3GPP TSG SA WG3 (Security)meeting #34 **S3-040588**

6-9 July 2004

Acapulco, Mexico

Source:	Lucent Technologies
Title:	3GPP2 Security – Report to 3GPP
Document for:	Information
Agenda Item:	5.5
Contact:	Michael Marcovici marcovici@lucent.com

Note: The majority of the 3GPP2 Security work (WG4) is being conducted in joint meetings between the security group and relevant development standards group within 3GPP2, as well as during WG4 independent working sessions. The attached summary reports, as a general rule, the work done during independent WG4 working sessions.

- The IMS Security Framework document has been approved for publication as S.R0086-0. Revision A is in the review process for publication, with publication expected by Aug. 2004. The new version includes the "information acquisition authentication" enhancement to the BCMS security framework document, as well as some minor enhancements to Rev. 0.

- WLAN-CDMA2000 Interworking Security Specifications, incorporated in the 3GPP2 specification X.P0028, is progressing on schedule. The current working assumption is that the WLAN-CDMA Interworking Specifications will require the securing of the WLAN access to the AN based on psk-TLS, EAP-AKA. Both methods will use a pre-shared key bootstrapped from:
  - Mobile IP: MN-AAA key, or
  - Legacy authentication – CAVE: e.g., SMEKEY (signaling message encryption)

  To ensure cryptographic key separation between the 3G access and WLAN access, as well as perfect forward secrecy (PFS), the current proposal is to use the password protected D-H (incorporated in 3GPP2 OTA HRPD specifications) to generate a WLAN master key, where the password for the D-H is based on the key material bootstrapped from one of the above-mentioned protocols (e.g., SMEKEY).

  The X.P0028 is expected to be base lined by Aug. 2004.

- 3GPP2 is currently developing Network Firewall Configuration and Control specifications (stage 1). The firewall functionality shall be adopted for wireless applications.

- Other work items:
  - Security requirements for PoC (Push-to-Talk over Cellular) are being developed.
  - Mobile IP V6

Reference: 3GPP2 TSG-S WG4 (3GPP2 Security report).

S00-20040607-104__WG4 Summary_Philly_June_2004.zip

3GPP2 TSG-S Working Group 4
(Security)
Summary of Meeting

June 2004 – Philadelphia, PA, USA

Michael Marcovici, Chair	Masayoshi Ohashi, Vice Chair	Greg Rose, Vice Chair
Lucent Technologies Inc.	KDDI R&D Labs. Inc	Qualcomm Incorporated
Tel +1-630-979-4062	Tel +81-492-78-7862	Tel +61-2-9817-4188
Fax +1-630-224-9955	Fax +81-492-78-7532	Fax +61-2-9817-5199
marcovici@lucent.com	ohashi@kddilabs.jp	ggr@qualcomm.com

1. Call to Order & Opening Remarks

The TSG-S WG4 meeting was called to order on June 7, 2004 at 0800 local time by the Chair, Michael Marcovici (Lucent).

2. Attendance

See the TSG-S Attendance List.

3. Numbering of Contributions

Contributions were accepted and numbered; see the Document Register below.

4. Adoption of Agenda

The agenda, contribution **S40-20040607-001**, was submitted and accepted as modified (R5).

5. Review & Approval of Previous Meeting Summary

The summary of the April (Coeur d'Alene, Idaho) meeting, contribution **S40-20040607-002**, was approved as modified (R1). The summary of the March (Vancouver, BC) meeting, **S40-20040419-002** was approved also, as this had been overlooked at the April meeting.

6. Correspondence, Liaison Reports and Remanded Documents

The following plenary meeting documents have been remanded to WG4 (agenda item in parentheses indicates to be discussed under that agenda item):

S00-20040419-103D__HAT_Auth.doc **(9a)**
S00-20040607-013__3GPP2-SEC_re_Distribution_of_S.S0055-cover.txt
S00-20040607-013A__Distribution_of_S.S0055.txt
S00-20040607-020__3GPP2-SEC_200406_TSG-S_Workplan.zip
S00-20040607-024__ITU-T_SG4_LS_re_security_on_Mgmt_Plane-014e.doc
S10-20040419-009A__HAT Authentication Stage 1.doc **(9a)**
S10-20040419-010__samsung network dependent mms requirements.doc

S10-20040607-005__NFCC-Draft-Stage-1-Comments [Nokia].pdf **(7e)**
S10-20040607-003R1__mark_up_PoC_System_Requirements.zip

The following documents have been sent for review by other groups:

Part-312 Baseline-with WG4 comments RM.zip **(7f)**
X20-20040607-xxx ESA-AKAv14 V&V[Qualcomm].pdf
X20-20040607-xxx LearnByYourErrors[Qualcomm].pdf
X20-20040607-xxx Procedure Reducks[Qualcomm].pdf
X31-20040419-008R1-Nortel-MIPv6-MN-HA-session-keys.doc **(9c)**
X34-20040419-006 X.P0016-370-0-1.doc
A00-200400607-010 TSG-S_corr_to_AX_re_LMSD.pdf

S00-20040607-013 is a correspondence from 3GPP secretariat regarding their intended actions to remove documents with cryptographic algorithms from the 3GPP2 server. It was noted that this appears to be a wrong-minded. **S40-20040607-013** is a reply correspondence.

S00-20040607-020 is remanded work plan documents. We have a correction to WI 00058, which lists S.R0083 (BCMCS Security Framework); this is incorrect and should be S.R0082. Under 3GPP2-2000-002, we need to add S.S0083-A with a start date of April 19. Corresponding corrections should be made to all relevant document.

S00-20040607-024 is an LS from ETSI regarding Security for the Management Plane. Noted. Lucent won big in their effort to have “shall” replaced by “should”.

S10-20040419-010 examines MMS items that should not be completely handed over to OMA. WG4 agrees that section 5.1.28 (Security) may require 3GPP2 specific development.

X20-20040607-xxx (3 documents) were brought to WG4’s attention. It was agreed that WG4 members should review and provide feedback to their company representatives in TSG-X.

X34-20040419-006, regarding MMS-MM7, was sent for review. This specification does not appear to have any security functionality. It was noted by Motorola that the font size was arbitrarily changed in mid document. WG4 noted that SOAP should be carried over a secure transport.

A00-20040607-010 is a copy of WG4’s correspondence to TSGs –A and –X requesting a joint meeting. A suitable time could not be found during the June meeting. We propose to schedule a joint meeting in July or teleconference.

7. Old Business

a. **IMS Security Framework (S.R0086-0)**

S00-20040607-012 was reviewed and minor changes were made (R1). WG4 approves this document and requests TSG-S approval for publication.

b. **Broadcast-Multicast Service Security (S.P0083-A)**

S00-20040607-005 is the current revision of BCMCS Security Framework. Some markups were forwarded back to the editor for incorporation. It was agreed that privacy of the Information Acquisition messages was covered by encryption of the underlying traffic

channel.

WG4 decided that, with addition of normative text, the document should change to a specification. The Chair will raise this issue in plenary to decide how to proceed.

c. **WLAN Security (S.P0098)**

Contribution **S40-20040607-006** from Lucent contains an explanation for the principal of key separation, in response to a request from PDS. WG4 agrees that this explanation is reasonable.

S40-20040607-003A/B/C from Motorola propose an architecture for EAP authentication using CDMA2000 CAVE operations. There was discussion whether shared SSD should be supported or not.

WG4 met jointly with TSG-X WG3.1 from 14:30 to 17:30. Working baseline text for EAP-AKA was accepted. A merged version of the various EAP-CAVE proposals is to be developed and reviewed by WG4. **S40-20040607-014** is a one-slide presentation used to state requirements for the merged proposal. WKEY Generation Method based on Legacy Authentication Parameters was accepted “in concept” pending baseline text. EAP-FAST was presented, and remanded for review by WG4 to be carried out offline. It was noted in the meeting that there was some discrepancy between the submitted description of EAP-FAST and the draft RFC, leading to potential insecurity, thus requiring the review.

A conference call shall be held 16:00 CDT of July 13.

d. **New Algorithms (S.P0055-A)**

S40-20040607-009/A/B (Qualcomm) discusses some proposed modifications to S.S0055 and S.S0078. The question of whether `f11` should be defined in both documents was incorrect; the author was working from an incorrect version of the document. Other modifications to S.S0055 were deemed typographical and rejected. The proposed modification of S.S0078 is to be checked by the group and if agreed will be forwarded to the Editor.

S40-20040607-010 (Qualcomm) proposes removing CMEA and ORYX from S.S0032-A, and correspondingly updating other standards to make use of CMEA and ORYX optional. It was agreed to revisit this question at the next meeting.

S40-20040607-011/A/B/C (Qualcomm) discusses two new attacks on CAVE. **/C** is a draft correspondence to all TSGs alerting them to the impending publication of one of these attacks. WG4 members are to review the attacks against CAVE and comment.

e. **Firewall Work Item**

No contributions. An Ad-Hoc group will be formed with members from WG1 and WG4 to work on S.P0103.

f. **MMS-MM1 Security Review**

Part-312 Baseline-with WG4 comments RM.zip was remanded for our review. Comments made at Coeur d’Alene seemed to have been incorporated correctly; a minor confusion with references was clarified. **S40-20040607-015** contains our modifications. This agenda item is now complete.

8. OMA

No contributions.

9. New Business

a. **HRPD Authentication**

S40-20040607-007 from Lucent proposes to use SMEKEY and PLCM to form an intermediate key to answer HRPD CHAP challenges. It was agreed that this contribution may be premature. **S40-20040607-008** contains numerous changes to the proposed HAT stage 1 document. A joint meeting with TSG-S WG1 was held from 13:00-14:00, in which Samsung agreed to redraft and resubmit the HAT stage 1 document, making this contribution moot.

b. **CDMA2000/GPRS Roaming Security Requirements**

S40-20040607-007 (Qualcomm) was reviewed. No action is to be taken at this time, as contributions are expected in future meetings.

c. **Mobile IPv6 Security Issues**

X31-20040419-008R1 was briefly reviewed. It was agreed to review it further and request contributions for the next meeting. At least one problem was noted.

d. **PoC**

S10-20040607-003R1__mark_up_PoC_System_Requirements.zip was reviewed. Some comments were reflected in **S40-20040607-015** to be taken back to the WG1 joint meeting.

10. Assignments

See above.

11. Future Meetings

- **Next TSG-S meeting in Los Angeles, CA - July 19-22, 2004.**

WG4 chair requests the TGS-S chair to allocate 16 hours of meeting time in Los Angeles for Tuesday and Wednesday.

WG4 adjourned at 18:00 on Wednesday June 9, 2004.

TSG-S Working Group 4 Contributions Log

Contribution Number	Title	Source
S40-20040607-001	**TSG-S WG4 Agenda**	Chair
S40-20040607-002	**WG-4 Summary of Previous Meeting**	Chair

S40-20040607-003	**EAP-CDMA2000**	Motorola
S40-20040607-004	**CDMA2000-GPRS roaming security requirements**	Qualcomm
S40-20040607-005	**Draft S.P0083-A (BCMCS Security Framework)**	Editor (QC)
S40-20040607-006	**EAP-SSD**	Lucent
S40-20040607-007	**HRPD Authentication Method**	Lucent
S40-20040607-008	**HRPD Authentication Stage 1**	Lucent
S40-20040607-009	**Update to S.S0055 & S.S0078**	Qualcomm
S40-20040607-010	**Deprecate CMEA and ORYX**	Qualcomm
S40-20040607-011	**Attacks on CAVE**	Qualcomm
S40-20040607-012	**Update to S.R0086 (IMS Security Framework)**	Editor (LT)
S40-20040607-013	**Correspondence to Secretariat re web site**	Qualcomm
S40-20040607-014	**Response to TSG-X 3.1 re MMS MM7**	Chair
S40-20040607-015	**MMS MM1 corrections**	Chair
S40-20040607-016	**Amended PoC requirements**	Chair

1