3GPP TSG SA WG3 Security — S3#22 **S3-020170**

14 - 17 May 2002

Victoria, Canada

3GPP TSG SA WG3 Security — S3#22b **S3-0200xx**

8-9 April 2002

Fort Lauderdale, USA

Source: **Secretary 3GPP TSG-SA WG3**

Title: **Draft Report of meeting #22b**

Document for: **Comment**

Contents

1 Opening of the meeting

Valtteri Niemi, SA WG3 Vice-Chairman opened the meeting and welcomed delegates to Fort Lauderdale, USA.

2 Meeting objectives and approval of the agenda

The objectives and priorities for the meeting were outlined by the Chairman:

- To progress work on IMS Security
- Prepare the joint meetings with CN1 and CN4

TD S3-02z0050 Draft Agenda for meeting #22b. The draft agenda was introduced by the Chairman and approved (Note: a new additional agenda item was included to take into account reviewing CN documents relevant for the joint).

It was outlined that the ad hoc group did not have mandate to approve changes but could suggest them and introduce them in the plenary #23.

3 Assignment of input documents

The available documents were assigned to their respective agenda items, taking into account the urgent items to be dealt with early in the meeting.

4 Report from SA#15

S3 chairman report of main points at SA#15. SA stressed that LI work item was behind schedule and that some efforts had to be made in this area in order to have LI support for IMS. SA also decided that S3 should have a vote on the SIP integrity issue in order to select one mechanism. This vote was done by email (see 5).

5 Results of IMS integrity vote

The results of the IMS integrity vote were examined. The IPSec solution was chosen with a large majority (18 votes to 6). It was therefore decided to move the IPSec solution from the annex into the main body in TS 33.203 and delete the http-digest based solution from TS 33.203.

TD S3-02z0059 aSIP rapporteur presentation (KB). KB briefly introduced this presentation that is meant to present status of the IMS Security Architecture for the joint session with the CN groups. PH commented that T3 has proposed to modify slightly the ISIM scenarios, stating that when the ISIM shares security functions and/or parameters with the USIM, the ISIM is actually part of the USIM (not a distinct application).

Error handling was discussed in authentication scenario in order to precise P-CSCF and S-CSCF behaviour in case of user authentication failure. It was clarified that even if integrity check is successful in the P-CSCF, the S-CSCF shall successfully check that the RES value sent by the UE is correct.

SIP signalling confidentiality was discussed again. S3's working assumption is that IPSec ESP could be used in future releases to provide confidentiality for SIP signalling. It was stated that the impact of confidentiality over SIP compression remained to be examined.

KB reported that some changes are expected in the way security mode set-up is performed. Current requirement in TS 33.203 is that the P-CSCF selects the integrity algorithm to be used, while the mechanism planned to achieve security mode set-up (TD S3-02z0057) has the UE selecting the integrity algorithm used. OP pointed out that there was a flow in the proposed mechanism for now because the mechanism has the UE select a mechanism and algorithm and send a protected message to the P-CSCF (since the P-CSCF has no clue which mechanism and algorithm were selected by the UE, the P-CSCF will receive IPSec protected packets that cannot be verified).

OP asked for clarification of downloading the list of IMPUs associated to an IMPI to the P-CSCF, to know whether all IMPUs linked to one IMPI are downloaded or only the IMPUs linked to the service profile the IMPI is registering for.

6 Status of IETF Drafts and reporting from IETF#53

6.1 Algorithm agreement, Digest AKA & Extended HTTP Digest

TD S3z020051 AKA in SIP. Status reports of having AKA been mapped into HTTP Digest. The IETF has stated that they would prefer to have RES be hashed rather than sent in clear text. This issue was discussed in an email discussion on S3 reflector, the comments being that there is no reason to hash the value of RES since RES is not used as a password. It was noted in the contribution that the main reason to keep the RES value hashed was that it would be easier to meet the timescales of release 5 since the mechanism needs to be approved by June 2002. OP pointed out that the draft describing that mechanism should become an informational RFC because standard RFC would give control over to the IETF. Right now it seems that the draft would go through standard track as it has been included as a working group item in the IETF. The discussion of whether to use RES as a password was postponed to agenda item 7.3.

TD S3z020053 Security Mode Set-up in SIP. The need for security mode set-up in SIP has been endorsed by IETF and is now an official work item of the SIP WG. A new version of the draft (TD S3z020057) will be submitted to the IETF soon, after S3 comments are taken into account. The current draft is very general and does not mention any mechanism used for providing security. Some work is definitely needed to specify how this generic security mode set-up mechanism is used to provide parameters for IPSec in the way it is used by 3GPP to provide security between the UE and the P-CSCF. Due to time constraints it was proposed that the specific work for IPSec should be handled at the same time in 3GPP TS 33.203 and introduced in a new draft for the IETF.

6.2 Other drafts

TD S3z020052 Key transport in SIP. It was recognized in IETF-53 that it was extremely unlikely that key transport could be standardized within the IETF in 3GPP time schedule. Therefore 3GPP was unofficially encouraged to specify its own solution without IETF involvement. There currently are a number of proposals on how to handle key transport, but no agreement. This was highlighted as an important open issue to be discussed with CN1 during the joint meeting.

7 aSIP Technical Issues

7.1 SA Handling

TD S3z020054 SA Handling. This contribution addresses a problem identified in previous meetings about the lack of clear SA handling in some scenarios where somehow three different SAs are established between the UE and the P-CSCF. There was some discussion to decide whether that scenario was actually happening or not, due to the way retransmissions work. It was noted that the S-CSCF must be aware that a message is a retransmission or not (message SM8), because in the case of a retransmission it shall not establish a new SA and just skip the regular process and answer with a 2xx Auth_Ok. Simultaneous registrations are normally not possible according to SIP RFC. Therefore it was stated that S-CSCF behaviour needed to be specified in order to enforce that only one on-going registration happens at a given time. A number of problems were outlined related to potential denial of service attacks. Since no clear conclusion could be reached, it was decided to postpone the issue offline.

TD S3z020064 Proposed CR for SA Handling. This CR proposes to use a timer in the P-CSCF which is the same duration as the retransmission timer in the UE. This allows the P-CSCF to be certain registration is completed when that timer expires if it does not receive any retransmission during this period of time. However, it was pointed out that the P-CSCF should not take unprotected registration into account while waiting for this timer to expire, because else an attacker could force deletion of SA. Since the issues in this contribution were linked to TD S3z020054, it was decided to discuss this as well in the offline discussion.

7.2 Integrity protection IPSec ESP based

TD S3z020056 Allocation of port numbers for protected and unprotected SIP messages. This contribution suggests that the way port numbers are allocated for SIP signalling messages is reversed. Currently, the port for IPSec protected messages is fixed and the unprotected messages port number is negotiated through the security mode set-up procedure. Siemens' proposal is to reverse this and negotiate the port for protected messages and use a fixed port for unprotected messages. The reason

behind this change is it makes things simpler to have the fixed port for unprotected messages (since initial messages need to be sent over this port). That proposal was accepted by the ad hoc group. It was however unclear whether it was entirely needed to negotiate the protected messages port number. It was suggested that the UE could use the same port for sending and receiving, in which case negotiation is not needed since the P-CSCF knows which port number to use by checking the port number the first protected message was received from the UE.

It was also noted that the current text in TS 33.203 was not correct regarding the IP address range that the P-CSCF needs to cover (the UE gets a 64 bits prefix and can pick any IP address in the 2^64 available to it, therefore the P-CSCF needs to consider only the prefix to associate the SA to the range of potential IP addresses of the UE).

TD S3z020058 Key derivation for unidirectional SAs between UE and P-CSCF. This contribution suggests that the key derivation functions are located in the MT rather than in the ISIM. It was noted that it seems that T3 specifications include storage of CK and IK in the ISIM and that S3 did not have any requirements for this since there is no need for the ISIM to store these keys. It was agreed to move these functions to the MT, and that they needed to be standardize to ensure interoperability.

It also introduces a number of requirements on the key derivation functions. It was agreed that using the same key for both directions was a problem because of reflections attacks. Vodafone suggested that the knowledge of one of the key shall not reveal information on the other key. However, it was stated that it was not clear there was a requirement for this, and a discussion followed on whether introducing cryptographic functions to derive keys was needed. It was stated that maybe these derivation functions could be done without because SPI was included in the ESP header and was protected, which would defeat reflection attacks. Since no immediate conclusions could be reached, it was postponed to an offline discussion.

TD S3z020062 Integrity check failures between the UE and P-CSCF. This contribution addresses the handling of incorrectly integrity protected SIP messages. Since the integrity protection is done by IPSec, the rejection of the wrongly protected packet will be done at the IPSec layer without the SIP layer being aware of it. It was argued that the principle was to reject messages that fail integrity check and therefore it was not a problem. Also, it was also stated that modifying the IPSec layer so that it checks a wrongly protected message and sends information to the SIP layer would be a huge change to IPSec and was not acceptable. However, if the integrity check fails, it may happen that the SIP message that failed will be repeated a large number of times (11 according to SIP standard), thus creating large delays. It was agreed to raise again this problem at the joint session with CN1.

TD S3z020063 ESP mode for SIP integrity. This contribution suggests to allow the use of tunnel mode as well as transport mode for SIP integrity. The reason for this is that allowing only transport mode prevent the use of IPSec gateways that are very common to protect LANs. The contribution suggests a mechanism to send required parameters to the UE (indication of transport mode and IP address of the IPSec gateway). OP also clarified that this solution was not currently deployable because there is a lack of mechanism to distribute the SA from the P-CSCF to the IPSec gateway.

It was accepted in principle by the group that the proposed scenario should be kept open for future releases. It was pointed out that the current security mode set-up allow negotiation of security mechanism. Therefore, it was agreed that IPSec/ESP with transport mode would be the mechanism standardised for release 5, and IPSec/ESP with tunnel mode would be introduced in release 6 as another mechanism (which would include the negotiation/sending of added parameters).

The need for an informational RFC to specify the list of parameters that needs to be negotiated between the UE and the P-CSCF was also discussed. The security mode set-up procedure will be very generic and allow negotiation of a security mechanism and the cryptographic algorithms and parameters needed to implement that mechanism. There is a need to describe all the parameters needed to use IPSec/ESP to provide SIP integrity. Due to time constraints, it seems that this description will be included in 3GPP TS 33.203 and will be submitted as an informational RFC that will be approved at a later point.

Action point #1: Nokia and Siemens to produce an annex for TS 33.203 and an informational RFC describing the extensions to the SIP-Sec agreement draft in order to specify all the parameters needed to use IPSec/ESP for SIP integrity.

During the discussion that followed, it was outlined that there was a flaw in the current security mode set-up mechanism, because when the UE selects the security mechanism and sends a protected message to the P-CSCF, the P-CSCF must have established the IPSec tunnel (this is linked to the fact that key agreement has been done previously during the AKA procedure. In normal IPSec operation,

IKE would happen and the tunnel would be established). A proposed solution to this problem was that the P-CSCF replies to first message with only one choice, which would solve the issue. It was stressed that this matter needed to be solved urgently in order to meet the IETF deadlines.

TD S3z020065 Accepting unprotected re-registration messages. This is a correction to the text in TS 33.203 about sending unprotected messages to the P-CSCF. The proposal is to state that only REGISTER messages are accepted if unprotected because the “initial registration” is not defined. The proposal was agreed by the ad hoc group and a proper CR will be submitted to S3#23.

7.3 Digest AKA

TD S3z020055 Use of MD5 with digest AKA. This contribution addresses the problem of using RES as a password in http-digest to answer some concerns raised on the S3 email reflector. The contribution compares the difficulty to guess RES (breaking UMTS AKA) and breaking digest with RES as a password. It argues that it is at least as hard to break digest AKA than guessing RES. It was argued that the arguments against the use of digest AKA seemed limited from a security point of view and did not weigh much compared to the constraints of schedule of release 5. Considering the lack of an alternative solution, it was decided to proceed with the draft digest AKA.

7.4 Issues related to IMS identities

Void.

7.5 Other technical issues

TD S3z020061 Support for http digest authentication in IMS. This contribution underlines the requirement to implement http digest in SIP entities (UA, P-CSCF…). It also points at the lack of clear statements in the 3GPP specifications about this requirement. This contribution was noted.

TD S3z020060 New version of TS 33.203 produced by aSIP work item rapporteur. It was noted that this version was not official and would be the base for the CR submitted to S3#23.

8 CN1 and CN4 issues

8.1 Questions from S3

Included in S3z020067 (list of opened issues).

8.2 Review of contributions for the joint sessions

9 Review of output documents

9.1 For joint session with CN1 and CN4

S3z020059 was updated into S3-z020067 that will be presented at the joint session with CN1 and CN4.

S3z020060 will be presented for information.

9.2 For S3 plenary, SA3#23

No CRs were actually produced but a number of working assumptions were agreed by the ad hoc group:

- Port number for unprotected SIP message will be fixed. The port number for protected SIP messages should be negotiated (further study needed).
- SA between the P-CSCF and UE shall be valid over the range of IP addresses available to the UE (the P-CSCF must check the 64 bits prefix).
- Key derivation functions may be needed for protecting the link between UE and P-CSCF. This requires further study if using the same key for both directions is sufficient. If key derivation functions are needed, they shall reside in the MT and shall be standardized.

- The security set-up procedure shall for release 5 use IPSec/ESP with transport mode, but it shall be clearly possible to use a different security mechanism based on IPSec/ESP with tunnel mode in future releases.
- There is a need to specify exactly what are the parameters needed to be able to use IPSec/ ESP to secure SIP messages between the UE and the P-CSCF. An informational RFC must be produced, but due to time constraints it is likely that it will be included in an annex of TS 33.203 till the RFC is approved (see action point).
- Unprotected SIP messages shall be discarded by the P-CSCF unless they are a SIP REGISTER message (whether it is an initial registration or re-registration does not matter).
- Due to time constraints and the lack of a more satisfactory solution, it was decided to adopt digest AKA as the basis for IMS authentication.
- Security set-up procedure needs to be modified in order to avoid the problem that the P-CSCF cannot handle the first protected SIP message.

Following these working assumptions, CRs will be produced for S3#23 in Victoria. However, it was noted that work involving IETF specifications shall be completed very shortly because of IETF deadlines.

10 Any other business

Void.

11 Close of meeting

The Chairman thanked the delegates for their hard work and good co-operation during the meeting and the host, The North American Friends of 3GPP, for the meeting venue and closed the meeting.

Annex A: List of attendees at the SA WG3#22b meeting

Name	Company	e-mail	3GPP ORG	
Mr. Gabor Bajko	NOKIA Corporation	mailto:gabor.bajko@nokia.com	FI	ETSI
Mr. Krister Boman	ERICSSON L.M.	krister.boman@emw.ericsson.se	SE	ETSI
Mr. David Castellanos	ERICSSON L.M.	mailto:david.castellanos-zamon@era.ericsson.se	SE	ETSI
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	GB	ETSI
Ms. Tao Haukka	NOKIA Corporation	tao.haukka@nokia.com	FI	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	GB	ETSI
Mr. Dirk Kroeselberg	Siemens AG	dirk.kroeselberg@mchp.siemens.de	DE	ETSI
Mr. Luis Lopez-Soria	ERICSSON INC.	luis.lopez-soria@ece.ericsson.se	US	T1
Mr. Tomi Mikkonen	SSH Communications Security	tomi.mikkonen@ssh.com	FI	ETSI
Mr. Sebastien Nguyen Ngoc	Orange France	sebastien.nguyenngoc@rd.francetelecom.com	FR	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	FI	ETSI
Mr. Olivier Paridaens	ALCATEL S.A.	mailto:Olivier.Paridaens@alcatel.be	FR	ETSI
Mr. Hugh Shieh	AT&T Wireless	hugh.shieh@attws.com	US	T1
Mr. Vesa Torvinen	ERICSSON L.M.	vesa.torvinen@ericsson.fi	SE	ETSI
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	valerius@nortelnetworks.com	GB	ETSI

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by
S3z020050	Draft agenda for IMS ad-hoc meeting	Chairman (V. Niemi)	2	Approval	
S3z020051	IETF Status - AKA-SIP	Ericsson	6.1	Information	
S3z020052	IETF Status - Key transport in SIP	Ericsson	6.2	Information	
S3z020053	IETF Status - Secure mode set-up in SIP	Ericsson/Nokia	6.1	Information	
S3z020054	SA Handling	Hutchinson 3G	7.1	Discussion	
S3z020055	Use of MD5 with IMS AKA	Nokia	7.3	Discussion	
S3z020056	Allocation of port numbers for SIP integrity	Siemens	7.2	Approval	
S3z020057	IETF Draft: Security mechanism agreement for SIP sessions	Ericsson	6.1	Discussion	
S3z020058	Key derivation	Vodafone	7.2	Discussion	
S3z020059	Presentation of aSIP status	aSIP WI rapporteur	5	Approval	S3z020067
S3z020060	New proposed TS 33.203	aSIP WI rapporteur	8		

TD number	Title	Source	Agenda	Document for	Replaced by
S3z020061	Digest discussion	Ericsson	7.5	Information	
S3z020062	Integrity check failure	Ericsson	7.2	Discussion	
S3z020063	ESP mode in SIP integrity	Alcatel	7.2	Discussion	
S3z020064	Proposed CR on SA lifetime	Nokia	7.1	Approval	
S3z020065	Proposed CR on accepting unprotected messages in the P-CSCF	Nokia	7.2	Approval	
S3z020066	Report from SA#14 by S3 Chairman	S3 Chairman	4	Information	
S3z020067	Updated presentation of aSIP status	ASIP WI rapporteur			

Annex C: List of Actions from the meeting

Action point #1: Nokia and Siemens to produce an annex for TS 33.203 and an informational RFC describing the extensions to the SIP-Sec agreement draft in order to specify all the parameters needed to use IPSec/ESP for SIP integrity.