Title

Ad Hoc Authentication Group Meeting Summary

July 18-19, 2000 in Colorado Springs, CO

Source

Christopher Carroll (GTE Labs), AHAG Chair

Recommendation

Approve and forward to the TIA. All contribution numbers pertain to AHAG, unless otherwise specified.

Summary:

- The AHAG received a series of correspondence related to the website posting of export controlled AHAG documentation TIA.
- The AHAG was tasked to review TR-45.2's S3 collaboration document and provide comments for the joint TR-45.2/AHAG meeting in August.
- Lucent provided the AHAG will an estimate of SHAZAM's efficiency at approximately 6% load on an ARM7 processor.
- TR-45.5 has requested that the AHAG present the ESP candidates for discussion at the August 21-25 TR-45.5 meeting in San Francisco, CA.
- The May 19, 2000 SHA-1 Conference Call meeting summary is included in this report.

1. Call to Order and Opening Remarks. TR45.AHAG met July 18, 2000 in Colorado Springs, CO. Christopher Carroll (AHAG Chair) called the meeting to order at 9:00 AM MDT, asking, "Does anyone present know of any patents, the use of which may be essential to any standards being considered by AHAG?" Certicom, Ericsson, AT&T, Lucent, Nokia, Qualcomm, CipherIT, GTE, and LG SANSYS have previously responded in the affirmative, indicating they have a letter on file with the TIA.

2. Meeting Attendance was:

1. Frank Quick (Qualcomm)	2. Terry Jacobson (Lucent)	3. Chris Carroll (GTE Labs)
4. Bob Slocum (Ericsson)	5. .Michael Marcovici (Lucent)	6. Jason Brown (SBC TRI)
7. Dan Brown (Motorola)		

3. Meeting Agenda (2000.07.18.01, approved as modified)

1. Call to Order and Opening Remarks
2. Attendance Registration
3. Introduce Contributions and Associate with Agenda
4. Agenda Review and Approval
5. Review Meeting Summary
6. Correspondence
7. Liaison Reports
    a. Committee TR-45
    b. Subcommittee TR-45.1
    c. Subcommittee TR-45.2
    d. Subcommittee TR-45.3
    e. Subcommittee TR-45.4
    f. Subcommittee TR-45.5
    g. Subcommittee TR-45.6
    h. Subcommittee TR-45.7
    i. 3GPP Security Group
8. Old Business
    a. Enhanced Subscriber Authentication
    b. Enhanced Subscriber Privacy
    c. Export Issues
    d. UIM
    e. Transport Security using IP
    f. 3GPP Issues
    g. Corrections to CCA Revision D
9. New Business
    a. To be determined.
10. Presentations
11. Schedule of Meetings
12. Assignments
13. Open Discussion
14. Adjournment

4. TR45.AHAG/2000.03.14-15 AHAG Contributions (T=TIA,E=EAR[1] Sensitive).

.##	Title	Sens.	Source	Agenda	Status
.01	Agenda	-	Chair	4.0	
.02	Meeting Summary, Ottawa, Ontario (June 2000)	-	Vice Chair	5.0	
.03	TIA Correspondence Export	-	Chair	6.0	
.04	Use of Affine Transformations	-	Qualcomm	8.a	
.05	Performance of SHAZAM	-	Lucent	8.b	
.06	TR-45.2 Visited Timer Correspondence	-	TR-45.2	7.c	
.07	S3 Liaison	-	3GPP S3	8.a	

[1]As specified in the Export Administration Regulations (EAR), Title 15 CFR parts 730 through 774 inclusive.

5. The Meeting Summary.

The June 20-21 (Ottawa, Canada) meeting summary (2000.07.18.02) was approved.

6. Correspondence

- C. Carroll (Chair) introduced contribution #3 *TIA Export Correspondence* which included the following correspondence:

1. *E-mail from John Derr* to the TR-45 AHAG, TR-45 Chair, and TIA Counsel providing notification that a TIA web page will be allocated for AHAG export controlled documents.

2. *Export Notification Letter* from John Derr, TIA to the U.S. Department of Commerce informing the Bureau of Export Administration (BXA) of TIA intent to post CCA, Rev. D and CCA, Rev. C on a TIA web site.

3. *NSA Questions to BXA regarding Export Control* from Charles Kolodgy, Export Control Project Manager to BXA providing a list of questions regarding the posting of encryption materials on a website and requesting BXA comment.

4. *BXA Response to NSA* stating that "the AHAG may post encryption source code considered publicly available on its website and remain in compliance with the Export Administration Regulations (EAR) by notifying BXA by the time of posting."

7. Liaison Reports

7.a TR45 (Committee)

- There was no report.

7.b TR-45.1 (Analog)

- D. Brown (Motorola) provided the TR-45.1 liaison report. PN-4662 (IS-817 Geolocation) was approved for publication. PN-4640 completed ballot resolution. The next meeting is August 8-9 in Portland, OR.

7.c TR-45.2 (Intersystem)

- T. Jacobson (Lucent) provided a verbal report. TR-45.2 is working on a 3GPP AKA collaboration document to submit to S3. TR-45.2 has received two contributions with proposals to address the rogue MS-Shell problem.

7.d TR-45.3 (TDMA)

- B. Slocum (Ericsson) noted that TR-45.3 currently working on V&V for TIA/EIA ANSI -136 Rev. C.

7.e TR-45.4 (Radio to Switching Technologies)

- D. Brown (Motorola) provided the TR-45.4 liaison report. IOS v4.1 is currently frozen. IOS v4.2 has been proposed.

7.f TR-45.5 (CDMA)

- TR-45.5 has requested that the AHAG provide a presentation regarding the ESP candidates at their August 21-25 meeting is San Francisco, CA. C. Carroll (Chair) has been tasked to contact the TR-45.5 Chair and arrange the ESP presentation. It was also noted that Data Service Phase I security issues should be addressed.

7.g TR-45.6 (CDPD)

- There was no report.

7.h TR-45.7 (OAM&P)

- There was no report.

7.j 3GPP Security Group (S3)

- M. Marcovici (Lucent) provided an update on S3's activities. S3 has identified a list of documents for joint TIA/3GPP control.

8. Old Business

8.a Enhanced Subscriber Authentication

- T. Jacobson (Lucent) introduced contribution #06 *TR-45.2 Visited System AV Timer Correspondence* which stated that TR-45.2 has no objection to the removal of the visited system security association timer requirement provided that 3GPP add signaling to enable the Home System to revoke the current Authentication Vector (AV) and thereby cause an AV update without revoking the registration.

- F. Quick (Qualcomm) recommended that the AV revoke and refresh issue be raised at the joint TR-45.2/AHAG meeting to ensure that TR-45 clarify its position on this issue before the S3 meeting in September. Revocation of the AV is a must, however, refresh would be useful.

- M. Marcovici (Lucent) noted that S3 was waiting for feedback from CN4 regarding revoke and refresh of the AV and a final recommendation from TR-45. Contribution #07 *S3 Liaison to CN4* was introduced for the AHAG 's review. C. Carroll was tasked to send contribution #07 to TR-45.2 in preparation for a joint discussion on the issue at the joint TR-45.2/AHAG meeting in August.

- F. Quick (Qualcomm) introduced contribution #04 *Use of Affine Transformations in SHA-based AKA*. According to Qualcomm, the affine transformation Ax + B in the current SHA-based AKA has not been subjected to the required public scrutiny and should not be adopted. C. Carroll (Chair) requested that Lucent provide some addition justification for the inclusion of the affine transformation.

8.b Enhanced Subscriber Privacy

- M. Marcovici (Lucent) introduced contribution #05 *Performance of SHAZAM algorithm*. According to Lucent, performance tests of SHAZAM on an ARM7 processor (typical for future cdma2000 phones) resulted in a 6% processor load which is acceptable for cdma2000. F. Quick (Qualcomm) believed that the 6% estimate was optimistic and expressed concern about the algorithm's impact on cellular telephone battery life. He also noted that memory wait states within a cellular telephone may impact performance.

8.c Export Issues

- C. Carroll (Chair) introduced contribution #3 *TIA Export Correspondence* which included the following correspondence:

    5. *E-mail from John Derr* to the TR-45 AHAG, TR-45 Chair, and TIA Counsel providing notification that a TIA web page will be allocated for AHAG export controlled documents.

6. *Export Notification Letter* from John Derr, TIA to the U.S. Department of Commerce informing the Bureau of Export Administration (BXA) of TIA intent to post CCA, Rev. D and CCA, Rev. C on a TIA web site.

7. *NSA Questions to BXA regarding Export Control* from Charles Kolodgy, Export Control Project Manager to BXA providing a list of questions regarding the posting of encryption materials on a website and requesting BXA comment.

8. *BXA Response to NSA* stating that "the AHAG may post encryption source code considered publicly available on its website and remain in compliance with the Export Administration Regulations (EAR) by notifying BXA by the time of posting."

8.d UIM

- TR-45.2 is currently reviewing two contributions that provide potential solutions to the Rogue MS-Shell problem.

8.e Transport Security using IP

- T. Jacobson (Lucent) noted that TR-45.2 is continuing to investigate IP security based on the AHAG's comments.

8.f 3GPP Issues

- F. Quick (Qualcomm) reviewed TR-45.2's recommendation for collaboration with 3GPP S3 regarding 3GPP AKA and noted the following: 1) The level of connection/collaboration between S3 and TR-45 must be clarified, 2) There should be more detail on how coordination between S3 and TR-45 is to be achieved, and 3) A representative should be designated within TR-45 to represent the TR-45's interests with S3. C. Carroll (Chair) tasked the AHAG to review the TR-45.2 recommendations and provide comments at the August AHAG meeting.

8.g Correction to CCA, Rev. D

- There was no contribution.

9. New Business

None.

10. Presentations

None.

11. Schedule of Meetings

Date	Time	Location	Hotel	Rate	Cut-off	Co-Located
September 12-13	9-5	Washington, D.C.	Crown Plaza	$175		3GPP S3
October 24-25	9-5	Phoenix, AZ	Scottsdale Marriot Suites	$169	9/23	
November 14-15	9-5	Boulder, C0	TBD			TR-45.2
December 12-13	9-5	Maui, Hawaii	TBD (Hyatt Regency)			TR-45.2

12. Assignments

1. Chair to submit meeting report for ESA conference call.

2. Lucent to provide further explanation of questions related to SHAZAM.

3. AHAG members to review TR-45.2's S3 collaboration document and provide comments at the next meeting.

13. Open Discussion

None.

14. Adjournment

The meeting was conducted in accordance with the TIA Manual and adjourned at 12:30 PM MDT on July 18, 2000.

_____

Chair, Christopher Carroll

AHAG Interim Conference call (May 19, 2000 at 1:00 pm EST)

The Interim AHAG meeting was held at the request of Lucent Technologies in order to submit a proposal to 3GPP S3 to adopt the SHA-1 algorithm as the AKA algorithm.

Attendees:

1. Frank Quick (Qualcomm)
2. Dan Robertson (Denso)
3. Chris Carroll (GTE Labs)
4. Savar Patel (Lucent)
5. .Marcus Wong (Lucent)
6. Jason Brown (SBC TRI)
7. M. Marcovici (Lucent)
8. T. Inklebarger (AT&T)
9. Ganesh Sundaram (Lucent)
10. S. Mizikovsky (Lucent)
11. L. Chen (Motorola)

Contributions:

1. SHA based functions for Authenticated Key Agreement (with reference to Qualcomm) (2000.05.09.10)
2. SHA based functions for Authenticated Key Agreement (reference removed)
3. Cover Page for S3.

S. Mizokovsky introduced contributions #1 and #2. The contributions are nearly identical except that contribution #2 has been modified to eliminate any TR-45 AHAG specific information that may be irrelevant or confusing to 3GPP S3. Contibution #2 provides an overview of the properties of the SHA-1 based function. For functions F1, F1*, and F2, the MAC properties of SHA-1 are utilized. For functions F3, F4, and F0, the Psuedorandom number generation (PRG) features of the SHA-1 based function is used. According to Lucent, the MAC function does not require "whitening", however the PRG do require "whitening" to cancel any leakage from one iteration of the SHA-1 algorithm to another. Whitening is achieved using the function Ax +B to allow spreading of the SHA-1 output bits. According to Lucent, the coefficient values (A and B) need not be secret, but should be chosen at random. Qualcomm expressed concern that the Ax + B function may not be necessary. In the interest of submitting a contribution to S3 in a timely meeting, Qualcomm agreed to submit contribution #2 provided that the AHAG liaison (M. Marcovici) state that the contribution represents a work-in-progress within the AHAG. The AHAG agreed to change the abstract to read "This contibution presents an adaptation of the SHA-1 algorithm for functions f0, f1, f1*, f2, f3, f4, and f5 needed in the AKA scheme." The AHAG agreed to remove Counter from all exhibits. In exhibit 2.1.4, 32 bits was changed to 48 bits. Also, under step 2, the end of the sentence was changed to "48 bit SQN is XORed into the 8^{th} and 9^{th} words and the AMF is XORed into the 10^{th} word."

The AHAG approved submission of the modified contribution #2 to 3GPP S3 for consideration as the 3GPP AKA algorithm.