AAA Working Group
INTERNET-DRAFT
Category: Informational
<draft-ietf-aaa-na-reqts-00.txt>
20 October 1999

Mark Beadles, UUNET
Bernard Aboba
Glen Zorn
Microsoft
Tom Hiller
Pete McCann
Hajime Shiino
Lucent
Gopal Dommety, Cisco Systems, Inc.
Steven M. Glass
Charles Perkins
Nokia Telecommunications
Stuart Jacobs, GTE Laboratories
Basavaraj Patil
Serge Manning
Nortel Networks
Pat Walsh, Ameritech
Xing Chen, Alcatel
Mark Munson, GTE Wireless
Sanjeevan Sivalingham
Ericsson Wireless Communications
Byng-Keun Lim, LG Information & Communications, Ltd.
Brent Hirschman, Motorola
Ray Hsu, Qualcomm, Inc.
Haeng Koo, Samsung Telecommunications America, Inc.
Mark Lipford, Sprint PCS
Pat Calhoun, Sun Microsystems
Eric Jaques, Vodaphone Airtouch
Yingchun Xu, 3Com Corporation
Shinich Baba, Toshiba America Research, Inc.
Takahiro Ayaki, DDI Corporation
Takuo Seki, IDO Corporation
Alan Hameed, Fujitsu

Criteria for Evaluating AAA Protocols for Network Access

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at

http://www.ietf.org/shadow.html.

To view the list Internet-Draft Shadow Directories, see

http://www.ietf.org/shadow.html.

The distribution of this memo is unlimited. It is filed as <draft-ietf-aaa-na-reqts-00.txt>, and expires May 1, 2000. Please send comments to the authors.

1. Copyright Notice

2. Abstract

This document represents a summary of AAA protocol requirements for network access. In creating this documents, inputs were taken from documents produced by the NASREQ, ROAMOPS, and MOBILEIP working groups, as well as from TIA 45.6. This document summarizes the requirements collected from those sources, separating requirements for authentication, authorization and accounting. Details on the requirements are available in the original documents.

3. Introduction

This document represents a summary of AAA protocol requirements for network access. In creating this documents, inputs were taken from documents produced by the NASREQ, ROAMOPS, and MOBILEIP working groups, as well as from TIA 45.6. This document summarizes the requirements collected from those sources, separating requirements for authentication, authorization and accounting. Details on the requirements are available in the original documents.

3.1. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

Please note that the requirements specified in this document are to be used in evaluating AAA protocol submissions. As such, the requirements language refers to capabilities of these protocols; the protocol documents will specify whether these features are required, recommended, or optional. For example, requiring that a protocol support confidentiality is NOT the same thing as requiring that all protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or more of the MUST or MUST NOT requirements for the capabilities that it implements. A protocol submission that satisfies all the MUST, MUST NOT, SHOULD and SHOULD NOT requirements for its capabilities is said to

be "unconditionally compliant"; one that satisfies all the MUST and MUST NOT requirements but not all the SHOULD or SHOULD NOT requirements for its protocols is said to be "conditionally compliant."

4. Requirements Summary

The criteria for evaluation of AAA protocols for network access are summarized below. Details of the requirements are available from the references described in the footnotes.

4.1. Authentication Requirements

Authentication Reqts.	NASREQ	ROAMOPS	MOBILE IP	TIA 45.6
PPP Support	M 8	M 1	O 29	M 42
SLIP Support		O 1	O	
Scripting Support		B 1	O	
NAI Support	M 9	M 2	S 30	M 43
CHAP Support	M 10	M 3	O	M 44
EAP Support	M 10	S 3	O	

PAP Support	M 10	B 3	O	
Scalability		M 3	M	M 44
Bi-directional Auth	M 16			
Dynamic Authentication	M 17			
Indentification Only without Authentication	M 9			S
End-to-End per-attribute confidentiality	M 26	M 6	S 31	
End-to-End per-attribute integrity		M 6	S 31	
Certificate validation			S 38	S 45
Trust establishment via brokers			M 31	

Anonymous access by local AAA server			M 36	
Reliable AAA transport mechanism			M 36	M 43
Support Proxy and Non-Proxy Brokers				M 43

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

4.2. Authorization Requirements

Authorization Reqts.	NASREQ	ROAMOPS	MOBILE IP	TIA 45.6
IPv4 Support	M 11	M 1	M 32	M
IPv6 Support	M 11	1	S 33	
non-IP Support		O 1	O	
RADIUS gateway capability	S 12	M 3	O	M 46
Policy compatibility		M 4		
Dynamic address assignment	M 11	M 5	M 34	M
Static address assignment		O 5	M 32	
Precludes layer 2 tunneling	N 11	N 5	O	

Precludes Mobile IP		N 5	N	N
Non-repudiation		6	O 35	M 43
Fraud prevention and detection		M 6	O	S
Hop-by-hop security (privacy, integrity)		M 6	S 35	M 43
IPSEC compatibility	S 28	O 6	O	M 43
End-to-End per-attribute confidentiality	M 13, 27	M 6	O	M 43
End-to-End per-attribute integrity		M 6	O 31	M 43
Dynamic Authorization	M 18		S	
Support for Access Rules, Restrictions, Filters	M 11, 19		O	

Resource Management	M 20			
Ability to obtain QoS info from AAA			S 36	M 47
Certificate validation			S 38	M 45
Trust establishment via brokers			M 31	
Allocation or coordinate IP address assignment			S 37	S 47
Reliable AAA transport mechanism			M 36	M 43
Support Proxy and Non-Proxy Brokers				M 43

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

4.3. Accounting Requirements

Accounting Reqts.	NASREQ	ROAMOPS	MOBILE IP	TIA 45.6
Real-time accounting	M 14	M 7	O 35	M 43
Standard Accounting Record		M 7	M	M
Compact Accounting Record		M 7	O	O
Accounting Record Extensibility	M 15	M 7	O	M
Batch Accounting	S 21			O
Guaranteed Delivery	M 22		M 35	M 43
Accounting Time Stamps	M 23			M 43
End-to-End per-attribute integrity	M 24	M 6	M 31	O

End-to-End per-attribute confidentiality	S 24	M 6	M 31	O
Non-repudiation	S 25		S 35	M 43
Trust establishment via brokers			M 31	
Reliable AAA transport mechanism			M 36	M 43
Support Proxy and Non-Proxy Brokers				M 43

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

4.4. Unique Mobile IP requirements

In addition Mobile IP also has the following requirements:

Dynamic Setup of security assoc. between local AAA and external authority			S 36	S 43
Security Assoc. between attendant and local AAA			S 36	M 43
Local AAA capability to gather (secret) info about a MN			N 36	
AAA protocol extensions for including Mobile IP registration messages			M 38	S 48
Enable key distribution for setting up security assoc between mip agents			M 38	S 49
Firewall traversal capability			M 39	
Allocation of local Home agent			S 40	M 50
Act as a KDC for fast handoffs			S 41	S 51

Perform pre-shared key distribution for IKE			S	S 52

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Footnotes

[1] Section 4.2.1 of [2]
[2] Section 4.2.2 of [2]. Also see [8].
[3] Section 4.2.3 of [2]. Also see [14].
[4] Section 4.2.4 of [2].
[5] Section 4.2.5 of [2].
[6] Section 4.2.6 of [2].
[7] Section 4.3 of [2].
[8] Section 6 of [3]. Also see [6].
[9] Section 8.2.2.2 of [3]. Also see [14].
[10] Section 8.2.2.1 of [3]. Also see [14].
[11] Section 8.3.2.2 of [3]. Also see [7].
[12] Section 8.1.1 of [3].
[13] Section 8.1.4.4 of [3].
[14] Section 8.4.1.2 of [3].
[15] Section 8.4.2 of [3].
[16] Section 8.2.1.1 of [3].
[17] Section 8.2.1.2 of [3].
[18] Section 8.3.1.1 of [3].
[19] Section 8.3.2.1 of [3]. Also see [7].
[20] Section 8.3.2.3 of [3]. Also see [6], [7].
[21] Section 8.4.1.3 of [3].
[22] Section 8.4.1.1 of [3].
[23] Section 8.4.1.4 of [3].
[24] Section 8.4.3.1 of [3].
[25] Section 8.4.3.2 of [3].
[26] Section 8.2.3.1 of [3].
[27] Section 8.3.3.1 of [3].
[28] Section 8.1.4.1 of [3].
[29] Refer [15]
[30] Refer [16]
[31] Section 6 and 3.1 of [5]
[32] Refer [17]

[33] Refer [18]
[34] Section 5.1 of [5]
[35] Section 3.1 of [5]
[36] Section 3 of [5]
[37] Section 4 of [5]
[38] Section 5 of [5]
[39] Section 5.2 of [5]
[40] Section 5.3 of [5]
[41] Section 5.5 of [5]
[42] Section 1.1 of [4]
[43] Section 3.1 of [4]
[44] Section 3.2 of [4]
[45] Section 4 of [4]
[46] Section 3.4 of [4]
[47] Section 2.2 of [4]
[48] Section 3.2.1 of [4]
[49] Section 3.2.2,3.2.4 and 3.2.5 of [4]
[50] Section 3.2.2 of [4]
[51] Section 3.2.3 and 3.2.5 of [4]
[52] Section 3.3 of [4]

5. References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Aboba, B., and G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.

[3] Beadles, M., "Criteria for Evaluating Network Access Server Protocols", Internet draft (work in progress), draft-ietf-nasreq-criteria-03.txt, October 1999.

[4] Hiller, T., et al., "Cdma2000 Wireless Data Requirements for AAA", Internet draft (work in progress), draft-hiller-cdma2000-AAA-00.txt, October 1999.

[5] Glass, S., Jacobs, S., Perkins, C., "Mobile IP Authentication, Authorization, and Accounting Requirements", Internet draft (work in progress), draft-ietf-mobileip-aaa-reqs-01.txt, October 1999.

[6] Mitton, D., Beadles, M., "Network Access Server Requirements Next Generation (NASREQNG) NAS Model", Internet draft (work in progress), draft-ietf-nasreq-nasmodel-01.txt, October 1999.

[7] Mitton, D., "Network Access Server Requirements: Extended RADIUS Practices", Internet draft (work in progress), draft-ietf-nasreq-

ext-radiuspract-01.txt, October 1999.

[8] Aboba, B., and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[9] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April, 1997.

[10] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997.

[11] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[12] Sklower, K., Lloyd, B., McGregor, G., Carr, D., and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[13] Simpson, W., Editor, "PPP LCP Extensions", RFC 1570, January 1994.

[14] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[15] Solomon, J., Glass, S., "Mobile-IPv4 Configuration Option for PPP IPCP" RFC 2290, Feb 1998

[16] Calhoun, P., Perkins, C. "Mobile IP Network Access Identifier Extension", draft-ietf-mobileip-mn-nai-05.txt, Oct 1999

[17] Perkins, C., "IP Mobility Support", RFC 2002, Oct 1996

[18] Johnson, D., Perkins, C., "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-08.txt, June 1999

6. Security Considerations

This document, being a requirements document, does not have any security concerns. The security requirements on protocols to be evaluated using this document are described in the referenced documents.

7. IANA Considerations

This draft does not create any new number spaces for IANA administration.

8. Acknowledgements

Thanks to the members of the Mobile IP, AAA, and NASREQ working groups who have discussed and commented on these requirements.

9. Authors' Addresses

Mark Anthony Beadles
UUNET, an MCI WorldCom Company
5000 Britton Rd.
Hilliard, OH 43026

Phone: +1 (614) 723-1941
EMail: mbeadles@wcom.net

Tom Hiller
Wireless Data Standards & Architectures
Lucent Technologies
263 Shuman Drive
Room 1HP2F-218
Naperville, IL 60563

Phone: +1 (630) 976-7673
Email: tom.hiller@lucent.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 936-6605
Fax: +1 (425) 936-7329
EMail: bernarda@microsoft.com

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 703-1559
Fax: +1 (425) 936-7329
EMail: glennz@microsoft.com

Gopal Dommety
IOS Network Protocols
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: +1 (408) 525-1404
Fax: +1 (408) 526-4952
Email: gdommety@cisco.com

Steven M. Glass
Sun Microsystems
1 Network Drive
Burlington, MA. 01845

Phone: +1 (781) 442-0504
Fax: +1 (781) 442-1677
Email: steven.glass@sun.com

Stuart Jacobs
Secure Systems Department
GTE Laboratories
40 Sylvan Road,
Waltham, MA 02451-1128

Phone: +1 (781) 466-3076
Fax: +1 (781)466-2838
Email: sjacobs@gte.com

Basavaraj Patil
Wireless Technology Labs
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082-4399

Phone: +1 (972) 684-1489
Fax: +1 (972) 685-3207
Email: bpatil@nortelnetworks.com

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California

Phone: +1 (650) 625-2986
Fax: +1 (650) 691-2170
EMail: charliep@iprg.nokia.com

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025

Phone: +1 (650) 786-7733
EMail: pcalhoun@eng.sun.com

Ed Campbell
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056

Phone: +1 (847) 342-6769
EMail: ed_campbell@3com.com

Raymond T. Hsu
Qualcomm Inc.
6455 Lusk Blvd.
San Diego, CA 92121

Phone: +1 (619) 651-3623
EMail: rhsu@qualcomm.com

Mark A. Lipford
Sprint PCS
8001 College Blvd.; Suite 210
Overland Park, KS 66210

Phone: +1 (913) 664-8335
EMail: mlipfo01@sprintspectrum.com

Serge Manning
Nortel Networks
2201 Lakeside Blvd
Richardson, TX 75082-4399

Phone: +1 (972) 684-7277
EMail: smanning@nortelnetworks.com

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566

Phone: +1 (630) 713 9359
EMail: mccap@lucent.com

Mark Munson
GTE Wireless
One GTE Place
Alpharetta, GA 30004

Phone: +1 (678) 339-4439
EMail: mmunson@mobilnet.gte.com

Haeng Koo
Samsung Telecommunications America, Inc.
1130 E. Arapaho Road
Richardson, TX, USA 75025

Phone: +1 (972) 761-7735
EMail: hkoo@telecom.sna.samsung.com

Pat Walsh
Ameritech
2000 W. Ameritech Ctr. Dr.
Hoffman Estates, IL 60195

Phone: +1 (847) 765-5845
EMail: pwalsh@ameritechcell.com

Yingchun Xu
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056

Phone: +1 (847) 342-6814
EMail: Yingchun_Xu@3com.com

Brent Hirschman
1501 Shure Dr.
Arlington Hieghts, IL 60006

Phone: +1 (847) 632-1563
EMail: qa4053@email.mot.com

Eric Jaques
Vodafone AirTouch
2999 Oak Road, MS-750
Walnut Creek, CA 94596

Phone: +1 (925) 279-6142
EMail: ejaques@akamail.com

Sanjeevan Sivalingham
Ericsson Wireless Communications Inc.,
Rm Q-356C
6455 Lusk Blvd
San Diego, CA 92126

Phone: +1 (858) 332-5670
EMail: s.sivalingham@ericsson.com

Xing Chen
Alcatel USA
1000 Coit Road
Plano, TX 75075, USA

Phone: +1 (972) 519-4142
Fax: +1 (972) 519-4843
Email: xing.chen@usa.alcatel.com

Byng-Keun Lim
LG Information & Communications, Ltd.
533, Hogye-dong, Dongan-ku, Anyang-shi,
Kyungki-do,431-080, Korea

Phone: +82-343-450-7199
Fax: +82-343-450-7050
EMail: bklim@lgic.co.kr

Hajime Shiino
Lucent Technologies Japan Ltd.
25 Mori Bldg. 1-4-30 Roppongi,
Minato-ku Tokyo

Phone:+81-3-5561-3695
EMail: hshiino@lucent.com

Shinich Baba
Toshiba America Research, Inc.
PO Box 136,
Convent Station, NJ 07961-0136

Phone: +1 (973) 829-4795
EMail: sbaba@tari.toshiba.com

Takahiro Ayaki
DDI corporation
Ichibancho FS Bldg.
8, Ichibancho, Chiyoda-ku Tokyo

Phone: +81-3-3221-9682
EMail: ayaki@ddi.co.jp

Alan Hameed
Fujitsu
2801 Telecom Parkway
Richardson, Texas 75082

Phone: +1 (972) 479-2089

Takuo Seki
IDO Corporation
Gobancho YS Bldg.
12-3, Gobancho, Chiyoda-ku Tokyo

Phone: +81-3-3263-9660
EMail: t-seli@ido.co.jp

10. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

11. Full Copyright Statement

12. Expiration Date

This memo is filed as <draft-ietf-aaa-na-reqts-00.txt>, and expires May 1, 2000.