other specs affected:	⌘	☐ 24.228 ☐ ☐
Other comments:	⌘	

Section 6.1.1

The P-CSCF forwards the RES in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the RES to the S-CSCF.

Upon receiving the response, RES, the S-CSCF retrieves the active XRES for that user and checks if XRES=RES. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. To ensure that the S-CSCF is able to take the decision whether a subsequent registration shall trigger a new authentication and to be able to check that all INVITE messages will be sent to/from an authorized subscriber it shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

[Editor's note: Since implicitly registered IMPUs are not available in the P-CSCF this functionality opens up a weakness in the IMS security architecture. Requirements that closes this weakness needs to be defined and is left FFS.]

At this stage the S-CSCF shall send in the Cx-Put after receiving SM9 an update of the registration-flag. If the authentication of the subscriber is successful the registration flag shall take the value *registered.* When the authentication is unsuccessful the registration flag shall be set to *unregistered.*

When a subscriber has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. The UE initiated re-registration opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber in an unprotected message~~plain-text~~ and respond with the wrong RES and the HN could then de-register the subscriber. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

The authenticated re-registration looks the same as the initial registration except that CM1 and CM2 can be omitted as long as the S-CSCF has valid AV(s). At a re-registration the registration flag has already the value *registered.* The policy of the home provider states whether the flag shall be changed at a re-registration based on two scenarios. ~~There are two cases:~~

- ~~The IMS subscriber is de-registered after unsuccessful registration. In this case the registration flag shall be set to *unregistered* and an error message shall be sent to from the S-CSCF to the HSS.~~

- If the re-registration is successful, the registration status is re-freshed in the S-CSCF.

- The IMS subscriber remains registered after unsuccessful re-registration unless timer set for next re-registration is expired. In this case the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful. The S-CSCF shall not remove the data about subscriber's registration, it's path to be reached and it's contact IP address. The P-CSCF shall remain the old SA.

The lengths of the IMS AKA parameters are specified in section 6.3.7 of TS 33.102 [1].