

3GPP2 X.S0011-002-C

Version 2.0

Version Date: July 2005



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Services

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Content

1	<u>GLOSSARY AND DEFINITIONS</u>	2
2	<u>REFERENCES</u>	3
3	<u>SIMPLE IP OPERATION</u>	4
3.1	COMMON SERVICE SPECIFICATION	4
3.1.1	PPP SESSION	4
3.2	PDSN REQUIREMENTS	4
3.2.1	PPP SESSION	4
3.2.2	RADIUS SUPPORT	9
3.2.3	INGRESS ADDRESS FILTERING	10
3.3	RADIUS SERVER REQUIREMENTS	11
3.4	MS REQUIREMENTS	12
3.4.1	PPP SESSION	12
4	<u>MOBILE IPV4 OPERATION</u>	16
4.1	COMMON SERVICE SPECIFICATION	16
4.1.1	PPP SESSION	16
4.1.2	MOBILE IP	16
4.1.3	DYNAMIC HOME AGENT AND HOME ADDRESS ASSIGNMENT	16
4.2	PDSN REQUIREMENTS	17
4.2.1	PPP SESSION	17
4.2.2	MIP REGISTRATION	18
4.2.3	RADIUS SUPPORT	20
4.2.4	IP SECURITY SUPPORT	21
4.2.5	INGRESS ADDRESS FILTERING	22
4.3	HOME AGENT REQUIREMENTS	23
4.3.1	MULTIPLE REGISTRATIONS	23
4.3.2	MIP AUTHENTICATION SUPPORT	23
4.3.3	IPSEC SUPPORT	24
4.3.4	DYNAMIC HOME AGENT ASSIGNMENT	25
4.3.5	DNS ADDRESS ASSIGNMENT	25
4.4	RADIUS SERVER REQUIREMENTS	25
4.4.1	DYNAMIC HOME AGENT ASSIGNMENT	26
4.4.2	MN-HA SHARED KEY DISTRIBUTION	27
4.4.3	IKE PRE-SHARED SECRET DISTRIBUTION PROCEDURE	27
4.4.4	DNS ADDRESS ASSIGNMENT	27
4.5	MS REQUIREMENTS	27
4.5.1	PPP SESSION	27
4.5.2	MIP REGISTRATION	28
4.6	DNS SERVER IP ADDRESS NVSE	30
5	<u>SIMULTANEOUS SERVICES</u>	32
6	<u>IP REACHABILITY SERVICE</u>	33
6.1	SIMPLE IPV4 OPERATION	33
6.2	MOBILE IP OPERATION	34
6.2.1	DNS UPDATE BY THE HOME RADIUS SERVER	34
6.2.2	DNS UPDATE BY THE HA	34
6.3	SIMPLE IPV6 OPERATION	35
	<u>ANNEX A: IKE/ISAKMP PAYLOADS (NORMATIVE)</u>	36

ANNEX B: CERTIFICATES (NORMATIVE)..... 39
ANNEX C: PDSN TIMERS (NORMATIVE) 41

Figures

Figure 1 - Max PPP Inactivity Timer Packet.....	8
Figure 2- NVSE for DNS server IP address	30

Tables

Table 1 - Occurrence of RADIUS Attributes for Simple IP	9
Table 2 - Home Agent and Home Address Scenarios	17
Table 3 - Description of Scenarios	17
Table 4 - Occurrence of RADIUS Attributes for Mobile IP	26
Table 5 - MS Registration Scenarios.....	29

General Description

This Chapter describes the required capabilities at the MS, the PDSN, the HA and the RADIUS servers to provide Simple IPv4, Simple IPv6 and Mobile IPv4 access services over PPP. It describes the mechanisms of updating the DNS with the user's assigned IP address as described in the IP Reachability Service capability.

1 **1 Glossary and Definitions**

2 See X.S0011-001-C.

1 **2 References**

2 See X.S0011-001-C.

1 **3 Simple IP Operation**

2 This section describes the requirements and procedures for Simple IP operation for both IPv4
3 [RFC 791] and IPv6 [RFC 2460]. In this document, Simple IP refers to a service in which an MS
4 is assigned an IP address and is provided IP routing service by an access provider network. The
5 MS retains its IP address as long as a radio network that has connectivity to the same Serving
6 PDSN serves it. IP address mobility beyond the Serving PDSN and secure access to a home
7 network are beyond the scope of this document.

8 **3.1 Common Service Specification**

9 The common requirements for several network elements (e.g., PDSN and MS) for Simple IP
10 operation are described here.

11 **3.1.1 PPP Session**

12 PPP shall be the data link protocol between the MS and the PDSN. The PPP session shall be
13 established prior to any IP datagram being exchanged between the MS and the PDSN. Only one
14 PPP session shall be supported between the MS and the PDSN.

15 PPP shall be supported as defined in the following standards with any limitations or extensions
16 described in this document.

- 17 • Point to Point Protocol [RFC 1661];
- 18 • PPP in HDLC-like Framing [RFC 1662];
- 19 • IPCP [RFC 1332] (for IPv4);
- 20 • IPv6CP [RFC 2472] (for IPv6);
- 21 • CHAP [RFC 1994];
- 22 • PAP [RFC 1334].

23 PPP encryption is not supported in this document.

24 **3.2 PDSN Requirements**

25 The PDSN shall support Simple IP operation for both IPv4 and IPv6.

26 **3.2.1 PPP Session**

27 **3.2.1.1 Establishment**

28 If the PDSN supports multiple service instances, refer to X.S0011-004-C for details of PPP
29 negotiation, otherwise, when an R-P connection of SO type 33/59 is established it shall send an
30 LCP Configure-Request for a new PPP session to the MS.

31 PPP shall support transparency in accordance with Section 4.2 of RFC 1662. The PDSN shall
32 attempt to negotiate a control character mapping with the minimum number of escaped
33 characters by proposing an ACCM of 0x00000000.

34 **3.2.1.2 Termination**

35 The PDSN shall close the PPP session if there is no established R-P or P-P session for the MS.
36 If the PPP session timer is used and has expired, or if Always On service is not enabled and the
37 PPP inactivity timer for a PPP session expires, the PDSN shall close the PPP session. The
38 PDSN may receive the Always On attribute with value '1' from the Home RADIUS server in order
39 to activate the Always On service for a user. If the PDSN receives the Always On attribute with
40 value '1', it shall send the indicator to the RN as indicated in [4].

1 Upon receiving the Always On attribute with value '1' from the Home RADIUS server the PDSN
 2 shall utilize the expiration of the PPP inactivity timer and the procedures described in Section
 3 3.2.1.8 to determine if the PPP session should be closed.

4 When the PDSN determines that the PPP session shall be closed, it shall determine if an LCP
 5 Terminate-Request should be sent to the MS. For an Always On session, the PDSN shall send
 6 an LCP Terminate-Request to the MS. The PDSN should also send LCP Terminate-Request to a
 7 non-Always On session unless it has previously received the 'All Dormant Indicator' NVSE.

8 The PDSN shall clear the R-P and/or P-P session whenever the associated PPP session is
 9 closed. If the PDSN receives IP packet(s) for an MS for which there is no established PPP
 10 session, the PDSN shall silently discard the packet(s). The PDSN shall close the R-P and
 11 associated P-P session if it receives an LCP Terminate-Request message from the MS.

12 3.2.1.3 PPP Session Authentication

13 The PDSN shall support the two authentication mechanisms: CHAP and PAP. The PDSN shall
 14 also support a configuration option to allow an MS to receive Simple IP service without CHAP or
 15 PAP. The PDSN shall propose CHAP in an initial LCP Configure-Request message that the
 16 PDSN sends to the MS during the PPP establishment. If the PDSN receives an LCP Configure-
 17 NAK from the MS containing PAP, the PDSN shall accept PAP by sending an LCP Configure-
 18 Request message with PAP. If the PDSN receives an LCP Configure-Reject containing the
 19 Authentication-Protocol option and the PDSN is configured to allow the MS to receive Simple IP
 20 service without CHAP or PAP, the PDSN shall respond with an LCP Configure-Request without
 21 the Authentication-Protocol option and shall adhere to the guidelines in Section 3.2.2.1 for NAI
 22 construction for accounting purposes.

23 3.2.1.4 Addressing with IPCP

24 3.2.1.4.1 IPv4 Addressing

25 For IPv4, the PDSN shall assign the MS an IP address for Simple IP service when presented with
 26 a zero or non-zero IP address in the IP Address Configuration option, during the IPCP phase of
 27 PPP. The IP address may be a private address as per RFC 1918. If the MS requests a non-zero
 28 IP address during the IPCP phase, the PDSN shall send an IPCP Configure-Nak in response to
 29 the request in order to propose a different IP address. If the MS responds with an IPCP
 30 Configure-Request containing an IP address different from the one proposed by the PDSN, the
 31 PDSN shall re-transmit one time the IPCP Configure-Request containing the new IP address,
 32 and shall send an LCP Terminate-Request if the MS fails to accept the assigned IP address.

33 During IPCP phase, the PDSN shall include the IP Address Configuration option containing its IP
 34 address in the IPCP Configure-Request messages sent to the MS.

35 The PDSN shall implement IPCP configuration options as defined in RFC 1877 for the DNS
 36 server address negotiation. The PDSN shall negotiate Primary and Secondary DNS server IP
 37 addresses with the MS if the DNS Server Configuration options are received during the IPCP
 38 phase. ~~–If the PDSN supports DNS server IP address VSA, itThe PDSN shall determine if the M~~
 39 ~~bit is set in the DNS Server IP Address VSA received in the RADIUS Access-Accept message.~~
 40 ~~The PDSN shall select DNS Server IP Address VSA, with the M bit set, for DNS information. If~~
 41 ~~PDSN receives a RADIUS Access-Accept message from the Visited RADIUS server that has~~
 42 ~~DNS IP address VSA(s) with the following values included, then the PDSN shall apply local~~
 43 ~~policies to select the DNS IP Address VSA for DNS information.~~

- 44 ▪ ~~An DNS IP Address VSA with the Entity-Type subfield set to the value 1 (=HAAA) and~~
 45 ~~the M bit unset, and/or~~
- 46 ▪ ~~One or more DNS IP Address VSA(s) with the Entity-Type subfield set to the value 2~~
 47 ~~(=VAAA).~~

48 3.2.1.4.2 IPv6 Addressing

1 For an IPv6 MS, the PDSN shall be the default router and the PPP termination point. The PDSN
 2 shall allocate one globally unique /64 prefix to each PPP link. The PDSN shall not construct any
 3 global address from this prefix.

4 The PDSN shall support the following RFCs, with exceptions as noted in this document:

- 5 • An IPv6 Aggregatable Global Unicast Address Format [RFC 3587];
- 6 • Internet Protocol, Version 6 (IPv6) Specification [RFC 2460];
- 7 • Neighbor Discovery for IP Version 6 (IPv6) [RFC 2461];
- 8 • IPv6 Stateless Address Autoconfiguration [RFC 2462];
- 9 • Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6
 10 (IPv6) Specification [RFC 2463];
- 11 • IP Version 6 over PPP [RFC 2472];
- 12 • IP Version 6 Addressing Architecture [RFC 3513].

13 The PDSN shall perform Interface-identifier negotiation as described in RFC 2472. The PDSN
 14 shall provide a valid non-zero Interface-Identifier during its negotiation of the Interface-identifier.
 15 The PDSN shall not have more than one Interface Identifier associated with the PPP connection,
 16 i.e., the PDSN shall only use the Interface Identifier negotiated during the IPv6CP phase with the
 17 MS. Because the Interface-Identifier is negotiated in the IPv6CP phase of the PPP connection
 18 setup, it is not required to perform duplicate address detection for the link local address forms as
 19 part of IPv6 stateless address auto-configuration [RFC 2462].

20 Following successful IPv6CP negotiation and the establishment of a unique link-local address for
 21 both the PDSN and the MS, the PDSN shall immediately¹ transmit initial unsolicited Router
 22 Advertisement (RA) messages on the PPP link using its link-local address as a source address.
 23 The PDSN shall include a globally unique /64 prefix in the Router Advertisement message to the
 24 MS. The MS shall use this prefix to configure its global IPv6 addresses.

25 The PDSN shall send unsolicited Router Advertisement (RA) message for an operator
 26 configurable number of times. Also, the PDSN shall set the interval between initial RA messages
 27 to an operator configurable value, which may be less than
 28 MAX_INITIAL_RTR_ADVERT_INTERVAL. After the configurable number of initial unsolicited RA
 29 messages has been transmitted, the interval between the periodic transmissions of unsolicited
 30 RA messages shall be controlled by the router configurable parameters MaxRtrAdvInterval and
 31 MinRtrAdvInterval as defined in RFC 2461. The PDSN may set MaxRtrAdvInterval to a value
 32 greater² than 1800seconds and less than 1/3 of the AdvDefaultLifetime. The PDSN shall set
 33 MinRtrAdvInterval² to a fraction of MaxRtrAdvInterval as per RFC 2461.

34 The PDSN shall send a RA message in response to a Router Solicitation (RS) message received
 35 from the MS. The PDSN may set the delay between consecutive (solicited RA) or (solicited
 36 /unsolicited RA) messages sent to the all-nodes multicast address to a value less³ than that
 37 specified by the constant MIN_DELAY_BETWEEN_RAS, contrary to the specification in sec.
 38 6.2.6 of RFC 2461.

¹ This is an exception to RFC 2461 necessary to optimize applicability over the cdma2000 wireless air-interface.

² This may cause an exception to RFC 2461 as it may put the interval outside the normal range. This exception is allowed by this standard to optimize IPv6 RA over the cdma2000 wireless links.

³ This exception is allowed by this standard to optimize IPv6 RA over the cdma2000 wireless links.

- 1 The advertised /64 prefix⁴ identifies the subnet associated with the PPP link. The /64 prefix
 2 advertised by the PDSN shall be exclusive to the PPP session.
- 3 The PDSN shall set
- 4 • the M-flag = 0 and the O-flag = 0 in the RA message header;
 - 5 • the L-flag = 0 and the A-flag =1 in the RA message Prefix Information Option.
- 6 The PDSN shall set the Router Lifetime value in the Router Advertisement message to a value of
 7 $2^{16}-1$ (18.2 hrs).
- 8 The PDSN shall not send any redirect messages to the MS over the PPP interface.

9 **3.2.1.5 Dual Stack of IPv4 and IPv6 Requirements**

10 If the NCP transitions to the stopped state (either because the NCP failed to establish, or
 11 because the NCP was torn down gracefully) and the PDSN allows the establishment of that NCP
 12 at a later time upon the receipt of NCP configure request, the NCP shall remain in the stopped
 13 state.

14 **3.2.1.6 Compression**

15 The PDSN shall support the following header compression algorithms:

- 16 • Van Jacobson TCP/IP header compression [RFC 1144].

17 The PDSN may support the following header compression algorithms:

- 18 • ROHC, Framework and four profiles: RTP, UDP, ESP, and uncompressed [RFC
 19 3095] with ROHC over PPP [RFC 3241];
- 20 • ROHC: A Link Layer Assisted Profile for IP/UDP/RTP [RFC3242];
- 21 • IP Header Compression [RFC 2507] with IP Header Compression over PPP [RFC
 22 2509];
- 23 • Zero-byte Support for Bidirectional Reliable Mode (R-mode) in Extended Link-Layer
 24 Assisted ROHC Profile [RFC3408];
- 25 • Compressing IP/UDP/RTP headers on links with high delay, packet loss and
 26 reordering [RFC 3545] with IP Header Compression over PPP [RFC 3544].

27 If the PDSN is able to process received compressed header packets from the MS using various
 28 header compression protocols, the PDSN shall include the appropriate configuration option(s) to
 29 the MS to indicate which IP Header Compression protocol it supports in the IPCP or IPv6CP
 30 Configure-Request message as defined by RFC 1332, RFC 3241, RFC 2509, and RFC 3544.

31 The PDSN shall support CCP [RFC 1962] for the negotiation of PPP payload compression. The
 32 PDSN shall support⁵ the following algorithms of PPP payload compression:

- 33 • Stac-LZS [RFC 1974];
- 34 • Microsoft Point-To-Point Compression Protocol [RFC 2118];

35 The PDSN may support other PPP payload compression algorithms.

⁴ If the Access Service Provider desires to reduce frequent unsolicited RA for the prefix, it should set the 32-bit Valid Lifetime and Preferred Lifetime fields for the advertised /64 prefix in the RA message Prefix Information Option to a very high value (i.e., 0xFFFFFFFF to indicate prefix validity for the lifetime of the PPP session).

⁵ The PDSN shall not send compressed PPP frames when Multiple Service Instances are connected.

1 **3.2.1.7 PPP Framing**

2 The PDSN shall frame PPP packets sent on the PPP link layer using the octet synchronous
 3 framing protocol defined in RFC 1662, except that there shall be no inter-frame time fill (see 4.4.1
 4 of RFC 1662). That is, no flag octets shall be sent between a flag octet that ends one PPP frame
 5 and the flag octet that begins the subsequent PPP frame.

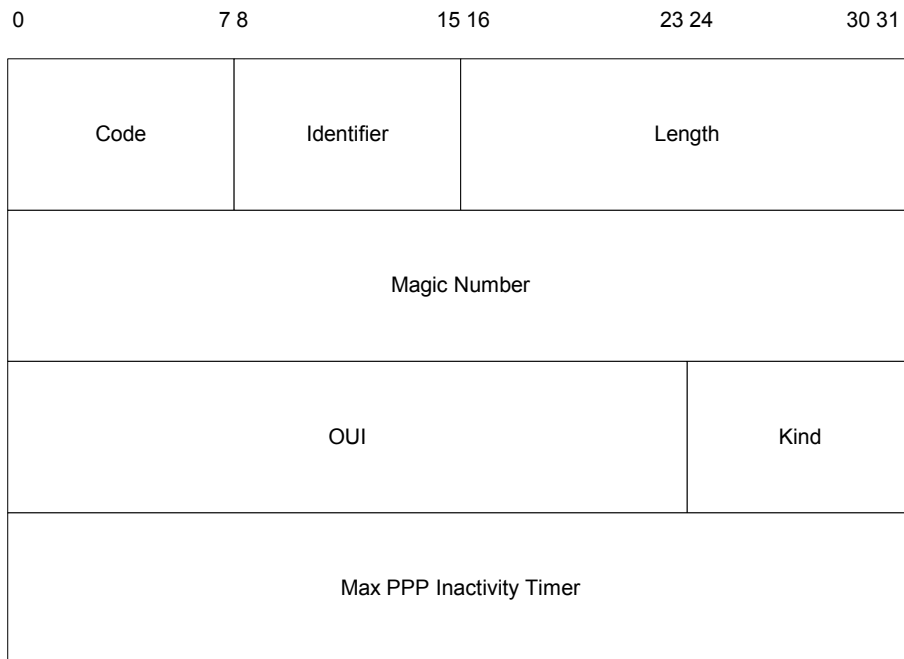
6 For IPv6, the PDSN shall set the MTU size as specified in RFC 2460.

7 **3.2.1.8 PPP Link Status Determination**

8 For Always On users, the PDSN shall support the 3GPP2 vendor specific Max PPP Inactivity
 9 Timer packet defined in PPP Vendor specific packet [RFC 2153] and the following configurable
 10 timer and counter:

- 11 • Echo-Reply-Timeout timer.
- 12 • Echo-Request-Retries counter.

13 The format of the Max PPP Inactivity Timer packet is shown in Figure 1



14 **Figure 1 - Max PPP Inactivity Timer Packet**

- 15
- 16
- Code = 0 (As defined in RFC 2153)
 - Identifier = The Identifier field shall be changed for each Vendor Specific packet sent
 - Length = 16(octets)
 - Magic Number = The Magic-Number field is four octets and aids in detecting links that are in the looped-back condition. Until the Magic-Number Configuration Option has been successfully negotiated, the Magic-Number shall be transmitted as zero. See the Magic-Number Configuration Option for further explanation.
 - OUI = 0xCF0002
 - Kind = 1

Max PPP Inactivity Timer = 32-bit value = PPP inactivity time + Echo_Reply_Timeout timer
×(Echo_Request_Retries + 1)

1 Upon entering the IPCP Opened state on a PPP session configured for Always On Service, the
2 PDSN shall start the PPP inactivity timer for the PPP session, and shall send the 3GPP2 vendor
3 specific Max PPP Inactivity Timer packet [RFC 2153] over the main service instance. The PDSN
4 should resend the Max PPP Inactivity Timer packet a configurable number of times if no
5 response from the MS is received. The value in the Max PPP Inactivity Timer field shall be equal
6 to [PPP inactivity timer + Echo_Reply_Timeout timer × (Echo_Request_Retries + 1)] for the PPP
7 session. The PDSN shall reset the PPP inactivity timer upon detection of traffic activity.

8 If the PPP inactivity timer value, Echo-Reply-Timeout timer and/or Echo-Request-Retries counter
9 have changed by an administrative action, the PDSN shall send the 3GPP2 vendor specific Max
10 PPP Inactivity Timer packet over the main service instance.

11 Upon expiration of the PPP inactivity timer, the PDSN shall send an LCP Echo-Request message
12 [RFC 1661] over the main service instance, and start the Echo-Reply-Timeout timer for the PPP
13 session. It shall also initialize the Echo-Request-Retries counter to a configurable integer value.

14 Upon receipt of an LCP Echo-Reply message, an LCP Code-Reject [RFC 1661], or any other
15 PPP packet for the PPP session, the PDSN shall stop and reset the Echo-Reply-Timeout timer,
16 reset the Echo-Request-Retries counter, and reset the PPP inactivity timer.

17 Upon expiration of the Echo-Reply-Timeout timer and when the Echo-Request-Retries counter
18 value is greater than zero, the PDSN shall send an LCP Echo-Request message, decrement the
19 Echo-Request-Retries counter by one, and start the Echo-Reply-Timeout timer. Upon expiration
20 of the Echo-Reply-Timeout timer and when the Echo-Request-Retries counter value is equal to
21 zero, the PDSN shall close the PPP session. In this case, the PDSN shall not send an LCP
22 Terminate-Request to the MS.

23 3.2.2 RADIUS Support

24 The PDSN shall act as a RADIUS client in accordance with RFC 2865 and shall communicate
25 CHAP or PAP authentication information to the Visited RADIUS server in a RADIUS Access-
26 Request message. Upon receipt of the CHAP or PAP response from the MS, the PDSN shall
27 create an RADIUS Access-Request message in accordance with Table 1.

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
User-Name	1	M	M	PDSN <-> AAA
User-Password	2	O Note 1		PDSN -> AAA
CHAP-Password	3	O Note 2		PDSN -> AAA
NAS-IP-Address	4	O Note 3		PDSN -> AAA
NAS-IPv6-Address	95	O Note 3		PDSN -> AAA
CHAP-Challenge	60	O		PDSN -> AAA
Correlation ID	26/44	M	O	PDSN <-> AAA
Calling-Station-ID	31	O		PDSN -> AAA
Always On	26/78		O	PDSN <- AAA
NAS-Port-Type ⁶	61	O		PDSN -> AAA

28 (M) Indicates Mandatory Attribute

29 (O) Indicates Optional Attribute

30 Note 1: User-Password is mandatory if PAP.

31 Note 2: CHAP-Password is mandatory if CHAP.

32 Note 3: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

33

Table 1 - Occurrence of RADIUS Attributes for Simple IP

⁶ The values are as follows: 22 (IS-2000) [5-9] or 24 (HRPD) [15], depending on the service option number connected to the PDSN.

1 Additional RADIUS attributes and VSAs may be returned in the RADIUS Access-Request and
2 RADIUS Access-Accept messages as per X.S0011-005-C.

3 The Correlation ID is in addition to those fields specified by RFC 2865 and RFC 3162.

4 The PDSN shall also act as a RADIUS accounting client in accordance with RFC 2866 and shall
5 communicate user accounting information to the Visited RADIUS server in RADIUS Accounting-
6 Request (Start and Stop) records. The RADIUS Accounting-Request message shall contain the
7 accounting attributes as specified in X.S0011-005-C. The PDSN may also send RADIUS
8 Accounting-Request (Interim-Update) records between the Accounting-Request Start and Stop
9 messages as necessary in accordance with Annex A of X.S0011-005-C.

10 The security of communications between the PDSN and the RADIUS server may optionally be
11 protected with IP security. The establishment of the security association is outside the scope of
12 this document.

13 When the PDSN sends a RADIUS Access-Request message, it may include both IPv4 and IPv6
14 specific attributes and/or VSAs. This is because the PDSN may not know a priori whether the MS
15 intends to use IPv4, IPv6, or both, since the address assignment does not occur until after
16 RADIUS authentication and authorization has completed. As per RFC 3162, the IPv6 attributes
17 may be sent along with IPv4-related attributes within the same RADIUS message. The PDSN
18 decides to use IPv4 and/or IPv6 specific attributes and/or VSAs that it receives in the RADIUS
19 Access-Accept message based on whether the MS initiates IPCP and/or IPv6CP.

20 3.2.2.1 NAI Construction in the Absence of CHAP or PAP

21 In the event that the MS does not negotiate CHAP or PAP, no MS NAI is received by the PDSN.
22 In this case, the PDSN shall not perform additional authentication of the user. If the PDSN is
23 capable of constructing a properly formatted NAI based on the MSID, using the syntax defined in
24 RFC 2486, then accounting records shall be generated and keyed on the user's constructed NAI.
25 The NAI shall be constructed using the syntax defined in RFC 2486, in the form
26 <MSID>@<realm>, where <MSID> is the MSID of the MS, and <realm> is the name of the home
27 network that owns the MS's MSID. If the PDSN is unable to construct an NAI for an MS, then the
28 PDSN may deny service to the MS.

29 The PDSN shall use one of the following MSID formats to construct the NAI, as provided by the
30 RN:

- 31 • International Mobile Subscriber Identity (IMSI) [E.212];
- 32 • Mobile Identification Number (MIN) [3];
- 33 • International Roaming MIN (IRM) [2].

34 The PDSN shall store the constructed NAI into the accounting records, and the Visited RADIUS
35 server may use the realm to forward these records to the correct Home RADIUS Server for
36 proper summary and settlement⁷. The constructed NAI shall not be used for authentication. If
37 configured by the operator, the PDSN shall send RADIUS accounting messages to the Visited
38 RADIUS server using the constructed NAI in the absence of CHAP or PAP.

39 3.2.3 Ingress Address Filtering

40 For IPv4, the Serving PDSN shall check the source address of every packet received on the PPP
41 link from the MS.

⁷ The Home RADIUS Server may require an MSID to user conversion table to map the constructed NAI ([msid@realm](#)) to the user's actual NAI ([user@realm](#)) to complete the billing process in cases where the constructed NAI differs from the actual NAI.

1 Upon receiving a packet from the MS with invalid⁸ source IP address, the PDSN shall discard the
 2 packet and may send an LCP Configure-Request message to restart the PPP session⁹ if IPCP
 3 has reached the open state.

4 If the PDSN receives an implementation-defined number of consecutive packets with an invalid
 5 source IP address from the MS, the PDSN shall send an LCP Configure-Request message to the
 6 MS.

7 ~~The PDSN shall send an LCP Configure-Request message to the MS if it continues to receive~~
 8 ~~packets with invalid source IP address from the MS.~~

9 For Mobile IP and simultaneous Simple IP and Mobile IP sessions see section 4.2.5.

10 For IPv6, the Serving PDSN shall check the prefix of the source IP address of every packet
 11 received on the PPP link from the MS. If the prefix is not associated with the PPP Session of the
 12 MS, then the PDSN shall discard the packet and send an LCP Configure-Request to restart the
 13 PPP session. If the source address is the IPv6 unspecified address and the message type is
 14 Neighbor Solicitation for Duplicate Address Detection (DAD), then the PDSN shall silently discard
 15 the packet received from the MS. If the source address is the IPv6 unspecified address for
 16 purposes other than Duplicate Address Detection (DAD) or the source address is the MS's IPv6
 17 link-local address, the PDSN shall respond according to RFC 2461.

18 **3.3 RADIUS Server Requirements**

19 The RADIUS Server shall follow the guidelines specified in RFCs 2865, 2866, and 3162.

20 The Visited and Home RADIUS server shall support the attributes as specified in Table 1 and
 21 X.S0011-005-C, the Interim Accounting Record as described in Annex A of Chapter X.S0011-
 22 005-C as well as the accounting attributes listed in X.S0011-005-C.

23 The Home RADIUS server may include the 'Always On' attribute in the RADIUS Access-Accept
 24 message to indicate an "Always On Service" for a user, based on the User Profile.

25 If the MS uses CHAP or PAP, the PDSN sends the Visited RADIUS server a RADIUS Access-
 26 Request message with CHAP or PAP authentication information. The Visited RADIUS server
 27 shall forward the RADIUS Access-Request message to the home network or a peer (e.g., a
 28 broker) if it does not have the authority to accept/deny the request. This is in accordance with
 29 RFC 2865. Upon receiving a RADIUS Access-Request message, the Home RADIUS server shall
 30 send a RADIUS Access-Accept message or RADIUS Access-Reject message to the Broker or
 31 Visited RADIUS server. The Visited RADIUS server shall send the received response to the
 32 PDSN.

33 If the PDSN includes IPv4 and IPv6 specific attributes and/or VSAs in the RADIUS Access-
 34 Request message, the RADIUS server should include the IPv4 and/or IPv6 attributes as
 35 provisioned in the user profile (e.g. Framed-Interface-Id, Framed-IPv6-Prefix etc.) and/or VSAs in
 36 the RADIUS Access-Accept message.

37 Upon receiving RADIUS Accounting-Request records from the PDSN, the Visited RADIUS
 38 server shall forward the RADIUS Accounting-Request records to the home or broker network.

39 The communication between RADIUS client and RADIUS server or between RADIUS servers
 40 shall be protected using the secret shared with the next hop RADIUS server using the
 41 procedures described in RFC 2865.

⁸ The source IP address from the MS is considered as invalid if it is not one of the addresses that have been assigned to the MS or if the MS has not been assigned any IP addresses.

⁹ The reason to restart PPP is because the user could have started a Simple IP session during a previous dormant handoff to another PDSN and returned; in this case the current PDSN would not know the MS had invoked Simple IP and received another IP address. Thus, restarting PPP will force the Simple IP session to get a topologically correct address.

1 **3.4 MS Requirements**

2 The MS may support Simple IP. The MS may choose Simple IP for IPv4 only, IPv6 only, or both
3 IPv4 and IPv6 simultaneously. The MS shall access the cdma2000^{®10} packet data service using
4 the cdma2000 air interface [5-9], [15].

5 **3.4.1 PPP Session**

6 The MS shall use PPP as the data link layer protocol for Simple IP.

7 **3.4.1.1 Establishment**

8 If the MS supports multiple service instances, refer to X.S0011-004-C for details of PPP
9 negotiation. Otherwise, for a new PPP session, the MS shall use a service instance of SO type
10 33/59 to perform PPP negotiation with the PDSN as described in RFC 1661.

11 PPP shall support control escaping in accordance with 4.2 of RFC 1662. The PPP Link Layer
12 shall support negotiation of Asynchronous Control Character Mapping as defined in RFC 1662.
13 The MS should negotiate a control character mapping. If the MS negotiates control character
14 mapping, it should attempt the minimum number of escapes by negotiating an ACCM of
15 0x00000000.

16 **3.4.1.2 Termination**

17 When the MS deactivates packet data service, the MS should send an LCP Terminate-Request
18 message to the PDSN to gracefully close the PPP session before releasing the packet data
19 service option connections with the RN. In the case of power-down registration [5-9], the MS shall
20 not send an LCP Terminate-Request message to the PDSN.

21 **3.4.1.3 Authentication**

22 The MS shall support CHAP and may support PAP authentication for Simple IP. If the MS is
23 configured to not use CHAP and PAP, the MS shall respond with an LCP Configure-Reject
24 message containing the Authentication-Protocol option proposed in the LCP Configure-Request
25 message received from the PDSN.

26 If the MS uses PAP, it shall respond to an LCP Configure-Request message for CHAP with an
27 LCP Configure-Nak proposing PAP.

28 For both CHAP and PAP, the MS shall send an NAI in the form of user@realm.

29 **3.4.1.4 Addressing with IPCP**

30 The MS may support simultaneous operation of IPCP and IPv6CP.

31 The MS may implement RFC 1877 in order to auto-configure DNS server IP addresses. The MS
32 may negotiate Primary and Secondary DNS server IP addresses during the IPCP phase. The MS
33 may use default of zero for DNS server address negotiation.

34 **3.4.1.4.1 IPv4 Addressing**

35 For IPv4, the MS should send an IP address of 0.0.0.0 during the IPCP phase to request an IP
36 address from the network. The MS shall accept the address provided by the PDSN. If the MS

¹⁰ cdma2000[®] is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000[®] is a registered trademark of the Telecommunications Industry Association (TIA USA) in the United States.

1 requests a non-zero IP address during the IPCP phase, the PDSN shall reply with an IPCP
 2 Configure-Nak in response to the request in order to propose a different IP address. The MS
 3 shall accept the new address, and shall send an IPCP Configure-Request to the PDSN with the
 4 new IP address.

5 3.4.1.4.2 IPv6 Addressing

6 For IPv6, the MS shall support the following RFCs, with exceptions as noted in this document:

- 7 • An IPv6 Aggregatable Global Unicast Address Format [RFC 3587];
- 8 • Internet Protocol, Version 6 (IPv6) Specification [RFC 2460];
- 9 • Neighbor Discovery for IP Version 6 (IPv6) [RFC 2461];
- 10 • IPv6 Stateless Address Autoconfiguration [RFC 2462];
- 11 • Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6
 12 (IPv6) Specification [RFC 2463];
- 13 • IP Version 6 over PPP [RFC 2472];
- 14 • IP Version 6 Addressing Architecture [RFC 3513].

15 The MS should support Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC
 16 3041]. To avoid disruption of an active session, e.g., Voice over IP, the MS should not change the
 17 IPv6 address used for that session.

18 For IPv6, the MS shall perform interface-identifier negotiation as described in RFC 2472. The MS
 19 shall construct the link-local IPv6 address by pre-pending the link-local prefix FE80:: /64 [RFC
 20 3513] to the interface identifier negotiated during the IPv6CP negotiation phase [RFC 2472].
 21 When the Interface-Identifier is negotiated in the IPv6CP phase of the PPP session setup, the MS
 22 should not perform duplicate address detection for the link local address as part of IPv6 stateless
 23 address auto-configuration [RFC 2462].

24 The MS shall construct global IPv6 addresses by pre-pending the prefix received from the Router
 25 Advertisement messages (see the following paragraph) to the interface identifier negotiated
 26 during the IPv6CP negotiation phase [RFC 2472] or to the interface identifiers generated using
 27 techniques defined in RFC3041. The MS should not perform Duplicate Address Detection for
 28 global IPv6 addresses (since the prefix used is a globally unique /64 and exclusive to the PPP
 29 session).

30 Following the successful IPv6CP phase and auto-configuration of link-local address, the MS may
 31 transmit a Router Solicitation (RS) message(s) if a Router Advertisement message has not been
 32 received from the PDSN within a random amount of time between 0 and
 33 MAX_RTR_SOLICITATION_DELAY seconds per RFC 2461.

34 The MS may set the upper bound of the delay to a value greater than that specified by the
 35 constant MAX_RTR_SOLICITATION_DELAY in RFC 2461. The MS may also set the lower
 36 bound of the delay to a value greater than 0. The MS may set the configurable number of RS
 37 messages to a value less¹¹ than that specified by the constant MAX_RTR_SOLICITATIONS in
 38 RFC 2461. The MS may set the interval between the configurable number of RS messages to a
 39 value less¹¹ than or greater than that specified by the constant RTR_SOLICITATION_INTERVAL
 40 in RFC 2461.

41 If the last RS message is sent and a RA message is not received after a router solicitation
 42 interval, the MS shall send an IPv6CP Configure-Terminate message to the PDSN. Upon
 43 reception of a RA message from the PDSN that contains the /64 globally unique prefix, the MS

¹¹ This exception is allowed by this standard to optimize IPv6 RA over the cdma2000 wireless links.

1 shall perform stateless address auto-configuration for global IPv6 addresses as per RFC 2462
2 (and RFC 3041 for privacy purposes).

3 After establishment of a PPP link with the PDSN, the MS shall treat that PDSN as the default
4 router until the PPP session is closed.

5 **3.4.1.5 Compression**

6 The MS shall support Van Jacobson TCP/IP header compression [RFC 1144]. The MS
7 additionally may support the following header compression algorithms:

- 8 • IP Header Compression [RFC 2507] with IP Header Compression over PPP [RFC
9 2509];
- 10 • ROHC Framework and four profiles: RTP, UDP, ESP, and uncompressed [RFC
11 3095] with ROHC over PPP [RFC 3241];
- 12 • ROHC: A Link Layer Assisted Profile for IP/UDP/RTP [RFC3242];
- 13 • Zero-byte Support for Bidirectional Reliable Mode (R-mode) in Extended Link-Layer
14 Assisted ROHC Header Compression (ROHC) Profile [RFC3408];
- 15 • Compressing IP/UDP/RTP headers on links with high delay, packet loss and
16 reordering [RFC 3545] with IP Header Compression over PPP [RFC 3544].

17 The MS shall use IPCP and/or IPv6CP to negotiate with the PDSN one or more header
18 compression capabilities.

19 If the MS is able to process received compressed header packets from the PDSN using various
20 header compression protocols, the MS shall include the appropriate configuration option(s) to
21 indicate to the PDSN which IP Header Compression protocol it supports in IPCP or IPv6CP
22 Configure-Request message as defined by RFC 1332, RFC 3241, RFC 2509, and RFC 3544.

23 ~~The MS shall support the PPP Compression Control Protocol [RFC 1962]. The MS may support
24 PPP payload compression. If the MS intends to use PPP payload compression, the MS shall use
25 PPP Compression Control Protocol to negotiate a PPP payload compression algorithm supported
26 by the MS. The MS shall support the PPP Compression Control Protocol [RFC 1962]. If the MS
27 uses PPP payload compression, the MS shall use PPP Compression Control Protocol to
28 negotiate a PPP payload compression algorithm, and the MS may support¹² PPP payload
29 compression.~~

30 **3.4.1.6 PPP Framing**

31 The MS shall use the octet-synchronous framing protocol defined in RFC 1662. One exception is
32 there shall be no inter-frame time fill (i.e., no flag octets shall be sent between a flag octet that
33 ends one PPP frame and the flag octet that begins the subsequent PPP frame)¹³.

34 **3.4.1.7 PPP Link Status Determination**

35 To support Always On service, the MS shall adhere to RFC 1661 section 5.8 "Echo-Request and
36 Echo-Reply" with regards to LCP Echo-Request message processing, and the MS should
37 support the 3GPP2 vendor specific Max PPP Inactivity Timer value packet [RFC 2153].

38 Upon receiving a Max PPP Inactivity Timer packet, the MS shall send a reply and should use the
39 value received in the packet to maintain Always On connectivity.

40 The MS shall reset the Max PPP Inactivity Timer when a PPP frame is sent or received.

¹² The MS shall not send compressed PPP frames when Multiple Service Instances are connected.

¹³ If the MS consists of a laptop and a relay-model handset, the laptop may send inter-frame time fill that prevents the mobile from becoming dormant.

- 1 Upon expiration of the Max PPP Inactivity Timer, the MS may initiate a new PPP session, or may
- 2 enter the inactive state.

1 4 Mobile IPv4 Operation

2 This section describes the requirements and procedures for Mobile IP operation for IPv4 [RFC
3 2002-2006]. In this document, Mobile IP refers to a service in which the user is able to maintain a
4 persistent IP address even when handing off between RNs connected to different PDSNs. Mobile
5 IPv4 provides the user IP routing service to a public IP network and/or secure IP routing service
6 to private networks.

7 4.1 Common Service Specification

8 The common requirements for several network elements (e.g., PDSN and MS) for Mobile IP
9 operation are described here.

10 4.1.1 PPP Session

11 See Section 3.1.1.

12 For Mobile IP, neither CHAP nor PAP should be performed. If CHAP or PAP is performed, longer
13 initial setup time and re-establishment time will occur as the result of an additional AAA traversal.

14 Note that the MN-FA Challenge Extension procedures [RFC 3012] are performed regardless of
15 whether or not CHAP/PAP is performed.

16 4.1.2 Mobile IP

17 The following standards shall be used for Mobile IPv4 operations with any limitations or
18 extensions described in this document:

- 19 • RFC 2002-2006;
- 20 • Reverse Tunneling [RFC 3024];
- 21 • Foreign Agent Challenge/Response [RFC 3012];
- 22 • NAI Extension [RFC 2794].

23 4.1.3 Dynamic Home Agent and Home Address Assignment

24 In this document, an MS may request dynamic HA and/or Home Address assignment during the
25 initial MIP registration according to the following scenarios of Table 2 and Table 3 (and also see
26 section 4.5.2.2).

27 If the network receives an RRQ from the MS with an HA Address value of 0.0.0.0, the network
28 shall treat the value as 255.255.255.255 (see section 4.5.2.2).

29

Scenarios	Type of Request	Home Address specified in RRQ	Home Agent Address specified in RRQ
Scenario 1	Dynamic case	0.0.0.0	255.255.255.255 or 0.0.0.0
Scenario 2	Semi-static case	x.x.x.x	255.255.255.255 or 0.0.0.0
Scenario 3	Semi-static case	0.0.0.0	y.y.y.y
Scenario 4	Static case	x.x.x.x	y.y.y.y

1

Table 2 - Home Agent and Home Address Scenarios

Scenarios	Description
Scenario 1	This is for dynamic Home Address assignment and a dynamic HA assignment.
Scenario 2	In this scenario, the Home RADIUS server shall assign an appropriate HA to the MS. The Home RADIUS server may use the specified Home Address to select an HA for the MS.
Scenario 3	This corresponds to dynamic Home Address assignment and static HA assignment.
Scenario 4	This is for static HA and static Home Address MIP registration, i.e., there is no dynamic assignment.

2

Table 3 - Description of Scenarios

3

For details on dynamic HA assignment see the following:

4

- Section 4.2.2.4 for the PDSN.

5

- Section 4.3.4 for the HA.

6

- Section 4.4.1 for the Home RADIUS server.

7

- Section 4.5.2.2 for the MS.

8

4.2 PDSN Requirements

9

The PDSN shall support Mobile IPv4 operation.

10

4.2.1 PPP Session

11

The PDSN shall support multiple Mobile IP Home Addresses over a single PPP session.

12

4.2.1.1 Establishment

13

See Section 3.2.1.1.

14

4.2.1.2 Termination

15

The Serving PDSN shall close the PPP session if there is no established underlying R-P session or P-P session for the MS, respectively. The PDSN shall clear the R-P session and P-P session, whenever the PPP session is closed. If the PDSN receives IP packets destined to an MS for which there is no established PPP session for the MS, the PDSN shall silently discard the packet.

19

20

21

22

If the PDSN receives a failure code in the RRP from the HA, then the PDSN shall deliver the RRP to the MS, and shall not close the PPP session before a configurable timer expires. If the PDSN generates a failure code, the PDSN shall deliver the RRP to the MS and shall not close the PPP session before a configurable timer expires.

23

See Annex C for description of PPP Inactivity Timer and Session Timer.

24

25

26

The PDSN may receive the Always On attribute with value '1' from the Home RADIUS server in order to activate the Always On service for a user. If the PDSN receives the Always On attribute with value '1', it shall send the indicator to the RN as indicated in [4].

27

28

If the MIP binding lifetime has expired for the Always On session and a MIP re-registration has not been received from the MS, the PDSN shall send an LCP Terminate-Request to the MS.

1 **4.2.1.3 Authentication**

2 The PDSN shall initially propose CHAP in an LCP Configure-Request message to the MS. The
3 PDSN shall re-send an LCP Configure-Request message without the authentication option after
4 receiving the LCP Configure-Reject (CHAP or PAP) from the MS.

5 **4.2.1.4 Addressing with IPCP**

6 When only Mobile IP service is requested by the MS and prior to the initial MIP registration, the
7 MS shall not include an IP Address Configuration Option in the IPCP Configure-Request
8 message to the PDSN. If the MS includes an IP Address Configuration Option in the IPCP
9 Configure-Request to the PDSN, the PDSN considers this as an MS using Simple IP service. In
10 this case, the PDSN shall send an IPCP Configure-NAK with a new proposed IP address for the
11 MS.

12 During IPCP phase, the PDSN shall include the IP Address Configuration option containing its IP
13 address in the IPCP Configure-Request messages sent to the MS.

14 The PDSN shall not support RFC 2290. If the PDSN receives an IPCP Configure-Request from
15 the MS containing the Mobile IPv4 Configuration Option [RFC 2290], the PDSN shall reply with
16 an IPCP Configure-Reject message.

17 The PDSN shall implement the IPCP configuration options as defined in RFC 1877 for DNS
18 server address negotiation. The PDSN shall negotiate Primary and Secondary DNS server IP
19 addresses with the MS, if DNS Server Configuration options are received during the IPCP phase.

20 **4.2.1.5 Compression**

21 See Section 3.2.1.6.

22 **4.2.1.6 PPP Framing**

23 See Section 3.2.1.7.

24 **4.2.2 MIP Registration**

25 **4.2.2.1 Agent Advertisements**

26 For the MS that uses Mobile IP, the PDSN shall begin transmission of an operator configurable
27 number of Agent Advertisements immediately following negotiation or re-negotiation of PPP, or
28 upon receipt of an Agent Solicitation message from the MS. Once the PDSN sends the
29 configurable number of Advertisements, the PDSN shall not send further Advertisements, unless
30 it receives an Agent Solicitation message from the MS. If the MS sends an RRQ to the PDSN, the
31 PDSN shall cease sending Agent Advertisements.

32 If the PDSN receives an Agent Solicitation from the MS following PPP establishment of a Simple
33 IP session, the PDSN shall send Agent Advertisements to the MS with the 'R' bit set. The PDSN
34 may also send an Agent Advertisement to the MS with the 'R' bit set if the PDSN receives a
35 packet with an invalid IP source address¹⁴ from the MS when the PDSN hasn't previously sent
36 Agent Advertisements. If Agent Advertisements are being sent, the PDSN shall not restart
37 sending the configurable number of Agent Advertisements.

38 If the PDSN receives an RRQ with the 'D' bit set, the PDSN shall send an RRP with code 65¹⁵. In
39 this case, the PDSN shall not close the PPP session.

40 The Mobile IP Registration Lifetime field in the Agent Advertisement shall be smaller than the
41 PPP inactivity timer value in use for the underlying PPP session.

¹⁴ The source IP address from the MS is considered as invalid if it is not one of the addresses that have been assigned to the MS or the MS has not been assigned with any IP addresses.

¹⁵ Previous version of this standard uses code 77. In this standard, the PDSN uses code 65, because code 77 is not used in RFC 2002.

1 Upon receiving a handoff indication including non-zero values of SID/NID/PZID of the previous
2 PCF and SID/NID/PZID of the current PCF, if the PDSN already supports a Mobile IP service for
3 the MS, the PDSN shall use this information to determine whether or not Mobile IP re-registration
4 is required for the MS. If re-registration is required, then the PDSN shall re-negotiate PPP and
5 begin transmission of an operator configurable number of Agent Advertisements.

6 In order to minimize Agent Advertisements sent over the air, the PDSN shall not send unsolicited
7 Agent Advertisements to an MS periodically to refresh the FA advertisement lifetime. The MS
8 may send Agent Solicitations, when the FA advertisement lifetime expires. The Advertisement
9 Lifetime is a configurable value, and shall be set to 9000 seconds (the maximum ICMP router
10 advertisement lifetime).

11 **4.2.2.2 Addressing and Mobile IP**

12 The PDSN shall support RFC 2794, and therefore, support zero and non-zero Home Address
13 values in the MIP RRQ. For dynamic Home Address assignment, the PDSN shall accept Mobile
14 IP RRQs with a 0.0.0.0 source address from the MS, and shall use the NAI instead of the Home
15 Address in it's pending registration request records, along with the Identification field [RFC 2794].
16 For dynamic Home Address assignment, the PDSN shall acquire the MS's Home Address from
17 the Mobile IP RRP.

18 In order to provide public network access and to provide private network access across the
19 Internet, the PDSN shall use a publicly routable and visible IP address as a FA address.

20 **4.2.2.3 MIP Extensions**

21 The PDSN shall include the MN-FA Challenge Extension [RFC 3012] in the Agent Advertisement.
22 Because Advertisements are rarely sent (to save air resources), the PDSN shall include in the
23 RRP a new challenge that the MS should use in its next re-registration with this PDSN. On re-
24 registration, the PDSN may communicate user FAC authentication information to the Home
25 RADIUS Server, via broker servers if required, in a RADIUS Access-Request message. The
26 frequency of this re-authentication and re-authorization is configurable by the operator. The
27 challenge shall be changed on a serving access provider configurable basis.

28 If the RADIUS attribute "MN-AAA Removal Indication" is included in the RADIUS Access-Accept
29 message, and if the RRQ contains an MN-HA Authentication Extension followed by the MN-FA
30 challenge and MN-AAA Authentication Extension, the PDSN shall remove the MN-FA challenge
31 and the MN-AAA Authentication Extensions when relaying the RRQ to the HA. Otherwise, the
32 PDSN shall relay the RRQ to the HA as received from the MS.

33 **4.2.2.4 Dynamic Home Agent Assignment**

34 The PDSN shall include the Home Address that it receives in the RRQ message from the MS in
35 the RADIUS Access-Request message in RADIUS attribute 8 (Framed-IP-Address). The PDSN
36 shall include the HA Address that it receives in the RRQ message from the MS in the RADIUS
37 Access-Request message in the HA attribute (see X.S0011-005-C). Upon receiving an RRP
38 message with successful registration indication (code 0) for the MS, the PDSN shall update the
39 mobility binding for the MS, which is indexed by the NAI and the Home Address (if non zero) in
40 the RRQ, with the HA Address and the Home Address from the RRP.

41 **4.2.2.5 Private Network Support**

42 It is possible that two different MSs served by a PDSN have the same, overlapping private
43 address because they belong to two different private networks. To support this scenario, the
44 PDSN forms a logical association that contains the R-P Connection ID, the MS's Home Address,
45 and the HA Address. When the PDSN receives a packet for a registered MS from the HA, the
46 PDSN maps the MS's HA Address and the Home Address to one association, and transmits the
47 packet on the R-P connection indicated by the R-P Connection ID of the association.

48 When processing additional MIP registrations for the same MS, if the PDSN receives an RRP
49 from a second HA that includes a private address as the Home Address, and if the private

1 address has already been assigned to the MS by another HA, the PDSN shall set the Code field
 2 to 65 (administratively prohibited) before forwarding the RRP to the MS. The first assigned
 3 address is not affected.

4 4.2.2.6 Reverse Tunneling

5 The PDSN shall reject a Mobile IP registration with an error code of 75, if a private Home
 6 Address as defined in RFC 1918 is present in either the RRQ or RRP, and the RRQ did not
 7 indicate reverse tunneling.

8 If the Home RADIUS Server sends a Reverse Tunnel Specification attribute in the RADIUS
 9 Access-Accept message indicating that reverse tunneling is required, and the MS did not indicate
 10 reverse tunneling in the RRQ, the PDSN shall reject the registration with an error code of 75.

11 If the MS negotiates reverse tunneling, then the PDSN shall tunnel both direct delivered and
 12 encapsulated packets back to HA. This applies to unicast, multicast, and broadcast IP destination
 13 addresses, even if the direct delivery mode is used. See Reverse Tunneling [RFC 3024] for an
 14 explanation of direct and encapsulated delivery styles.

15 The PDSN shall support both direct delivered and encapsulated packets.

16 4.2.2.7 DNS Address Assignment

17 If the PDSN supports the DNS Server IP Address VSA and NVSE and it receives a DNS Server
 18 IP Address VSA in the RADIUS Access-Accept message from the RADIUS server or/and a DNS
 19 Server IP Address NVSE in the MIP Registration Reply from the HA, then the PDSN may include
 20 each received DNS Server IP Address in a DNS Server IP Address NVSE in the MIP Registration
 21 Reply to the MS. The format of the DNS Server IP Address VSA is defined in Annex C, and the
 22 format of the DNS Server IP Address NVSE is defined in section 4.6.

23 If the PDSN receives a DNS Server IP Address from both the Visited RADIUS and Home
 24 RADIUS servers (entity type 1 and 2), and the PDSN supports the VSA, the PDSN shall
 25 determine if the M bit is set in the DNS Server IP Address VSA received in the RADIUS Access-
 26 Accept message to select the DNS Server IP Address VSA it forwards to the MS. The DNS
 27 Server IP Address VSA with the M bit set, shall have precedence over the VSA that does not
 28 have the M bit set. If the PDSN receives a RADIUS Access-Accept message from the Visited
 29 RADIUS server that has DNS IP address VSA(s) with the following values included, then the
 30 PDSN shall apply local policies to select the DNS IP Address VSA for DNS information.

- 31 ▪ An DNS IP Address VSA with the Entity-Type subfield set to the value 1 (=HAAA) and
 32 the M bit unset, and/or
- 33 ▪ One or more DNS IP Address VSA(s) with the Entity-Type subfield set to the value 2
 34 (=VAAA).

35 4.2.3 RADIUS Support

36 The PDSN shall act as a RADIUS client in accordance with RFC 2865. On initial mobile access,
 37 the PDSN shall communicate user FAC authentication information to the Home RADIUS Server,
 38 via the broker RADIUS servers if required, in a RADIUS Access-Request message. On receipt of
 39 the RRQ from the MS, and if SPI in the MN-AAA Authentication Extension is set to CHAP-SPI,
 40 the PDSN shall create a RADIUS Access-Request message in accordance with
 41 Table 4. See section 4.3.2 for how to construct CHAP-Password and CHAP-Challenge fields in
 42 the RADIUS Access-Request message.

43 If the SPI in the MN-AAA Authentication Extension is set to CHAP SPI as per RFC 3012, the
 44 PDSN shall use MD5 when computing the CHAP challenge. If the authentication succeeds, the
 45 Home RADIUS server shall send a RADIUS Access-Accept message to the PDSN. If the
 46 authentication fails, the Home RADIUS server shall send a RADIUS Access-Reject message to
 47 the PDSN.

48 The inclusion of the NAS-IP-Address or the NAS-IPv6-Address, or both in the RADIUS Access-
 49 Request message, depends on whether the PDSN has an IPv4 address or IPv6 address, or both.

1 The PDSN shall act as a RADIUS accounting client in accordance with RFC 2866 and shall
 2 communicate user accounting information to the Visited RADIUS server in RADIUS Accounting-
 3 Request messages. The PDSN shall determine at completion of the IPCP phase that an
 4 Accounting-Request (Start) record shall be sent to the RADIUS server following a successful
 5 Mobile IP Registration Reply received from the HA. The Accounting-Request (Start) record shall
 6 contain the Account Session ID and Correlation ID attribute generated by the PDSN.

7 The security of communications between the PDSN and the RADIUS server may be provided
 8 using IP security. The establishment of security is outside the scope of this document.

9 **4.2.4 IP Security Support**

10 There may be a statically configured shared key for computing the Mobile IP HA-FA
 11 Authentication Extension in Mobile IP registration messages. If such a shared key exists, the
 12 PDSN and the HA shall use it. Additional Security Associations (SAs) between the PDSN and HA
 13 may also be supported for the protection of Mobile IP control messages and user data. This
 14 document supports the following options for the establishment of such additional SAs:

- 15 • Public certificates¹⁶.
- 16 • Dynamic IKE pre-shared secret distributed by the Home RADIUS Server.
- 17 • Statically configured IKE pre-shared secret.

18 The PDSN shall support IPSec and IKE [RFC 2409]. An SA between the PDSN and the HA may
 19 be established using X.509 based certificates, or a pre-shared secret for IKE that may be
 20 statically configured or dynamically provisioned by the Home RADIUS server. Although ESP is
 21 preferred (and shall be implemented), AH shall also be implemented in order to maintain
 22 backward compatibility with previous versions of this document.

23 In the case of a carrier owned HA, and if mandated by carrier policy, the PDSN shall have a SA
 24 with the HA in order for a RRQ to be successfully processed. The SA may formally be via IPSec
 25 (i.e., ESP or AH) or Mobile IP HA-FA Authentication Extension.

26 An SA between the PDSN and the HA shall be established as follows:

27 When receiving a MIP RRQ containing a unicast HA Address, the PDSN shall verify if a SA
 28 currently exists with the HA. If an SA does not exist, the PDSN shall verify if HA X.509 certificates
 29 exists. If no HA X.509 certificate exists, the PDSN shall verify if a root certificate exists. If the
 30 necessary certificates do not exist, the PDSN shall verify if a statically configured pre-shared
 31 secret for IKE exists. If the static pre-shared secret for IKE is also not available, it shall include a
 32 request for a pre-shared secret for IKE in the RADIUS Access-Request message. The Home
 33 RADIUS server shall include the pre-shared secret for IKE and a KeyID in the RADIUS Access-
 34 Accept message if IPSec services are authorized for the user.

35 When the MS uses dynamic HA assignment (scenarios 1 and 2 from Section 4.1.3), the PDSN
 36 shall always request the IKE pre-shared Secret from the Home RADIUS server. IPSec support
 37 for dynamic HA assignment is further described in Section 4.2.4.3.

38 **4.2.4.1 IPSec Service Authorized**

39 The PDSN shall provide IPSec services as indicated by the Security Level attribute included in
 40 the RADIUS Access-Accept message. The Security Level attribute included in the RADIUS
 41 Access-Accept message allows the Home RADIUS server to indicate whether IP security should
 42 be applied to MIP registration messages and MIP tunneled data between the HA and the PDSN,
 43 or not to use IPSec at all. The same security level shall be applied by the PDSN for all users
 44 using the same Home Agent. If the PDSN receives the deprecated value of '1' or '2', the PDSN
 45 shall use a default value of '3'.

¹⁶ Refer to Annex A and B for details.

1 If the home network authorizes IPsec services, the PDSN shall not forward an RRQ to the HA
 2 unless an IPsec SA is established. The PDSN shall send a failed RRP with an error code of 65
 3 (Administratively Prohibited) to the MS if IPsec service is authorized by the Home RADIUS
 4 Server but it is unable to establish an IPsec SA to the HA. The Home RADIUS Server authorizes
 5 the PDSN to either use an existing SA with the corresponding HA or to establish a new SA if no
 6 prior SA exists.

7 If an IPsec SA does not exist and IPsec is authorized, the PDSN shall establish a SA using IKE
 8 with either X.509 or root certificates, or statically configured pre-shared secret for IKE, or
 9 dynamically distributed pre-shared secret for IKE. The PDSN shall comply with the specifications
 10 in IKE [RFC 2409] and the Annexes A and B in this document.

11 If reverse tunneling is required and IPsec security is authorized, then the PDSN shall provide
 12 security on the reverse tunnel.

13 If the PDSN does not receive the Security Level attribute from the Home RADIUS server, and an
 14 IPsec SA to the HA already exists, the PDSN shall continue to use the same SA. If it receives a
 15 new pre-shared secret for IKE and an SA already exists, the PDSN shall not renegotiate the
 16 ISAKMP SA and shall discard any pre-shared secret received in the RADIUS Access-Accept
 17 message. If no SA exists, then the PDSN shall follow local security policy.

18 If an IPsec SA already exists with the HA, the PDSN shall ensure the IPsec SA is maintained by
 19 periodically refreshing the SA for as long as valid Mobile IP bindings exist with that HA.

20 **4.2.4.2 IPsec Service Not Authorized**

21 If the Home RADIUS server does not authorize security for the MS, the PDSN shall not delete
 22 existing IPsec SA with an HA. This is because IPsec should be authorized per PDSN-HA pair
 23 and thus other MSs may be using the same IPsec SA.

24 **4.2.4.3 Dynamic HA Assignment**

25 When the PDSN receives a MIP RRQ containing a HA Address of 255.255.255.255 (or 0.0.0.0),
 26 it shall always include the IKE Pre-shared Secret Request attribute in the RADIUS Access-
 27 Request message sent to the Home RADIUS server. The Home RADIUS server responds with a
 28 RADIUS Access-Accept message containing the allocated HA Address and if IPsec services are
 29 authorized for the user, the corresponding dynamic pre-shared secret and KeyID for IKE are also
 30 included. The PDSN shall verify if IPsec services are authorized by the presence of the Security
 31 Level attribute. When IPsec service is authorized for the user, the PDSN shall then determine
 32 from the received HA Address whether an IPsec SA already exists. If an SA already exists with
 33 the HA, the PDSN shall use the existing SA as is and shall discard any pre-shared secret
 34 received in the RADIUS Access-Accept message.

35 If an SA does not exist, the PDSN shall determine if certificates or static pre-shared secret for IKE
 36 exist for the HA, otherwise the pre-shared secret for IKE, if provided by the Home RADIUS
 37 server, shall be used to establish the required SA.

38 **4.2.5 Ingress Address Filtering**

39 Upon receiving a packet from the MS, the PDSN shall discard the packet if one of the following
 40 conditions holds:

- 41 • the packet is received while the PPP negotiation is in progress (state is not open),
- 42 • the packet is received while MIP registration is pending¹⁷, but the source IP address
 43 of the packet is invalid¹⁸, and the packet is not a MIP control packet (MIP RRQ or
 44 Agent Solicitation).

¹⁷ i.e., between the NCP open state and completion of MIP registration.

1 For a Mobile IP session establishment over a Simple IP session, at the Simple IP establishment,

- 2 1. if the MS sends an Agent Solicitation to the PDSN, the PDSN shall respond with an
3 Agent advertisement and shall discard all IP packets with an invalid source IP
4 address while MIP registration is pending¹⁷.
- 5 2. If the MS doesn't send Agent Solicitations but sends IP packets with an invalid
6 Source IP address, the PDSN may discard the packets and may send an Agent
7 Advertisement to the MS. If the PDSN sends Agent Advertisements to the MS as a
8 result of an Invalid Source IP address, it shall discard all IP packets with an invalid
9 source IP address while MIP registration is pending¹⁷.

10 ~~If the PDSN receives an implementation-defined number of consecutive packets with an invalid
11 source IP address from the MS, the PDSN shall send an LCP Configure-Request message to the
12 MS. If the MS fails to register with the PDSN and continues to send IP packets with invalid source
13 IP address, the PDSN shall discard the packets and shall send an LCP Configure-Request
14 message to the MS to renegotiate the PPP session.~~

15 **4.3 Home Agent Requirements**

16 The HA shall support MIP [RFC 2002-2006], reverse tunneling [RFC 3024], FAC [RFC 3012],
17 and Mobile IP NAI Extension [RFC 2794]. In order to provide public network access and private
18 network access across the public network, the HA shall use a globally routable and visible IP
19 address.

20 **4.3.1 Multiple Registrations**

21 The HA shall support Multiple registrations with the same NAI but different static Home
22 Addresses.

23 **4.3.2 MIP Authentication Support**

24 When the HA receives an RRQ from a PDSN, it authenticates the RRQ using the MN-HA shared
25 key. At initial registration, if the HA does not have the MN-HA shared key, it shall retrieve the MN-
26 HA shared key from the Home RADIUS server. Based on the policy of the home network, the HA
27 may also process the MN-AAA Authentication Extension as specified in RFC 3012, if included in
28 the RRQ.

29 If the home network policy dictates that the HA shall process the MN-AAA Authentication
30 Extension, then the HA shall authenticate the request by including the following attributes in a
31 RADIUS Access-Request message to the Home RADIUS server:

- 32 • User-Name (1) = MN-NAI field in the MN-NAI Extension
- 33 • CHAP-Password (3) =
 - 34 ➤ CHAP Ident field = High-order byte of the Challenge Field in the MN-FA
35 Challenge Extension
 - 36 ➤ String field = Authenticator field from the MN-AAA Authentication
37 Extension
- 38 • CHAP-Challenge (60) = MD5 (Preceding MIP RRQ, Type, Subtype, Length, SPI),
39 followed by the least-order 237 bytes of the Challenge Field in the MN-FA Challenge
40 Extension. The MD5 checksum is computed over the MIP RRQ data preceding the
41 MN-AAA Authentication Extension and the Type, Subtype, Length, SPI fields of the
42 MN-AAA Authentication Extension.

¹⁸ The source IP address from the MS is considered as invalid if it is not one of the addresses that have been assigned to the MS or if the MS has not been assigned any IP addresses.

- 1 • MN-HA SPI = to request the MN-HA shared key if not available at the HA. The MN-
2 HA shared key corresponds to a single user's NAI, or NAI and non-zero static IP
3 address pair.

4 If the MN-AAA Authentication Extension is not present in the RRQ or HA policy dictates that the
5 HA shall not process the MN-AAA Authentication Extension (, and the HA requires the MN-HA
6 shared key from the RADIUS server), the HA shall send a RADIUS Access-Request¹⁹ message
7 that includes a User Name, a User-Password and an MN-HA SPI.

8 If the MN-HA shared key is requested, the Home RADIUS server shall encrypt the MN-HA
9 shared key in a RADIUS Access-Accept message using a method based on the RSA Message
10 Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of RFC 2868.

11 The HA shall save the MN-HA shared key received from the Home RADIUS server for the
12 duration of the MIP session with the MS. Based on the local policy, the HA may store the MN-HA
13 shared key a certain time skew after releasing the mobility binding for the MS.

14 The HA shall compute the MN-HA Authentication Extension, according to RFC 2002, based on
15 the MN-HA shared key. Computation of the extension shall include the Type and the SPI field of
16 the MN-HA Authentication Extension itself.

17 4.3.3 IPSec Support

18 The HA shall determine which type of security associations (if any) are required with a PDSN.
19 The HA and the PDSN shall use the same security policy as specified in the Home RADIUS
20 server. The policy may be locally configured at the HA or may be obtained from the Home
21 RADIUS server in the Security Level attribute~~The policy may be locally configured at the HA or~~
22 ~~may be obtained from the Home RADIUS server.~~

23 If IPSec is authorized and no SA is currently in place, the HA shall participate in IKE negotiation
24 with the PDSN. The negotiation will result in establishing an IPSec SA that will be used for all
25 traffic between the HA and the PDSN.

26 The HA shall perform a similar operation as the Home RADIUS server to generate the pre-shared
27 secret for IKE (i.e., K), see algorithm for K in Section 4.4.3.

28 When an IKE request is received, the HA shall validate the timestamp in the KeyID field. This
29 timestamp eliminates the possibility of re-using a previously generated shared-key for IKE 'K'
30 value while the secret key 'S' is still valid on the HA. The HA shall also use the 'S' Key indexed by
31 Home RADIUS server IP address from the KeyID field.

32 If there is no previously assigned 'S' Key, the S Key is not found, or the timestamp in the KeyID is
33 greater than the 'S' expiration time, then the HA shall send a RADIUS Access-Request message
34 to the Home RADIUS server to request the S Key.

35 That RADIUS Access-Request message shall contain:

- 36 • The User-Name attribute consisting of a concatenation of the PDSN's CoA and HA
37 Address.
38 • The 'S' Request attribute.

39 The User-Name attribute should be formatted using ASCII hexadecimal notation. Both addresses
40 are converted to hexadecimal and the ASCII codes of the hexadecimal characters and are
41 concatenated with the HA Address following the CoA. For example, CoA of 10.10.10.11 is
42 concatenated with an HA Address of 92.64.10.1 to yield "0A0A0A0B5C400A01".

43 The RADIUS Access-Accept message from the Home RADIUS server shall include the 'S' Key
44 and its lifetime, and may include the Security Level attribute. The HA shall save the 'S' Key

¹⁹ Construction of the message is implementation dependent.

1 received from the Home RADIUS servers. The HA shall compute the pre-shared secret "K" using
2 KeyID (X.S0011-005-C) and the 'S' Key (see Section 4.4.3).

3 Each HA shall have a configurable, allowable time skew to be used to validate the freshness of
4 'K'. The HA shall maintain expired 'S' keys for a configurable amount of time. This expired key
5 shall be used when KeyIDs are received that refer to the expired 'S' Key but falls within the
6 allowable time skew²⁰.

7 The security method used between the HA and the Home RADIUS server is outside the scope of
8 this document.

9 However, the Home RADIUS server may encrypt the 'S' Key and the 'S' Lifetime using a method
10 based on the RSA Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of
11 RFC 2868.

12 If mandated by an operator security policy, an operator's HA shall have a SA with the PDSN in
13 order for a registration request to be successfully processed. The SA may formally be via IPsec
14 (e.g., ESP or AH) or via a Mobile IP HA-FA Authentication Extension. Likewise, a HA shall accept
15 or reject a RRQ received directly from an MS with a 'D' bit set depending on security policy.

16 **4.3.4 Dynamic Home Agent Assignment**

17 During dynamic HA assignment, the HA Address that is specified by the MS in the RRQ message
18 and the IP address of the dynamically assigned HA may not be the same. Upon receipt of such a
19 RRQ message in an IP packet with the destination IP address set to the HA unicast IP address,
20 the HA may accept the RRQ contrary to the specification in RFC 2002 or may reject it with an
21 error code of 136 in accordance with RFC 2002. The HA shall follow the procedures described in
22 Section 4.3.2 to complete its authentication process for the RRQ message. The HA shall put its
23 IP address in the HA Address field of the RRP message to the MS.

24 **4.3.5 DNS Address Assignment**

25 The DNS server IP addresses may be configured at the HA, or received from the Home RADIUS
26 server in a RADIUS Access-Accept message. If the HA does not receive the DNS Server IP
27 Address VSA from the Home RADIUS server, then the HA may include configured²¹ DNS server
28 IP addresses in the DNS Server IP Address NVSE. If the HA includes the configured DNS server
29 IP addresses in the DNS Server IP Address NVSE, it shall set the Entity-Type field to 3 (see
30 section 4.6), and send the NVSE in a MIP Registration Reply message. If the HA receives the
31 DNS Server IP Address VSA from the Home RADIUS server, the HA may include the received
32 DNS server IP addresses in the DNS Server IP Address NVSE. If the HA includes the received
33 DNS server IP addresses in the DNS Server IP Address NVSE it shall set the Entity-Type field to
34 1 (see section 4.6) and send the NVSE in a MIP Registration Reply message.

35 **4.4 RADIUS Server Requirements**

36 See Section 3.3.

37 In order to provide the functions defined in this document, the Home and Visited RADIUS servers
38 shall support as required the attributes listed in Table 4 and X.S0011-005-C, in addition to the
39 standard RADIUS attributes. The Broker RADIUS server shall support the decryption and re-
40 encryption of the Pre-shared Secret attribute and the MN-HA Shared Key attribute.

²⁰ The skew serves to solve the case where RADIUS or IKE messages are lost and must be transmitted yet the 'S' Key expires in the meantime. An example of the skew could be one minute.

²¹ [The DNS information may be pre-configured in the HA or the HA may acquire the DNS information via other schemes.](#)

1

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
User-Name	1	M	M	PDSN -> AAA HA -> AAA
User-Password	2	O Note 1		HA -> AAA
CHAP-Password	3	M Note 2		PDSN -> AAA HA -> AAA
CHAP-Challenge	60	M Note 2		PDSN -> AAA HA -> AAA
NAS-IP-Address	4	O Note 3		PDSN -> AAA
NAS-IPv6-Address	95	O Note 4		PDSN -> AAA
Foreign Agent Address	26/79	O		PDSN -> AAA
Correlation ID	26/44	M	O	PDSN <-> AAA
Calling-Station ID	31	O		PDSN -> AAA
Home Agent	26/7	M	M	PDSN <-> AAA
Framed-IP-Address	8	M	O	PDSN <-> AAA
IKE Pre-shared Secret Request	26/1	O		PDSN -> AAA
Security Level	26/2		O	AAA -> PDSN, AAA -> HA
Pre-shared Secret	26/3		O	AAA -> PDSN
Reverse Tunnel Specification	26/4		O	AAA -> PDSN
KeyID	26/8		O	AAA -> PDSN
'S' Key	26/54		O	AAA -> HA
'S' Lifetime	26/56		O	AAA -> HA
'S' Request	26/55	O		HA -> AAA
MN-HA Shared Key	26/58		O	AAA -> HA
MN-HA SPI	26/57	O		HA -> AAA
Allowed Differentiated Services Marking	26/73		O	AAA -> PDSN
DNS Update Required	26/75		O	AAA -> HA
Always On	26/78		O	AAA -> PDSN
Service Option Profile	26/74		O	AAA -> PDSN
Remote IPv4 Address	26/59		O	AAA -> PDSN
Remote IPv6 Address	26/70		O	AAA -> PDSN
Remote Address Table Index	26/71		O	AAA -> PDSN
MN-AAA Removal Indication	26/81		O	AAA ->PDSN
NAS-Port-Type	61	O Note 5		PDSN -> AAA

2 (M) Indicates Mandatory attribute

3 (O) Indicates optional attribute

4 Note 1: The password is configured between the HA and the AAA.

5 Note 2: For Mobile IP, this attribute is mandatory for the PDSN, and optional for the HA.

6 Note 3: This is the IPv4 [Address](#) of the RADIUS server interface of the PDSN; at least one of
7 NAS-IP-Address or NAS-IPv6-Address must be included.

8 Note 4: This attribute is included if the PDSN supports IPv6 addressing.

9 Note 5: The values are as follows: 22 (IS-2000) [5-9] or 24 (HRPD) [15], depending on the
10 service option number connected to the PDSN.11 **Table 4 - Occurrence of RADIUS Attributes for Mobile IP**12 **4.4.1 Dynamic Home Agent Assignment**13 The Home RADIUS server shall implement an HA selection algorithm to perform dynamic HA
14 assignment. The implementation details of this algorithm are outside the scope of this document.

15 The HA selection algorithm shall satisfy the four scenarios described in Section 4.1.3. The Home

1 RADIUS server shall return the assigned HA Address in the HA attribute in the RADIUS Access-
2 Accept message to the PDSN.

3 **4.4.2 MN-HA Shared Key Distribution**

4 Upon receipt of a RADIUS Access-Request message from a HA containing the MN-HA SPI
5 attribute, the RADIUS server shall send a RADIUS Access-Accept message containing the MN-
6 HA shared key encrypted using a method based on RSA MD5 [RFC 1321] as described in
7 Section 3.5 of RFC 2868.

8 **4.4.3 IKE Pre-shared Secret Distribution Procedure**

9 When the RADIUS Access-Request message is received from the PDSN containing the IKE Pre-
10 shared Secret Request attribute, and IPSec services are authorized for the user, the Home
11 RADIUS server shall distribute a key identifier and pre-shared secret for IKE to the PDSN using
12 the Pre-shared Secret and KeyID attributes in the RADIUS Access-Accept message. The Home
13 RADIUS server generates a pre-shared secret for IKE by processing the Home RADIUS IP
14 address, FA IP address, and a timestamp as well as a secret key, known as the 'S' Key, through
15 the HMAC-MD5 hashing algorithm. The 'S' Key is known between the Home RADIUS server and
16 the HA. The 'S' Key is retrieved by the HA from the Home RADIUS server and has a configurable
17 lifetime. The lifetime of the 'S' Key is a Home RADIUS local policy, and is based on the
18 cryptographic strength of the 'S' Key. The pre-shared secret is generated using the following
19 formula:

20 **$K = \text{HMAC-MD5}(\text{Home RADIUS IP address} \mid \text{FA IP address} \mid \text{timestamp}, \text{'S'})$**

21 The Home RADIUS server hides pre-shared secrets for IKE using a method based on the RSA
22 Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of RFC 2868.

23 **4.4.4 DNS Address Assignment**

24 The RADIUS server may include the DNS Server IP Address VSA in the RADIUS Access-Accept
25 message in response to a RADIUS Access-Request message from the PDSN and/or the HA. If
26 the RADIUS server includes the DNS Server IP Address VSA, it shall include a Primary and a
27 Secondary DNS server IP addresses. The status of the 'M' bit in the DNS Server IP Address VSA
28 is controlled by the Home RADIUS server.

29 **4.5 MS Requirements**

30 The MS may support Mobile IPv4 service. The MS shall access cdma2000 packet data service
31 using the cdma2000 air interface [5-9] and [15].

32 **4.5.1 PPP Session**

33 The MS shall use PPP as the data link protocol for Mobile IP. The MS may support multiple
34 Mobile IP Home Addresses over a single PPP session.

35 **4.5.1.1 Establishment**

36 Same as Section 3.4.1.1.

37 **4.5.1.2 Termination**

38 Same as Section 3.4.1.2.

39 If the MS tries to register and receives an RRP message with a failure code, it shall do one of the
40 following:

- 41 • Retry Mobile IP registration over the existing PPP session.

- 1 • If existing Simple IP or Mobile IP sessions exist, give up on the failed Mobile IP
- 2 registration and continue using the existing sessions.
- 3 • Fall back to Simple IP by re-negotiating the PPP session.
- 4 • Terminate the PPP session.

5 **4.5.1.3 Authentication**

6 The MS should not use CHAP or PAP for Mobile IP. When the MS receives an LCP Configure-
7 Request message requesting CHAP authentication, the MS should reply with an LCP Configure-
8 Reject message requesting no PPP authentication. If the MS receives an LCP Configure-
9 Request message without the authentication option it shall respond with an LCP Configure-Ack
10 message as described in RFC 1661.

11 If CHAP is performed, performance degradation will occur as the result of an unnecessary AAA
12 traversal, a FAC shall be performed regardless of whether or not CHAP is performed. The MS
13 shall use the challenge received in the Agent Advertisement or RRP to compute the MN-AAA
14 authenticator.

15 As a further clarification to RFC 3012 section 8 (SPI For RADIUS Servers):

16 If the challenge has fewer than 238 bytes, this algorithm includes the high-order byte in the
17 computation twice, but ensures that the challenge is used exactly as is. Additional padding is
18 never used to increase the length of the challenge; the input data is allowed to be shorter than
19 237 bytes long.

20 **4.5.1.4 Addressing with IPCP**

21 If the MS uses Mobile IP only, the MS shall not use the IP Address Configuration Option [RFC
22 1332]. On subsequent PPP session establishments while the MS intends to maintain a Home
23 Address, the MS shall omit the option²². The MS shall not include the Mobile IPv4 Configuration
24 Option in the IPCP Configure-Request messages sent to the PDSN.

25 The MS may implement RFC 1877 in order to auto-configure DNS server IP addresses. The MS
26 may negotiate Primary and Secondary DNS server IP addresses during the IPCP phase. The MS
27 may propose a DNS server address of zero to indicate an explicit request that the PDSN
28 provides the DNS server address information in a Configure-Nak.

29 **4.5.1.5 Compression**

30 Same as Section 3.4.1.5.

31 **4.5.1.6 PPP Framing**

32 Same as Section 3.4.1.6.

33 **4.5.2 MIP Registration**

34 **4.5.2.1 Agent Discovery**

35 Immediately after a PPP session is established, the MS may send Agent Solicitations. In this
36 case, the MS should use the same procedure as described in Section 2.4 of RFC 2002. If the MS
37 does not have a Home Address, the MS shall use zero in the Source IP Address field of the IP
38 packet that contains the Agent Solicitation. The MS shall support RFC 3012.

²² If the MS that uses Mobile IP uses the IP Address Configuration Option [RFC 1332] to indicate the Home Address, the PDSN will consider it as an MS using Simple IP service and send a NAK with an alternative address to the MS. The MS will respond with an IP Configure Request with the alternative address.

1 4.5.2.2 Registration Messages

2 Upon receiving Agent Advertisements from the PDSN, the MS shall send an RRQ message.

3 The MS may request a non-zero home IP address belonging to its home IP network in the RRQ
 4 or indicate that the HA should dynamically assign it an IP address. If the MS requests a dynamic
 5 HA assignment, the MS shall set the HA Address to either 255.255.255.255 or 0.0.0.0. However,
 6 the MS should use 255.255.255.255. If the MS requests a static or already allocated HA Address,
 7 it should set the HA Address accordingly.

8 The Home and HA Address allocations are based on the scenarios described in Section 4.1.3.

9

Scenario 1	To request a dynamic Home Address and a dynamic HA assignment, the MS shall set the Home Address field to 0.0.0.0 and the HA Address field to 255.255.255.255 or 0.0.0.0 in the RRQ message.
Scenario 2	To request a dynamic HA assignment only while requesting a previously assigned Home Address, the MS shall set the Home Address field to the desired Home Address, and the MS shall set the HA Address field to 255.255.255.255 or 0.0.0.0 in the RRQ message. If the MS receives a failed RRP, the MS may retry a MIP registration under any of the scenarios.
Scenario 3	To request a dynamic Home Address allocation only while requesting a previously assigned HA, the MS shall set the Home Address field to 0.0.0.0 and the MS shall set the HA Address field to the desired HA Address in the RRQ message. If the MS receives a failed RRP, the MS may retry a MIP registration under any of the scenarios.
Scenario 4	When the MS is not requesting dynamic allocation of either a Home Address or a HA Address, the MS shall set the Home Address and HA Address fields with the desired IP addresses in the RRQ message. If the MS receives a failed RRP, the MS may retry a MIP registration under any of the scenarios.

10

Table 5 - MS Registration Scenarios

11 While requesting a dynamic Home Address assignment, the MS shall use zero in the Source IP
 12 Address field of the IP packet that contains the Mobile IP RRQ. In this case the NAI is used to
 13 identify the MS.

14 During MIP re-registrations, the MS shall use the same HA Address and the Home Address that
 15 were assigned to it during the initial MIP registration.

16 Upon receipt of an RRP message with successful registration indication (code 0) during initial
 17 registration, the MS shall accept the dynamically assigned HA Address contained in the RRP
 18 message, even if it is different from the HA Address provided in the RRQ message.

19 If the MS had set up a Simple IP session and decides to run Mobile IP simultaneously using the
 20 FA function in the PDSN, it shall send an Agent Solicitation to the PDSN. Upon receiving an
 21 Agent Advertisement, the MS shall register with the PDSN and shall not use collocated CoA. The
 22 MS may also register directly with the HA using a collocated CoA obtained from Simple IP IPCP
 23 negotiation.

24 If the MS desires reverse tunneling, the MS shall set the T-bit in the RRQ message.

25 The MS shall not set the "V" bit in the RRQ message.

26 4.5.2.3 MIP Extensions

27 The MS shall include the MN-NAI Extension [RFC 2794], MN-HA Authentication Extension [RFC
 28 2002], MN-FA Challenge Extension [RFC 3012], and MN-AAA Authentication Extension [RFC
 29 3012] in the RRQ message. Because advertisements are rarely sent to save air resources, when

1 the MS performs re-registration, the MS shall use the challenge value contained in the last
 2 received RRP as described in RFC 3012.

3 The MS shall compute the MN-AAA Authentication Extension, according to RFC 3012, based on
 4 the shared secret the MS has with the Home RADIUS server. The MS shall compute the MN-HA
 5 Authentication Extension, according to RFC 2002, based on the shared secret the MS has with
 6 the HA. Computation of the extension shall include the Type and SPI field of the MN-HA
 7 Authentication Extension itself. The MS may use the same shared-secret or different shared
 8 secrets in the computation of the MN-AAA Authentication Extension and MN-HA Authentication
 9 Extension. This is coordinated between the MS and its home network.

10 **4.5.2.4 Private Network Support**

11 If the MS wants private network access through Mobile IP, the MS shall use reverse tunneling.

12 **4.5.2.5 Termination**

13 When the MS wishes to terminate a MIP session, the MS may send a Mobile IP RRQ to the HA
 14 with a Registration Lifetime of zero to gracefully close the MIP session before terminating the
 15 packet data service with the RN²³.

16 **4.5.2.6 DNS address Assignment**

17 If the MS receives at least one DNS Server IP Address NVSE (as defined in section 4.6) in the
 18 MIP Registration Reply message, then the MS may use the DNS server IP address in the NVSE
 19 instead of the DNS server IP address received during IPCP. If the MS receives multiple DNS
 20 Server IP Address NVSEs, it may select an appropriate entity (i.e., HAAA/VAAA or HA), for
 21 acquiring the DNS information, based on its internal policy.

22 If Reverse Tunneling is applied for the MIP session, and the MIP Registration Reply includes at
 23 least one DNS Server IP Address NVSE with the entity-type field set to either 1 or 3 and the MS
 24 supports the DNS Server IP Address NVSE, then the MS shall use the DNS server IP addresses
 25 provided in the MIP Registration Reply. If the entity type is 3, the DNS information provided by
 26 the HA may have precedence over that provided by the HAAA or the VAAA.

27 **4.6 DNS Server IP Address NVSE**

28 The NVSE contains a Primary and a Secondary DNS IP address and may be included in the MIP
 29 Registration Reply message from the HA and/or the PDSN. The format of the NVSE shall be as
 30 follows:

31

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1					
<u>Type</u>										<u>Length</u>					<u>Reserved</u>											
<u>Vendor/Org-ID</u>																										
<u>Vendor-NVSE-Type</u>										<u>Entity-Type</u>					<u>Sub-Type1</u>											
<u>Length</u>										<u>Primary DNS IPv4 address</u>																
<u>.....</u>										<u>Sub-Type2</u>					<u>Length</u>					<u>Secondary DNS IPv4 address</u>						
<u>.....</u>										<u>Unused</u>																

32 **Figure 2- NVSE for DNS server IP address**

33 Type: 134

34 Length = 22

35 Vendor/Org-ID: 5535

²³ The MS should send the RRQ with a lifetime of zero to free resources such as public addresses in the HA.

1 Vendor-NVSE-Type: 17

2 Vendor-NVSE-Value: This field is formatted as follows:

3 Entity-Type: In the Registration Reply message this field identifies the network entity that
4 has provided the DNS information to the mobile station so that it is aware of the source of
5 the DNS information. Currently the following types are defined:

6 HAAA = 1

7 VAAA = 2

8 HA = 3

9 Sub-Type1 (=1): This field indicates that the associated value field contains the Primary
10 DNS server IP address.

11 Length: 6

12 Vendor-Value: IPv4 address of primary DNS server.

13 Sub-Type (=2): This field indicates that the associated value field contains the Secondary
14 DNS server IP address.

15 Length: 6

16 Vendor-Value: IPv4 address of secondary DNS server.

1 **5 Simultaneous Services**

2 The PDSN shall support, and the MS may support, any of the following simultaneous packet data
3 session combinations:

- 4 • Simple IPv4 service & Simple IPv6 service.
- 5 • Simple IPv4 service & Mobile IPv4 service.
- 6 • Simple IPv6 service & Mobile IPv4 service.
- 7 • Simple IPv4 service & Simple IPv6 service & Mobile IPv4 service.

8 Additionally, multiple Mobile IPv4 sessions may be operated simultaneously. Although any of
9 these may run simultaneously, individual services are distinct. Within a single PPP session, the
10 PDSN shall support simultaneous operation of IPCP [RFC 1332] and IPv6CP [RFC 2462].
11 Simultaneous services are supported through re-negotiation of IPCP, IPv6CP, or MIP as
12 appropriate.

13 Each packet data sessions shall be authenticated and authorized independently. In addition,
14 each such session shall have unique accounting records. However, simultaneous Simple IPv4
15 and Simple IPv6 share a common authentication and authorization procedure as described in
16 Section 3.2.2.

1 **6 IP Reachability Service**

2 IP Reachability Service is the capability to update a DNS server in the home network with the
 3 current authorized MS IP address. When the MS desires to be reached by a DNS hostname, the
 4 Home RADIUS server (in the case of Simple IP or Mobile IP) or the HA (in the case of Mobile IP
 5 only) may send a DNS Update [RFC 2136] to a DNS server to add an A Resource Record for
 6 IPv4 and AAAA or A6 Resource Record for IPv6 [RFC 1886, RFC 2874²⁴].

7 The Update section of the DNS Update message contains the following values in 'Host address'
 8 Resource Type Resource Record:

- 9 • Resource Name = username.realm²⁵
- 10 • Resource Class = Internet address class
- 11 • IP Address = newly assigned IP address

12 The TTL (Time To Live) of the Update section in the DNS Update message should be zero so
 13 that all queries for the address are resolved using the up to date authoritative server for the user.
 14 This is because after the MS is assigned a different address, if the TTL were non-zero, the cache
 15 entry of the querying endpoint would no longer be valid, and, in fact, the address may have been
 16 given to a different MS.

17 The security between the DNS Server and Home RADIUS server or the HA is outside the scope
 18 of this document.

19 The method used by the Home RADIUS server and/or HA to determine the IP address of the
 20 DNS server is outside the scope of this document.

21 IP Reachability Service as specified in this document shall not be provided for users with single
 22 NAI and Multiple static Home Addresses.

23 **6.1 Simple IPv4 Operation**

24 The Home RADIUS server shall request that the DNS server add an A Resource Record for the
 25 user under the following conditions:

- 26 • the Home RADIUS server receives a RADIUS Accounting-Request (Start) record
 27 containing the Beginning-Session VSA and the IP-Technology VSA indicates Simple
 28 IP, and
- 29 • the Home RADIUS server is configured to send DNS Update messages, and
- 30 • the user profile indicates that IP Reachability Service is enabled for the user.

31 The Home RADIUS server shall send a request to the DNS server to delete the A Resource
 32 Record for a user under the following conditions:

- 33 • the Home RADIUS server receives a RADIUS Accounting-Request (Stop) record
 34 from the PDSN currently serving the user, for a session, and the Session-Continue
 35 VSA is either absent or is included but the value is set to FALSE and the IP-
 36 Technology VSA indicates Simple IP.

²⁴ RFC 2874 is an experimental RFC as per RFC 3363 section 2.2.

²⁵ The MS sends the NAI as 'username @ realm', and the Home RADIUS Server converts the username@realm into 'username.realm'. When the HA performs DNS update, the HA shall convert the [username@realm](#) to username.realm.

1 **6.2 Mobile IP Operation**

2 The DNS server may be updated by either the Home RADIUS server or the HA.

3 **6.2.1 DNS Update by the Home RADIUS Server**

4 The Home RADIUS server shall request that the DNS server adds an A Resource Record for the
5 user under the following conditions:

- 6 • The Home RADIUS server receives an Accounting-Request (Start) record containing
7 the Beginning Session VSA and the IP-Technology VSA indicates Mobile IP, and
- 8 • the Home RADIUS server did not receive a RADIUSAccess-Request message from
9 the HA with the DNS-Update-Capability VSA, and
- 10 • the Home RADIUS server is configured to do DNS update, and
- 11 • the user profile indicates that IP Reachability Service is enabled for the user.

12 After performing DNS update for the user, the Home RADIUS server shall cache the User Name,
13 NAS IP Address, and Framed IP address as received in the Accounting-Request (Start) record
14 for the user.

15 The Home RADIUS server shall send a request to the DNS server to delete the A Resource
16 Record for a user under the following conditions:

- 17 • The Home RADIUS server receives an Accounting-Request (Stop) record containing
18 the IP-Technology VSA that indicates Mobile IP, and does not contain the Session-
19 Continue VSA or the Session-Continue VSA is included but the value is set to
20 FALSE, and
- 21 • the Home RADIUS server has previously sent request(s) to the DNS server to
22 add/update an A Resource Record for the corresponding user, and
- 23 • the user profile indicates that IP Reachability Service is enabled for the user.

24 **6.2.2 DNS Update by the HA**

25 An HA that supports DNS update capability shall send a RADIUS Access-Request message to
26 the Home RADIUS server at each initial MIP RRQ message it receives, and shall include the
27 DNS-Update-Capability VSA. The home RADIUS server determines based on its configuration
28 and user profile if the HA shall perform DNS update operations. The Home RADIUS server shall
29 include the DNS-Update-Required VSA in the RADIUS Access-Accept message if the DNS-
30 Update-Capability VSA was included in the RADIUS Access-Request message and it allows the
31 HA to perform DNS update for the user.

32 The HA shall request the DNS server to add an A Resource Record for a user under the following
33 conditions:

- 34 • The HA is capable of DNS update and it is configured to do so, and
- 35 • the HA is authorized by the Home RADIUS server to perform DNS update, and
- 36 • the Mobile IP Registration process is successful.

37 The HA shall send a request to the DNS server to delete the A Resource Record for a user under
38 the following conditions:

- 39 • The HA has previously sent request(s) to the DNS server to add/update an A
40 Resource Record for the corresponding user, and
- 41 • the mobility binding for the user is set to expire due to the following reasons:

- 1 ➤ The HA receives a Mobile IP RRQ with lifetime set to 0 from the user, or
- 2 ➤ the Mobile IP registration lifetime for the user has expired, or
- 3 ➤ the mobility binding for the user has been revoked by the FA or the HA,
- 4 or
- 5 ➤ administrative reset.

6 **6.3 Simple IPv6 Operation**

7 For IPv6 IRS support, the Home RADIUS server shall use the Resource Records defined in RFC
8 1886 as updated by RFC 2874 and RFC 3152. The operation of IRS service for IPv6 users is
9 identical to the procedures described for Simple IPv4 in Section 6.1.

10 If the MS uses both IPv4 and IPv6, the Home RADIUS server shall request that the DNS server
11 create or delete Resource Records for both IPv4 and IPv6.

1 **Annex A: IKE/ISAKMP Payloads (normative)**

2 This Annex addresses ISAKMP payloads in which multiple options exist (see RFC 2407-2409).
3 The following requirements shall be met by the PDSN and HA, assuming IP security between the
4 HA and PDSN is required. Payloads in which no options exist do not appear in this Annex.

5 Note: If the HA (home network) does not require any security then Annex A does not apply nor
6 does it apply to MSs using collocated CoA for Mobile IP.

7 **ISAKMP Fixed Header:**

8 The PDSN in this document shall use a Major and Minor Version of 0. The HA shall
9 minimally accept Major and Minor Version of 0. This document does not make use of the
10 Fixed Header Authentication (A) bit.

11 **Security Association Payload:**

12 All Security Association Payloads shall use the IPsec DOI. The Phase 1 ISAKMP
13 Security Payload shall specify a situation of SIT_IDENTITY_ONLY. Phase 2 ISAKMP
14 Security Payloads shall specify a situation of SIT_IDENTITY_ONLY for all cases where
15 privacy or only authentication applies (as outlined in the PDSN and HA "IP Security"
16 sections of this document).

17 **Proposal Payload:**

18 Because the MS first makes contact with the PDSN, the PDSN shall be the Initiator of the
19 Phase 1 ISAKMP SA. The HA shall be the Responder. The PDSN shall propose ISAKMP
20 to the HA for the Phase 1 ISAKMP SA.

21 For Phase 2 Quick Mode exchanges, both the PDSN and HA shall be Initiators and
22 Responders because symmetrical, bi-directional security between the PDSN and HA is
23 required. For message authentication, PDSNs conforming to this document shall propose
24 both AH²⁶ and ESP with the authentication option. The HA shall respond with ESP if the
25 PDSN has proposed it. For message privacy, the PDSN shall propose ESP. For
26 combined authentication and privacy, the PDSN shall propose ESP only.

27 Mobile IP registration control packets and IP in IP tunneled packets may be protected by
28 IPsec authentication, privacy, or both. Security policies to be used between the PDSN
29 and the HA in this document are dictated by the home network not the access provider
30 network. The PDSN shall be capable of proposing authentication only, privacy only, and
31 both authentication and privacy. Service provider owned HAs shall accept and propose
32 only one of these, and the PDSN shall accept this proposal. The Home RADIUS server
33 may deliver a User Profile to the Visited RADIUS server and PDSN that indicates
34 whether security should be supported for IP in IP packets. If the Home RADIUS server
35 indicates a request for no security on the IP-in-IP tunneled packets, the PDSN shall not
36 delete existing IPsec security associations to the HA. This is because IPsec should be
37 authorized per PDSN-HA pair and thus other MSs may be using those IPsec security
38 associations.

39 The SPI shall be four octets.

40 **Transform Payload:**

41 For Phase 1, the PDSN shall use KEY_IKE as the transform identifier. All
42 implementations shall support 3DES and RSA.

²⁶ Note that a future version of this standard is likely to no longer require AH, in accordance with industry trends.

1 For Phase 2 Quick Exchange, the PDSN shall minimally support the ESP_3DES
 2 transform identifier within a Transform Payload for IPsec ESP Proposal Payload. It shall
 3 also support both HMAC-MD5 and HMAC-SHA1 as transform identifiers within a
 4 Transform payload for IPsec AH Proposal Payload. Service provider HAs shall likewise
 5 support these two transforms. The PDSN may optionally support and propose other
 6 transforms. An HA shall select one of the transforms offered by the PDSN.

7 **Key Exchange Payload:**

8 The PDSN and HA will exchange D-H (Diffie-Hellman) public values computed in the D-H
 9 group negotiated as part of a protection suite in the first message exchange of Phase 1
 10 for ISAKMP SA establishment. The PDSN shall specify Phase 1 authentication with
 11 certificates when the HA's certificate or HA's root CA certificate is available.

12 Otherwise, if a Dynamic pre-shared IKE secret distributed by the Home RADIUS server is
 13 available, the PDSN shall specify Phase 1 authentication with a pre-shared secret mode
 14 of operation. In this case, the PDSN shall specify Phase 1 Aggressive mode only. This is
 15 necessary in order that the KeyID field can be transmitted in the clear. The Home
 16 RADIUS server shall insure that the value of the 'S' key is hard to guess (i.e., a properly
 17 generated random number) in order to prevent dictionary attacks that are possible with
 18 Aggressive mode. If the PDSN has a statically configured IKE secret for the SA with the
 19 HA, then the PDSN shall specify Phase 1 authentication with pre-shared secret mode of
 20 operation. In this case the PDSN may either use Main Mode or use Aggressive Mode.

21 **Identification Payload:**

22 For Phase 1 negotiation, the PDSN shall set the Protocol-Id field to zero or UDP. The
 23 port number shall be set to zero or 500. If the HA receives any other values for these two
 24 fields in the Identification Payload, IKE negotiation shall be aborted.

25 For IKE authentication using pre-shared secret the PDSN and HA shall minimally support
 26 ID_KEY_ID in the ID Type field. For IKE authentication using Revised Public Key
 27 Encryption with RSA using X.509 certificates, the PDSN and HA shall minimally support
 28 ID_DER_ASN1_DN in the ID Type field.

29 For Phase 2 (Quick Mode), both the PDSN and HA shall include the client identifiers in
 30 the form of optional Client Identification Payloads as specified in IKE (i.e., IDci and IDcr).

31 To apply IPsec on all traffic between the PDSN and the HA, the PDSN and the HA shall
 32 exchange IDci and IDcr. The protocol and port number fields shall be "don't care" by
 33 setting them to 0 in both IDci and IDcr. The following is an example of the format of the
 34 client identifiers.

35 **IDCi: Protocol field = 0, Port = 0, Idtype = ID_IPV4_ADDR,**
 36 **Identification_data = PDSN_IPV4_ADDR.**

37 **IDCr: Protocol field = 0, Port = 0, Idtype = ID_IPV4_ADDR,**
 38 **Identification_data = HA_IPV4_ADDR.**

39 **Certificate Payload:**

40 The Certificate Payload shall carry X.509 version 3 certificates.

41 **Signature Payload:**

42 The PDSN and HA shall not include this payload.

43 **Notification Payload:**

44 The Notification Payload carries error messages and reason codes regarding failure for a
 45 peer to be able to establish a security association. The PDSN and HA handling of a failed
 46 security association establishment is specified in the main body of the standard.

- 1 The PDSN and HA shall use the "SA Lifetime Notify" code as a trigger to refresh the
- 2 indicated security association.
- 3 **Delete Payload:**
- 4 The PDSN shall send a delete payload upon a SA refresh or upon request from a service
- 5 provider administrator.

1 **Annex B: Certificates (normative)**

2 PDSNs and HAs shall use X.509 Version 3 certificates in conformance with RFC 2459. Each
3 PDSN and HA in a service provider network may have a unique certificate which will be
4 configured into the PDSN and HA. The method of configuration of certificates is outside the
5 scope of this document.

6 Note: This Annex only applies to FA CoA. Security between a collocated CoA MS and the HA is
7 outside the scope of this document.

8 Each service provider may be a Certificate Authority for itself and its client private networks and
9 partner ISPs for PDSNs and for HAs that may be accessed by PDSNs. All PDSNs and HAs shall
10 be configured with all service provider CA certificates. There should be one CA root certificate
11 from each service provider.

12 **Certificates for PDSNs and HAs:**

13 The Distinguished Name [RFC 2459] contained in the Issuer field is of form:

14 **cdma2000.service-provider-name**

15 The PDSN or HA determines the issuing service-provider (i.e., the CA) from the *service-provider-*
16 *name* attribute of the Issuer's Distinguished Name. The PDSN and HA then use the *service-*
17 *provider-name* attribute to locally access the CA's public key.

18 The PDSN and HA shall use the SHA-1 as a hash function and either the RSA or DSA signing
19 algorithm, as specified in RFC 2459 to verify a certificate. The private network or ISP shall
20 provide the public key and Distinguished Name of the certificate.

21 The Distinguished Name contained in the Subject field is of form:

22 **cdma2000. service-provider-name.PDSN.service-provider-identifier**

23 **cdma2000. service-provider-name.HA.service-provider-identifier**

24 Certificates in the PDSN and HA will not use the Unique-Identifier field.

25 Certificate extensions for PDSN and HA certificates shall not be supported.

26 The method of providing PDSNs and HAs signed certificates to PDSNs and HAs is outside the
27 scope of this document.

28 **CA Certificates:**

29 Service provider CA certificates shall be configured into all PDSNs and HAs. A service provider
30 CA contains the public key that the PDSN or HA shall use to verify the signature of a certificate
31 received in a Phase 1 ISAKMP exchange.

32 A CA certificate shall conform to the X.509 V3 certificates in RFC 2459. Since the service
33 provider CA distributes its own certificate, the Authority Key Identifier and Subject Key Identifier
34 extensions shall not be included in the certificate.

35 The method by which service providers exchange their CA certificates, as well as of providing
36 certificates into PDSNs and HAs, is outside the scope of this document.

37 **Certificate Revocation List (CRL):**

38 CRLs shall be used to store the identities of certificates that have been compromised or are
39 otherwise invalid. CRLs shall conform to X.509 v2 as specified in RFC 2459. A future version of
40 this document may make use of the Online Certificate Status Protocol.

- 1 Service providers shall exchange revoked certificate information (e.g., serial number). The
2 frequency of the exchange is outside the scope of this document.
- 3 Possession of a certificate does not imply service since the RADIUS server and Mobile IP
4 functions still control the user obtaining service, as well as the HA allowing access to the PDSN.
- 5 The CA certificate shall indicate the service provider CA as Issuer of the CRL. The DN of the
6 Issuer shall be of form:
- 7 **cdma2000.service-provider-name**
- 8 CRLs exchanged between service providers shall use the SHA-1 as a hash function and either
9 the RSA or the DSA signing algorithm as specified in RFC 2459.
- 10 CRL extensions shall not be supported.
- 11 The method of exchanging CRLs between service providers, or to conveying certificates client
12 private network or partnering ISP, as well providing this information into PDSNs and HAs, is
13 outside the scope of this document.

1 **Annex C: PDSN Timers** (normative)

2 The PDSN shall implement a PPP inactivity timer and may implement a PPP session timer and
3 may implement an accounting interval timer. These timers are defined as follows.

4 PPP inactivity timer (4-byte unsigned integer): This mandatory timer is configured with the
5 maximum number of consecutive seconds that a PPP session may be idle. When a PPP session
6 has been idle for this amount of time, the PPP session may be terminated depending on the
7 user's Always On status (see 3.2.1.8).

8 PPP session timer (4-byte unsigned integer): This optional timer is configured with the maximum
9 number of total seconds for which a PPP session may be established. When a PPP session has
10 been established for this amount of time, the PPP session is terminated, regardless of whether it
11 is active or idle.

12 Accounting interval timer (4-byte unsigned integer): This optional timer is configured with the
13 number of total seconds between when the PDSN sends periodic interim accounting messages
14 to the RADIUS server.

15 The PPP inactivity timer and PPP session timer use the value of 0 to indicate infinity. When
16 timers are set to an infinity value, they will never expire.

17 **PPP Inactivity Timer**

18 The PPP inactivity timer shall be locally configured on the PDSN with a default value that is used
19 for all PPP sessions. However, this default value may be overridden on a per session basis with
20 a RADIUS Idle-Timeout (28) attribute [RFC 2865] that is returned from the RADIUS server in a
21 RADIUS Access-Accept message.

22 For Mobile IP service, the PPP inactivity timer shall always be greater than the Mobile IP
23 registration lifetime. Thus, the PDSN shall always advertise to the MS a maximum allowed Mobile
24 IP registration lifetime smaller than the PPP inactivity timer value currently in use for the PPP
25 session. The PDSN shall ignore a non-zero RADIUS Idle-Timeout value received in a RADIUS
26 Access-Accept message for a Mobile IP session, which is smaller than current PPP inactivity
27 timer for the PPP session. The PDSN may honor the RADIUS-Idle-Timeout value received in a
28 RADIUS Access-Accept message for a Mobile IP session if the received value is greater than the
29 one currently in use for the PPP session.

30 In case of Simple IP service, if the PPP session is marked as "Always-On" then the PDSN shall
31 perform the link status determination procedure upon expiry of the PPP inactivity timer [see
32 section 3.2.1.8].

33 **PPP Session Timer**

34 If the PPP session timer is used, then it shall be locally configured on the PDSN with a default
35 value that is used for all PPP sessions. However, this default value may be overridden on a per
36 session basis with a RADIUS Session-Timeout (27) attribute [RFC 2865] that is returned from the
37 RADIUS server in a RADIUS Access-Accept message. For Always On users, the PDSN shall
38 discard the PPP session timer.

39 In the case of multiple MIP sessions over a single PPP session, it is possible that the PDSN
40 receives different RADIUS-Session-Timeout values from different home networks. In this case,
41 the PDSN may honor the initial RADIUS-Session-Timeout value that it received and shall ignore
42 all subsequent RADIUS-Session-Timeout values that it receives.

43 **Accounting Interval Timer**

1 If the accounting interval timer is used, then it shall be locally configured on the PDSN with a
2 default value that is used for all sessions. However, this default value may be overridden on a per
3 session basis with a RADIUS Acct-Interim-Interval (85) attribute [RFC 2869] that is returned from
4 the RADIUS server in a RADIUS Access-Accept message. For a session using the prepaid
5 service, the RADIUS Acct-Interim-Interval shall not be used and the interval timer shall be
6 interpreted as per X.S0011-006-C (PrePaid Packet Data Service).