3GPP TSG SA WG3 Security — S3#23 S3-020225

14 - 17 May 2002, Victoria, Canada

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 ☐ Radio Access Network ☐ Core Network ☒

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

Reason for change:	⌘	TS33.203 suggests that a S-CSCF can increase the expiry time as proposed by the UE, which is not allowed according to SIP specification RFC 3261. TS33.203 also suggests that the P-CSCF can negotiate the expiry time but the decision is made by the S-CSCF.
Summary of change:	⌘	The change reflects that a SIP registrar cannot increase expiry time and that the registration timer is decided by the S-CSCF
Consequences if not approved:	⌘	Misalignment with SIP i.e. RFC 3261

Clauses affected:	⌘	7.1
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~~ reject the proposed expiration time from the UE and the final value or an error message 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 deleted if the registration timers expires in the P-CSCF or in the S-CSCF.

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