3GPP TSG SA WG3 Security — S3#22 **S3-020137**

25 - 28 February 2002

Bristol, UK

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

CR-Form-v4

CHANGE REQUEST

⌘ **33.203** **CR** ⌘ ev **-** ⌘ Current version: **1.1.0** ⌘

*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, 7.3.3	
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). The P-CSCF shall forward the unprotected re-registration to S-CSCF with an indication that the existing SA is not applied. As the consequence, the S-CSCF shall trigger a new authentiation procedure. 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 existing SA.

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

…

7.3.3 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. The authenticated re-registration shall initially utilize the existing SA. This is the normal case. ~~In normal conditions, both the UE and P-CSCF shall use the existing SA to protect re-register messages (e.g. SM1/SM4).~~ However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA authentication procedure as described in chapter 6.1.1.

~~*[Editors Note: It is under investigation if unprotected re-registration shall be allowed during the SA-Lifetime.]*~~

Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.