3GPP TSG SA WG3 Security — S3#19 **S3-010328**
3 - 6 July, 2001, Newbury, UK

Agenda Item: 7.3

Source: Ericsson

Title: Validation of public user identity in registration

Document for: Discussion and decision

---

1. Scope and objectives

During last S2 meeting (25th – 29th June), Ericsson presented a contribution that tried to solve a potential problem when Public Identities are misused at User Registration.

Since this was considered by S2 as having too many security implications and there were not time enough to draft a LS to S3, Ericcson was asked to raise this issue in S3 directly.

S2 contribution and CR to 23.228 below introduces the problem and proposes a solution. This shall be discussed now by S3#19 in order to provide guidance as requested by S2.

It shall be also noted that this issue shall be dealt with along with other discussions regarding the correct handling of Private and Public User Identities in IMS.

3GPP TSG-SA WG2 drafting
25-29 June, 2001
Dallas (US)

Tdoc S2-011634

Agenda item: 4

Source: Ericsson

Title: Validation of public user identity in registration

Document for: discussion and decision

---

1. Introduction

In SA2 # 17, the role of the identifiers in IMS was defined. A description of the usage of public and private user identities is shown in TS 23.228 in section 4.3.3 Identification of users. The following statements are captured from this section:

- *The Private User Identity is authenticated only during registration of the subscriber, (including re-registration and de-registration).*
- *Public User Identities are not authenticated by the network during registration.*

The current assumption is that the REGISTER message contains both identities, the private user identity to authenticate the user and the public user identity for the registration process itself. According to the discussions in last SA3-SA2 joint meeting held in Madrid, there is no security relation between both user identities. Therefore, the validation of the private user identity through the user authentication procedure does not preclude the fraudulent usage of the public user identity, above all during an initial registration when no integrity protection is provided yet.

---

2. Discussion

The fact that there is no security relation between the private user identity and the public user identities, brings up the need of validating the public user identity that the end user is trying to use to register in the IMS. This means that the network shall check that the public user identity intending to register is included in the list of public user identities subscribed for that user.

The HSS is the network entity that owns the subscription of the user. This subscription contains the list of valid public user identities for a given private user identity (user). Therefore, it is proposed that the HSS checks the validity of a public user identity during the registration process. It is considered that the sooner this check is done the better, so the allocation of resources to a user that might not have a valid identifier is avoided. It is proposed that the HSS performs this check when a Cx- Query is received from the I-CSCF. This Cx-Query message shall contain both user identities sent in the REGISTER message.

---

3. Proposal

The following CR contains the proposed modifications in the registration information flows of 23.228 (section 5.2.2.3).

CR-Form-v3

CHANGE REQUEST

⌘ 23.228 CR 57 ⌘ rev - ⌘ Current version: 5.0.0 ⌘

*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:	⌘	Validation of public user identity in registration
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	2001-06-20
Category:	⌘	**B**
Release:	⌘	REL-5

Use one of the following categories:
F *(essential 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:	⌘	User authentication procedures only authenticate the private user identity. There is no security relation between the private user identity and the public user identity, therefore, the network shall ensure that a valid public user identity is being used for registering the IMS.
Summary of change:	⌘	During the registration process, the HSS checks that the public user identity is valid according to the subscription information.
Consequences if not approved:	⌘	Fraudulent usage of public identities. This may cause security problems and MT routing problems.

Clauses affected:	⌘			
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

First Change

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the subscriber is considered to be always roaming. For subscribers roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.

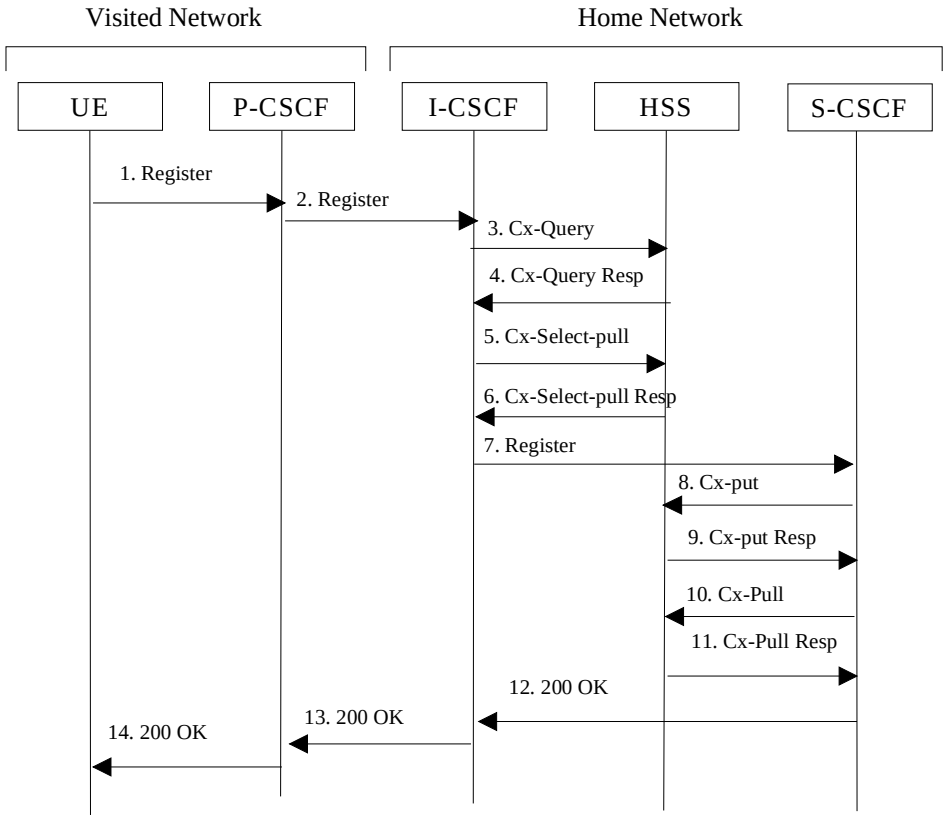

Figure 5.1: Registration – User not registered

1. After the UE has obtained a signalling channel through the access network, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (private user identity, public user identity,~~subscriber identity,~~ home networks domain name).

2. Upon receipt of the register information flow, it shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCFs "name" in the contact header, private user identity, public user identity,~~subscriber identity,~~ visited network contact name). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. When the I-CSCF receives the registration information flow from the proxy, it shall examine the subscriber identity and the home domain name, and employ the services of a name-address resolution mechanism, to determine the HSS address to contact.

3. The I-CSCF shall send the Cx-Query information flow to the HSS (P-CSCF name, ~~subscriber identity~~private user identity, public user identity, home domain name, visited network contact name). The P-CSCF name is the contact name that the operator wishes to use for future contact to that P- CSCF.

Editors Note: It is FFS whether the terminal name, or proxy name, or both is included within this and subsequent register messages.

The Cx-query (P-CSCF name, ~~subscriber identity~~private user identity, public user identity, home domain name, visited network contact name) information flow is sent to the HSS. The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that visited network according to the User subscription and operator limitations/restrictions if any. The HSS shall validate the public user identity according to the subscription information.

4. Cx-Query Resp is sent from the HSS to the I-CSCF. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

5. At this stage, it is assumed that the authentication of the user has been completed (although it may have been determined at an earlier point in the information flows). The I-CSCF shall send Cx-Select-Pull (serving network indication, subscriber identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function.

6. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.

7. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the register information flow (P-CSCFs "name" in the contact header, subscriber identity, visited network contact name) to the selected S-CSCF.

8. The S-CSCF shall send Cx-Put (subscriber identity, S-CSCF name) to the HSS. The HSS stores the S-CSCF name for that subscriber.

9. The HSS shall send Cx-Put Resp to the I-CSCF to acknowledge the sending of Cx-Put.

10. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE.

11. The HSS shall return the information flow Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

12. The S-CSCF shall determine whether the home contact name is the S-CSCF name or an I-CSCF name. If an I-CSCF is chosen as the home contact name, it may be distinct from the I-CSCF that appears in this registration flow. The home contact name will be used by the P-CSCF to forward signalling to the home network. The S-CSCF shall return the 200 OK information flow (serving network contact name, S-CSCF name) to the I-CSCF.

13. The I-CSCF shall send information flow 200 OK (serving network contact name) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

14. The P-CSCF shall store the serving network contact name, and shall send information flow 200 OK to the UE.