CR-Form-v5

CHANGE REQUEST

⌘	**33.203** CR	⌘ **rev**	⌘	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 **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Handling the lifetime of an SA	
Source:	⌘	Ericsson	
Work item code:	⌘	IMS-ASEC	*Date:* ⌘ 06/05/2002

Category:	⌘	**F**	*Release:* ⌘ Rel-5

Use <u>one</u> 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 <u>one</u> 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:	⌘	The requirements in the Annex of TS33.203 is not consistent with the requirements in the main body
Summary of change:	⌘	The SA lifetime shall be time limited and equal to the registration timer in the S-CSCF
Consequences if not approved:	⌘	Conflicting requirements in TS33.203

Clauses affected:	⌘	7.1, Annex D.1

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

Other comments:	⌘	

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

7.1　Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys provided by IMS AKA, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the security association to be used for a protection method.

The security mode setup shall support the negotiation of different protection mechanisms. It shall be able to negotiate or exchange the SA parameters required for these different protection mechanisms. Although the supported protection mechanisms could be quite different, there is a common set of parameters that have to be negotiated for each of them. This set of parameters includes:

- Authentication (integrity) algorithm, and optionally encryption algorithm;

- SA_ID that is used to uniquely identify the SA at the receiving side;

- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Parameters specifically related to certain protection methods are kept in the annexes describing the protection methods.

The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to accept, decrease or increase the proposed expiration time from the UE and the final value is sent in the response to the UE. The expiry time in the UE will be shorter than the expiry time in the S-CSCF, such that the UE is able to re-register. For each new successful authentication the SA shall be updated. The S-CSCF shall align the expiration of subsequent registrations with any existing registration timer. The SA ~~is~~ shall be deleted and the SA cannot be used anymore if the ~~registration~~IPSec SA lifetime ~~timers expires~~ expires in the P-CSCF or in the ~~S-CSCF~~UE.

[Editors Note: The support of different mechanisms is FFS.]

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

D.1   Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF (if not otherwise stated), are

- ESP transform identifier

- Authentication (integrity) algorithm

- SPI

Further parameters:

- Life type: the life type is always seconds

- SA ~~duration~~lifetime: the SA ~~duration has a fixed length of $2^{32}-1$~~lifetime equals the registration timer as negotiated between the UE and the S-CSCF.

- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.

2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.

3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.

4. The UE may send only the following messages to the fixed port for unprotected messages:

   - initial REGISTER message;

   - REGISTER message with network authentication failure indication;

   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

   [Editors' note: It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.