3GPP WSG – SA3 Meeting #26
Oxford, UK, 19th – 22nd November

Tdoc ⌘S3-020643

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** ⌘**rev** **-** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Registration and SA lifetimes
Source:	⌘	
Work item code:	⌘	IMS-ASEC
Date:	⌘	09/10/2002
Category:	⌘	**F**
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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The current method for handling the combination of registration and SA lifetimes could leave an IMPU registered but with no SA available to contact the UE
Summary of change:	⌘	Ensures that any new SA created lives at least as long as the previous SA and the SA lifetime is updated if the expiry time of a registartion without an authentication exceeds the current lifetime. Provides a maximum lifetime that an SA can live in the UE.
Consequences if not approved:	⌘	A registered IMPU may be unreachable causing a loss of service.

Clauses affected:	⌘	7.4.1a, 7.4.2a

		Y	N			
Other specs affected:	⌘	Y		Other core specifications	⌘	24.229
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with an existing pair of SAs. This will be referred to as the old SAs. The authentication produces a pair of new SAs. These new SAs shall not by used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.
- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.
- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to section 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication. Furthermore for outbound traffic, the new SA shall be used.
- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.
- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs using the maximum of registration timer in the message and the lifetime of the old SAs. The old SAs are now deleted. The new SAs are used to protect all traffic.

A failure in the authentication means the UE shall delete the new SAs. If the SM1 was not protected, then no protection shall be applied to the failure messages. If SM1 was protected, the old SAs shall be used to protect these messages.

The UE shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

In addition to the individual SA lifetimes, the UE shall maintain a maximum lifetime for an SA. If an SA exists for longer than this maximum lifetime, the UE shall send an unprotected REGISTER message to force an authentication with the network in order to generate fresh SAs.

Note: This maximum lifetime determines the minimum rate at which authentications occur and should accordingly be set to a reasonably long time, e.g. 24 hours.

The UE shall delete any SA whose lifetime is exceeded.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain an existing pair of SAs from a previously completed authentication. It may also contain an existing pair of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces a pair of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.
- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.
- The P-CSCF then creates the new SAs, which are derived according to section 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.
- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication.
- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs equal to the maximum of registration timer in the message and the lifetime of the old SAs, and deletes the old SAs. The new SAs are used to protect all traffic.

A failure in the authentication means the P-CSCF shall delete the new SAs. If the SM1 was not protected, then no protection shall be applied to the failure messages. If SM1 was protected, the old SAs shall be used to protect these messages.

The P-CSCF shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

The P-CSCF shall delete any SA whose lifetime is exceeded.