SP-000418

3GPP TSG-SA WG3 (Security)

Status report to SA#9

25-28 September, 2000

Kapolei, Hawaii, USA

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of presentation

- Document list
- Report and review of progress in SA WG3 (AI 7.3.1)
- Questions for advice from SA WG3 (AI 7.3.2)
- Approval of contributions from SA WG3 (AI 7.3.3)

Document list

- SP-000407, Status report of SA WG3 to SA#09
- SP-000408, Reports of SA WG3 meetings held since SA#08
- SP-000419, Recommendations for joint AKA control
- CRs to 33.102 “Security architecture” (R99)
  - SP-000442, 23 Corrective CRs to TS 33.102
  - SP-000411, 1 Corrective CR to TS 33.102: Re-transmission of authentication request using the same quintet
  - SP-000412, 1 Functional CR to TS 33.102: Profiles for sequence number management

Document list

- CRs to 33.103 “Integration guidelines” (R99)
    - SP-000443, 1 Corrective CR to 33.103
- CR to 33.105 “Algorithm requirements” (R99)
    - SP-000444, 1 Corrective CR to 33.105
- SP-000445, CRs to 33.102, 33.103, 33.105 on anonymity key calculation during re-synchronisation (R99)
- SP-000446, CRs to 33.102, 33.103 to clarify integrity and ciphering (R99)
- SP-000420, Revised work item descriptions (R00)
- SP-000421, New work item descriptions (R00)

Report and review of progress in S3 (AI 7.3.1)

- Contents for agenda item 7.3.1
  - General overview of progress
  - Confidentiality/integrity algorithms
  - Authentication algorithm
  - Harmonisation of 3GPP/3GPP2 authentication
  - Specifications and reports
  - Work programme
  - Outlook for future meetings
  - Meetings scheduled after SA#9

General overview of progress

- SP-000408, Reports of SA WG3 meetings held since SA#08 ***- for information***
  - Report of SA WG3 meeting #14, 1-4 August 2000, Oslo, Norway
  - Draft report of SA WG3 meeting #15, 12-14 September 2000, Washington DC, USA
- Focus has been on completing R99 and addressing feedback from other groups
- SA3 has also reviewed R00+ work programme and has produced a number of new and revised work item descriptions

Publication of KASUMI: Confidentiality & integrity algorithms

- SA#7 approved report on the work performed by SAGE task force
  - Published as 3G TR 33.908
- And approved algorithms for distribution to 3GPP partners
  - Publication of algorithm specifications and report on evaluation results was delayed for procedural reasons
- Algorithm specification published on ETSI web site on 4 September 2000 (3G TS 35.20x series)
  - http://www.etsi.org/dvbandca/
- Evaluation results will now also be published as 3G TR 33.909

Authentication algorithm

- SA#7 approved the development of standard authentication algorithm and SAGE work plan tabled at SA#7
  - Funding approved by 3GPP in June 2000
  - Work is proceeding in SAGE
  - Algorithm publication scheduled for November 2000

Harmonisation of 3GPP/3GPP2 authentication

- Second joint meeting with AHAG during S3#15 (September 2000)
- SP-000419, Recommendations for joint AKA control ***- for information***
  - S3 and AHAG are working on procedures for joint control
  - recommendations will also be presented to TR-45 by AHAG
  - target approval at SA#10
- AHAG require enhanced control of security by HE
  - to provide positive authentication reporting and authentication vector revocation
  - new WID presented to SA#9 (see later)

Specifications and reports

- CRs on 33.102, 33.103, 33.105 (R99) are presented to SA#9 for approval (see later)
- New technical reports have been created in the following areas
  - Principles for network domain security (R00)
  - Principles for IM subsystem security (R00)
- These will result in the following new technical standards
  - Network domain security architecture (R00)
  - IM subsystem security architecture (R00)

Work programme (R00+)

- Structured programme of security work items has been created and is being reviewed and maintained
  - 15 WIDs approved at SA#8
  - 2 revised WIDs presented to SA#9 for approval (see later)
  - 6 new WIDs presented to SA#9 for approval (see later)
  - See also latest project plan and security IGC report from S2

Outlook for future meetings

- With the stability of R99, SA3 will now continue with the work for R00.
- An ad hoc meeting will be held to progress work items concerning network domain security and IM subsystem security

Meetings scheduled after SA#9

- S3 ad hoc on network domain security and IM subsystem security, 8-9 November 2000, Munich, Germany
- S3#16, 28-30 November 2000, Jerusalem, Israel
- S3#17, 27 February - 1 March 2001, Sophia Antipolis, France
- S3#18, 21 or 22 - 24 May 2001, Location TBA

Questions for advice from S3 (AI 7.3.2)

- No items

Approval of contributions from S3 (AI 7.3.3)

- Contents for agenda item 7.3.3
  - CRs to 33.102 “Security Architecture” (R99)
  - CRs to 33.103 “Integration Guidelines” (R99)
  - CRs to 33.105 “Algorithms Requirements” (R99)
  - CRs to 33.102, 33.103, 33.105 on anonymity key calculation during re-synchronisation (R99)
  - CRs to 33.102, 33.103 to clarify ciphering and integrity (R99)
  - Revised work item descriptions (R00+)
  - New work item descriptions (R00+)

CRs to TS 33.102 “Security architecture” *(1/6)*

- SP-000442, 22 Corrective CRs to 33.102
  - CR095R2 Handling of emergency call
  - CR105 Corrects the length of CFN (should be 8 bits)
  - CR106 Replaces SEQ with SQN in main body
  - CR107 Replace IMUI and TMUI with IMSI and TMSI
  - CR108 Replace quintuplet by quintet
  - CR109 Modification of conversion function c2 to support lengths of RES which are not multiples of 32

...continued on next slide

CRs to TS 33.102 “Security architecture” *(2/6)*

- SP-000442, 22 Corrective CRs to TS 33.102 (continued)
  - CR110 Replace “MSC/VLR or SGSN” with “VLR/SGSN”
  - CR111 Alignment of the description of how ciphering is started with the stage 3 specification
  - CR112 Removal of ME triggered authentication during RRC connection because it is not implemented in the stage 3
  - CR113 Removal of EUIC because it is not implemented in the stage 3
  - CR114 Removal of duplicate text on USIM toolkit security and addition of references to 02.48 and 03.48 instead

...continued on next slide

CRs to TS 33.102 “Security architecture” *(3/6)*

- SP-000442, 22 Corrective CRs to TS 33.102 (continued)
  - CR115 Removal of secure authentication mechanism negotiation because it is not implemented in the stage 3
  - CR116 Removal of HE control of some aspects of security configuration because it is not implemented in the stage 3
  - CR117 Clarification on the correct ordering authentication vectors in serving network nodes
  - CR118 Update of references section

…continued on next slide

CRs to TS 33.102 “Security architecture” *(4/6)*

- SP-000442, 22 Corrective CRs to TS 33.102 (continued)
  - CR120 Change of parameter value x regarding the capability of the USIM to store information on past successful authentication events
  - CR123 Clarification on conditions for triggering a re-authentication at connection establishment (when to reject CK and IK)
  - CR124 Clarification on the handling of the START parameter and the hyperframe number (HFN)

…continued on next slide

CRs to TS 33.102 “Security architecture” *(5/6)*

- SP-000442, 22 Corrective CRs to TS 33.102 (continued)
  - CR125 Clarification on how the new FRESH value is sent to the ME at SRNC relocation
  - CR126 Addition of authentication parameter lengths
  - CR127 Clarification on the handling of the COUNT parameters
  - CR128 Minor editorial changes

CRs to TS 33.102 "Security architecture" *(6/6)*

- SP-000411, 1 Corrective CR to TS 33.102:
  - CR104 Re-transmission of authentication request using the same quintet
- SP-000412, 1 Functional CR to TS 33.102:
  - CR119 Profiles for sequence number management

CRs to TS 33.103 “Integration Guidelines”

- SP-000443, 1 Corrective CR to 33.103
  - CR010 Removal of network wide confidentiality because it is not implemented in the stage 3

CRs to TS 33.105 “Algorithm Requirements”

- SP-000444, 1 Corrective CR to 33.105
  - CR013 Deletion of enhanced user identity confidentiality because it is not implemented in the stage 3

CRs on anonymity key calculation during re-synchronisation

- SP-000445, CRs to 33.102, 33.103 and 33.105 on anonymity key calculation during re-synchronisation
  - 33.102 CR122 Changing the calculation of the anonymity key in the re-synchronisation procedure
  - 33.103 CR012 Changing the calculation of the anonymity key in the re-synchronisation procedure
  - 33.105 CR012 Changing the calculation of the anonymity key in the re-synchronisation procedure
  - 33.105 CR014 Changing the calculation of the anonymity key in the re-synchronisation procedure

CRs to clarify integrity and ciphering

- SP-000446, CRs to 33.102 and 33.103 to clarify integrity and ciphering
  - 33.102 CR121 Clarification that integrity and ciphering is applied to radio bearers rather than logical channels and that only one RRC connection is established
  - 33.103 CR011 Clarification that integrity and ciphering is applied to radio bearers rather than logical channels and that the length of the BEARER identity should be 5 bits
    - note that the BEARER length in 33.102 is correct

Revised work item descriptions

- SP-000420, Revised work item descriptions
  - S3-000606, Network domain security
    - revised title and scope to include Iu interface
  - S3-000626, Access security for IP-based services
    - end date 06/01 (was 03/01)

New work item descriptions

- SP-000421, New work item descriptions
  - S3-000488, UE triggered authentication during connections
  - S3-000490, Enhanced home control of security by HE
  - S3-000599, USIM toolkit security
  - S3-000609, Location services security
  - S3-000610, VHE security
  - S3-000611, Study on network-based denial of services attacks