3GPP TSG SA WG3 Security — S3#23 **S3-020268**
14 - 17 May 2002
Victoria, Canada

CR-Form-v4

CHANGE REQUEST

⌘ **33.203 CR** ⌘ ev **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	The use of Ipv6 addressing privacy within IMS		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	May 15 2002
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:	⌘	Align TS33.203 with TS23.228 requirements for IPv6 privacy
Summary of change:	⌘	Adding rules for SA handling when the UE changes IP address
Consequences if not approved:	⌘	TS33.203 is not consistent with TS23.228

Clauses affected:	⌘	7.3.3, 7.3.3.1	
Other specs affected:	⌘	☒	24.229
		□	
		□	
Other comments:	⌘		

************* FIRST CHANGED SECTION **************

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. 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 clause 6.1.1.

[Editors Note: The exact mechanism for changing SAs is currently under investigation.]

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

[Editors Note: The exact mechanism when to change SA1 to SA2 under certain error conditions is FFS.]

When a UE has changed its IP address that it intends to use for subsequent SIP signaling, it should initiate a re-registration procedure.

************** NEXT CHANGED SECTION ***************

7.3.3.1 Handling of security associations in authenticated re-registrations (successful case)

Before re-registration begins the following SAs exist:

- SA1 from UE to P-CSCF;
- SA2 from P-CSCF to UE.

The re-registration then is as follows:

1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.

   If the re-registration was initiated due to the allocation of a new IP address, the UE shall use the old IP address when sending SM1. If the old IP address is no longer usable, SM1 shall not be integrity protected. Inside the SIP message SM1, the UE shall advertise a contact address that it wants to use after the re-registration is complete. This address may be different from the source address used to send SM1 when the UE has allocated a new address. If this is the case, the UE shall also include the old address in SM1 and advertise it to expire immediately.

[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]

2) The P-CSCF waits for the response SM4 from the S-CSCF and then sends SM6 to the UE, using the already existing SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations SA11 and SA12, in parallel to the existing ones, in its database.~~:~~

   However SM6 shall be sent to the IP address that was used when SA2 was originally created, regardless of the contact address advertised by the UE in SM1.

   - SA11 from UE to P-CSCF;
   - ~~-~~SA12 from P-CSCF to UE.

   In these security associations, the IP address of the UE shall be the contact address advertised by UE in SM1.

3) If SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM7 is protected with the new SA11.

   The UE shall now use the same source address in sending this message as it advertised as its contact address in SM1.

4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12. SM12 shall be sent to the source address that was used when sending SM7.

5) After the reception of SM12 by the UE, the re-registration is complete.

The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.

The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.