3GPP TSG CN Plenary Meeting #21 **NP-030357**
17th - 19th September 2003. Frankfurt, Germany.

Title:	Response LS on Security Association Lifetime Management
Response to:	LS (S3-030336 = NP-030308) on Security Association Lifetime Management and LS (S3-030330 and LS (S3-030330 = NP-030918) on Security Association Lifetimes
Release:	5
Work Item:	IMS-CCR
Source:	SA3
To:	CN, CN1
Cc:	

3GPP TSG-SA WG3 Security – S3#29 **S3-030441**
San Francisco, USA, 15th – 18th July 2003.

Contact Person:
Name: Adrian Escott
Tel. Number: +44 7782 325254
E-mail Address: adrian.escott@three.co.uk

Attachments: S3-030442

1. Overall Description:

SA3 would like to thank CN and CN1 for their liaisons on Security Association Lifetimes.

In their liaison CN ask SA3 several questions to get some clarifications to enable CN1 to apply the correct changes to TS 24.229. SA3 have considered the questions and agreed on the following answers.

Q1*. In 33.203 section 7.1, bullet point number 8 it states that the SA lifetime should be set to the Registration lifetime. Further, in section 7.4.1a it is stated that the SA lifetime is set to the maximum of the SA lifetime or the registration. Is the correct understanding of these two statements that a) if there are no existing registrations related to an IMPI then 7.1 applies, and b) if there are already existing registrations related to an IMPI then 7.4.1a applies ?*

Answer: The understanding is correct. In fact, given that there are no existing registrations there are no SAs, hence in this case the two methods are equivalent. Bullet 8 in section 7 will be removed to avoid confusion.

Q2*. It has also been noted that the definition of the setting of the lifetime is not clear (in 33.203 and 24.229) as the Expires header in a registration is a 'relative' time i.e. the registration will be valid for that time, starting from the registration point. It is possible that a re-registration results in an end time earlier or later than that set by existing registrations, even when this expires value is shorter than one received for a previous registration (e.g. the previous registration may be close to expiry). Can SA3 please confirm that when setting the lifetime of the SA the intent is to utilise the latest end time ?*

Answer: The lifetime of the SA must be set to the latest end time to ensure the SA does not expire before all registrations have expired, otherwise the UE may become unreachable. The text in TS 33.203 will be changed to read "The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life" with a similar change for the P-CSCF and registrations without authentications to avoid possible mis-interpretations.

Q3*. The proposals in the postponed CR's allow for the SA lifetime to be shortened to match the longest remaining registration. The existing text in 7.4.1a of 33.203 would not result in a shortening of the SA lifetime (it is either*

lengthened or unchanged) until the final registration is removed, when the SA will be deleted. Do SA3 see an advantage in including a mechanism to allow the SA lifetime to be shortened ?

Answer: SA3 sees no value shortening the lifetime of the SA based on de-registrations. Of course this does not preclude deleting SAs that have become redundant (e.g. new SAs replacing the old SAs or all IPMUs are deregistered).

Q4*. It has been questioned why the SA needs to be assigned a lifetime at all. It is noted that the SA will be deleted when the last registration related to an IMPI expires in any event (24.229 includes the necessary mechanisms to inform the PCSCF of this event). At other times it will be valid during an ongoing registration, and with the existing 33.203 text the lifetime may be longer than the longest remaining registration. Does SA3 believe that there is a requirement for a defined SA lifetime ?*

Answer: SA3 believe there is a need for an SA lifetime. This is particularly true when there are two sets of SAs (because of a re-authentication), as there is a security requirement to limit the lifetime of old SAs. SA3 will add text to state that the SAs are deleted, once the associated IMPUs are de-registered. The mechanism mentioned could be used for this, if CN1 feel this is appropriate.

SA3 hope that the answers the above questions will enable CN1 to make the necessary changes to their specifications.

2. Actions:

To CN1:
CN1 are kindly requested to consider the above responses to the questions raised by CN and the attached CR when implementing changes to their specifications.

3. Date of Next TSG-SA WG3 Meetings:

TSG-SA WG3 Meeting #30	6th – 10th October 2001	TBD
TSG-SA WG3 Meeting #31	18th – 21st November 2001	TBD