3GPP TSG SA WG3 Security — S3#24 **S3-020404**

9 - 12 July, 2002

Helsinki, Finland

Source: **Nokia**

Title: **Utilizing SIP parameter to handle SA database optimally in P-CSCF**

Agenda item: **7.1, IMS**

Document for: **DISCUSSION/APPROVAL**

Abstract

This paper proposes utilizing SIP parameter to handle SA database optimally in P-CSCF.

1. INTRODUCTION AND EXPLANATION

The current TS 33.203 v5.2.0 specifies P-CSCF behavior: if the temporarily stored SA is expired, the P-CSCF shall deleted the SA both at the application layer and in IPsec module as well. There are a couple of clauses read as such:

- Clause 7.1, Security association parameters, “The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the registration period.”
- Clause 7.3.1.1 User authentication failure, “In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out.”
- Clause 7.3.1.4 Incomplete authentication, “If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.”

The text is ambiguous at the meaning; it does not indicate from which SIP message the registration timer that P-CSCF should copy from to application layer, neither does it specify how long the lifetime may be. In CN1 specification TS 24.229 v5.1.0, the latest version, UE’s initial REGISTER message has 600 000 seconds (t1) requested period, about 6.94 days. Alternatively, the 4xx message also contains an expiration timer (t2) issued by the S-CSCF to identify when the UE should re-register to the network.

There are shortcomings either timer taken as the initial lifetime of SA. Timer t1 is meant as default value proposed by UE, it is in initial REGISTER message that is unprotected. Thus it should not be trusted and used as parameter of SA lifetime. Timer t2 means the valid period in case the authentication is approved. If t2 is used in P-CSCF, it shall last till next registration timer, or must be informed by S-CSCF of cancellation. The latter case is not permitted if response fails integrity and never received by the S-CSCF. Thus using t2 introduces redundancy to IPsec database in P-CSCF in authentication failure case.

2. PROPOSAL

We propose a default lifetime to be used for SA at SIP application in P-CSCF, when 401 message is sent from P-CSCF to the UE. This default value shall expire automatically, if the response is not received for whatever reason. In this case, in line with current specification, the UE shall re-start a new registration request. And P-CSCF can delete the corresponding SA in IPsec SA database in optimized way. It is seen a good optimization in resource consumption. In case a successful registration/authentication, the 200 (OK) contained Expire timer shall be copied to SIP level lifetime.

The default value should equal to the re-transmission for same method, so that re-transmission attempts are handled. In [IETF_SIP], the re-transmission timer is defined as Timer F =64*T1= 32 seconds, where T1 is round-trip time (RTT). (Timer F's definition in [IETF_SIP] is "non-INVITE transaction timeout timer".

Note please, that the optimization does not involve UE side, partially because SA database management in P-CSCF is much bigger that benefit significantly from this optimization; also in case UE does not receive 200 (OK) and re-start the procedure, P-CSCF can not know it, therefore it is another independent issue.

A CR is attached looking for approval from this meeting.

3. REFERENCE

[IETF_SIP] J. Rosenberg et al., SIP. RFC 3261, IETF. June 2002.

(CR attached)

CHANGE REQUEST

⌘ **33.203 CR CRNum** ⌘ **rev -** ⌘ Current version: **5.2.0** ⌘

*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 ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Utilizing SIP parameter to handle SA database optimally in P-CSCF		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	4 July 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:	⌘	Current spec text is ambiguous at the meaning of lifetimer, from which it comes and what the meaning stands for.
Summary of change:	⌘	A default lifetime to be proposed for SA at SIP application in P-CSCF.
Consequences if not approved:	⌘	Resource on SA management in P-CSCF application layer as well as IPsec layer may be wastered.

Clauses affected:	⌘	7.1, 7.3.1.1, 7.3.1.4				
		Y				
Other specs affected:	⌘	**X**		TS 24.228, 24.229	⌘	
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.

7.1 Security association parameters

omitted

8. The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the re-transmission timer as default value, and then copy the registration period value from 200 (OK) issued by S-CSCF as lifetime.

omitted

7.3.1.1 User authentication failure

In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out of the re-transmission timer.

omitted

7.3.1.4 Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

If the P-CSCF deletes a registration SA due to its re-transmission lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.