3GPP TSG SA WG3 Security — S3#31 **S3-030657**
18 - 21 November 2003
Munich, Germany

3GPP TSG SA WG3 (Security) meeting #30 **Draft Report version 0.0.2rm**

6-10 October 2003

Povoa de Varzim, Portugal

Source:	**Secretary of SA WG3 (M. Pope, MCC)**
Title:	**Draft Report of joint SA WG3/CN WG1 session on IMS security. 6 October 2003**
Document Status:	**Draft report version 0.0.2 (with revision marks)**

1 Opening of the meeting

The SA WG3 Chairman opened the joint meeting and welcomed delegates to Porto. A role call was made around the room. Conclusions of the joint session were to be presented in SA WG3 meeting #30 on Tuesday 7th October and all potential SA WG3 decisions were to be presented for endorsement.

2 Agreement of the agenda and meeting objectives

TD S3-030483 Draft agenda for joint SA WG3/CN WG1 session on IMS security. The draft agenda was introduced by the SA WG3 Chairman and was approved.

2.1 3GPP IPR Declaration

The chairman made the following call for IPRs, and asked ETSI members to check the latest version of ETSI's policy available on the web server:

> The attention of the members of this Technical Specification Group is drawn to the fact **that 3GPP Individual Members have the obligation** under the IPR Policies of their respective Organizational Partners to **inform their respective** Organizational Partners **of Essential IPRs they become aware of**.
>
> The members take note that they are hereby invited:
>
> - to investigate in their company whether their company does own IPRs which are, or are likely to become Essential in respect of the work of the Technical Specification Group.
>
> - to notify the Director-General, or the Chairman of their **respective** Organizational Partners, of all potential IPRs that their company may own, by means of the IPR Statement and the Licensing declaration forms (e.g. see the ETSI IPR forms http://webapp.etsi.org/Ipr/).

3. Assignment of input documents

The relevant documents were identified for discussion from the SA WG3 meeting #30 document list.

4. Status of relevant specifications

4.1 SA WG3 specifications on IMS

Mr. K Boman, Ericsson welcomed CN WG1 experts to the joint discussions and outlined the status of IMS work in SA WG3 and the issues being tackled.

4.2 CN1 specifications on IMS

TD S3-030500 Liaison statement (from CN WG1) on requesting a joint CN1-SA3 meeting. The LS was introduced for information, as the joint meeting was taking place. The LS was noted.

5. Technical issues in Release 5

5.1 RES/XRES generation and usage

TD S3-030493 Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-5). This was introduced by 3. It was reported that the corresponding changes in TS 22.228 and TS 22.229 should not be a problem for CN WG1. It was agreed that the changes in 5.1.1 should be made into a note and the reason for change should refer to the pending CN WG1 CRs. With these changes, the CR was then agreed (to be endorsed by SA WG3 meeting).

TD S3-030494 Proposed CRs to 33.203: Correcting the text on sending an authentication response (Rel-6). This was a Release 6 mirror CR to the CR in TD S3-030493. The CR would be updated to reflect the changes agreed for the CR in TD S3-030493 and the CR was then agreed (to be endorsed by SA WG3 meeting).

5.2 Security Association (SA) management issues

TD S3-030554 Handling of Security Associations. This was introduced by Siemens in order to clarify the behaviour of the P-CSCF in case a REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid (indicated by the AUTS parameter in the REGISTER) and to clarify the necessary parameters for IPSec in a re-REGISTER request. There was some discussion on the re-use of the security client parameters rather than generating new parameters and either deleting the old SAs or letting them expire naturally, as this would then allow the use of the same procedures whatever happens and simplify the P-CSCF state machine. It was noted that there were proposals from Nokia on the generation of new parameters in case of failure and this would be look at later in the meeting. There would be a slight security risk while there are more than one SA at the same time (i.e. the correct SA and the invalid SA which has not yet expired) although it was recognised that the risk appeared to be low. It was decided to re-discuss this after the proposed CRs to 33.203.

For the second proposal, there was a request from CN WG1 that the Security-Verify header should be sent in Re-registration anyhow, again as this allows a simplification of the UE procedures and may be useful for a future implementation where this parameter may be useful. It was agreed that the re-registration should be treated in the same way as an initial registration and Siemens agreed to write the necessary CRs to include this in TS 22.229. Delegates were also asked to double-check that no changes would be needed in TS 33.203.

TD S3-030560 Correction and Alignment of SA handling procedures. This was introduced by 3 and proposed some of small corrections to the SA handling procedures in TS 33.203. It also noted that the text in TS 24.229 on SA handling is not inline with TS 33.203 and proposed changes that could be made to TS 24.229 to align it with TS 33.203. It was recognised that in the TCP case, the SIP message needs to be sent over the old SA, and in the UDP case this is not always necessary. It was thought best to clarify this in the CN WG1 specifications, rather than in TS 33.203. There was much discussion on the wording of the proposals and it was clear that the full understanding of the mechanisms was not fully understood. It was decided to discuss this further in an evening session and attempt to produce a revised version of the proposals which is clear to everyone. After the evening session, CRs provided for SA WG3 consideration in TD S3-030603 and TD S3-030604.

TD S3-030563 Proposed CR to 33.203: Lifetime of old SAs (Rel-5). This was introduced by Nokia and proposed clarification to the SA WG3 specification on the lifetime of old SAs. It was agreed to take the concepts proposed in this CR along with those in TD S3-030560 in the evening session and try to provide a combined CR to 33.203.

Secretary Note: **These CRs were discussed in SA WG3, were updated in TD S3-030619 and TD S3-030620 respectively and were approved.**

TD S3-030567 Proposed CR to 33.203: SA Management (Rel-5). This was introduced by Nokia and proposed text to allow any SAs established with a synchronisation failure could expiry naturally via their expiry timers. It was reported that if this was accepted, then possible abnormal cases (e.g. a register message received on this old SA) would need to be investigated. It was concluded that the acceptability to allow the Temporary SAs to expire rather than deleting them depends on the value of the expiry timer chosen by CN WG1 as this would be directly related to the seriousness of a DoS attack against user registration. It was agreed that the impacts of these changes on the specifications should be investigated in the evening session.

Report from the evening session on handling of multiple SAs at the P-CSCF:

Agreement found during SA WG3/CN WG1 evening session (6th October 2003).

1. AGREEMENT

It was agreed that the following paragraphs should be added to 24.229 in the P-CSCF section:

Paragraph 1:
Message on SA2 drop SA1 (reduce Lifetime of SA1 to 64*T1)

Paragraph 2:
Message on SA1 don't drop anything

Paragraph 3:
at the point the 200 OK for the Authentication is sent out, all SA's that did not protect the first REGISTER are dropped

unprotected REGISTER means that after 200 OK all old SA's are dropped

Paragraph 4:
SA1 expires SA2 taken into use automatically

The UE cases were regarded as required to be re-worded, but this should be a "easy piece".

2. OLD MATERIAL

Below is the material that was written down during the evening session, before the above conclusion was drawn. There might be mistakes in the below material – it was not checked again and it is just included for information.

Scenario A: old SA1 established
new SA2 established
nothing sent forth/back since that

All following messages in the cases are received at the P-CSCF from the UE
SAx = a set of two pairs of SAs

(*) including REGISTER = case 4

Paragraph 1:

Case 1	Request(*) on SA2	drop SA1 (reduce Lifetime of SA1 to 64*T1)
Case 6	Response on SA2	drop SA1 (reduce Lifetime of SA1 to 64*T1)
Case 4	REG on SA2	drop SA1 (reduce Lifetime of SA1 to 64*T1)

Receipt of REG on SA2:
- if re-authentication happens, delete SA1 after 200 OK sent
- if no re-authentication, reduce Lifetime of SA1 to 64*T1 after 200 OK sent

Paragraph 2:

Case 2	Request on SA1	don't drop anything
Case 7	Response on SA1	don't drop anything

Paragraph 3:

Case 3	REG unprotected	drop SA1 and SA2 (after 200 OK sent out)

Paragraph 4:

Case 5	REG on SA1	drop SA2 (after 200 OK sent out)

Paragraph 5:

Case 8	SA1 expires	SA2 taken into use automatically

TD S3-030568 Proposed CR to 33.203: SA procedures (Rel-5). This was introduced by Nokia and proposed to clarify the SA management procedures in TS 33.203. It was clarified that the SM1 referred to is the one in the same SA, and not related to a new unprotected registration request. It was agreed to clarify this and the CR was updated in TD S3-030594.

Secretary Note: **This CR was discussed in SA WG3, and was updated in TD S3-030609 and approved.**

TD S3-030569 Proposed CR to 33.203: SA parameters and management (Rel-5). This was introduced by Nokia. It was discussed and agreed to revise the proposed changes just to correct the specification where it is wrong, and not to make the changes that do not change the functionality. It was also clarified that the re-use of an existing TCP connection should not be ~~done~~ mandated, as a second connection may be set up on demand. It was also considered that the figure 1 should be left in, but clarified that this is a possible example for information. Modifications were therefore agreed and the CR was updated in TD S3-030596.

Secretary Note: **This CR was discussed in SA WG3, and was updated in TD S3-030610 and approved.**

TD S3-030570 Security issues. This was introduced by Nokia and discussed. Some parts were covered by discussions on other documents. **It was discussed and agreed tat the content of "Security Server" shall be mirrored in the "Security Verify header". CN WG1 were asked to take this into account in their work.**

5.3 Clean-up and alignment of TS 33.203 and TS 24.229

TD S3-030562 Proposed CR to 33.203: Terminology alignment (Rel-5). This was introduced by Nokia. Auth_Failure was changed to Error_Response to align with Stage 3 terminology and other changes were proposed to clarify and correct the terminology of 33.203. It was commented that there are many other items which may need to be changed if 4xx_Auth_Failure is accepted to be changed and that the Stage 2 terminology need not be exactly the same as the Stage 3 protocol names. It was considered that the change of 4xx_Auth_Failure was unnecessary from a Stage 2 viewpoint. Other editorial clean-up changes may be included in other related CRs and proposed for Rel-6 (to be decided by SA WG3). The changes in 7.3.1.1 and 7.3.2.2 were agreed for Rel-6 and the references will be changed in another related CR, checking other occurrences of superseded references. SA WG3 were asked to check with SA WG2 specifications on

whether any IMPI related information is stored in the I-CSCF in the case of Authentication failure. If none, as stated by CN WG1 experts, then the sentence in 6.1.2.2 can be deleted (for Rel-6). A revised CR was provided in TD S3-030597.

Secretary Note: **This CR was discussed in SA WG3, and was updated in TD S3-030613 and approved.**

TD S3-030566 Proposed CR to 33.203: Reject instead of discard (Rel-5). This was introduced by Nokia. There was some confusion over the proposal and it was thought that such a change should be made symmetrical for the UE and the P-CSCF. The CR was updated in TD S3-030598.

Secretary Note: **This CR was discussed in SA WG3, and was updated in TD S3-030614 and approved.**

5.4 Trusted domain concept

TD S3-030564 Trustworthiness of the previous hop (IMS?) network (Rel-6). It was clarified that it was the assumption for CN WG1 that Rel-5 is a **closed (trusted) network** and therefore this change is only necessary for Rel-6. Documents presented below were considered and this contribution revisited. It was decided that SA WG3 should analyse this and try to provide a solution for Rel-6 as soon as possible. Contributions were invited to SA WG3 on this issue for Rel-6.

TD S3-030526 Proposed CR to 33.203: UE populates RAND and AUTN when sending Digest response to the network (Rel-5). This was introduced by Nokia. It was noted that the AUTN parameter was already in Digest and the Stage 3 specification and it was not the intension of the Stage 2 specification to list all possible parameters in the messages, but only those parameters necessary to perform the Security procedures. It was decided to reject this CR and instead to send a LS to CN WG4 and CN WG1 in order to clarify that the non-security Related parameters are also included as required by RFC 3310. The LS was provided in TD S3-030599.

Secretary Note: **This LS was discussed in SA WG3, and was updated in TD S3-030616 and approved.**

TD S3-030527 Proposed CR to 33.203: UE populates RAND and AUTN when sending Digest response to the network (Rel-6). This was a mirror CR to TD S3-030526 for Rel-6 and was also rejected and the LS in TD S3-030599 was sent instead.

6. Technical issues in release 6

6.1 Openness of IMS

TD S3-030497 Liaison statement (from CN WG1) on Profiling of RFC3325 for IMS. This was introduced by Nokia and reported the assumptions made by CN WG1 regarding trust models for IMS. CN WG1 have assumed that the Rel-5 IMS is a closed, trusted domain. For Rel-6, an open domain is to be expected and the trust models and mechanisms need to be developed. It was reported that the SA WG3 assumption is that Technical Trust is built upon "**Interconnect Agreements**". It was clarified that SA WG3 concur with CN WG1 that for release 5 IMS, the 3GPP IMS Networks form the Trusted domain and P-Asserted-Identities should only be sent to recognised IMS networks. NDS (or proprietary security systems) is designed for and will be used between Operators to establish the trust relationships. It was decided to consider the other related contributions. This was further discussed in the evening session and it was concluded that it was not necessary to send a reply LS on this subject to CN WG1.

TD S3-030565 Trustworthiness of the next hop (IMS?) network. This was introduced by Nokia and described some methods for handling and forwarding IMS data to trusted and non-trusted networks. This was proposed for Rel-6 and it was noted that the proposal 3 would only work for Rel-5. It was noted that the source network would need to be verified as well as the next-hop network to fully secure this system. It was agreed that SA WG3 need to ensure there are adequate mechanisms to enable the Closed IMS domain for Rel-5 and need to identify the methods needed for the Rel-6 IMS Interconnected networks. For Rel-5, approach 3 was considered acceptable and it was suggested that this is covered by Annex C of TS 33.102. This was to be checked and clarified with CN WG1 experts in the evening session. For Rel-6 approach 1 was considered a good basis for further development of a more future-proof solution. It was decided that SA WG3 should discuss this at their meeting and try to find a solution to satisfy CN WG1 timescales.

TD S3-030541 Proposed CR to 33.203: Introducing the SIP Privacy mechanism (Rel-6). This was introduced by Ericsson. There was some discussion and some criticism that the CR was written more like a Stage 3 specification. It was reported that the mechanism was already available in Rel-5 as described. It was clarified that this is not strictly a Security issue, but due to misunderstandings in other groups, it was decided to clarify the Privacy mechanisms in the specifications. It was agreed to accept these changes in paragraph 1 in 5.3 for Rel-5 and to develop further if needed for Rel-6. References to RFCs were considered necessary and contribution was requested to SA WG3 delegates, using this contribution as a basis, ensuring that Stage 2 and Stage 3 content are appropriate.

7. Any other business

There were no specific contributions under this agenda item.

8. Close of the Monday joint session

The Chairman thanked SA WG3 and CN WG1 delegates for their co-operation and participation in the discussions and set the details for an evening session to discuss outstanding items, which would be reported back to the SA WG3 meeting on Tuesday 7 October. The result of this evening session is reported under agenda item 5.2.