3GPP TSG SA WG3 Security — S3#22 **S3-020106**

25 - 28 February 2002

Bristol, UK

Source: **Nokia**
Title: Unprotected registrations during SA lifetime
Document for: Discussion/ Approval
Agenda: **7.3, IP multimedia subsystem security**

1. Scope and objectives

In 33.203 version 1.0.0 re-registration procedure, It is FFS if the agreed SA bundle shall be applied to protect the first two messages, namely SM1(register) and SM4 (authentication-challenge) in Figure 1.

In this Tdoc, we discuss should the network accept the unprotected re-registration messages sent from a registered UE. The discussion shows why that is a necessary requirement to the network. Furthermore, we propose a couple of basic anti-attack solutions to some attacks relevant to that requirement. The attached CR is proposed to reflect the conclusion.

Motivation of this Tdoc is to keep consistency with CN1's stage 3 work from S3 perspective.

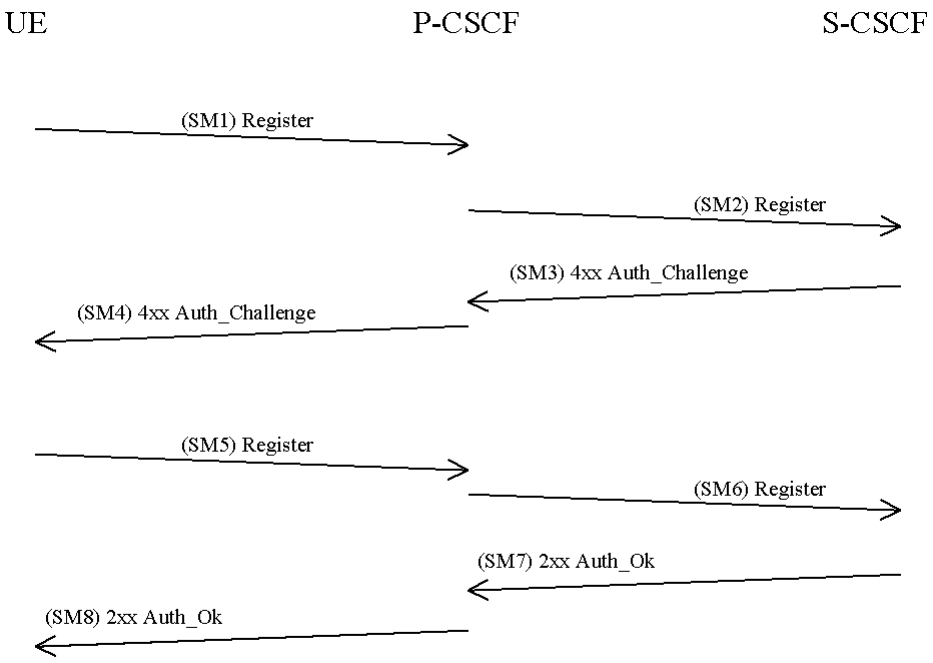

Figure 1: Security association set up

2. Discussion and conclusion

2.1 Unprotected registration requirement

When a re-registration takes place, the old SA is still valid, since re-registration timer is set a bit shorter than SA lifetime. Therefore the network shall always accept the first 2 messages to be protected by the old yet valid SA. 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, it shall send REGISTER in unprotected format since last session's keys and parameters are lost. From network point of view, it may be considered a re-registration message from that registered UE. Obviously the network should allow it happening 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 of UDP and therefore not received by the UE. So UE waits a time-out. It considers it as a failed case and declares an unprotected registration again, though P-CSCF has last valid SA stored.

To satisfy the two cases, CN1 made their decision that re-registration is *allowed* to be un-protected during their ad hoc meeting (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 registration

2.2.1 Change the registration status

The both cases reveal a possibility of inconsistent registration statuses stored in network and in UE. It opens a chance to impersonate 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 network permits the bad-RES abuse to flip the registration flag as unregistered, it is possible every time when UE starts INVITE, it finds out the status is un-registered. The network must reject it since there is no information stored regarding to the user. Consequently, the network must challenge it again, which leads to challenge every INVITE. The other way round, when S-CSCF receives an INVITE, it checks the status of the UE is un-registered, so it does not divert the mobile terminated call. Both cases would cause huge reachability problems.

To prevent the abuse, the network should not allow an un-authenticated RES response effect on user database. In other words, only correct RES, authenticated de-registration or expiration of that timer can change registration status and timer of its validity. A CR below is proposed to TS 33.203 to reflect it. Please refer to the CR for wording.

Put it in detail, the registration flag is kept in HSS to the value registered regardless of bad-RES. The S-CSCF does not remove the data of subscriber's registration, it's path and it's contact IP address for bad-RES. When re-registration timer expires, because the true user does not "refresh" it, or user de-registers himself with message integrity, the SA will be discarded in S-CSCF and P-CSCF, status in HSS is set to unregistered.

2.2.2 Network challenges the re-registration request

It is a working assumption that the network shall not challenge every re-registration message. They can be sent by protection of currently valid SA, so re-authentication happens much rare than the re-registration messages. Therefore, the network needs to differentiate true user (due to inability of using last session's SA in case 1 or case 2), and the attacker who keeps sending bad-RESs to pester the network. For the true user's request, 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.

To the attacker behave that keeps sending bad-RES to pester network, the network should not answer every message due to the heavy load to server and core network traffic. We propose that network must implement such function to detect intensive registrations burst. Once found the network can send 403

Forbidden response to that site. This is from CN1's approved Tdoc N1-020158. and it is also IETF SIP people's consensus. Further more, it is proposed that a 100 trying response to UE is used during registration procedure, for P-CSCF rejecting DoS registration messages from attacker. 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. The SIP client may need corresponding intelligence not to re-send REGISTER too often.

2.3 Network initiated re-authentication

This section 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 Figure 2 is the procedure specified in TS 24.228 section 6.8 for no hiding case. The notification 3 is to inform a re-authentication event assigned by the S-CSCF is occurred to that user.

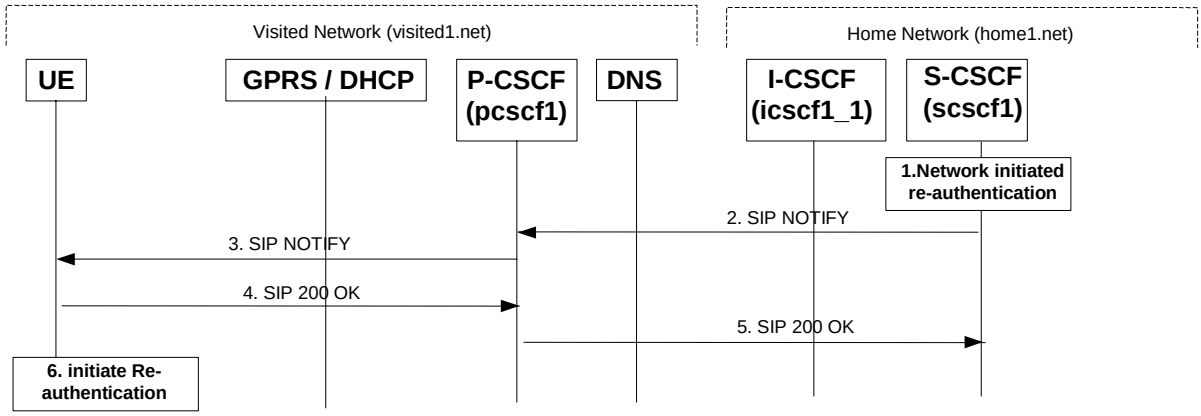

Figure 2: Network initiated re-authentication.

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*.

3 Summary

In this document, it is proposed:

- to reflect the acceptance of unprotected registration messages, namely, SM1 and SM4 in TS 33.203 due to the realism requirements;
- to disallow any change to registration status unless it is authenticated RES, authentication de-register or expiration of re-registration timer;
- that P-CSCF needs to inform 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 fake re-registration to abuse 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 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 keeps registered and timer for next registration is refreshed in the S-CSCF.

- The IMS subscriber remains registered after unsuccessful re-registration until timer set for next re-registration is expired. ~~In this case~~Before that 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].