Network Working Group
INTERNET-DRAFT
Category: Informational
<draft-hiller-cdma2000-aaa-01.txt>
5 June 2000

Tom Hiller (Editor)
Lucent Technologies
Pat Walsh
Ameritech
Xing Chen, Alcatel
Mark Munson, GTE Wireless
Gopal Dommety, Cisco Systems
Sanjeevan Sivalingham, Ericsson Wireless Communications
Byng-Keun Lim, LG Information & Communications, Ltd.
Pete McCann
Hajime Shiino
Lucent Technologies
Brent Hirschman, Motorola
Serge Manning
Nortel Networks
Ray Hsu, Qualcomm, Inc.
Haeng Koo, Samsung Telecommunications America, Inc.
Mark Lipford, Sprint PCS
Pat Calhoun
Sun Laboratories, Inc.
Charles Lo
Eric Jaques
Vodaphone Airtouch
Ed Campbell
Yingchun Xu
3Com Corporation
Shinich Baba, Toshiba America Research, Inc.
Takahiro Ayaki, DDI Corporation
Takuo Seki, IDO Corporation
Alan Hameed, Fujitsu

CDMA2000 Wireless Data Requirements for AAA

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

> 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.

.

1. Copyright Notice

2. Abstract

This draft specifies cdma2000 wireless data AAA requirements associated with third generation wireless architecture that supports roaming among service providers for traditional PPP and Mobile IP services. The architecture is designed for use with a cellular network as an access medium.

Sections 3, 4, present a brief high level review of the cdma2000 wireless data architecture. Section 5 presents cdma2000 AAA requirements.

3. Introduction

This draft specifies AAA requirements associated with a third generation cdma2000 wireless architecture that supports roaming among service providers for traditional PPP and Mobile IP services. The architecture is designed for use with a cellular network as an access medium.

Sections 3 and 4 present a brief, high level review of the cdma2000 wireless data architecture as an aid to interested AAA WG members. Section 5 presents cdma2000 AAA requirements, and is self contained relative to the architecture review.

3.1. Changes

-01: Fixed problems with section number references.

3.2. 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 [RFC2119].

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."

3.3. General Service Requirements

- Provide service during subscriber visiting between wireless networks systems while maintaining a formal customer-service provider relation with only one wireless service provider.
- Support Traditional PPP and Mobile IP services:
  - Support dynamic and static home address assignments for Mobile IP
  - Support a Home Agent in the mobile's home wireless network, home ISP, or private network.
  - Support IP Security on the Mobile IP tunnel between Foreign Agent and Home Agent, in order to avoid the overhead of a voluntary tunnel on the radio interface.
- Provide robust authentication, authorization and accounting services (AAA):
  - Provide separation of airlink resource AAA services and data resource AAA services.
  - Authenticate and authorize a mobile based on an IMSI and an NAI. The architecture allows for a carrier to determine if billing is based on the IMSI or the NAI.
  - Support optional AAA broker services between wireless carriers and between wireless carriers and other external data networks.
  - Allow for distribution of specific Mobile IP security key information to support home agent assignment, fast handoff, and fast HA-FA authentication assignment during registration.
- Provide QoS

4. High Level Architecture

The high level architecture is shown in Figure 1. The six major entities that compose the network are the Home Agent, the PDSN, the AAA Server, the Radio Network, the HLR/VLR, and Mobile Client.

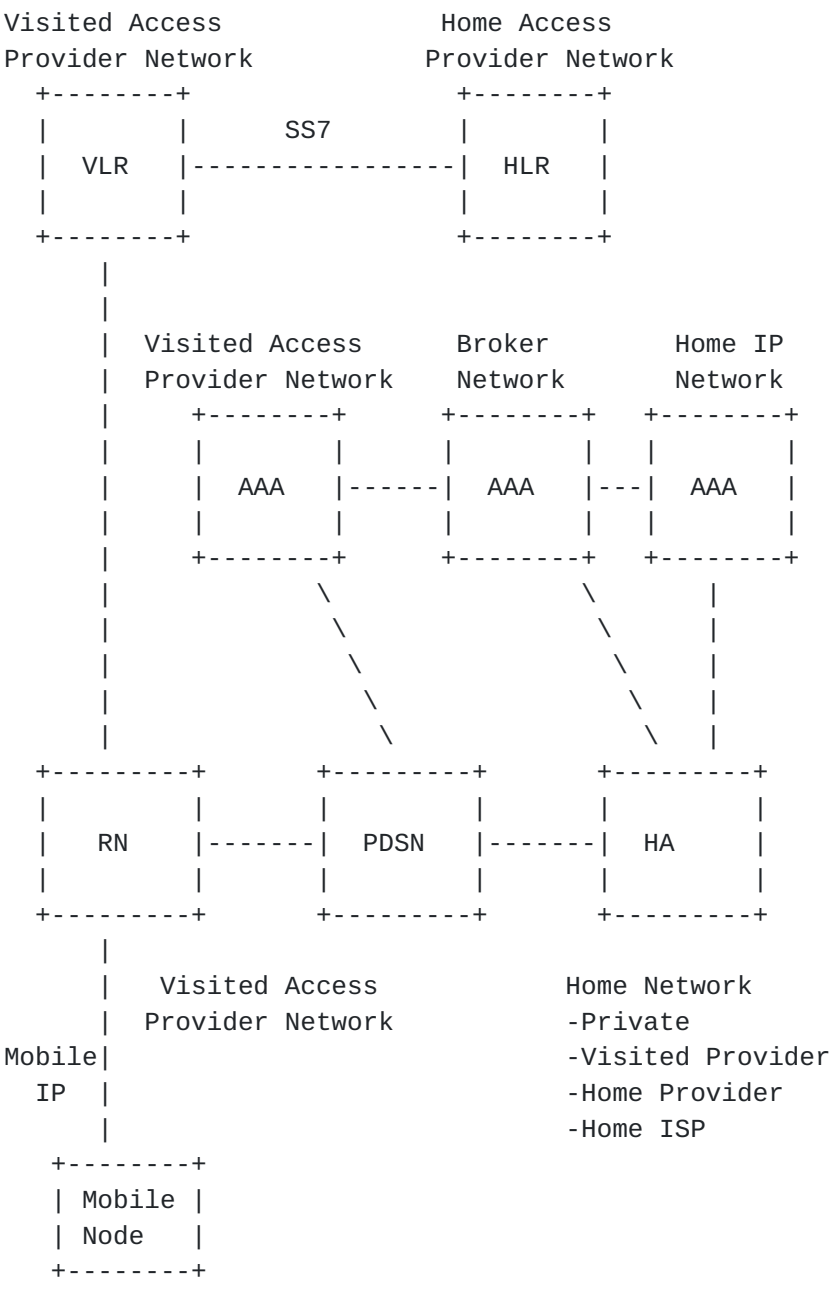

Figure 1: General cdma2000 Wireless IP Architecture

4.1. PDSN

- o Acts as a Foreign Agent;
- o Establish, maintain, and terminate link layer to the mobile client;
- o Initiate the authentication, authorization and accounting for the mobile client;
- o Optionally, securely tunnel using IP security to the Home Agent;
- o Receives service parameters from AAA for mobile client;

- o Collect usage data for accounting purposes to be relayed to AAA;
- o Routes packets to external packet data networks or to the HA in the case of reverse tunneling;
- o Maps home address and Home Agent address to a unique link layer identifier used to communicate with Radio Network.

4.2. Authentication, Authorization, and Accounting Server

- o Interact with the Foreign Agent and other AAA servers to authorize, authenticate and perform accounting for the mobile client;
- o Provides mechanism to support security association between PDSN/FA and HA and between the MN and PDSN/FA;
- o For dynamic Home Agent assignment, dynamically identify an HA and assign a MN on that HA, and provide the security association between the MN and HA;
- o Provide QoS information to the PDSN;
- o Optionally, assign dynamic home address.

4.3. Radio Network

- o Maps Mobile Client identifier reference to a unique link layer identifier used to communicate with PDSN;
- o Validates Mobile Station for access service;
- o Manages physical layer connection to the Mobile Client;
- o Maintain state of reachability for packet service between the access radio network and the mobile station;
- o Buffers packets arriving from the PDSN, when radio resources are not in place or are insufficient to support the flow from the PDSN;
- o Relays packets between the mobile station and the PDSN.

4.4. Location Registers (VLR/HLR)

- o Stores authentication and authorization information for the radio network.

4.5. Home Agent

- o Maintains user registration and redirects packets to the PDSN;
- o Optionally, establish an IP secure tunnel to the PDSN/FA;
- o Supports the dynamic Home Agent assignment;
- o Optionally, assigns dynamic home address;
- o Support reverse tunneling.

4.6. Mobile Node

- Support PPP;
- Can act as a Mobile IP Node; and support Foreign Agent Challenge and NAI;
- Interacts with the Radio Network to obtain appropriate radio resources from the network for the exchange of packets;
- Maintains knowledge of status of radio resources (e.g., active, standby, dormant);
- Buffers packets when radio resources are not in place or are insufficient to support the flow to the network.

5. AAA Requirements

5.1. Core AAA Requirements

The following is a summary of cdma2000 AAA specific requirements. In these requirements, the serving network and home network may or may not have a direct business relationship. In such cases in which there is not a direct business relationship, service may be supported indirectly via broker.

- Authenticate and authorize a user NAI in a roaming environment. The NAI is obtained via CHAP (for traditional PPP service) or a Foreign Agent Challenge (for Mobile IP service). A shared secret exists between the mobile and its HAAA. The FAC will typically be computed in a manner consistent with CHAP.
- Transport wireless data attributes from the home network to the Serving network. This may often take the form of a user profile.
- Encrypt or sign one or more AVPs in an AAA message between home, serving network, or some broker across multiple AAA server hops.
- Support a reliable AAA transport mechanism.
  - This transport mechanism will be able indicate to an AAA application that a message was delivered to the next peer AAA application or that a time out occurred.
  - Retransmission is controlled by the reliable AAA transport mechanism, and not by lower layer protocols such as TCP.
  - Even if the AAA message is to be forwarded, or the message's options or semantics do not conform with the AAA protocol, the transport mechanism will acknowledge that the peer received the AAA message. However, if the message fails to pass authentication, it will not be acknowledged.
  - Acknowledgements should be allowed to be piggybacked in AAA messages
  - The reliable transport mechanism features shall have the capability to detect silent failures of the AAA peer or path to the AAA peer, to manage failure on a proactive basis.

- o Transport a digital certificate in an AAA message, in order to minimize the number of round trips associated with AAA transactions. Note: This requirement applies to AAA applications and not mobile stations.
- o Support both proxy and non-proxy brokers, where non-proxy brokers imply the broker terminates an entire request and initiates a new request. AAA brokers should have the capability to modify certain parts of AAA messages whereby to operate to in non-proxy or proxy environments.
- o Provide message integrity and identity authentication on a per hop (AAA node) basis.
- o Support replay protection and optional non-repudiation capabilities for all authorization and accounting messages. The AAA protocol must provide the capability for accounting messages to be matched with prior authorization messages.
- o Support accounting via both bilateral arrangements and via broker AAA servers providing accounting clearinghouse and reconciliation between serving and home networks. There is an explicit agreement that if the private network or home ISP authenticates the mobile station requesting service, then the private network or home ISP network also agrees to reconcile charges with the home service provider or broker. Real time accounting must be supported.
- o Provides security between AAA servers, and between AAA server and PDSN or HA via IP security.

5.2. Mobile IP Specific Requirements and AAA

5.2.1. Mobile IP Security Discussion

Three Mobile IP security extensions are defined in RFC 2002:

. HA - FA
. MN - FA
. HA - MN

Therefore, Mobile IP and IPsec security models differ in that Mobile IP provides its own authentication mechanisms calculated within the Mobile IP registration procedures whereas IPsec uses IPsec AH.

The keys and SPIs associated with the MN-FA and HA-FA extensions need to be dynamically established in a roaming wireless carrier environment. The MN-FA extension is useful for allowing a new FA (PDSN) to quickly authenticate a mobile using the previous foreign agent extension. The HA-FA extension is useful for the HA to ensure that only FAs from carrier's with roaming agreements access the HA. The MN-HA is usually provisioned, but for dynamic Home Agent assignment, this security association must be dynamically created.

It is possible to use IPsec AH between MN and FA, FA and HA, and MN and HA. IKE may be used to establish security associations between these entities. However, use of IKE may pose a problem for smaller mobiles and may introduce unacceptable delays for certain applications (e.g. Voice Over IP). The following three sections outline Mobile IP specific functions that benefit from AAA based key distribution.

5.2.2. Dynamic Home Agent Assignment

A visited or home AAA server will optionally be able perform dynamic HA assignment. For dynamically assigned HA, the visited AAA server will indicate to the home AAA server whether it supports dynamic HA assignment in those cases in which the mobile node requests dynamic assignment. If so indicated, the home AAA server may choose to allow the visited AAA server to perform the HA assignment. Otherwise, the home AAA assigns the HA.

5.2.3. Fast Handoff

To achieve a faster handoff, the mobile may attempt to avoid an AAA transaction with the home AAA server. To accomplish this, the mobile may send the PDSN the Previous FA address in the RRQ message from the mobile, along with the MN-FA authentication extension. The new PDSN passes the Previous FA address and MN-FA authentication extension to the visited AAA server. If the visited AAA server is able authenticate the MN-FA authentication extension for the mobile, then the visited AAA may be able to avoid an actual transaction to the home AAA server.

5.2.4. HA-FA Authentication

To achieve a fast registration for the case of a mobile station with a Home Agent, the PDSN and HA may receive from the AAA mechanism a HA-FA key and SPI that is used to authenticate the PDSN and the HA to each other.

5.2.5. Key Distribution

These functions are primarily useful in a wireless environment in which handoffs may occur rapidly (implying a need for low latency), or where mobile devices have limited computing power. To achieve these functions, AAA will be used to securely pass keys and SPIs between the serving network and target network in encrypted form. These keys are then used for the specific functions outlined in this draft.

5.3. IKE and AAA

The use of IKE in the cdma2000 wireless architecture requires the use of certificates. However, the AAA servers may be able to distribute a pre-

shared key to the Mobile IP Agents for use during Phase 1 ISAKMP exchanges. This may lessen the need for on-line revocation checks.

5.4. Interoperability with RADIUS

Users with a home AAA server based on RADIUS may desire to roam into a wireless carrier network that uses "new" AAA servers based on the requirements in this draft, and vice verse. The AAA protocol should be designed in a way so as to make conversions to and from RADIUS messages straight forward. This will allow for the development of gateway processes to aid in interoperability. Note: The features of the new AAA protocols which are beyond the feature set of the RADIUS protocol will not be available for users while on home or serving networks based on RADIUS.

6. References

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7. Security Considerations

This document is very much about security. These requirements do not require the serving and home networks to not be in the same domain nor must they have a direct relationship. The serving network requires authorization from the home network so that the serving network obtains proof it will get paid for services rendered to the mobile. This implies the home network must authenticate the user. AAA functions must be performed in a secure manner. The requirements contained in section 3 outline the security required.

Mobile IP supports authentication mechanisms outside IP Security. These mechanism may be enhanced in a cellular wireless environment by allowing a home AAA server to distribute keys to the serving network. Additionally, the home AAA server may be able to send a pre-shared key to be used in Phase 1 ISAKMP security association establishment between FA and HA. These keys would sent in encrypted form from the home network to the serving network. As supported in the requirements contained in section 3, the encryption could be handled via public cryptography and certificates.

8. IANA Considerations

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

9. Acknowledgements

The authors are active members of the TIA TR45.6 committee.

10. Authors' Addresses

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
Phone: (650)-786-7733
E-mail: pcalhoun@eng.sun.com

Ed Campbell
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056
Phone: (847) 342-6769
E-Mail: ed_campbell@3com.com

Gopal Dommety
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
e-mail: gdommety@cisco.com

Tom Hiller
Rm 2F-218
263 Shuman Dr.
Lucent Technologies
Naperville, IL
Phone: (630) 979-7673
E-mail: tom.hiller@lucent.com

Raymond T. Hsu
Qualcomm Inc.
6455 Lusk Blvd.
San Diego, CA 92121
Phone: (619) 651-3623
E-Mail: rhsu@qualcomm.com

Mark A. Lipford
Sprint PCS
8001 College Blvd.; Suite 210
Overland Park, KS 66210
Phone: (913) 664-8335
E-Mail: mlipfo01@sprintspectrum.com

Serge Manning
Nortel Networks
2201 Lakeside Blvd
Richardson, TX 75082-4399
Phone: (972) 684-7277
E-Mail: smanning@nortelnetworks.com

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566
Phone: (630) 713 9359
E-Mail: mccap@lucent.com

Mark Munson
GTE Wireless
One GTE Place
Alpharetta, GA 30004
Phone: (678) 339-4439
E-Mail: mmunson@mobilnet.gte.com

Haeng Koo
Samsung Telecommunications America, Inc.
1130 E. Arapaho Road
Richardson, TX, USA 75025
Phone: (972) 761-7735
E-Mail: hkoo@telecom.sna.samsung.com

Pat Walsh
Ameritech
2000 W. Ameritech Ctr. Dr.
Hoffman Estates, IL 60195
Phone: (847) 765-5845
E-Mail: pwalsh@ameritechcell.com

Yingchun Xu
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056
Phone: (847) 342-6814
E-Mail: Yingchun_Xu@3com.com

Brent Hirschman
1501 Shure Dr.
Arlington Hieghts, IL 60006
Phone: (847) 632-1563
E-Mail: qa4053@email.mot.com

Eric Jaques
Vodafone AirTouch
2999 Oak Road, MS-750
Walnut Creek, CA 94596
Phone: +1-925-279-6142
E-mail: ejaques@akamail.com

Sanjeevan Sivalingham
Ericsson Wireless Communications Inc.,
Rm Q-356C
6455 Lusk Blvd
San Diego, CA 92126
Phone: (858) 332-5670
E-mail: s.sivalingham@ericsson.com

Xing Chen
Alcatel USA
1000 Coit Road
Plano, TX 75075, USA
Phone: 972-519-4142
Fax: 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
E-mail: bklim@lgic.co.kr
Phone: +82-343-450-7199
Fax: +82-343-450-7050

Hajime Shiino
Lucent Technologies Japan Ltd.
25 Mori Bldg. 1-4-30 Roppongi,
Minato-ku Tokyo
Phone:+81-3-5561-3695
E-mail:hshiino@lucent.com

Shinich Baba
Toshiba America Research, Inc.
PO Box 136,
Convent Station, NJ 07961-0136
Phone: (973) 829-4795
E-mail: sbaba@tari.toshiba.com

Takahiro Ayaki
DDI corporation
Ichibancho FS Bldg.

8, Ichibancho, Chiyoda-ku Tokyo
Phone: +81-3-3221-9682
E-mail: ayaki@ddi.co.jp

Alan Hameed
Fujitsu
2801 **Telecom Parkway**
Richardson, Texas 75082
Phone: (972) 479-2089

Charles N. Lo
Vodafone AirTouch
2999 **Oak Rd**

Walnut Creek, CA 94596
Phone: (925) 210-3460
E-Mail: charles.lo@airtouch.com

Takuo Seki
IDO Corporation
Gobancho YS Bldg.
12-3, Gobancho, Chiyoda-ku Tokyo
Phone: +81-3-3263-9660
E-mail: t-seki@ido.co.jp.fi

11. Full Copyright Statement

12. Expiration Date

This memo is filed as <draft-hiller-cdma2000-aaa-01.txt>, and expires January 1, 2001.