

3GPP2 X.S0059-100-A

Version 1.0

Date: December 2011



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

---

## ***cdma2000 Femtocell Network: Packet Data Network Aspects***

### **COPYRIGHT 2011**

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](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.

## Revision History

---

<b>Revision</b>	<b>Description of Changes</b>	<b>Date</b>
Rev. 0 v1.0	Initial Publication	January 2010
Rev. A v1.0	Updated Publication	December 2011

## cdma2000 Femtocell Network: Packet Data Network Aspects

**CONTENTS**

1	List of Figures .....	iv
2	List of Tables.....	v
3	Foreword .....	vi
4	1 Introduction .....	1
5	1.1 Scope.....	1
6	2 References.....	2
7	2.1 Normative References.....	2
8	2.2 Informative References .....	5
9	3 FAP Network Connectivity Procedures .....	6
10	3.1 General.....	6
11	3.2 Tunnel Management Procedures.....	6
12	3.2.1 Discovery and Selection of SeGW from FAP .....	6
13	3.2.2 Tunnel Establishment .....	7
14	3.2.3 Tunnel Disconnection.....	8
15	3.3 Authentication and Authorization.....	9
16	3.3.1 Authentication Procedures.....	9
17	3.4 FAP Auto-configuration .....	10
18	3.4.1 FMS Discovery.....	10
19	3.4.2 FAP Auto-configuration Procedures .....	11
20	3.4.3 Location Determination of the FAP.....	11
21	3.5 Quality of Service (QoS) Considerations.....	12
22	3.5.1 CHILD_SA.....	12
23	3.5.2 Reverse Link Packet Classifier in FAP.....	13
24	4 Mobility Management.....	14
25	5 Local IP Access for HRPD.....	15
26	5.1 LIPA Requirements and Procedures .....	16
27	5.1.1 LIPA Protocol Reference Model .....	16
28	5.1.2 AN-PPP Session .....	17
29	5.1.3 Addressing with IPCP .....	18
30	5.1.4 PPP Framing.....	21
31	5.1.5 Ingress Address Filtering at the FAP.....	21
32	5.1.6 Egress Address Filtering/Routing at the MS .....	21
33	6 Remote IP Access .....	23
34	6.1 General.....	23
35	6.2 Discovery and Selection of SeGW by MS .....	24

6.2.1	MS Requirements .....	24	1
6.2.2	SeGW Requirements .....	25	2
6.2.3	Femtocell AAA Requirement .....	25	3
6.2.4	Home AAA Requirements .....	25	4
6.3	Remote IP Access Tunnel Establishment .....	25	5
6.3.1	IKEv2 PSK Key Generation .....	26	6
6.3.2	MS Requirements .....	26	7
6.3.3	SeGW Requirements .....	28	8
6.3.4	Home AAA Requirements .....	30	9
6.3.5	FAP Requirements .....	31	10
6.4	IP Traffic Processing for Remote IP Access .....	31	11
6.4.1	MS Requirements .....	31	12
6.4.2	FAP Requirements .....	32	13
6.4.3	SeGW Requirements .....	32	14
6.5	Tunnel Disconnection .....	33	15
6.5.1	MS Procedures .....	33	16
6.5.2	SeGW Requirements .....	33	17
6.5.3	Home AAA Requirements .....	33	18
6.5.4	FAP Requirements .....	34	19
7	Accounting .....	35	20
8	RADIUS Considerations .....	36	21
8.1	RADIUS Attributes between SeGW and Femtocell AAA for FAP Authorization .....	36	22
8.2	RADIUS Attributes between SeGW and HAAA for RIPA .....	36	23
8.3	RADIUS Attributes between FAP and AN- AAA for LIPA .....	38	24
8.4	RADIUS Vendor Specific Attributes .....	38	25
8.4.1	Session-Key-Method .....	38	26
8.4.2	RIPA-Info .....	39	27
8.4.3	Local-IP-Access-Authorized .....	39	28
9	Diameter Considerations .....	41	29
9.1	Diameter Applications and Commands .....	41	30
9.1.1	FAP Authorization .....	41	31
9.1.2	RIPA Authentication .....	41	32
9.2	Diameter AVPs .....	45	33
9.2.1	Master-Security-Association .....	46	34
9.2.2	SFF-KEY-Nonces .....	46	35
9.2.3	RIPA-Info .....	47	36
9.3	Experimental Result-Code AVP Values .....	47	37
9.3.1	Permanent Failures .....	47	38
10	eHRPD Packet Data Femtocell Operation .....	48	39
A	Annex – Call Flow Examples (Informative) .....	49	40
A.1	Femtocell Network Connectivity Call Flow .....	49	41
A.1.1	Femtocell Network Connectivity Call Flow without Redirection .....	49	42
			43
			44
			45
			46
			47
			48
			49
			50
			51
			52
			53
			54
			55
			56
			57
			58
			59

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

- A.1.2 Femtocell Network Connectivity Call Flow with Redirection to Serving System ..... 50
- A.2 SeGW Discovery ..... 52
- A.3 FAP-SeGW IPsec Tunnel Establishment..... 52
- A.4 Local IP Access Call Flows ..... 54
  - A.4.1 Successful LIPA Session Establishment..... 55
  - A.4.2 LIPA not Supported at MS ..... 56
  - A.4.3 LIPA Terminated after Handoff ..... 58
- A.5 Remote IP Access Call Flows..... 59
  - A.5.1 Redirection Based SeGW Discovery with EAP Authentication..... 59
  - A.5.2 Redirection Based SeGW Discovery with IKEv2 PSK Authentication ..... 60
  - A.5.3 Tunnel Establishment for Remote IP Address with EAP Authentication..... 62
  - A.5.4 Tunnel Establishment for Remote IP Access with IKEv2 PSK Authentication ..... 63

## LIST OF FIGURES

---

Figure 1	Example of Security Associations and associated QoS classes of traffic with two SAs.....	12
Figure 2	IP Access Bearer and Interfaces.....	15
Figure 3	HRPD LIPA Protocol Reference Model.....	16
Figure 4	Femtocell Remote IP Access Architecture .....	23
Figure 5	Femtocell Network Connectivity Call Flow without Redirection.....	49
Figure 6	Femtocell Network Connectivity with Redirection .....	51
Figure 7	SeGW Discovery .....	52
Figure 8	IPsec Tunnel Establishment.....	53
Figure 9	Successful LIPA Session Establishment.....	55
Figure 10	LIPA not Supported by MS: Session Establishment Failure .....	57
Figure 11	LIPA Terminated After Handoff.....	58
Figure 12	Redirection Based SeGW Discovery with EAP Authentication .....	59
Figure 13	Redirection Based SeGW Discovery with IKEv2 PSK Authentication.....	61
Figure 14	Tunnel Establishment for Remote IP Access with EAP Authentication.....	62
Figure 15	Tunnel Establishment for Remote IP Access with IKEv2 PSK Authentication .....	64

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# LIST OF TABLES

---

1			
2			
3			
4	Table 1	IPCP Vendor Specific Option.....	21
5	Table 2	Value(s) Field for the IPv4 Packet Filter Criteria.....	22
6	Table 3	Value(s) Field for the IPv6 Packet Filter Criteria.....	22
7	Table 4	Additional Parameters in A10 Connection Setup Airlink Fields.....	35
8	Table 5	Additional Parameters in PDSN UDR.....	35
9	Table 6	Additional Accounting Parameter Attribute RADIUS Definitions.....	35
10	Table 7	Meaning of the Request, Accept, Reject, Challenge columns of Table 8 and Table 9.....	36
11	Table 8	RADIUS Attributes exchanged between the SeGW and the Femtocell AAA for FAP Authorization.....	36
12			
13	Table 9	RADIUS Attributes exchanged between the SeGW and the HAAA.....	37
14	Table 10	Additional RADIUS Attributes exchanged between the FAP and AN- AAA for LIPA.....	38
15	Table 11	Session-Key-Method VSA.....	38
16	Table 12	RIPA-Info VSA.....	39
17	Table 13	Local-IP-Access-Authorized VSA.....	39
18	Table 14	Diameter Command Codes for FAP Authorization.....	41
19	Table 15	Diameter Command Codes for EAP based IKEv2.....	42
20	Table 16	Diameter Command Codes for PSK based IKEv2.....	43
21	Table 17	Meaning of the Request, Answer columns.....	45
22	Table 18	Diameter AVP exchanged between the SeGW and the HAAA.....	45
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			

# FOREWORD

---

(This foreword is not part of this specification.)

This document was prepared by the Third Generation Partnership Project 2 (3GPP2).

This document is Revision A of X.S0059-100. eHRPD Femtocells are newly supported.

This document is part of a multi-part document consisting of multiple parts that together describes specifications for cdma2000 Femtocell Network.

This document is subject to change following formal approval. Should this document be modified, it will be re-released with a change of release date and an identifying change in version number as follows:

X.S0059-100-X-n

where:

- X an uppercase numerical or alphabetic character [A, B, C, ...] that represents the revision level.
- n a numeric string [1, 2, 3, ...] that indicates a point release level.

Note that there is one annex section in this document. Annex A is informative and not considered part of this document.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# 1 Introduction

---

This document provides a packet data specifications for the HRPD, eHRPD and 1x packet data Femtocell network.

## 1.1 Scope

---

This series of documents defines packet data specifications for an HRPD, eHRPD and 1x packet data Femtocell network that can support existing services provided by HRPD, eHRPD and 1x. This revision of the Femtocell network specification includes the following capabilities:

- FAP-SeGW Tunnel Management
- FAP Authentication and Authorization
- FAP Auto-Configuration
- Quality of Service (QoS) Support between FAP and SeGW
- FAP Remote IP Access
- Mobility Management between macro cell and Femtocell
- Accounting Enhancements
- FAP Local IP Access

## 1.2 Document Conventions

---

“Shall” and “shall not” identify requirements to be followed strictly to conform to this document and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the document. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical or causal.

## 2 References

---

### 2.1 Normative References

---

This section provides references to other specifications and standards that are necessary to implement this document.

References are either specific (identified by date of publication, revision identifier, and version number) or non-specific.

- For a specific reference, subsequent revisions may not apply.
- For a non-specific reference, the latest revision applies.

- [1] 3GPP2: A.S0024-A v1.0, “Interoperability Specification (IOS) for Femtocell Access Points”; April 2011.
- [2] 3GPP2: X.S0011-D v2.0, “cdma2000 Wireless IP Network Standard”; November 2008.
- [3] 3GPP2: X.S0044-0 v1.0, “MIPv4 Enhancements”; September 2010.
- [4] 3GPP2: X.S0047-0 v1.0, “MIPv6 Enhancements”; February 2009.
- [5] 3GPP2: X.S0061-0 v1.0, “Network PMIP Support”; December 2008.
- [6] 3GPP2: S.S0132, “Femtocell Security Framework”; January 2010.
- [7] 3GPP2: X.S0059-200-A v1.0, “cdma2000 Femtocell Network: 1x and IMS Network Aspects”; September 2011.
- [8] 3GPP2: C.S0005, “Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems”.
- [9] 3GPP2: C.S0024, “cdma2000 High Rate Packet Data Air Interface Specification”.
- [10] IETF: RFC 4306, Kaufman, “Internet Key Exchange (IKEv2) Protocol”; December 2005.
- [11] IETF: RFC 3948, Huttunen, et. al., “UDP Encapsulation of IPsec ESP Packets”; January 2005.
- [12] IETF: RFC 2406, Kent, et. al., “IP Encapsulating Security Payload (ESP)”; November 1998.
- [13] IETF: RFC 5176, Chiba, et. al., “Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)”; January 2008.
- [14] IETF: RFC 4005, Calhoun, et. al., “Diameter Network Access Server Application”; August 2005.
- [15] Broadband Forum: TR-069 Amendment 2, “CPE WAN Management Protocol v1.1”; December 2007.
- [16] 3GPP2: X.S0063-0 v1.0, “Femtocell Management Object”, TBD

[Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor's Note is removed, the inclusion of the above document is for informational purposes only.]

- 1  
2  
3  
4  
5 [17] IETF: RFC 5280, D. Cooper, et. al., "Internet X.509 Public Key  
6 Infrastructure Certificate and Certificate Revocation List (CRL) Profile";  
7 May 2008.  
8  
9 [18] IETF: RFC 1541, R. Droms, "Dynamic Host Configuration Protocol";  
10 March 1997.  
11  
12 [19] IETF: RFC 3315, R. Droms, et. al., "Dynamic Host Configuration Protocol  
13 for IPv6 (DHCPv6)"; July 2003.  
14  
15 [20] IETF: RFC 5685, Devarapalli, et. al., "Redirect Mechanism for the Internet  
16 Key Exchange Protocol Version 2 (IKEv2)"; November 2009.  
17  
18 [21] IETF: RFC 5295, J. Salowey, et. al., "Specification for the Derivation of  
19 Root Keys from an Extended Master Session Key (EMSK)"; August 2008.  
20  
21 [22] National Institute of Standards and Technology: "Secure Hash Standard",  
22 FIPS 180-2, With Change Notice 1 dated February 2004: August 2002.  
23  
24 [23] IETF: RFC 4187, J. Arko, "Extensible Authentication Protocol Method for  
25 3rd Generation Authentication and Key Agreement (EAP-AKA)";  
26 January 2006.  
27  
28 [24] IETF: RFC 3579, B. Aboba, P. Calhoun, "RADIUS Support for EAP";  
29 September 2003.  
30  
31 [25] IETF: RFC 826, D. C. Plummer, "An Ethernet Address Resolution  
32 Protocol"; November 1982.  
33  
34 [26] IETF: RFC 2548, G. Zorn, "Microsoft Vendor-specific RADIUS  
35 Attributes"; March 1999.  
36  
37 [27] IETF: RFC 2401, S. Kent, "Security Architecture for the Internet Protocol";  
38 November 1998.  
39  
40 [28] IETF: RFC 2865, C. Rigney, et. al., "Remote Authentication Dial In User  
41 Service (RADIUS)"; June 2000.  
42  
43 [29] IETF: RFC 3588, P. Calhoun, et. al., "Diameter Base Protocol";  
44 September 2003.  
45  
46 [30] IETF: RFC 4072, P. Eronen, et. al., "Diameter Extensible Authentication  
47 Protocol (EAP) Application"; August 2005.  
48  
49 [31] IETF: draft-ietf-dime-ikev2-psk-diameter-08  
50  
51 [Editor Note: The above document is a work in progress and should not be referenced  
52 unless and until it is approved and published. Until such time as this Editor's Note is  
53 removed, the inclusion of the above document is for informational purposes only.]  
54  
55 [32] Broadband Forum: TR-106 Amendment 3, Data Model Template for TR-  
56 069-Enabled Devices; September 2009.  
57  
58 [33] Broadband Forum: TR-131, ACS Northbound Interface Requirements;  
59 November 2009  
60  
61 [34] IETF: RFC 1332, The PPP Internet Protocol Control Protocol (IPCP);  
62 May 1992.

[35]	IETF: RFC 1334, PPP Authentication Protocols; October 1992.	1
[36]	IETF: RFC 1661, Point-to-Point Protocol; July 1994.	2
[37]	IETF: RFC 1662, PPP in HDLC-Like Framing; July 1994.	3
[38]	IETF: RFC 1877, PPP Internet Protocol Control Protocol Extensions for Name Server Addresses; December 1995.	4
[39]	IETF: RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP); August 1996.	5
[40]	IETF: RFC 2153, PPP Vendor Extensions; May 1997.	6
[41]	IETF: RFC 2460, Internet Protocol, Version 6 (IPv6) Specification; December 1998.	7
[42]	IETF: RFC 2461, “Neighbor Discovery for IP Version 6 (IPv6); December 1998.	8
[43]	IETF: RFC 2462, “IPv6 Stateless Address Auto-configuration”; December 1998.	9
[44]	IETF: RFC 2463, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification RFC 2463”; December 1998.	10
[45]	IETF: RFC 2472, “IP Version 6 over PPP”; December 1998.	11
[46]	IETF: RFC 3513, “IP Version 6 Addressing Architecture”; April 2003.	12
[47]	IETF: RFC 3587, “IPv6 Global Unicast Address Format”; August 2003.	13
[48]	IETF: RFC 3646, “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”; December 2003.	14
[49]	IETF: RFC 3736, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”; April 2004.	15
[50]	3GPP2: C.S0087, “E-UTRAN - cdma2000 HRPD Connectivity and Interworking Air Interface”.	16
[51]	3GPP2: X.S0057, “E-UTRAN – eHRPD Connectivity and Interworking: Core Network Aspects”.	17
[52]	3GPP2: A.S0022, “Interoperability Specification (IOS) for Evolved High Rate Packet Data (eHRPD) Radio Access Network Interfaces and Interworking with Enhanced Universal Terrestrial Radio Access Network (E-UTRAN)”.	18
[53]	3GPP2: A.S0008-C v2.0, “Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network”; January 2009.	19
[54]	3GPP2: A.S0009-C v2.0, “Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function”; January 2009.	20
		21
		22
		23
		24
		25
		26
		27
		28
		29
		30
		31
		32
		33
		34
		35
		36
		37
		38
		39
		40
		41
		42
		43
		44
		45
		46
		47
		48
		49
		50
		51
		52
		53
		54
		55
		56
		57
		58
		59

## 2.2 Informative References

---

This section provides references to other documents that may be useful for the reader of this document.

- <1> 3GPP2: A.S0017-D v2.0, "Interoperability Specification (IOS) for cdma2000 Access Network Interfaces - Part 7 (A10 and A11 Interfaces)"; August 2009.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## 3 FAP Network Connectivity Procedures

### 3.1 General

Before the FAP can serve the cdma2000<sup>®1</sup> MS, the FAP completes the neighborhood discovery (see [1]) and network connectivity procedures.

Network connectivity procedures of the FAP include the following procedures:

- SeGW discovery and secure tunnel establishment procedures as described in section 3.2;
- FAP mutual authentication with the SeGW and the FAP authorization procedures as described in section 3.3;
- FAP auto-configuration procedures as described in section 3.4;
- 1x RTT capable FAP registration procedures as described in [7].

To be able to perform network connectivity procedures, the FAP needs to be configured by means outside the scope of this document with the following minimum information:

- FEID and associated security parameters (see [6]);
- Home Domain Name.

In addition, the FAP can be pre-configured with the SeGW's FQDN(s) or IP address(es) and the FSM URL.

### 3.2 Tunnel Management Procedures

#### 3.2.1 Discovery and Selection of SeGW from FAP

If the FAP needs to obtain the IP address of the SeGW, the FAP shall use the FQDN of the SeGW and DNS mechanisms to retrieve the IP address of the SeGW.

The FQDN may be pre-provisioned in the FAP, otherwise, the FAP shall perform the following using the preconfigured home domain name for SeGW discovery:

- If FAP has obtained BASE\_ID, NID and SID over 1x air interface (see [8]), the FAP shall build FQDN of SeGW by using the format of <1x-BASE\_ID>.<NID>.<SID>.1x.SeGW.<home domain name> for the DNS request, where, <1x-BASE\_ID>, <NID>, and <SID> shall be encoded using hexadecimal uppercase ASCII characters.
- If the FAP has obtained the HRPD Subnet and HRPD SectorID over the HRPD air interface (see [9]), the FAP shall build the FQDN of the SeGW by using the format of <HRPD-SectorID>.<HRPD-Subnet>.HRPD.SeGW.<home domain name> for the

<sup>1</sup> cdma2000<sup>®</sup> 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 DNS request, where, <HRPD-Subnet> and <HRPD-SectorID> shall be encoded as  
2 hexadecimal uppercase in ASCII characters.

- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 73
- 74
- 75
- 76
- 77
- 78
- 79
- 80
- 81
- 82
- 83
- 84
- 85
- 86
- 87
- 88
- 89
- 90
- 91
- 92
- 93
- 94
- 95
- 96
- 97
- 98
- 99
- 100
- 101
- 102
- 103
- 104
- 105
- 106
- 107
- 108
- 109
- 110
- 111
- 112
- 113
- 114
- 115
- 116
- 117
- 118
- 119
- 120
- 121
- 122
- 123
- 124
- 125
- 126
- 127
- 128
- 129
- 130
- 131
- 132
- 133
- 134
- 135
- 136
- 137
- 138
- 139
- 140
- 141
- 142
- 143
- 144
- 145
- 146
- 147
- 148
- 149
- 150
- 151
- 152
- 153
- 154
- 155
- 156
- 157
- 158
- 159
- 160
- 161
- 162
- 163
- 164
- 165
- 166
- 167
- 168
- 169
- 170
- 171
- 172
- 173
- 174
- 175
- 176
- 177
- 178
- 179
- 180
- 181
- 182
- 183
- 184
- 185
- 186
- 187
- 188
- 189
- 190
- 191
- 192
- 193
- 194
- 195
- 196
- 197
- 198
- 199
- 200
- 201
- 202
- 203
- 204
- 205
- 206
- 207
- 208
- 209
- 210
- 211
- 212
- 213
- 214
- 215
- 216
- 217
- 218
- 219
- 220
- 221
- 222
- 223
- 224
- 225
- 226
- 227
- 228
- 229
- 230
- 231
- 232
- 233
- 234
- 235
- 236
- 237
- 238
- 239
- 240
- 241
- 242
- 243
- 244
- 245
- 246
- 247
- 248
- 249
- 250
- 251
- 252
- 253
- 254
- 255
- 256
- 257
- 258
- 259
- 260
- 261
- 262
- 263
- 264
- 265
- 266
- 267
- 268
- 269
- 270
- 271
- 272
- 273
- 274
- 275
- 276
- 277
- 278
- 279
- 280
- 281
- 282
- 283
- 284
- 285
- 286
- 287
- 288
- 289
- 290
- 291
- 292
- 293
- 294
- 295
- 296
- 297
- 298
- 299
- 300
- 301
- 302
- 303
- 304
- 305
- 306
- 307
- 308
- 309
- 310
- 311
- 312
- 313
- 314
- 315
- 316
- 317
- 318
- 319
- 320
- 321
- 322
- 323
- 324
- 325
- 326
- 327
- 328
- 329
- 330
- 331
- 332
- 333
- 334
- 335
- 336
- 337
- 338
- 339
- 340
- 341
- 342
- 343
- 344
- 345
- 346
- 347
- 348
- 349
- 350
- 351
- 352
- 353
- 354
- 355
- 356
- 357
- 358
- 359
- 360
- 361
- 362
- 363
- 364
- 365
- 366
- 367
- 368
- 369
- 370
- 371
- 372
- 373
- 374
- 375
- 376
- 377
- 378
- 379
- 380
- 381
- 382
- 383
- 384
- 385
- 386
- 387
- 388
- 389
- 390
- 391
- 392
- 393
- 394
- 395
- 396
- 397
- 398
- 399
- 400
- 401
- 402
- 403
- 404
- 405
- 406
- 407
- 408
- 409
- 410
- 411
- 412
- 413
- 414
- 415
- 416
- 417
- 418
- 419
- 420
- 421
- 422
- 423
- 424
- 425
- 426
- 427
- 428
- 429
- 430
- 431
- 432
- 433
- 434
- 435
- 436
- 437
- 438
- 439
- 440
- 441
- 442
- 443
- 444
- 445
- 446
- 447
- 448
- 449
- 450
- 451
- 452
- 453
- 454
- 455
- 456
- 457
- 458
- 459
- 460
- 461
- 462
- 463
- 464
- 465
- 466
- 467
- 468
- 469
- 470
- 471
- 472
- 473
- 474
- 475
- 476
- 477
- 478
- 479
- 480
- 481
- 482
- 483
- 484
- 485
- 486
- 487
- 488
- 489
- 490
- 491
- 492
- 493
- 494
- 495
- 496
- 497
- 498
- 499
- 500
- 501
- 502
- 503
- 504
- 505
- 506
- 507
- 508
- 509
- 510
- 511
- 512
- 513
- 514
- 515
- 516
- 517
- 518
- 519
- 520
- 521
- 522
- 523
- 524
- 525
- 526
- 527
- 528
- 529
- 530
- 531
- 532
- 533
- 534
- 535
- 536
- 537
- 538
- 539
- 540
- 541
- 542
- 543
- 544
- 545
- 546
- 547
- 548
- 549
- 550
- 551
- 552
- 553
- 554
- 555
- 556
- 557
- 558
- 559
- 560
- 561
- 562
- 563
- 564
- 565
- 566
- 567
- 568
- 569
- 570
- 571
- 572
- 573
- 574
- 575
- 576
- 577
- 578
- 579
- 580
- 581
- 582
- 583
- 584
- 585
- 586
- 587
- 588
- 589
- 590
- 591
- 592
- 593
- 594
- 595
- 596
- 597
- 598
- 599
- 600
- 601
- 602
- 603
- 604
- 605
- 606
- 607
- 608
- 609
- 610
- 611
- 612
- 613
- 614
- 615
- 616
- 617
- 618
- 619
- 620
- 621
- 622
- 623
- 624
- 625
- 626
- 627
- 628
- 629
- 630
- 631
- 632
- 633
- 634
- 635
- 636
- 637
- 638
- 639
- 640
- 641
- 642
- 643
- 644
- 645
- 646
- 647
- 648
- 649
- 650
- 651
- 652
- 653
- 654
- 655
- 656
- 657
- 658
- 659
- 660
- 661
- 662
- 663
- 664
- 665
- 666
- 667
- 668
- 669
- 670
- 671
- 672
- 673
- 674
- 675
- 676
- 677
- 678
- 679
- 680
- 681
- 682
- 683
- 684
- 685
- 686
- 687
- 688
- 689
- 690
- 691
- 692
- 693
- 694
- 695
- 696
- 697
- 698
- 699
- 700
- 701
- 702
- 703
- 704
- 705
- 706
- 707
- 708
- 709
- 710
- 711
- 712
- 713
- 714
- 715
- 716
- 717
- 718
- 719
- 720
- 721
- 722
- 723
- 724
- 725
- 726
- 727
- 728
- 729
- 730
- 731
- 732
- 733
- 734
- 735
- 736
- 737
- 738
- 739
- 740
- 741
- 742
- 743
- 744
- 745
- 746
- 747
- 748
- 749
- 750
- 751
- 752
- 753
- 754
- 755
- 756
- 757
- 758
- 759
- 760
- 761
- 762
- 763
- 764
- 765
- 766
- 767
- 768
- 769
- 770
- 771
- 772
- 773
- 774
- 775
- 776
- 777
- 778
- 779
- 780
- 781
- 782
- 783
- 784
- 785
- 786
- 787
- 788
- 789
- 790
- 791
- 792
- 793
- 794
- 795
- 796
- 797
- 798
- 799
- 800
- 801
- 802
- 803
- 804
- 805
- 806
- 807
- 808
- 809
- 810
- 811
- 812
- 813
- 814
- 815
- 816
- 817
- 818
- 819
- 820
- 821
- 822
- 823
- 824
- 825
- 826
- 827
- 828
- 829
- 830
- 831
- 832
- 833
- 834
- 835
- 836
- 837
- 838
- 839
- 840
- 841
- 842
- 843
- 844
- 845
- 846
- 847
- 848
- 849
- 850
- 851
- 852
- 853
- 854
- 855
- 856
- 857
- 858
- 859
- 860
- 861
- 862
- 863
- 864
- 865
- 866
- 867
- 868
- 869
- 870
- 871
- 872
- 873
- 874
- 875
- 876
- 877
- 878
- 879
- 880
- 881
- 882
- 883
- 884
- 885
- 886
- 887
- 888
- 889
- 890
- 891
- 892
- 893
- 894
- 895
- 896
- 897
- 898
- 899
- 900
- 901
- 902
- 903
- 904
- 905
- 906
- 907
- 908
- 909
- 910
- 911
- 912
- 913
- 914
- 915
- 916
- 917
- 918
- 919
- 920
- 921
- 922
- 923
- 924
- 925
- 926
- 927
- 928
- 929
- 930
- 931
- 932
- 933
- 934
- 935
- 936
- 937
- 938
- 939
- 940
- 941
- 942
- 943
- 944
- 945
- 946
- 947
- 948
- 949
- 950
- 951
- 952
- 953
- 954
- 955
- 956
- 957
- 958
- 959
- 960
- 961
- 962
- 963
- 964
- 965
- 966
- 967
- 968
- 969
- 970
- 971
- 972
- 973
- 974
- 975
- 976
- 977
- 978
- 979
- 980
- 981
- 982
- 983
- 984
- 985
- 986
- 987
- 988
- 989
- 990
- 991
- 992
- 993
- 994
- 995
- 996
- 997
- 998
- 999
- 1000

The FAP determines the IP address of the DNS server by means that are outside the scope of this document.

## 3.2.2 Tunnel Establishment

---

The tunnel establishment message exchange to setup the IPsec tunnel between the FAP and the SeGW is shown in A.3.

### 3.2.2.1 FAP Requirements

---

The FAP shall support the IKEv2 procedure for key exchange and IPsec tunnel establishment with the SeGW. The FAP shall support the NAT traversal per IKEv2 [10] and the UDP encapsulation of IPsec ESP in tunnel mode [11]. The FAP shall support IPv4 and may support IPv6 for inner IP address. Upon selection of the SeGW, the FAP shall initiate Internet Key Exchange [10] by sending the IKE\_SA\_INIT Request message to the SeGW in order to establish secure IP tunnel with the SeGW. Upon receiving the IKE\_SA\_INIT Response message, the FAP shall send the IKE\_AUTH Request message to the SeGW.

Upon receiving the IKE-AUTH Response message from the SeGW, the FAP shall establish an IPsec ESP tunnel to the SeGW according to [12].

### 3.2.2.2 SeGW Procedure

---

The SeGW shall support the IKEv2 procedure for key exchange and IPsec tunnel establishment with the FAP. The SeGW shall support the NAT traversal per IKEv2 [10] and the UDP encapsulation of IPsec ESP packets [11]. The SeGW shall support both IPv4 and IPv6 as inner IP address for the IPsec tunnel.

Upon receiving the IKE SA\_INIT Request message, the SeGW shall perform IKEv2 procedures by sending the IKE SA\_INIT Response message [10] in order to establish a secure IP tunnel with the FAP.

If the operator policy requires Femtocell subscription authorization, upon receiving IKE\_AUTH request from the FAP, after successful authentication (see section 3.3), the SeGW shall send RADIUS Access-Request or Diameter AAR command to the Femtocell AAA including NAI which uses FEID in FQDN format as the username in NAI format (i.e., FAP-FQDN@realm) to verify that the FAP identified by FEID is authorized to provide service. If the RADIUS Access-Accept message or Diameter AAA command is received from the Femtocell AAA indicating successful authorization, the SeGW shall continue IKEv2 procedures by sending an IKE\_AUTH Response message to the FAP. If a RADIUS Access Reject or Diameter AAA command with Experimental Result-Code AVP (see section 9.3) is

received from Femtocell AAA, the SeGW shall send an IKEv2 Notification message to the FAP indicating authorization failure.

Upon completion of the IKEv2 procedures, the SeGW shall establish an IPsec in ESP tunnel mode between itself and the FAP [12].

### 3.2.2.3 Femtocell AAA Requirements

---

The Femtocell AAA shall perform service authorization for the FAP if operator's policy dictates so.

#### 3.2.2.3.1 Diameter Authorization Procedures

---

Upon receipt of an Diameter AAR command, the Femtocell AAA shall check for the FAP authorization information. If there is no authorization information for the FAP (identified by FEID), the Femtocell AAA shall return a Diameter AAA command with the Experimental-Result-Code set to DIAMETER\_ERROR\_NO\_FAP\_AUTHORIZATION to the SeGW. If the Femtocell AAA has authorization information for the FAP, the Femtocell AAA shall send a Diameter AAA command with DIAMETER\_SUCCESS in the Result code AVP indicating successful authorization to the SeGW.

#### 3.2.2.3.2 RADIUS Authorization Procedures

---

Upon receipt of a RADIUS Access-Request message from the SeGW, the Femtocell AAA shall check for the FAP authorization information. If there is no FAP authorization information for the FAP (identified by FEID), the Femtocell AAA shall return a RADIUS Access-Reject message to the SeGW. If the Femtocell AAA has authorization information for the FAP, the Femtocell AAA shall send a RADIUS Access-Accept message to the SeGW.

### 3.2.3 Tunnel Disconnection

---

Tunnel disconnection may be initiated from the FAP or from the SeGW, e.g., due to a timeout of the IKE SA lifetime set internally in the FAP or SeGW, or due to a request from the Femtocell AAA server.

The tunnel disconnection message exchanges between the FAP and the SeGW are performed via IKEv2.

#### 3.2.3.1 FAP Procedures

---

The FAP shall use the procedures specified in IKEv2 [10] to delete one or more IPsec tunnel(s) to the SeGW.

#### 3.2.3.2 SeGW Procedures

---

The SeGW shall use the procedures specified in IKEv2 [10] to delete IPsec tunnel to the FAP.

Upon reception of either the RADIUS Disconnect-Request message [13] or Diameter Abort-Session-Request command [14] from the Femtocell AAA (for the Femtocell AAA initiated tunnel disconnection), the SeGW shall check whether the FAP has any active SA(s). If the check indicates that the referenced SAs exist, the SeGW shall perform tunnel disconnection procedures for all the IPsec SA(s) and IKE\_SA by sending the IKEv2 INFORMATIONAL request message with Protocol ID set to 1 (IKE) in the DELETE payload to the FAP.

1 Otherwise, the SeGW shall send a RADIUS Disconnect-NAK or Diameter Abort-Session-  
2 Answer with Result-Code AVP set to DIAMETER\_UNKNOWN\_SESSION\_ID or  
3 DIAMETER\_UNABLE\_TO\_COMPLY to the Femtocell AAA.  
4

5  
6 If the SeGW does not receive an IKEv2 INFORMATIONAL response from the FAP, it shall  
7 resend the INFORMATIONAL message with the same DELETE payloads that it sent before.  
8 After resending the INFORMATIONAL message to the FAP for a configurable number of  
9 times (e.g., using an exponential backoff algorithm), if the SeGW still does not receive any  
10 response from the FAP, the SeGW assumes that the FAP has disconnected and removes all  
11 incoming and outgoing SAs for the FAP.  
12

13  
14 If the SeGW receives an IKEv2 INFORMATIONAL response from the FAP without any  
15 DELETE payload, the SeGW shall remove all the SAs corresponding for the FAP.  
16

### 17 **3.2.3.3 Femtocell AAA Procedures**

---

18  
19 When the FAP subscription for the user to access cdma2000 packet data services has been  
20 deleted/prohibited, the Femtocell AAA shall instruct the SeGW to disconnect a particular  
21 session for a specific FAP by sending the RADIUS Disconnect-Request or Diameter Abort-  
22 Session-Request message.  
23  
24

## 25 **3.3 Authentication and Authorization**

---

26  
27 This section describes the authentication and authorization procedures between the FAP and  
28 the SeGW.  
29

### 30 **3.3.1 Authentication Procedures**

---

#### 31 **3.3.1.1 General**

---

32  
33 In order to establish a connection to the cdma2000 home network, the FAP performs  
34 authentication with a SeGW located in the home network. If the policy of the home network  
35 requires authorization of the FAP before access to the network can be granted, the SeGW  
36 contacts the Femtocell AAA using either RADIUS or Diameter protocol.  
37  
38  
39

#### 40 **3.3.1.2 FAP Authentication**

---

41  
42 The authentication between the FAP and the SeGW (referred to as the FAP authentication)  
43 shall be performed using IKEv2 with X.509 digital certificates.  
44  
45

46  
47 The FAP shall be authenticated by the SeGW using the FAP's certificate. The FAP's  
48 certificate is installed by the FAP vendor during its manufacturing. The FAP certificate shall  
49 be compliant to [17] and shall support the FAP certificate profile specified in [6].  
50

51  
52 The FAP certificate is identified using the device identifier of the FAP (i.e., FEID) and shall  
53 be compliant to the IEEE Extended Unique Identifier-64 (EUI-64) format containing the  
54 IEEE hardware address of the device. The EUI-64 format supports encapsulation of both 48-  
55 bit and 64-bit IEEE hardware addresses such as the MAC address. The FEID shall be encoded  
56 in FQDN format (e.g., FEID.devicemodel.vendor.com) in the subjectAltName extension [17]  
57 of the FAP certificate. The same FEID in FQDN format shall be used in the IKEv2  
58 Identification payload (i.e., IDi field) of the IKE\_AUTH request from the FAP. The SeGW  
59 shall check the FAP certificate validity time as specified in [17].

The SeGW shall be authenticated by the FAP using the SeGW's certificate. The SeGW certificate is assigned to the SeGW by the cdma2000 network operator. The SeGW server certificate shall be compliant to [17] and shall support the SeGW certificate profile specified in [6].

The SeGW certificate shall be identified by using either the SeGW's FQDN or its IP address in the subjectAltName extension of the SeGW certificate. The SeGW's FQDN (or the IP address) shall be used in the IKEv2 Identification payload (i.e, IDr field) of the IKE\_AUTH response from the SeGW. The FAP shall check that the subjectAltName extension in the SeGW certificate matches the value received in the IDr field. The FAP shall check the SeGW certificate validity time as specified in [17].

At least one CA certificate in the trust chain of the SeGW certificate shall be pre-provisioned in the FAP for verifying the SeGW certificate.

At least one CA certificate in the trust chain of the FAP certificate shall be pre-provisioned in the SeGW for verifying the FAP certificate.

### 3.3.1.3 FAP Authorization

---

After the FAP is successfully authenticated by the SeGW, based on the network policy, (e.g., FAP authorization is required), the SeGW shall contact the Femtocell AAA for authorization using FEID in FQDN format received in the IDi payload as the FAP username in NAI format (i.e., FAP-FQDN@realm) using AAA protocols as specified in 3.2.2.2.

The Femtocell AAA shall check the FAP authorization policy based on the FEID received in the AAA message. If the FAP authorization check fails, the Femtocell AAA shall send an AAA message to the SeGW indicating authorization failure. The Femtocell AAA shall maintain the FAP authorization policy. The authorization policy may be based on a black list/white list of FEIDs or a profile for each FAP. The FAP authorization policy may be associated with the existing user profile at the AAA.

If the Remote IP Access service (see section 6) is supported, the Femtocell AAA shall store the mapping information between the FAP and the SeGW IP address received in the AAA message.

## 3.4 FAP Auto-configuration

---

Following a secure tunnel establishment with the SeGW, the FAP shall perform FMS discovery as specified in section 3.4.1 and then connect to the FMS to perform the auto-configuration procedures using the Fm interface [15] as specified in section 3.4.2. The Secure tunnel between the FAP and SeGW provides confidentiality, data integrity and certificate based mutual authentication.

### 3.4.1 FMS Discovery

---

#### 3.4.1.1 FAP Requirements

---

After successful IPsec tunnel establishment, if the FAP needs to obtain IP address(es) of the FMS, the FAP shall use the FQDN of the FMS and use DNS mechanisms to retrieve the IP address(es) of the FMS. If the FQDN is not pre-provisioned in the FAP, the FAP shall build the FQDN by using the format of FMS.<home.domain name> for the DNS request. The FAP

1 shall identify the operator's network in <home.domain name>. If the FAP is pre-provisioned  
2 with multiple FQDNs of the FMS, the selection of using which FQDN is outside the scope of  
3 this document.  
4

## 5 **3.4.2 FAP Auto-configuration Procedures**

---

6 The FMS and the FAP shall follow the procedures specified in [15] for FAP auto-  
7 configuration. Informative call flows including the auto-configuration of the FAP are shown  
8 in section A.3. The detailed configuration parameters and their associated management  
9 objects/ data models exchanged between the FAP and the FMS are described in [16].  
10

11 The FAP (acting as CPE) or the FMS (acting as ACS) may initiate an auto-configuration  
12 session as specified in [15].  
13

### 14 **3.4.2.1 FAP Requirements**

---

15 The FAP shall establish connection with the FMS.  
16

17 The FAP shall support all the baseline RPC methods including generic methods and CPE  
18 methods as specified in Annex A.3.1 and A.3.2 of [15]. In addition the FAP should support  
19 Upload and FactoryReset as specified in Annex A.4.1.5 of [15]. The FAP may support other  
20 optional CPE methods as specified in Annex A.4.1 of [15].  
21

22 After auto-configuration is successfully completed, the 1x or 1x/HRPD Hybrid FAP shall  
23 perform registration procedures with the CSCF/FCS as described in [7]. Section A.1 shows  
24 informative call flows including the auto-configuration aspects of FAP network connectivity  
25 procedures.  
26

### 27 **3.4.2.2 FMS Requirements**

---

28 The FMS shall support all the baseline RPC methods including Generic methods and ACS  
29 methods as specified in Annex A.3.1 and A.3.3 of [15]. The FMS may support optional ACS  
30 methods as specified in Annex A.4.2 of [15].  
31

32 The FMS shall support a Northbound Interface (NBI) that satisfies the requirements in [33].  
33 The FMS shall support the use of the NBI to delegate the processing of TR-069 vendor-  
34 specific parameters (as specified in section 3.3 of [32]) to the vendor-specific parameter  
35 processing entities. A vendor-specific parameter processing entity can be collocated with the  
36 FMS or can be a separate entity.  
37

38 The selection of applicable <VENDOR> strings for the vendor-specific parameters depends  
39 on operator's policy and is outside the scope of this document.  
40

## 41 **3.4.3 Location Determination of the FAP**

---

### 42 **3.4.3.1 FMS Requirements**

---

43 The FMS shall verify the FAP's location. The FMS shall not configure FAP to provide the  
44 services to the MS unless the location of the FAP is verified by the FMS. How FMS verifies  
45 the FAP's location is outside of the scope of this document.  
46  
47  
48  
49  
50  
51

## 3.5 Quality of Service (QoS) Considerations

The FAP and the SeGW shall support multiple Quality of Service (QoS) classes/profiles required for providing QoS to all the different classes of traffic from/to the MS. The different QoS classes of traffic shall be managed using different CHILD\_SA pairs between the FAP and the SeGW.

### 3.5.1 CHILD\_SA

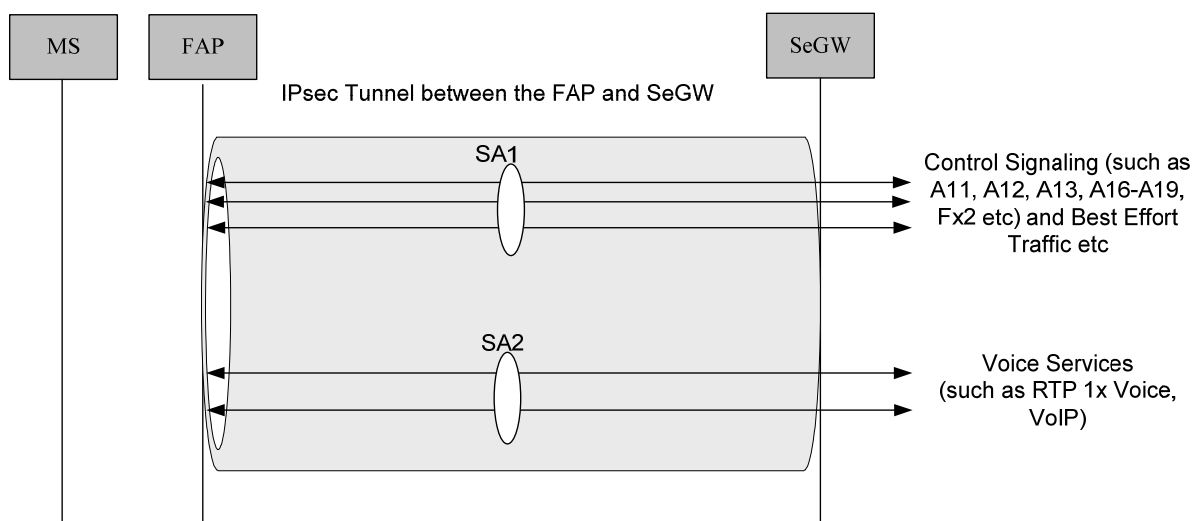
If different classes of traffic (distinguished by Differentiated Services Code Point (DSCP) bits) are sent on the same SA, and if the FAP/SeGW is employing the optional anti-replay feature available in both AH and ESP, this could result in inappropriate discarding of lower priority packets due to the windowing mechanism used by this feature. Therefore, the FAP and SeGW use multiple Security Associations to provide the appropriate QoS services. Traffic from multiple MSs but belonging to the same QoS class should reuse the same CHILD\_SA that provides that QoS.

Once the IKE\_SA has been authenticated, more than one CHILD\_SA pair can be negotiated inside the IKE\_SA. The CREATE\_CHILD\_SA exchange is protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange. Therefore, creation of additional CHILD\_SA pairs between the FAP and SeGW does not trigger further authentication and authorization messaging to the Femtocell AAA.

Both the FAP and the SeGW shall support at least two CHILD\_SA pairs for QoS support. The multiple CHILD\_SA pairs are shared by all MSs served by the FAP. If more than one CHILD\_SA pair is required, the FAP and SeGW shall perform CREATE\_CHILD\_SA exchange procedures and include traffic selectors as specified in [10].

Figure 1 shows an example of the security associations and the associated QoS classes of traffic with two SAs established between the FAP and the SeGW.

- SA1 (base SA) contains all control signaling and best effort traffic,
- SA2 carries RTP 1x Voice and/or VoIP traffic.



**Figure 1 Example of Security Associations and associated QoS classes of traffic with two SAs**

### 3.5.2 Reverse Link Packet Classifier in FAP

---

The Reverse Link Packet Classifier shall map traffic belonging to different QoS classes to the appropriate SA by using the Protocol Type (GRE, UDP, TCP) as a traffic selector. It may also employ different GRE keys (i.e., based on different A10 connections) as traffic selectors to map to different CHILD\_SAs. The FAP shall ensure the proper DSCP marking both on the inner and outer IP packet headers.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## 4 Mobility Management

---

Handoff between macro cell and Femtocell cell is specified in [1].

IP services available to the MS through a Femtocell are specified in [2], [3], [4], and [5].

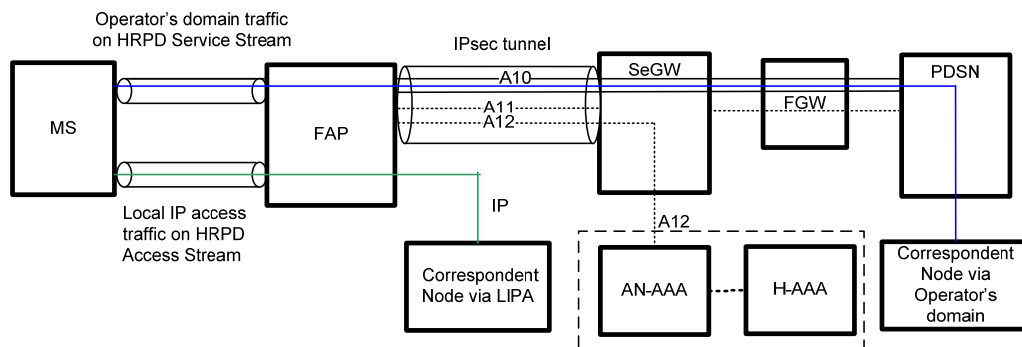
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## 5 Local IP Access for HRPD

Local IP access at the HRPD FAP provides for IP connectivity to allow a MS to access either local IP networks or the Internet through the local interface. For local IP access, the MS connects through the FAP to the local network by configuring an additional IP interface on the existing HRPD access stream 0. At the same time, the MS can still have IP connectivity to the operator's IP domain via the PDSN. In this model, the MS can have IP connectivity with:

- Correspondent Node via LIPA in the same subnet with the FAP.
- Correspondent Node via the operator's domain. The MS can still use the IP service provided by the PDSN. Therefore, the MS can access all services available on the macro network while simultaneously accessing the home intranet.
- Correspondent Node in the Internet. The Internet may be reached either on the local IP interface or through the PDSN IP interface. Operator may configure the FAP and the MS to use local IP interface for internet communications.

Figure 2 shows the bearer and interfaces related to Local IP Access.



**Figure 2 IP Access Bearer and Interfaces**

The AN-AAA may be used to authorize an MS for LIPA service during HRPD access authentication on the A12 interface as specified in this document. For LIPA authorization, the AN-AAA may access the HAAA for authorization information, but this interface is outside the scope of this document.

Refer to [1] for general requirements and procedures on the AN-PPP and A12 interfaces for HRPD.

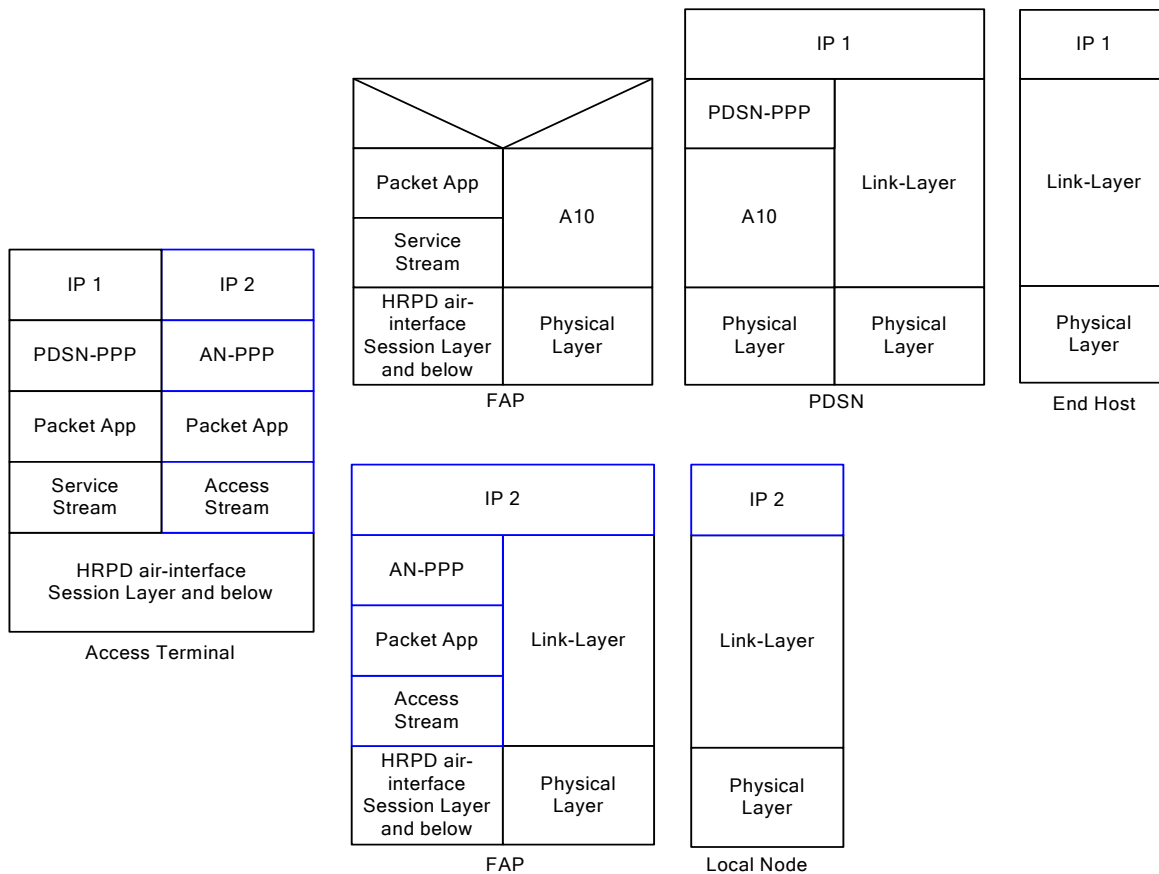
The LIPA feature supports the ability of an MS to perform session establishment with a FAP, establish an AN-PPP session, perform access authentication and then use the AN-PPP session to acquire a locally assigned IP address. The MS can have both a local IP address and an operator assigned IP address acquired over its AN-PPP session and PDSN-PPP session, respectively. The MS can simultaneously use the local IP address over the AN-PPP session and the operator assigned IP address over the PDSN-PPP session. Upon completion of the handoff out of the FAP, the MS and the FAP can each drop the AN-PPP session and release the locally assigned IP address.

## 5.1 LIPA Requirements and Procedures

This section describes the requirements and procedures for simple IP operation to support LIPA. In this context, simple IP refers to a service in which an MS is assigned either an IPv4 address or an IPv6 prefix and is provided IP routing service by the FAP. If LIPA is supported, the MS shall support two IP interfaces (one with the PDSN and another one with the FAP) and the FAP shall support allocating an IP address to the MS.

### 5.1.1 LIPA Protocol Reference Model

The following figure shows the protocol reference model for supporting LIPA at an HRPD FAP.



**Figure 3 HRPD LIPA Protocol Reference Model**

When LIPA is supported, there are two IP interfaces at the MS.

- The PDSN-PPP session (IP 1) for network operator connectivity is established on the service stream (see A.S0008/A.S0009) [53], [54], and the A10 interface carries user traffic between the FAP and the PDSN. Refer to X.S0011 [2].
- The AN-PPP session (IP 2) for LIPA connectivity is established on the access stream (see A.S0008/A.S0009) [53], [54]. Refer to section 5.1.2

## 5.1.2 AN-PPP Session

---

PPP shall be the data link protocol between the MS and the FAP. This PPP session is referred to as AN-PPP. The AN-PPP session shall be established prior to any IP datagram being exchanged between the MS and the FAP. Only one AN-PPP session shall be supported between the MS and the FAP. If access authentication is performed, LIPA shall reuse the AN-PPP session that is established between the MS and the FAP for access authentication (refer to A.S0008 and A.S0009, [53], [54]). If access authentication is not performed, the FAP shall establish an AN-PPP session without specifying either CHAP or PAP as a PPP option in an initial LCP Configure-Request message during the PPP establishment. PPP shall be supported as defined in the following standards with any limitations or extensions described in this document.

- Point to Point Protocol (RFC 1661 [36]);
- PPP in HDLC-like Framing (RFC 1662 [37]);
- IPCP (RFC 1332 [34]) for IPv4;
- IPv6CP (RFC 2472 [45]) for IPv6;
- CHAP (RFC 1994 [39]);
- PAP (RFC 1334 [35]).

### 5.1.2.1 Establishment

---

After the MS indicates it is ready to exchange data on the access stream, the FAP shall initiate PPP procedures according to RFC 1661 [36] by sending an LCP Configure-Request message to the MS. PPP shall support transparency in accordance with section 4.2 of RFC 1662 [37]. The FAP and MS shall attempt to negotiate a control character mapping with the minimum number of escape characters by proposing an Async-Control-Character-Map (ACCM) of 0x00000000.

Additionally, the FAP may establish an AN-PPP session with the MS at any time (e.g., following session transfer to the FAP).

### 5.1.2.2 Authentication

---

The MS shall support CHAP for the PPP instance on the access stream. If the FAP supports access authentication, the FAP shall support CHAP for the PPP instance on the access stream. In this case, the FAP shall always propose CHAP as a PPP option in an initial LCP Configure-Request message during the PPP establishment.

### 5.1.2.3 Termination

---

If the FAP does not support LIPA, the FAP may release the PPP connection after the access authentication of the MS has been performed. If the FAP supports LIPA, then it proceeds to the IPCP phase as described in section 5.1.3.

The FAP and the MS should support PPP link status determination as specified in section 3.2.1.10 of X.S0011-002 [2] on the AN-PPP. The FAP shall close the PPP session when the Max PPP Inactivity Timer expires.

The FAP shall terminate the PPP session with the MS when the HRPD session for the MS is terminated. The MS shall locally terminate its PPP session when the HRPD subnet changes or the HRPD session is terminated.

#### 5.1.2.4 AN-AAA Support

---

Upon successful access authentication, the visited AN-AAA may include the RADIUS attribute “Local-IP Access-Authorized” (refer to section 8) in an Access-Accept message to the FAP on the A12 interface (see A.S0008/A.S0009, [53], [54]). The value of the attribute is based on operator policy.

#### 5.1.3 Addressing with IPCP

---

A FAP shall not assign an IPv4 address or IPv6 Prefix to the MS if the RADIUS attribute, Local-IP-Access-Authorized, from the AN-AAA does not authorize the FAP to do so. A FAP may assign an IPv4 address or IPv6 Prefix to the MS if the RADIUS attribute, Local-IP-Access-Authorized, from the AN-AAA authorizes the FAP to do so. If the RADIUS attribute Local-IP-Access-Authorized is not received by the FAP, the FAP may allocate an IPv4 address or IPv6 prefix to the MS based on its local policy.

##### 5.1.3.1 IPv4 Addressing

---

The FAP assigns a local IPv4 address to the MS on the AN-PPP via IPCP negotiation by sending an IPCP Configure-Request message. This message includes the FAP’s own IP address. If the MS supports LIPA, the MS shall respond with an IPCP Configure-Ack message upon receipt of the IPCP Configure-Request message.

If the MS does not support LIPA, the MS may send an IPCP Configure-Reject or ignore all IPCP packets.

Upon responding with an IPCP Configure-Ack to the IPCP Configure-Request from the FAP, the MS may request a NULL or non-zero IPv4 address in its IPCP Configure-Request message. The MS should also include the request for egress packet filter criteria from the FAP in its IPCP Configure-Request message as described in section 5.1.6.

If the MS requests a NULL or non-zero IPv4 address<sup>2</sup>, the FAP should assign an IPv4 address to the MS with an IPCP Configure-Nak message. This message shall also include the egress packet filter criteria the MS should use to determine for each IP packet whether it should traverse through the LIPA interface as defined in section 5.1.6.

If the MS requests a non-zero IPv4 address during the IPCP phase, and if the FAP is unable to assign the requested address, the FAP shall send an IPCP Configure-Nak containing the new IPv4 address. This message shall also include the egress packet filter criteria the MS should use to determine for each IP packet whether it should traverse through the LIPA interface.

The MS should acknowledge the IPv4 address assigned to it and the egress packet filter criteria it should use, in the subsequent IPCP Configure-Request message.

If the MS fails to accept the assigned IPv4 address, the FAP shall send an LCP Terminate-Request.

---

<sup>2</sup> The MS can request a non-zero IP address in case the MS wants to retain the existing local IP address.

1 The FAP shall implement IPCP configuration options as defined in RFC 1877 [38] for the  
2 Domain Name System (DNS) server address negotiation.  
3

4  
5 The FAP shall remove the binding created for this IPv4 address assigned to the MS if either  
6 the HRPD session or the AN-PPP session for the MS is terminated.  
7

### 8 **5.1.3.2 IPv6 Addressing**

---

9  
10 If IPv6 addressing is supported, both the MS and the FAP shall support the MS-PDSN  
11 Version Capability Indication (refer to X.S0011 [2]).  
12

13  
14 If the FAP supports IPv6 addressing, the MS-PDSN Version Capability Indication (refer to  
15 X.S0011 [2]) is used, and the MS signaled that it does not support Simple IPv6, then the FAP  
16 shall not negotiate IPv6CP with the MS and shall not send IPv6 Router Advertisements to the  
17 MS.  
18

19  
20 If the MS-PDSN Version Capability Indication is used, and the MS signaled that it supports  
21 Simple IPv6 (C2 bit set to 1), then the FAP shall provide Simple IPv6 service to the MS as  
22 described in the remainder of this section.  
23

24 When IPv6 addressing is being used, the FAP shall be the PPP termination point.  
25

26  
27 If the FAP supports IPv6 addressing, the FAP shall support the following RFCs, with  
28 exceptions as noted in this document:

- 29     ▪ An IPv6 Aggregatable Global Unicast Address Format RFC 3587[47];
  - 30     ▪ Internet Protocol, Version 6 (IPv6) Specification RFC 2460 [41];
  - 31     ▪ Neighbor Discovery for IP Version 6 (IPv6) RFC 2461[42];
  - 32     ▪ IPv6 Stateless Address Auto-configuration RFC 2462 [43];
  - 33     ▪ Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6  
34 (IPv6) Specification RFC 2463 [44];
  - 35     ▪ IP Version 6 over PPP RFC 2472 [45];
  - 36     ▪ IP Version 6 Addressing Architecture RFC 3513 [46].
- 37  
38  
39  
40  
41  
42

43  
44 The FAP shall perform Interface-Identifier negotiation as described in RFC 2472 [45].  
45 Interface-Identifiers used by the FAP and the MS are configured via IPv6CP. The FAP shall  
46 provide to the MS a valid non-zero Interface-Identifier of the FAP in the IPv6CP Configure-  
47 Request. The FAP shall provide a valid non-zero Interface-Identifier for the MS in IPv6CP  
48 Configure-NAK if the MS's proposed IID is not acceptable to the FAP. While communicating  
49 with the MS, the FAP shall use only the link local address that it constructed with its  
50 Interface-Identifier that it provided to the MS (i.e., the FAP's Interface-Identifier) during  
51 IPv6CP phase. Because the Interface-Identifier negotiated in the IPv6CP phase of the PPP  
52 connection setup is unique for the AN-PPP connection, it is not required to perform duplicate  
53 address detection for the link local address formed as part of IPv6 stateless address auto-  
54 configuration RFC 2462 [43].  
55  
56  
57  
58  
59

Following successful IPv6CP negotiation and the establishment of a unique link-local address for both the FAP and the MS, the FAP shall immediately<sup>3</sup> transmit initial unsolicited Router Advertisement (RA) messages on the AN-PPP link using its link-local address as a source address. The FAP shall include a prefix in the RA message to the MS. The MS uses this prefix to configure its global IPv6 addresses.

The FAP shall send unsolicited RA messages for an operator configurable number of times. Also, the FAP shall set the interval between initial RA messages to an operator configurable value, which may be less than MAX\_INITIAL\_RTR\_ADVERT\_INTERVAL. After the configurable number of initial unsolicited RA messages has been transmitted, the interval between the periodic transmissions of unsolicited RA messages shall be controlled by the router configurable parameters MaxRtrAdvInterval and MinRtrAdvInterval as defined in RFC 2461 [42]. The FAP may set MaxRtrAdvInterval to a value greater than 1800 seconds and less than 1/3 of the AdvDefaultLifetime. The FAP shall set MinRtrAdvInterval<sup>4</sup> to a fraction of MaxRtrAdvInterval as per RFC 2461[42].

The FAP shall send a RA message in response to a Router Solicitation (RS) message received from the MS. The FAP may set the delay between consecutive (solicited RA) or (solicited /unsolicited RA) messages sent to the all-nodes multicast address to a value less<sup>5</sup> than that specified by the constant MIN\_DELAY\_BETWEEN\_RAS, contrary to the specification in section 6.2.6 of RFC 2461 [42].

The advertised prefix<sup>6</sup> identifies the subnet associated with the AN-PPP link. The prefix advertised by the FAP shall be exclusive to the AN-PPP session.

The FAP shall set:

- the M-flag = 0 in the RA message header;
- the L-flag = 0 and the A-flag =1 in the RA message Prefix Information Option.
- The FAP shall set the Router Lifetime value in the RA message to a value of 216-1 (18.2 hrs).

The FAP shall not send any redirect messages to the MS over the AN-PPP interface.

#### **5.1.3.2.1 Stateless DHCPv6 Support**

The FAP shall support Stateless DHCPv6 as specified in RFC 3736 [49], and shall set the O bit to 1 in the RA messages sent to the MS.

Upon receiving a DHCPv6 Information-Request packet from the MS, the FAP shall respond with a Dynamic Host Configuration Protocol (DHCP) Reply message. The FAP should include DNS configuration options as specified in RFC 3646 [48]).

<sup>3</sup> This is an exception to RFC 2461 necessary to optimize applicability over the cdma2000 wireless air-interface.

<sup>4</sup> This may cause an exception to RFC 2461 as it may put the interval outside the normal range. This exception is allowed by this document to optimize IPv6 RA over the cdma2000 wireless links.

<sup>5</sup> This exception is allowed by this document to optimize IPv6 RA over the cdma2000 wireless links

<sup>6</sup> If the network operator desires to reduce frequent unsolicited RA for the prefix, they should set the 32-bit Valid Lifetime and Preferred Lifetime fields for the advertised 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).

1 **5.1.4 PPP Framing**  
 2

3 The FAP shall frame PPP packets sent on the PPP link layer using the octet synchronous  
 4 framing protocol defined in RFC 1662 [37], except that there shall be no inter-frame time fill  
 5 (refer to section 4.4.1 of RFC 1662 [37]). I.e., no flag octets shall be sent between a flag octet  
 6 that ends one PPP frame and the flag octet that begins the subsequent PPP frame. For IPv6,  
 7 the FAP shall set the MTU size as specified in RFC 2460 [41].  
 8

9  
 10 **5.1.5 Ingress Address Filtering at the FAP**  
 11

12 For each IP packet received from the MS, the FAP should check whether the source IP  
 13 address of the IP packet matches with the local IP address assigned to the MS. If the source IP  
 14 address differs from the local IP address assigned to the MS, the FAP shall discard the packets.  
 15

16  
 17 **5.1.6 Egress Address Filtering/Routing at the MS**  
 18

19 For each IP packet, the MS determines the interface through which the packet will be  
 20 transmitted based on a packet filtering criteria.  
 21

22 During the IPCP negotiation phase, the FAP shall send an IPCP Configure-Nak message to  
 23 assign an IP address to the MS and to update the MS with the criteria to be applied for packet  
 24 filtering. Table 1 defines the format of the vendor specific option that includes the packet  
 25 filter criteria.  
 26

27 This vendor specific option should be appended to the IPCP Configure-Nak message from the  
 28 FAP when assigning a local IP address to the MS and should also be appended to the IPCP  
 29 Configure-Request message from the MS acknowledging the IP address it received from the  
 30 FAP.  
 31

32  
 33 **Table 1 IPCP Vendor Specific Option**  
 34

35  
 36  
 37

	1							2							3																
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Length								OUI															
...								Kind								Value(s) ...															

38  
 39  
 40  
 41  
 42

- 43 Type: Type shall be set to zero to indicate vendor specific option (RFC 2153 [40]).  
 44 Length: Length of the vendor specific option in bytes (from Type field through Value(s)  
 45 field).  
 46 OUI: The Organizationally Unique Identifier (OUI) field shall be set to “CF0002H”  
 47 indicating 3GPP2 vendor specific option.  
 48 Kind: 01H value indicates that the IPv4 egress packet filter criteria to be used by MS is  
 49 contained in the Value(s) field.  
 50 02H value indicates that the IPv6 egress packet filter criteria to be used by MS is  
 51 contained in the Value(s) field.  
 52 All other values are reserved.  
 53 Value(s): If the Kind field is set to 01H, then the Value(s) field is coded as shown in Table 2.  
 54  
 55  
 56  
 57  
 58  
 59

**Table 2 Value(s) Field for the IPv4 Packet Filter Criteria**

										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Count										Subnet 1																			
Subnet 1 (cont)																				Subnet Mask 1																			
Subnet Mask 1 (cont)																				Subnet 2																			
Subnet 2 (cont)																				Subnet Mask 2																			
Subnet Mask 2 (cont)																				...																			

Type: A Type of 0 identifies the range of subnets that are accessible through the LIPA interface. A Type of 1 identifies the range of subnets that are not accessible through the LIPA interface.

Count: This field indicates the number of subnets and subnet masks (each) associated with this type.

Subnet: This field contains a 32-bit value in IPv4 format.

Subnet Mask: This field contains a 32 bit subnet mask applied to the IP address to yield the non-host portion of the address.

If the Kind field is set to 02H, then the Value(s) field is as shown in Table 3.

**Table 3 Value(s) Field for the IPv6 Packet Filter Criteria**

																1																2																3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9																								
Type																Count																Reserved																Subnet Length 1															
Subnet 1																																																															
Subnet 1 (cont)																																																															
Subnet 1 (cont)																																																															
Subnet 1 (cont)																																																															
Reserved																Subnet Length 2																Subnet 2																															
Subnet 2 (cont) ...																																																															

Type: A Type of 0 identifies the range of subnets that are accessible through the LIPA interface. A Type of 1 identifies the range of subnets that are not accessible through the LIPA interface.

Count: This field indicates the number of subnet length and subnet (each) associated with this type.

Subnet Length: This field contains the number of valid leading bits in the following subnet. The bits in the subnet after the length are reserved and shall be set to zero.

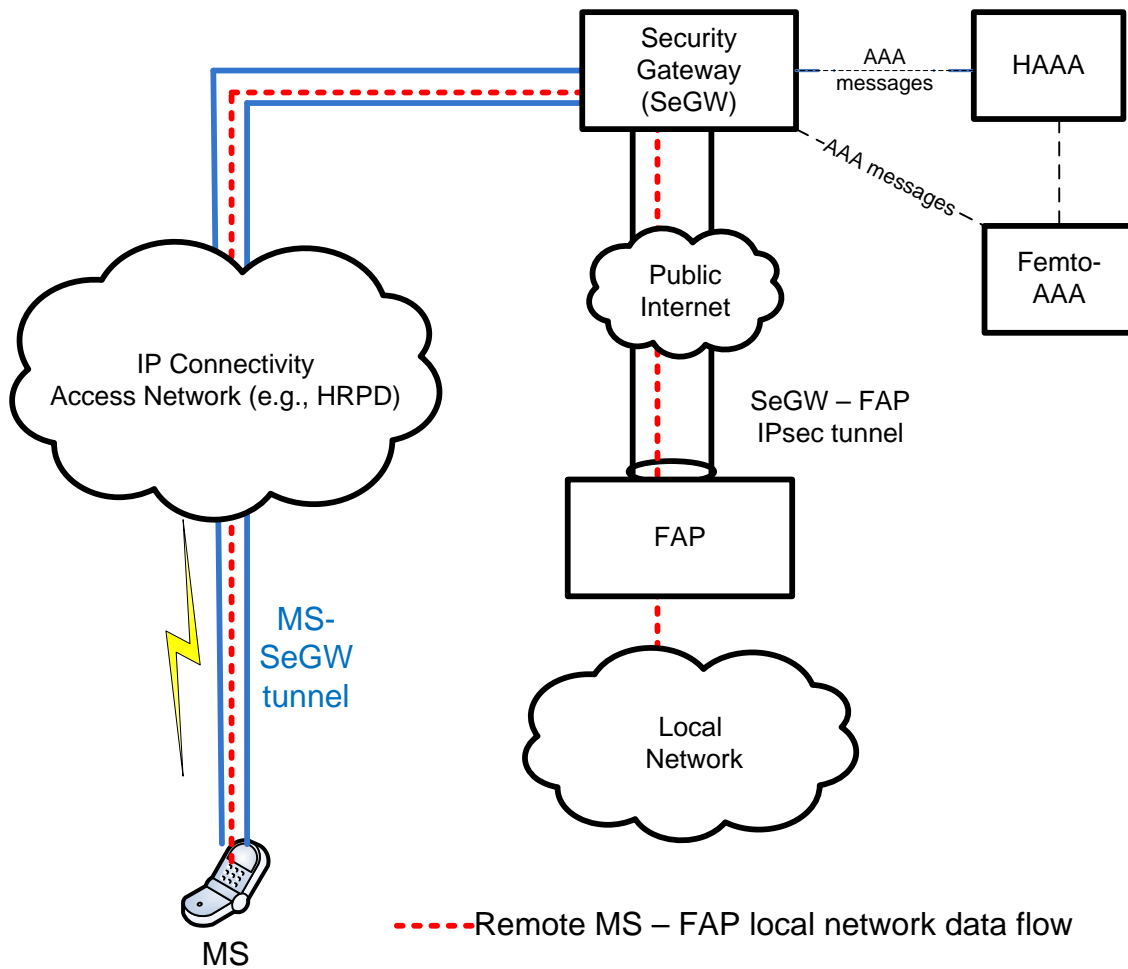
Subnet: This field contains a 128 bit value in IPv6 format.

## 6 Remote IP Access

### 6.1 General

Remote IP Access allows a given MS to reach the IP network local to the FAP using any IP connectivity available to the MS (e.g., through macro network IP connection) while the MS is not directly connected to the FAP. This service is assumed to be invoked on the MS on demand by the user.

Remote IP Access is achieved by using IPsec tunnels between the MS and SeGW and between the SeGW and FAP. A given MS establishes an IPsec tunnel to the SeGW, which has an IPsec tunnel pre-established to the FAP(s). The remote IP access architecture is specified in Figure 4.



**Figure 4 Femtocell Remote IP Access Architecture**

Remote IP Access is achieved by performing the following procedures:

- The MS performs SeGW discovery as described in section 6.2;

- Tunnel establishment, MS authentication and authorization by the HAAA as described in section 6.3;
- Assignment of local IP address by the FAP (or by local DHCP Server) to the MS.

In order to perform Remote IP Access procedures, the following requirements shall be met by means outside the scope of this document.

- The FAP(s) that can be remotely accessed by a given MS shall be configured as part of the MS subscription profile at the operator's HAAA.
- The FAP(s) shall be identified by its FEID(s) and/or by realm. The realm may be used in cases where multiple FAPs are connected to the same local network.
- The MS shall be pre-configured with at least one FQDN or shall form the FQDN for discovering the SeGW.
- The FAP shall support DHCP as specified in [18] to allocate IP addresses for the MS. The FAP may support DHCPv6 as specified [19] to allocate IP addresses for the MS.

## 6.2 Discovery and Selection of SeGW by MS

In order to access a local IP network connected to a FAP, the MS needs to first establish an IPSec tunnel to the same SeGW that is serving the FAP. Since the SeGW needs to be discovered by the MS using an IP connection, the SeGW needs to be publicly reachable. In order to discover the correct SeGW, the MS first uses the DNS Discovery for SeGW IP address. Additionally, the MS can use the SeGW Redirection method specified in this section to connect to the SeGW serving the FAP.

When an MS tries to connect to a SeGW that is not serving the desired FAP, the current SeGW can redirect the MS to an alternative SeGW using the redirection procedure specified in section 6 (section titled "Redirect during IKE\_AUTH Exchange") of [20]. The following functions need to be supported for SeGW redirection:

- When the MS tries to connect to a SeGW, the SeGW performs the access request procedure to the HAAA for authentication and authorization.
- The HAAA maintains a list of FAPs and/or realm(s) that a given MS can access as part of MS subscription profile.
- The Femtocell AAA maintains the association between the FAP's FEID and the SeGW that is currently serving the FAP.
- The HAAA interacts with the Femtocell AAA to retrieve the SeGW IP address and the FAP(s) associated with the local network (e.g., identified by the FEID or the realm) that the MS is trying to access. In case multiple FEIDs are available, the Femtocell AAA may return a list of FEID and SeGW IP address pairs to the HAAA. The HAAA includes this list to the SeGW in the HAAA authorization response. The interface between the HAAA and the Femtocell AAA is outside the scope of this document.

### 6.2.1 MS Requirements

To discover a target SeGW, the MS shall query the DNS server for candidate SeGW(s) using the pre-configured FQDN of the SeGW at the MS, if the FQDN is available. Otherwise, the MS shall form the FQDN for Remote IP Access as RemoteIPAccess.SeGW.<operator's

1 domain name>. The DNS server address is made available to the MS using means outside the  
2 scope of this document.  
3

4  
5 By using the SeGW's IP address received from the DNS query, the MS shall start the tunnel  
6 establishment procedures specified in section 6.3. In case multiple SeGW IP addresses are  
7 returned by the DNS server, the MS shall try to establish an IPsec tunnel to each of the  
8 returned SeGW IP addresses, until the MS can successfully connect to a SeGW. If all returned  
9 SeGW IP addresses have been tried and the tunnel establishment is unsuccessful, the MS shall  
10 treat it as no SeGW is currently serving the target FAP, and therefore, Remote IP Access is  
11 not available. If during the IKEv2 tunnel establishment, the MS receives a redirection, the MS  
12 shall follow the procedure specified in section 6.3.2.1. When the correct SeGW is found, the  
13 MS should cache the SeGW IP address for future use. In case the MS cannot connect to the  
14 cached SeGW IP address in a subsequent try, the MS should restart with a DNS query to  
15 discover the SeGW.  
16

## 17 **6.2.2 SeGW Requirements**

---

18  
19 Upon receiving an IPsec tunnel establishment request from the MS, the SeGW shall send the  
20 Remote IP Access service identity received in the IDi payload (in the form of NAI) to the  
21 HAAA using RADIUS or Diameter protocol according to section 6.3.3. If the Remote IP  
22 Access authentication and authorization with HAAA fails, the SeGW shall send a Notify  
23 message to the MS indicating authentication failure.  
24

25  
26 If the SeGW Redirection method is supported, then upon receiving an address for a different  
27 SeGW address from the HAAA, the serving SeGW shall use the IKEv2 redirection  
28 mechanism to redirect the MS to the specified SeGW using procedures specified in section  
29 6.3.3 of this document.  
30

## 31 **6.2.3 Femtocell AAA Requirement**

---

32  
33 The Femtocell AAA shall maintain association between the FAP identity (i.e., FEID) and the  
34 SeGW address. The Femtocell AAA shall provide such association information upon request  
35 from the HAAA.  
36

## 37 **6.2.4 Home AAA Requirements**

---

38  
39 The HAAA shall maintain the NAI used for Remote IP Access as well as either one of or both  
40 of the corresponding FEID(s) and the realm(s) as part of MS subscription profile. The HAAA  
41 shall authenticate and authorize the Remote IP Access service request from the MS using one  
42 of the methods specified in section 6.3.4.  
43

44  
45 During the tunnel establishment (see section 6.3), if SeGW Redirection based SeGW  
46 discovery is supported by the HAAA, the HAAA shall obtain the correct SeGW and the  
47 FEID/realm address for a given MS (identified by the NAI) by contacting the Femtocell AAA.  
48 If the current SeGW that the MS requests IPsec connection to is not the correct SeGW, the  
49 HAAA shall return the SeGW address together with the FEID/realm to the requesting SeGW  
50 using the RADIUS or Diameter message.  
51

## 52 **6.3 Remote IP Access Tunnel Establishment**

---

53  
54 Upon discovering the SeGW IP address, the MS shall use IKEv2 [10] to setup the IPsec  
55 tunnel between the MS and the SeGW. The IPsec tunnel establishment shall be authenticated  
56  
57  
58  
59

using either the IKEv2 Pre-Shared Key (PSK) method or IKEv2 EAP-AKA method as specified in this section.

A dedicated CHILD\_SA pair between the SeGW and the FAP shall be created to handle traffic for Remote IP Access service. Traffic for other purposes shall not use this dedicated SA.

### 6.3.1 IKEv2 PSK Key Generation

The Remote IP Access IKEv2 Root Key (RIPA-IKEv2-RK) used in the IKEv2 PSK authentication method shall be 64 octets and be derived from Extended Master Session Key (EMSK), MN-AAA, or CHAP-SS as per [21] with the following considerations:

- The Key Derivation Function (KDF) shall be HMAC-SHA256 as per [22].
- If EMSK is available, the EMSK shall be used as specified in [21].
- If EMSK is not available, the MN-AAA shared secret shall be used as the EMSK in the formulas specified in [21].
- If neither EMSK nor MN-AAA is available, the CHAP-SS (Shared Secret) shall be used as the EMSK in the formulas specified in [21].
- The key label shall be “ripaikev2pskrk@femtocell.3gpp2.org” specified in lower case printable ASCII and the string shall not be null terminated.
- Optional Data is not used.
- The length shall be 0x0040 in network byte order.

Since HMAC-SHA256 produces an output of 32 octets and the required RIPA-IKEv2-RK size is 64 octets, the procedure in section 3.1.2 of [21] shall be used to create the key of required length.

The RIPA-IKEv2-Key is then derived from the RIPA-IKEv2-RK using the HMAC-SHA256 KDF function as specified below. The RIPA-IKEv2-Key shall be of size 32 octets.

$$\text{RIPA-IKEv2-Key} = \text{KDF}(\text{RIPA-IKEv2-RK}, \text{Ni}|\text{Nr}, \text{“ripaikev2pskkey@femtocell.3gpp2.org”}),$$

where Ni and Nr are nonces exchanged between MS and SeGW as specified in [10], and the key label “ripaikev2pskkey@femtocell.3gpp2.org” is specified in lower case printable ASCII and the string shall not be null terminated.

### 6.3.2 MS Requirements

The MS shall support IKEv2 [10] and ESP [12] for key exchange and IPsec tunnel establishment with the SeGW. The MS shall support IKEv2 EAP-AKA or IKEv2 PSK for authentication with the HAAA.

The MS shall setup the IPsec tunnel with the SeGW for each of the FAPs it wants to connect to, and shall follow the procedures described below.

The MS shall initiate the IKEv2 key exchange protocol with the SeGW as specified in [10]. The MS shall include the Security Parameter Index in the IKE Header (HDR) of the

IKE\_SA\_INIT message. The MS shall also include SAi1 payload, Key Exchange initiator (KEi) payload (with the initiator's Diffie-Hellman value) and the Initiator's Nonce (Ni).

Once the initial exchange is finished, in the first IKE\_AUTH Request message, the MS shall identify itself by including its Network Access Identifier (NAI) in the IDi payload with ID type set to ID\_RFC822\_ADDR. The IDi payload shall identify the Remote IP Access service. For example, if the MS has subscription NAI of the form user@realm that is used for IP connectivity authentication, then the Remote IP Access NAI can be formed as {RemoteIPAccess}.{[localIPnetworkId]}.user@realm, where the localIPnetworkId is optional (i.e., can be omitted) and can be either the selected FEID or the local network realm. The curly bracket “{}” is used as delimiter. If the localIPnetworkId is omitted, it is used as an indication to the network that the MS wishes to connect to the default local IP network (identified by the default FEID or realm) in the MS subscription profile at the HAAA. The localIPnetworkId, if used, is assumed to be configured on the MS.

The NAI used to form the Remote IP Access NAI shall be selected using the following procedure. If EMSK is available, the MS shall use the NAI associated with the EMSK for forming the Remote IP Access NAI. If EMSK is not available, but EAP-AKA is supported, then the NAI associated with EAP-AKA shall be selected by the MS. Otherwise, the MS shall use the NAI associated with the MN-AAA key (used for mobile IP service authentication) or the CHAP Shared Secret (SS) (used for simple IP service authentication).

In the first IKE\_AUTH Request message, the MS shall also include a CP(CFG\_REQUEST) payload containing at least one INTERNAL\_ADDRESS attribute (either IPv4 or IPv6) for tunnel internal address assignment by the targeted local network. Upon successful authentication and authorization, the MS shall extract from the CP(CFG\_REPLY) payload in the last IKE\_AUTH Response message an assigned internal address (IPv4 or IPv6) from the SeGW. For IPv6, the MS shall perform IPv6 autoconfiguration procedures upon receiving an IPv6 prefix from the SeGW. The MS shall use this address as the internal address in the IPsec tunnel for future communication with the targeted local network.

Upon the completion of the IKEv2 procedures, the MS shall establish an IPsec ESP tunnel to the SeGW according to [12].

### 6.3.2.1 SeGW Redirection

---

The MS shall support the requirements specified in this section for SeGW Redirection method.

The MS shall include in the initial IKE\_INIT request message a Notify payload with REDIRECT\_SUPPORTED indication as specified in [20]. The SeGW redirection takes place during the final IKE\_AUTH Response message. Upon receiving the final IKE\_AUTH Response from the SeGW, the MS shall verify the SeGW's AUTH payload before acting on the Redirect payload, as specified in section 6 of [20].

### 6.3.2.2 IKEv2 Pre-Shared Key Method

---

If the MS supports the IKEv2 Pre-Shared Key method, the MS shall support the requirements specified in this section.

The MS shall generate RIPA-IKEv2-RK and RIPA-IKEv2-Key as specified in section 6.3.1.

In the first IKE\_AUTH request message, the MS shall prove the knowledge of the secret corresponding to IDi by signing the first IKE\_SA\_INIT message using the RIPA-IKEv2-Key and including the signature in the AUTH payload. Upon receiving the IKE\_AUTH Response message from the SeGW, the MS shall verify the signature in the AUTH payload.

### 6.3.2.3 IKEv2 EAP-AKA Method

If the MS supports IKEv2 EAP-AKA, the MS shall support the requirements specified in this section.

The MS shall support EAP-AKA [23]. In the first IKE\_AUTH Request message, the MS shall not include the AUTH payload, which is an indication of using EAP authentication. Upon receiving the EAP-Success, the MS shall use the Master Session Key (MSK) derived according to [23] to generate an AUTH payload and send to the SeGW. Upon receiving the final IKE\_AUTH Response message, the MS shall verify the AUTH payload from the SeGW using the MSK.

### 6.3.3 SeGW Requirements

The SeGW shall support IKEv2 [10] and ESP [12]. As initiated by the MS, the SeGW shall perform IKEv2 procedures to establish an IPsec tunnel with the MS.

Upon receiving the IKE\_SA\_INIT Request message from the MS, the SeGW shall choose a cryptographic suite from the initiator's offered choices and express that choice in the first Security Association responder (SAr1) payload, complete the Diffie-Hellman exchange with the Key Exchange responder (KEr) payload, and send its nonce in the Nonce responder (Nr) payload. The SeGW shall also fill the Security Parameter Index responder (SPIr) field in the HDR with the random value. The HDR, SAr1, KEr, Nr payloads shall be included in the IKE\_SA\_INIT Response message and sent to the MS.

Once the MS is authenticated and authorized, the SeGW shall verify that it has an existing IPsec tunnel with any of the FEIDs authorized by the HAAA. Otherwise, the SeGW shall abort the tunnel establishment procedure and send the error code of 8195 to indicate the MS that the Remote IP access service is not available at this time. If the existing IPsec tunnel with the FAP is available and a CHILD\_SA pair of RIPA has not been established for other MSs, the SeGW shall send a CREATE\_CHILD\_SA request to the FAP to create a separate CHILD\_SA pair by including a nonce Ni [10]. Upon receiving the CREATE\_CHILD\_SA response from the FAP, the SeGW shall derive the keying material for the CHILD\_SA pair according to [10]. If the CHILD\_SA pair cannot be created successfully, the SeGW shall abort the tunnel establishment procedure and send an IKEv2 Notification message to the MS with NO\_ADDITIONAL\_SAS in a Notify payload. The SeGW shall only use the newly created CHILD\_SA pair for Remote IP Access service.

If the existing IPsec tunnel with the FAP is available and the CHILD\_SA pair for RIPA service has already been established, the SeGW shall use the existing CHILD\_SA to request local IP address for the MS.

Using the CHILD\_SA pair for RIPA service, the SeGW shall forward the internal address request from the MS to the FAP in a DHCP message [18] for IPv4 address assignment, DHCPv6 message [19] for IPv6 address assignment, or both for IPv4 and IPv6 addresses assignment as specified in the following:

- 1           ▪ For an IPv4 address request, the SeGW shall use either DHCPDISCOVER with  
2           Rapid Commit Option or DHCPDISCOVER without Rapid Commit Option. The  
3           Client Identifier Option shall be set to the NAI received from IDi payload received  
4           from the MS (see section 6.3.2).
- 5           ▪ For IPv6 address request, the SeGW shall use the REQUEST message. The DUID  
6           type in Client Identifier option shall be set to 2 (Vendor-assigned unique ID based on  
7           Enterprise Number, see section 9.1 of [19]). The Enterprise Number shall be set to  
8           5535 and the identifier shall be set to NAI received from IDi payload received from  
9           the MS (see section 6.3.2).

10           Upon receiving an assigned local network address from the FAP in a DHCPACK (for IPv4)  
11           or DHCP REPLY (for IPv6), the SeGW shall include this assigned address in an  
12           CP(CFG\_REPLY) Payload in the IKE\_AUTH Response message to the MS.

13           Upon the completion of the IKEv2 procedures with successful authentication of the MS, the  
14           SeGW shall establish an IPsec ESP tunnel with the MS according to [12].

### 15           6.3.3.1    SeGW Redirection

16           If the SeGW supports redirection, the SeGW shall support the requirements specified in this  
17           section.

18           The SeGW shall support and only use IKEv2 redirection during the IKE\_AUTH exchange as  
19           specified in section 6 of [20]. After receiving an IKE\_INIT message from the MS with a  
20           REDIRECT\_SUPPORTED payload, the SeGW shall verify the AUTH payload if the AUTH  
21           payload is present (i.e., when IKEv2 PSK is used) in the IKE\_AUTH Request message from  
22           the MS before sending the REDIRECT Payload. If the AUTH payload is not present (i.e.,  
23           when EAP is used), the SeGW shall start the EAP authentication method and if authentication  
24           is successful then send the REDIRECT payload. The SeGW shall include the REDIRECT and  
25           IP\_R in a Notify payload in the IKE\_AUTH Response message, as specified in section 6 of  
26           [20]. The SeGW shall only use the IP address as the redirected address.

### 27           6.3.3.2    IKEv2 Pre-Shared Key Method

28           If the IKEv2 PSK method is used for authentication, upon receiving the IKE\_AUTH Request  
29           message from the MS, the SeGW shall send a RADIUS Authorize-Only (Service-Type set to  
30           “Authorize-Only”) Access Request message or Authorize-Only (Auth-Request-Type set to  
31           “Authorize-Only) Diameter message with received NAI, Ni and Nr to the HAAA to obtain the  
32           RIPA-IKEv2-Key. The SeGW shall set the Session-Key-Method VSA to 2 (RIPA IKEv2  
33           PSK method).

34           Once the SeGW receives the RIPA-IKEv2-Key from the HAAA, the SeGW shall verify the  
35           AUTH payload in the IKE\_AUTH Request message. If the verification of the AUTH payload  
36           is successful, the SeGW shall send an IKE\_AUTH Response message to the MS. The SeGW  
37           shall assert its identity with the IDr payload, sign the IKE\_SA\_INIT Response message using  
38           the RIPA-IKEv2-Key and include the signature in the AUTH payload. If the SeGW received  
39           either a Session-Timeout VSA (RADIUS) or an MSA-Lifetime of the Master-Security-  
40           Association AVP (Diameter) from the HAAA, the SeGW shall set the lifetime of the IKEv2  
41           SA to the value received in Session-Timeout VSA (RADIUS) or MSA-Lifetime of the  
42           Master-Security-Association AVP (Diameter).

### 6.3.3.3 IKEv2 EAP Method

If the IKEv2 EAP method is used for authentication, upon receiving indication to use EAP in the IKE\_AUTH message from the MS, the SeGW shall forward the EAP messages (extracted from the EAP payload) to the HAAA server via the RADIUS EAP-Message attribute in a RADIUS Access Request message [13] or Diameter EAP-Payload AVP in a Diameter DER command [30]. Upon receiving the RADIUS EAP-Message attribute in a RADIUS Access Accept message or Diameter EAP-Payload AVP in a Diameter DEA command from the HAAA, the SeGW shall forward the EAP message to the MS via the EAP payload in the IKE\_AUTH message.

Upon receiving the AUTH payload in the IKE\_AUTH message from the MS, the SeGW shall verify it using the MSK received from the AAA server. In return, the SeGW shall use the MSK to generate the AUTH payload in the IKE\_AUTH message sent to the MS.

### 6.3.4 Home AAA Requirements

The HAAA shall perform authentication and service authorization per operator's policy. The HAAA shall support IKEv2 PSK [10] and/or IKEv2 EAP-AKA [23] for authenticating the MS. The HAAA shall support RADIUS [13] or Diameter [14] protocols.

The HAAA shall maintain MS's NAI used for Remote IP Access as well as either one of or both of the corresponding FEID(s) and the realm(s) as part of the MS subscription profile. Upon receiving RADIUS Access Request or Diameter DER command containing the NAI for Remote IP Access, the HAAA shall retrieve the FEID(s) of the FAP(s) that is accessible to the MS, and contact the Femtocell AAA to obtain the SeGW identity that is currently serving the FAP. The HAAA shall return the SeGW address and FEID identity to the requesting SeGW via RADIUS (see section 8.2) or Diameter (see section 9.1.2) protocol. The HAAA shall only return the IP address of the redirected SeGW.

#### 6.3.4.1 IKEv2 Pre-Shared Key Method

If the IKEv2 Pre-Shared Key method is used for authentication, upon receiving a RADIUS Access Request message or a Diameter DER command with MS's NAI, Ni, and Nr from the SeGW, the HAAA shall use the NAI to retrieve the associated RIPA-IKEv2-RK key, generate the RIPA-IKEv2-Key as specified in section 6.3.1 and return the RIPA-IKEv2-Key to the SeGW using the MS-MPPE-Send-Key attribute (RADIUS) or the Master-Security-Association AVP (Diameter) without the SPI.

The HAAA shall set the Session-Timeout VSA (RADIUS) or MSA-Lifetime of the Master-Security-Association AVP (Diameter) to a value not greater than the lifetime of the associated EMSK if the RIPA-IKEv2-RK is generated from the EMSK. Otherwise if the RIPA-IKEv2-RK is generated directly from the MN-AAA, the HAAA should set the Session-Timeout VSA (RADIUS) or MSA-Lifetime (Diameter) to the Lifetime of the session.

#### 6.3.4.2 IKEv2 EAP-AKA Method

The HAAA shall support EAP-AKA [23], RADIUS Support for EAP [24], and Diameter IKE EAP (IKEEAP) specified in this document.

If the EAP authentication is successful, the HAAA server shall derive the MSK according to [23]. If RADIUS is used, the HAAA server shall send the MSK to the SeGW via the MS-MPPE-Recv-Key attribute (for the first 32 bytes of the MSK) and MS-MPPE-Send-Key

1 attribute (for the second 32 bytes of the MSK) [23][25]. If Diameter is used, the HAAA  
2 server shall send the MSK to the SeGW via the EAP-Master-Session-Key AVP.  
3

4  
5 If RADIUS is used, the HAAA server shall include the Message-Authenticator attribute [24]  
6 for protecting the integrity of the RADIUS messages that carry the EAP-Message attribute  
7 [26].  
8

### 9 **6.3.5 FAP Requirements**

---

10  
11 Upon receiving the CREATE\_CHILD\_SA request message from the SeGW, the FAP shall  
12 respond with a CREATE\_CHILD\_SA response message and include a nonce Nr in the  
13 response. The FAP shall derive the keys associated with the newly created CHILD\_SA pair  
14 according to [10]. The FAP shall use only the newly created CHILD\_SA pair for Remote IP  
15 Access services.  
16

17  
18 The FAP shall support DHCP relay/proxy or server functionality[18]. Upon receiving the  
19 request from the SeGW for an internal address for the MS, the FAP shall allocate an IPv4  
20 address from the local network subnet, either by itself or from another entity in the local  
21 network (e.g., DHCP server), and shall return this address to the SeGW via a DHCPACK  
22 message using the existing IPsec tunnel with the SeGW.  
23

24  
25 The FAP may support DHCPv6 as specified in [19]. Upon receiving the request from the  
26 SeGW for an internal address for the MS, the FAP shall allocate an IPv6 addresses from the  
27 local network subnet, either by itself or from another entity in the local network (e.g.,  
28 DHCPv6 server), and shall return this address to the SeGW via a DHCP REPLY message  
29 using the existing IPsec tunnel with the SeGW.  
30

## 31 **6.4 IP Traffic Processing for Remote IP Access**

---

32  
33 The MS and SeGW use the IPsec tunnel created according to section 6.3.2 for Remote IP  
34 Access service. The FAP and SeGW only use the CHILD\_SA pair created according to  
35 section 6.3.3 for sending and receiving IP traffic related to Remote IP Access service.  
36

37  
38 Since there are more than one CHILD\_SA pair between the SeGW and the FAP, for traffic  
39 from the FAP to the MS, the FAP needs to determine if the traffic is intended for the Remote  
40 IP Access service (i.e., based on the local IP address assigned by the FAP for RIPA) and  
41 encapsulate the traffic using the corresponding CHILD\_SA. If the FAP receives broadcast and  
42 multicast traffics from the local network, the FAP may encapsulate these packets to the  
43 corresponding CHILD\_SA. How the FAP decides whether it sends broadcast and multicast  
44 packets is outside the scope of this document. For traffic from the MS to the FAP, the SeGW  
45 determines (i.e., based on the IP address assigned using DHCP procedures for IPv4 or  
46 DHCPv6 procedures for IPv6) whether the traffic is intended for Remote IP Access service  
47 and encapsulates the traffic using the corresponding CHILD\_SA.  
48

### 49 **6.4.1 MS Requirements**

---

50  
51 Once the MS completes IPsec tunnel establishment with the SeGW, the MS shall operate in  
52 the ESP tunnel mode for Remote IP Access, as specified by section 3 of [12].  
53  
54  
55  
56  
57  
58  
59

### 6.4.1.1 Outbound IP Traffic Processing

---

The MS shall use the SA with the SeGW to process the outbound traffic for remote IP service according to section 3 of [12].

### 6.4.1.2 Inbound IP Traffic Processing

---

Upon receiving an IPsec packet from the SeGW, the MS shall perform inbound packet processing according to section 3.4 of [12].

## 6.4.2 FAP Requirements

---

The FAP shall only use the dedicated CHILD\_SA pair created during the tunnel establishment procedure for Remote IP Access according to section 6.3.5.

### 6.4.2.1 Outbound Traffic Processing

---

The FAP shall monitor the local network traffic. For any packet that is not originated by the FAP and has the remote MS's local network address as the destination address, the FAP shall send it using the CHILD\_SA for Remote IP Access to the SeGW. The FAP shall send the packet to the MS using ESP tunnel mode as specified in [12]. Except for the RIPA traffic, the FAP shall not forward traffic from any other nodes to the SeGW.

### 6.4.2.2 Inbound Traffic Processing

---

Upon receiving an IPsec packet from the SeGW via the CHILD\_SA for Remote IP Access, the FAP shall perform inbound packet processing according to section 3.4 of [12]. The FAP shall send the packets to the destination address at the local network.

## 6.4.3 SeGW Requirements

---

Upon the creation of the IPsec SA with the MS, and the IPsec CHILD\_SA with the FAP for Remote IP Access service, the SeGW shall tunnel the Remote IP Access traffic from the MS to the target FAP using the dedicated CHILD\_SA. In the other direction, the SeGW shall tunnel all traffic from the CHILD\_SA for Remote IP Access (from the FAP) to the MS using the IPsec tunnel with the MS.

### 6.4.3.1 Traffic from the MS to the FAP

---

Upon receiving any IPsec packets from the MS, the SeGW shall use the Security Association (SA) with the MS to perform inbound packet processing as specified in section 3.4 of [12], including but not limited to removing the outer headers, decrypting and verifying the integrity of the ESP payload, and reconstructing the entire IP datagram in the ESP Payload field.

The SeGW shall determine the target FAP associated with the MS (e.g., based on mapping between the IPsec tunnel with the FAP and the address assigned to the MS for RIPA service). The SeGW shall select the CHILD\_SA for Remote IP Access with the target FAP. The SeGW shall use the selected CHILD\_SA to perform outbound packet processing to the reconstructed IP datagram according to section 3.3 of [12], including but not limited to encapsulating and encrypting the entire reconstructed IP datagram, calculating the integrity check value, and constructing the outer header [27]. The SeGW shall send the resulting outbound IPsec packet to the target FAP via the CHILD\_SA for Remote IP Access.

### 6.4.3.2 Traffic from the FAP to the MS

---

For any IPsec packet received via the CHILD\_SA for Remote IP Access from the FAP, the SeGW shall perform inbound packet processing and reconstruct the entire IP datagram in the ESP payload as specified in section 3.4 of [12].

The SeGW shall first determine the set of MSs associated with the FAP (e.g., based on mapping between the IPsec tunnel with the MS and the IP address assigned to the MS for RIPA service). The SeGW shall then identify which MS the reconstructed IP datagram is intended for by comparing the destination IP address with the assigned internal IP address to the MS by the FAP's local network. The SeGW shall select the SA with the target MS. The SeGW shall perform outbound traffic processing to the IP datagram using the selected SA in the tunnel mode as specified in section 3.3 of [12]. The SeGW shall send the resulting IPsec packet to the target MS.

If the destination IP address from the reconstructed IP datagram does not match the MS's assigned IP address and it is not broadcast and multicast IP address, but received from the FAP using the CHILD\_SA for RIPA service, the SeGW shall discard the reconstructed IP datagram. If the destination IP address from the reconstructed IP datagram is the broadcast and multicast IP address, the SeGW shall encapsulate these packets to the corresponding CHILD\_SA for each MS that is associated with the FAP from which the packets are received.

## 6.5 Tunnel Disconnection

---

Tunnel disconnection may be initiated from the MS or from the SeGW, e.g., due to a timeout of the IKE SA lifetime set internally in the MS or SeGW, or due to a request from the HAAA server.

The tunnel disconnection procedure between the MS and the SeGW is performed via IKEv2.

### 6.5.1 MS Procedures

---

The MS shall use the procedures specified in IKEv2 [10] to delete the IPsec tunnel with the SeGW.

### 6.5.2 SeGW Requirements

---

The SeGW shall use the procedures specified in IKEv2 [10] to delete the IPsec tunnel with the MS. If there are no more MSs using RIPA with the given FAP, the SeGW shall use the IKEv2 procedures to close the CHILD\_SA pair with the FAP that was specifically created for the RIPA service.

If the CHILD\_SA pair for RIPA service with a FAP is terminated, the SeGW shall use the procedure specified in IKEv2 [10] to delete the RIPA IPsec tunnel with all the MSs that use RIPA service with the FAP.

### 6.5.3 Home AAA Requirements

---

When the remote IP access services has been terminated for the MS, the HAAA shall instruct the SeGW to disconnect the session for the MS by sending the RADIUS Disconnect-Request message or Diameter Abort-Session-Request command.

## 6.5.4 FAP Requirements

---

The FAP shall use the procedures specified in IKEv2 [10] to delete the CHILD\_SA pair for RIPA with the SeGW if the FAP decides to terminate the RIPA service for all MSs.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# 7 Accounting

The FAP performs the RAN accounting procedure as specified in [53] and [54]. The PDSN shall follow accounting procedures as specified in [2]. In addition, the FAP and PDSN may support FEID in A10 Connection Setup airlink records and PDSN UDR as specified in this section.

**Table 4 Additional Parameters in A10 Connection Setup Airlink Fields**

Item	Parameter	Max Payload Length (octets)	Format
Dx	FEID	16	String

**Table 5 Additional Parameters in PDSN UDR**

Item	Parameter	Description
D. Infrastructure Identifiers		
Dx	FEID	FEID of the FAP

**Table 6 Additional Accounting Parameter Attribute RADIUS Definitions**

RADIUS Attribute Definitions						
Item	Parameter	Type/ Vendor Type	Maximum Payload Length (in octets)	Format	Field	Special Values
D. Infrastructure Identifiers						
Dx	FEID	26/216	16	String	3GPP2_FEID	The FEID of the FAP.[6]

## 8 RADIUS Considerations

Table 7 shows the meaning of the RADIUS message coding in the columns of Table 8 and Table 9.

**Table 7 Meaning of the Request, Accept, Reject, Challenge columns of Table 8 and Table 9**

Coding	Meaning
0	This attribute shall not be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute may be present.
1	Exactly one instance of this attribute shall be present.

### 8.1 RADIUS Attributes between SeGW and Femtocell AAA for FAP Authorization

Table 8 summarizes the RADIUS attributes in the RADIUS messages exchanged between the SeGW and the Femtocell AAA.

**Table 8 RADIUS Attributes exchanged between the SeGW and the Femtocell AAA for FAP Authorization**

Attribute	Type	Value Type	Request	Accept	Reject	Disconnect	Comments
User-Name	1	String	1	0-1	0	1	User's NAI, Case Sensitive. [28] NAI format is FAP-FQDN@realm)
Class	25	String	0	0-1	0	0	[28]
Service-Type	6	Integer	1	0	0	0	[28] Set to "Authentication Only" per [28]
Session-Timeout	27	Integer	0	0-1	0	0	[28]
NAS-Identifier	32	String	0-1	0	0	0	[28]
NAS-IP-Address	4	Address	0-1 Note 1	0	0	0	[28]
NAS-IPv6-Address	95	Address	0-1 Note 1	0	0	0	[28]
Message-Authenticator	80	String	1	1	1	1	[28]

Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

### 8.2 RADIUS Attributes between SeGW and HAAA for RIPA

Table 9 summarizes the RADIUS attributes in the RADIUS messages exchanged between the SeGW and the HAAA.

**Table 9 RADIUS Attributes exchanged between the SeGW and the HAAA**

Attribute	Type	Value Type	Request	Accept	Reject	Challenge	Disconnect	Comments
User-Name	1	String	1	0-1	0	0	1	User's NAI, Case Sensitive. [28]
Class	25	String	0	0-1	0	0	0	
NAS-Identifier	32		0-1	0	0	0	0	[28]
NAS-IP-Address	4	Address	0-1 Note 1	0	0	0	0	[28]
NAS-IPv6-Address	95	Address	0-1 Note 1	0	0	0	0	[28]
EAP-Message	79	String	1+	1+	1+	1+	0	Used only for EAP.
MS-MPEE-Send-Key	26/*/16 (Vendor Type = 311)	String	0	0-1	0	0	0	If PSK is used, contains RIPA-IKEv2-Key. If EAP is used, contains the second 32 bytes of the MSK.
MS-MPPE-Recv-Key	26/17 (Vendor Type = 311)	String	0	1	0	0	0	Contains the first 32 bytes of the MSK. Only used for EAP.
Session-Timeout	27	Integer	0	0-1	0	0	0	[28]
Message-Authenticator	80	String	1	1	1	1	1	[28]
Session-Key-Nonces	26/212	String	0-1	0	0	0	0	Nonces exchanged between MS and SeGW, and sent from SeGW to HAAA for Key generation. Used only for PSK.[4]
Session-Key-Method	26/213	Integer	0-1	0	0	0	0	Indication that authorization for IKEv2 PSK is needed. Used only for PSK.
RIPA-Info	26/215	String	0	0+	0	0	0	

Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

### 8.3 RADIUS Attributes between FAP and AN- AAA for LIPA

Table 10 summarizes additional RADIUS attributes in the RADIUS messages exchanged between the FAP and the AN-AAA used for LIPA. Other attributes refer to [53] and [54].

**Table 10 Additional RADIUS Attributes exchanged between the FAP and AN- AAA for LIPA**

Attribute	Type	Value Type	Request	Accept	Reject	Disconnect	Comments
Local-IP-Access-Authorized	26/208	String	0	0-1	0	0	

### 8.4 RADIUS Vendor Specific Attributes

#### 8.4.1 Session-Key-Method

The Session-Key-Method VSA conveys the method for which the key included is used. This attribute shall be included in the RADIUS Access-Request message sent to the HAAA.

**Table 11 Session-Key-Method VSA**

1												2												3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type						Length						Vendor-ID																											
Vendor-ID (cont)						Vendor-Type						Vendor-Length																											
Vendor Value																																							

Type: 26

Length: 12

Vendor ID: 5535

Vendor-Type: 213

Vendor-Length: 6

Vendor-Value: A 32 bit unsigned integer representing an enumeration with the following values:

1: MIP6 IKEv2 PSK method (see [4])

2 RIPA IKEv2 PSK method.

3 and above are reserved.

8.4.2 RIPA-Info

Table 12 RIPA-Info VSA

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type						Length						Vendor-ID									
Vendor-ID (cont)											Vendor-Type					Vendor-Length					
Sub-Type (=1)						Length						Value (SeGW IPv4 or IPv6 address)									
Value (SeGW IPv4 or IPv6 address)											Value (SeGW IPv6 address)										
Value (SeGW IPv6 address)											Value (SeGW IPv6 address)										
Value (SeGW IPv6 address)											Sub-Type (=2)					Length					
Value (FEID)																					

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 215

Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for SeGW IP address

Length: Length of SeGW IP address (IPv4 = 6 octets, IPv6= 18 octets)

SeGW IP address:

This subtype is optional, The HAAA indicates the address of the SeGW IP address which has IPsec tunnel with associated FEID(s). If this subtype is not present, it implies that the SeGW that sent the RADIUS Access Request message is the serving SeGW which has the IPsec tunnel with the FAP's FEID(s).

Sub-Type (=2): Sub-Type for FEID

Length: Length of FEID

FEID:

This subtype shall be present one or more times. The HAAA indicates the FAP's FEID that is authorized to be accessed by the MS.

8.4.3 Local-IP-Access-Authorized

The Local-IP-Access-Authorized VSA indicates if the MS is authorized to use LIPA (i.e., receive a local IP address from the FAP). This attribute may be included in the RADIUS Access-Accept message sent from the AN-AAA to the FAP on the A12 interface.

Table 13 Local-IP-Access-Authorized VSA

1											2											3										
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
Type						Length						Vendor-ID																				
Vendor-ID (cont)											Vendor-Type					Vendor-Length																
Vendor Value																																

Type: 26  
Length: 12  
Vendor ID: 5535  
Vendor-Type: 208  
Vendor-Length: 6  
Vendor-Value: A 32 bit unsigned integer representing an enumeration with the following values:  
    0: MS is not authorized to be assigned a local IP address.  
    1: MS is authorized to be assigned a local IP address.  
    2 and above are reserved.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## 9 Diameter Considerations

### 9.1 Diameter Applications and Commands

#### 9.1.1 FAP Authorization

This document uses the Diameter NASREQ Application for FAP authorization (see [23]).

An SeGW supporting this authorization scheme shall advertise support by including Diameter NASREQ Application ID in the Diameter capability exchange procedure define by Diameter base [29].

##### 9.1.1.1 Command Codes

FAP Authorization uses the following command codes:

**Table 14 Diameter Command Codes for FAP Authorization**

Command-Name	Abbreviation	Code	Reference
AA-Request	AAR	265	[14]
AA-Answer	AAA	265	[14]
Session-Termination-Request	STR	275	[29]
Session-Termination-Answer	STA	275	[29]
Abort-Session-Request	ASR	274	[29]
Abort-Session-Answer	ASA	274	[29]

Command AAR is sent by the SeGW to the Femtocell AAA to initiate a FAP authorization procedures. Command AAA is sent in response to the AAR.

STR is used by the SeGW to inform the Femtocell AAA when the IPsec tunnel between the FAP and the SeGW has terminated. The Femtocell AAA acknowledge reception of the STR with an STA.

ASR is used by the Femtocell AAA to terminate a IPsec session between the FAP and SeGW. ASA is used by the SeGW to acknowledge receipt of the ASR.

#### 9.1.2 RIPA Authentication

This document uses two Diameter Applications as follows to support RIPA:

- EAP based IKE Authentication uses 3GPP2 Diameter IKE EAP (IKEEAP) specified in this document; and
- PSK based IKE Authentication used 3GPP2 Diameter IKE PSK Authentication IKEPSK specified in this document.

An SeGW supporting either of these two IKE Authentication schemes shall advertise support by including these Application IDs in the Diameter capability exchange procedure define by Diameter base [29].

### 9.1.2.1 Command Codes for Diameter EAP based IKEv2 Authentication

The EAP based IKEv2 Authentication Application supports the following command codes:

**Table 15 Diameter Command Codes for EAP based IKEv2**

Command-Name	Abbreviation	Code	Reference
Diameter-EAP-Request	DER	268	[30]
Diameter-EAP-Answer	DEA	268	[30]
Session-Termination-Request	STR	275	[29]
Session-Termination-Answer	STA	275	[29]
Abort-Session-Request	ASR	274	[29]
Abort-Session-Answer	ASA	274	[29]

Command DER is sent by the SeGW to the HAAA to initiate a Remote IP access service authentication and authorization procedures. Command DEA is sent in response to the DER. If the RIPA authentication and authorization is successful, the DEA shall also include the information of the SeGW IP address and FEID(s). The Application-ID field of the Diameter header shall be set to the Diameter IKEv2-EAP Application ID (value of TBD).

STR is used by the SeGW to inform the HAAA when the IPsec tunnel between the MS and the SeGW has terminated. The HAAA acknowledges reception of the STR with an STA. These commands are used as per [29].

ASR is used by the HAAA to terminate a IPsec session between the MS and SeGW. It is used as per [29]. ASA is used by the SeGW to acknowledge receipt of the ASR. Subsequently the SeGW shall take further actions to terminate the corresponding IPsec tunnel between the MS and the SeGW and release the corresponding CHILD\_SA pair between the SeGW and the FAP if there is no other MSs using RIPA with the given FAP.

#### 9.1.2.1.1 Diameter-EAP-Request Command

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    { User-Name }
    [ Destination-Host ]
    [ NAS-Identifier ]
    [ NAS-IP-Address ]
    [ NAS-IPv6-Address ]
    [ NAS-Port-Type ]
    { EAP-Payload }
    * [ AVP ]
```

#### 9.1.2.1.2 Diameter-EAP-Answer Command

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
```

- { Origin-Host }
- { Origin-Realm }
- [ User-Name ]
- [ EAP-Payload ]
- [ EAP-Reissued-Payload ]
- [ EAP-Master-Session-Key ]
- [ EAP-Key-Name ]
- [ Multi-Round-Time ]
- [ RIPA-Info]
- \* [ AVP ]

**9.1.2.2 Command Codes for Diameter Authentication using PSK based IKEv2**

The PSK based IKEv2 Authentication Application supports the following command codes:

**Table 16 Diameter Command Codes for PSK based IKEv2**

Command-Name	Abbreviation	Code	Reference
IKEv2-PSK-Request	IKEPSKR	TBD	[4]
IKEv2-PSK-Answer	IKEPSKA	TBD	[4]
Session-Termination-Request	STR	275	[29]
Session-Termination-Answer	STA	275	[29]
Abort-Session-Request	ASR	274	[29]
Abort-Session-Answer	ASA	274	[29]

[Editor Note: Assignment for Diameter command codes has been requested to IETF.]

Commands IPR/IPA are specified below and are used by the SeGW to retrieve the Preshared Key needed to authenticate the MS. The IKEv2-PSK-Request /Answer commands are exchanged between the SeGW and the HAAA. The commands are exchanged in order to provide the SeGW with keys necessary to validate the AUTH message of the IKEv2 exchange. If the RIPA authentication and authorization is successful, the IPA shall also include the information of the SeGW IP address and FEID(s). The Application-ID field of the Diameter header shall be set to the Diameter IKE PSK Authentication IKEPSK Application ID (value of TBD). [Editor Note: Assignment for Diameter application ID has been requested to IETF.]

STR is used by the SeGW to inform the HAAA when the IPsec tunnel has terminated. The HAAA acknowledge reception of the STR with an STA. These commands are used as per [29].

ASR is used by the HAAA to terminate a IPsec session between the MS and SeGW. It is used as per [29]. ASA is used by the SeGW to acknowledge receipt of the ASR. Subsequently the SeGW shall take further actions to terminate the corresponding IPsec tunnel.

**9.1.2.2.1 IKEv2-PSK-Request Command**

The IKEv2-PSK-Request message, indicated with the Command-Code set to TBD, is sent from the SeGW to the HAAA to initiate IKEv2 PSK authentication and authorization. The Application-ID field of the Diameter Header shall be set to the Diameter IKEv2-PSK-Request Application ID (value of TBD).

```

<IKEPSKR> ::= <Diameter Header: TBD IKEPSKR, PXY>
               <Session-Id>
               { Auth-Application-Id }
               { Origin-Host }
               { Origin-Realm }
    
```

```

    { Destination-Realm }
    { Auth-Request-Type }
    { User-Name }
    { SFF-KEY-Nonces }
    [ Destination-Host ]
    [ Origin-State-Id ]
    [ Auth-Session-State ]
    [ NAS-IP-Address ]
    [ NAS-IPv6-Address ]
    [ NAS-Port-Type ]
    [ NAS-Identifier ]
    *[Proxy-Info]
    *[Route-Record]
    *[AVP]

```

Note 1: Auth-Request-Type value shall be set to AUTHORIZE\_ONLY (2) as specified in [29].

Note 2: SFF-KEY-Nonces contains nonces used for RIPA-IKEv2-Key generation.

#### 9.1.2.2.2 IKEv2-PSK-Answer Command

The IKEv2-PSK-Answer message, indicated by the Command-Code field set to TBD, is sent by the HAAA to the SeGW in response to the IKEPSKR command. If the RIPA authorization procedure was successful then the response shall include Master-Security-Association. The Application-ID field in the Diameter header shall be set to the Diameter PSK based IKE Authorization Application-ID (value of TBD). The following specifies the allowed AVPs in the command:

```

<IKEPSKA> ::= < Diameter Header: TBD IKEPSKA, PXY >
    <Session-Id>
    { Auth-Application-Id }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [Master-Security-Association ]
    [ User-Name ]
    [ Origin-State-Id ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    [ Re-Auth-Request-Type ]
    * [ Redirected-Host ]
    [ Redirected-Host-Usage ]
    [ Redirected-Max-Cache-Time ]
    [RIPA-Info]
    *[Proxy-Info ]
    *[Route-Record ]
    *[ AVP ]

```

Note 1: Master-Security-Association is a grouped AVP that contains the RIPA-IKEv2-Key that corresponds to the NAI that was requested in the IPR command. This AVP shall be returned unless there is a failure.

## 9.2 Diameter AVPs

Table 17 shows the meaning of the Diameter AVPs specified in columns of Table 18.

**Table 17 Meaning of the Request, Answer columns**

Coding	Meaning
0	This attribute shall not be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute may be present.
1	Exactly one instance of this attribute shall be present.

Table 18 lists the Diameter AVPs used in the Diameter commands exchanged between the SeGW and the HAAA.

**Table 18 Diameter AVP exchanged between the SeGW and the HAAA**

Attribute	AVP	Code Value Type	Request	Answer	Comments
User-Name	1	UTF8String	1	0-1	User's NAI, Case Sensitive.[29]
NAS-IP-Address	4	OctetString	0-1	0	IP Addr of NAS in SeGW
Session-Timeout	27	Unsigned32	0	0-1	Seconds until forced session termination and re-authentication required.[29]
Idle-Timeout	28	Unsigned32	0	0-1	Seconds of idle time before auto-termination of session.[29]
Authorization-Lifetime	291	Unsigned32	0-1	0-1	0-Immediate re-authentication [29]
NAS-Identifier	32	UTF8String	0-1	0	Alternative to NAS-IP_Address to identify NAS.[29]
NAS-Port-Type	61	Enumerated	0-1	0	5 = virtual.[14]
NAS-IPv6-Address	95	OctetString	0-1	0	IPv6 Addr of NAS in SeGW.[14]
Master-Security-Association	5535/49	Grouped	0	0-1	Grouped AVP that includes session key related information.
SFF-KEY-Nonces	5535/46	Grouped	0-1	0	Grouped AVP that describes Ni and Nr nonces exchanged between MS and SeGW, and sent from SeGW to HAAA for RIPA-IKEv2-Key generation.
Ni	5535/47	Unsigned32	0-1	0	The IKEv2 Initiator's nonce. [4]
Nr	5535/48	Unsigned32	0-1	0	The IKEv2 Responder's nonce. [4]

Attribute	AVP	Code Value Type	Request	Answer	Comments
RIPA-Info	5535/ 53	Grouped	0-1	0	
FEID	5535/ 54	EUI-64	0	1+	
SeGW-IP-Address	5535/ 55	IP address	-	0	

## 9.2.1 Master-Security-Association

The Master-Security-Association (AVP Code 5535/49) is of type Grouped and contains the session related information for use with the IKEv2 PSK method (see [31]).

```
Master-Security-Association ::= < AVP Header: 5535/49 >
    { Key }
    [ MSA-Lifetime ]
    [ MSA-SPI ]
    * [ AVP ]
```

### 9.2.1.1 Key

Key AVP (Code 5535/50) is of type OctetString and contains the session key RIPA-IKEv2-Key for the associated RIPA IKEv2 PSK authorization. When the Diameter server computes the session key it is placed in this AVP most significant byte first.

### 9.2.1.2 MSA-Lifetime

MSA-Lifetime AVP (Code 5535/51) is of type Unsigned32 and represents the period of time (in seconds) for which the RIPA-IKEv2-Key is valid. The associated RIPA-IKEv2-Key shall not be used if the lifetime has expired.

### 9.2.1.3 MSA-SPI

MSA-SPI AVP (Code 5535/52) is of is of type Unsigned32 and contains an SPI associated with the RIPA-IKEv2-Key.

## 9.2.2 SFF-KEY-Nonces

The IKEv2-Nonces AVP (Code 5535/46) is of type Grouped and contains the nonces exchanged between MS and HA during IKEv2 initial exchange and used for RIPA-IKEv2-Key generation (see [31]).

### 9.2.2.1 Ni

The Ni AVP (Code 5535/47) is of type Unsigned32 and contains IKEv2 initiator nonce.

### 9.2.2.2 Nr

The Ni AVP (Code 5535/48) is of type Unsigned32 and contains IKEv2 responder nonce.

### 9.2.3 RIPA-Info

---

The RIPA-Info AVP (Code 5535/53) is of type Grouped and contains the SeGW IP address and FEID exchanged between SeGW and HAAA during RIPA authentication and authorization.

```
RIPA-Info ::= < AVP Header: 5535/53>
                *{FEID}
                [SeGW-IP-Address]
                *[AVP]
```

#### 9.2.3.1 FEID

---

FEID AVP (Code 5535/54) is of type EUI-64 and contains the FEIDs of FAP(s) that is accessible to the MS through Remote IP Access service.

#### 9.2.3.2 SeGW-IP-Address

---

SeGW-IP-Address AVP (Code 5535/55) is of type IPv4 or IPv6 address and contains the IPv4 or IPv6 address of the SeGW that is currently serving the FAP(s) accessible to the MS through Remote IP Access.

## 9.3 Experimental Result-Code AVP Values

---

This section defines new result code values that shall be supported by all Diameter implementations that conform to this document. When one of the result codes specified here is included in a response, it shall be inside an Experimental-Result AVP, and the Result-Code AVP shall be absent.

### 9.3.1 Permanent Failures

---

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again. The following Diameter Experimental Result Codes are 3GPP2 specific.

**DIAMETER\_ERROR\_USER\_NO\_FAP\_SUBSCRIPTION (5003)**

A command was received for a FAP with no FAP subscription.

## 10 eHRPD Packet Data Femtocell Operation

---

The UE shall follow the procedures specified in [50] and [51] to connect to Evolved Packet Core (EPC).

The UE and eFAP shall follow the procedures in this document for Local IP access and Remote IP access.

The eFAP shall follow the FAP procedures defined in this document and [52], except the following operations:

- eFAP shall follow the eAN procedures to interface with the HSGW as specified in [52] and [51] with the following exception:
  - The A11 interface may include the FEID parameter as specified in section 7 of this document<sup>7</sup>.
- eFAP shall follow the eAN procedures to interface with the UE as specified in [50].

---

<sup>7</sup> In 3GPP Release 9, this indication is used only for accounting purpose.

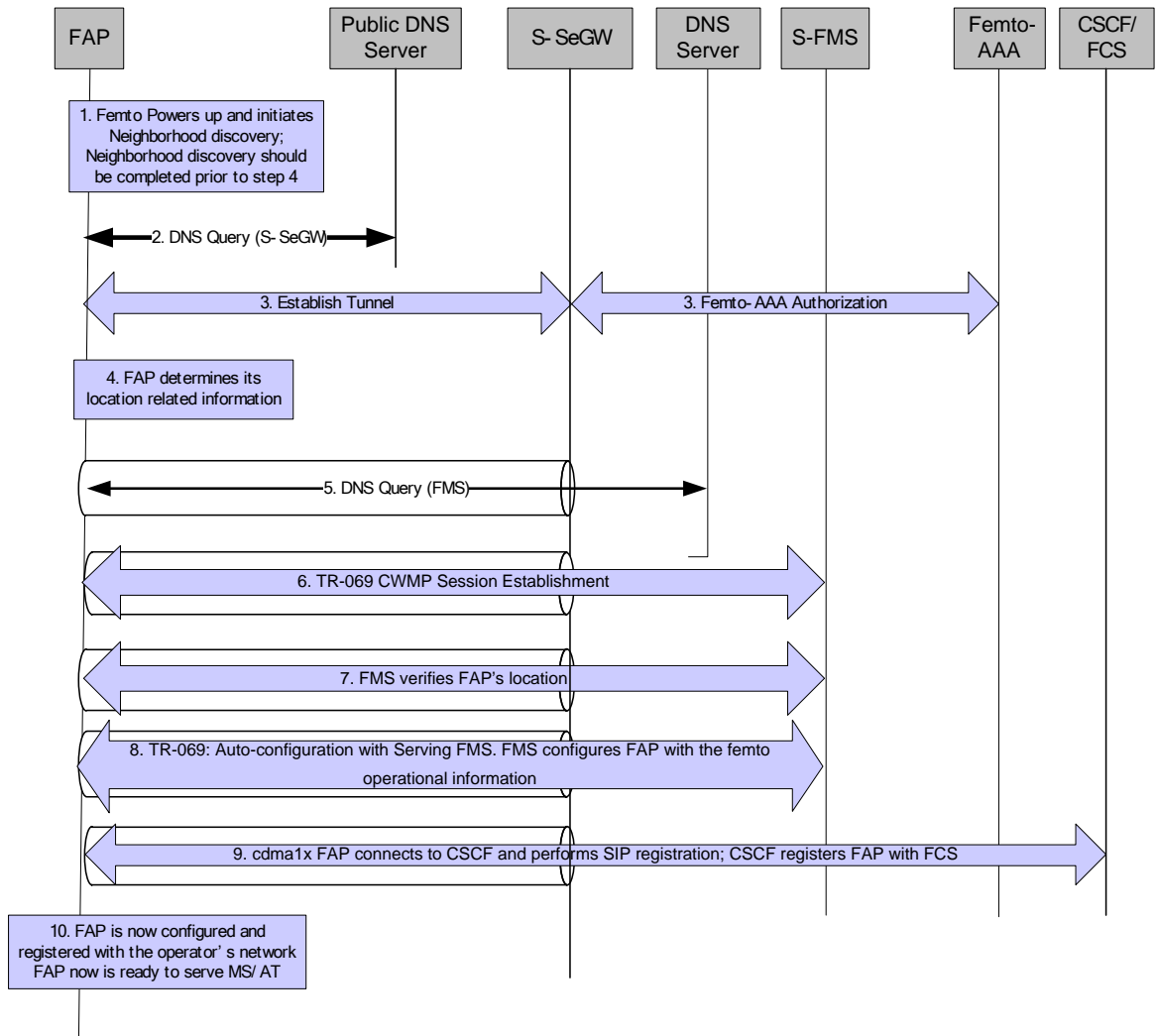
# A Annex – Call Flow Examples (Informative)

This Annex is informative.

## A.1 Femtocell Network Connectivity Call Flow

### A.1.1 Femtocell Network Connectivity Call Flow without Redirection

Figure 5 shows the Femtocell network connectivity call flow without redirection for 1x FAP, HRPD FAP, or HRPD and 1x Hybrid FAP unless noted in the step descriptions.



**Figure 5 Femtocell Network Connectivity Call Flow without Redirection**

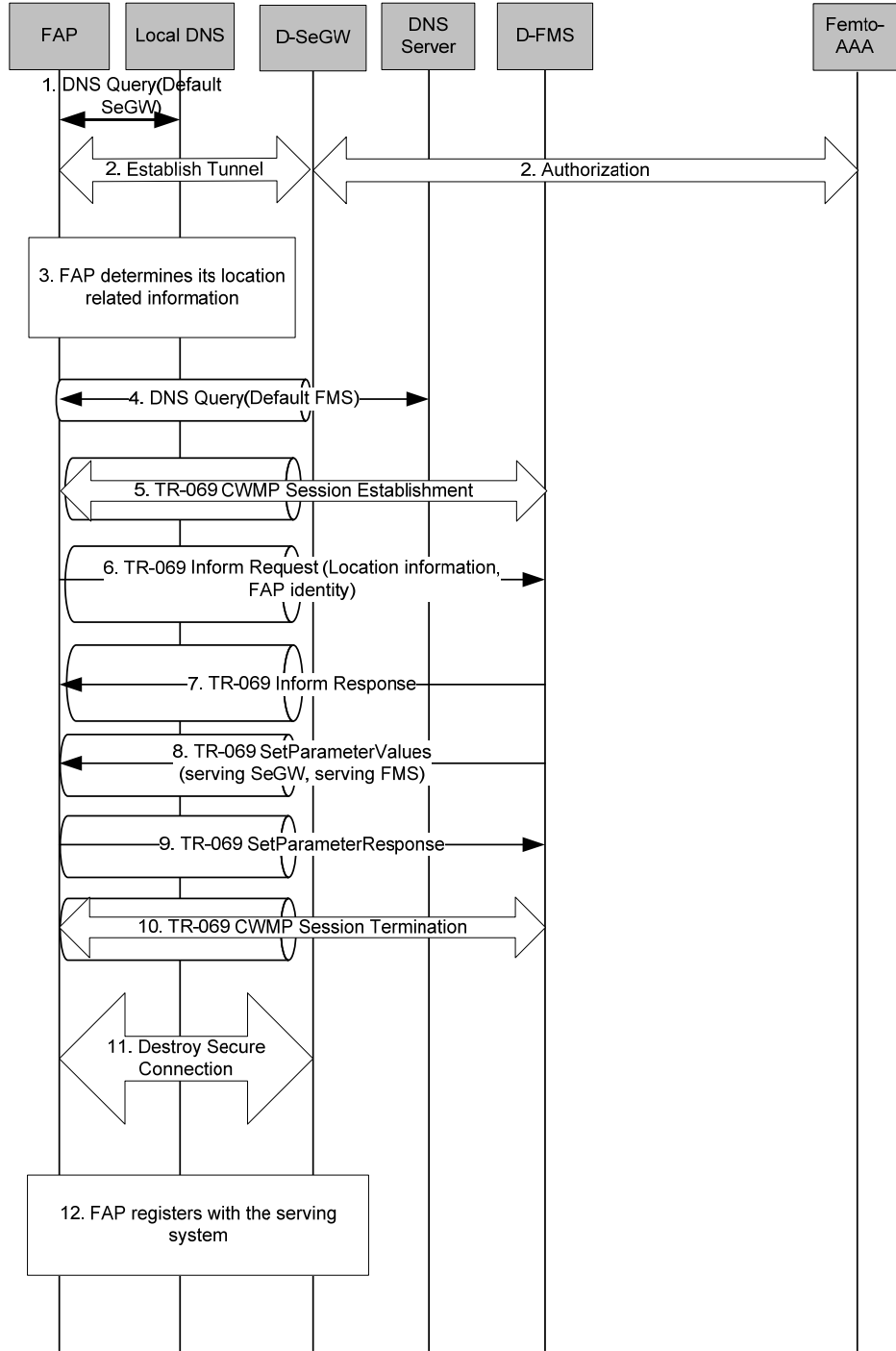
1. The FAP performs neighborhood discovery as specified in [1]. This step may include the position location determination, for example, using GPS and/or macro system overhead information. The FAP also reads the system parameter messages of the strongest neighboring macro cell to obtain the system information such as SID, NID, Subnet ID etc.

2. After obtaining an IP address from the local/private network, the FAP performs SeGW discovery through the public DNS server. 1
3. The FAP establishes an IPsec tunnel with the SeGW discovered in step 2. In this step, FAP subscription authorization is also performed. Refer to sections 3.2 and 3.3. 2
4. The FAP determines its location related information. How the FAP determines its location related information is outside of the scope of this document. 3
5. The FAP performs FMS discovery through the established IPsec tunnel. 4
6. The FAP and FMS establish a TR-069 CWMP session. 5
7. The FAP connects with the FMS and provides its location information to the FMS and the FMS verifies the geo-location for the FAP. 6
8. The FMS performs FAP provisioning and configuration. The FAP sends its neighborhood information during the auto-configuration stage. The FAP is configured with the Femtocell parameters and identities and the IP addresses of the network elements as specified in section 3. 7
9. The FAP performs SIP registration with the CSCF. The CSCF performs third party registration of the FAP with the FCS. This step only applies to a 1x FAP or a 1x/HRPD Hybrid FAP. 8
10. The FAP has now completed the network connectivity procedure and is ready to serve the MS. 9

### A.1.2 Femtocell Network Connectivity Call Flow with Redirection to Serving System

Figure 6 shows the FAP network connectivity call flow with FMS redirection for 1x FAP, HRPD FAP, or HRPD and 1x Hybrid FAP unless noted in the step descriptions.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59



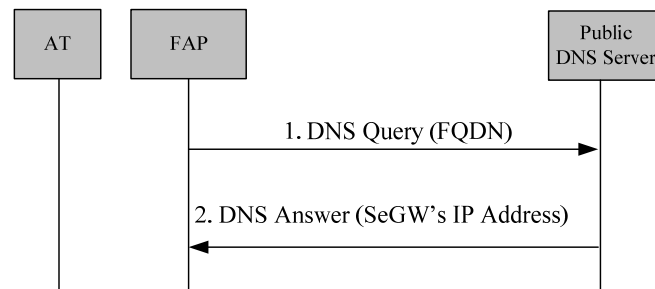
**Figure 6 Femtocell Network Connectivity with Redirection**

1. After obtaining an IP address from the local/private network, the FAP performs FSGW discovery through the local DNS server.
2. The FAP establishes an IPsec tunnel with the FSGW discovered in step 1. In this step, FAP subscription authorization is also performed.
3. The FAP determines its location related information. How the FAP determines its location related information is outside of the scope of this document.

4. The FAP performs FMS discovery through the established IPsec tunnel. 1
5. The FAP and the default FMS establish a TR-069 CWMP Session. 2
6. The FAP sends to the FMS an Inform Request containing location parameters and FAP identity, etc. 3
7. The FMS returns an Inform Response to accept the FAP location information. 4
8. The FMS then prepares for the local access information (including serving Security Gateway and serving FMS) and sets the values on the FAP using the SetParameterValues message. 5
9. The FAP acknowledges the update by returning a SetParameterValues Response message. 6
10. The FAP releases the TR-069 CWMP Session between the FAP and the default FMS. 7
11. The IPsec tunnel between the FAP and the default SeGW is terminated. 8
12. The FAP then registers with the serving system using the provisioned identity of the serving SeGW and the serving FMS. Refer to appendix A.1.1. 9

## A.2 SeGW Discovery

Figure 7 shows SeGW Discovery if the IP address of the SeGW is unknown to the FAP.



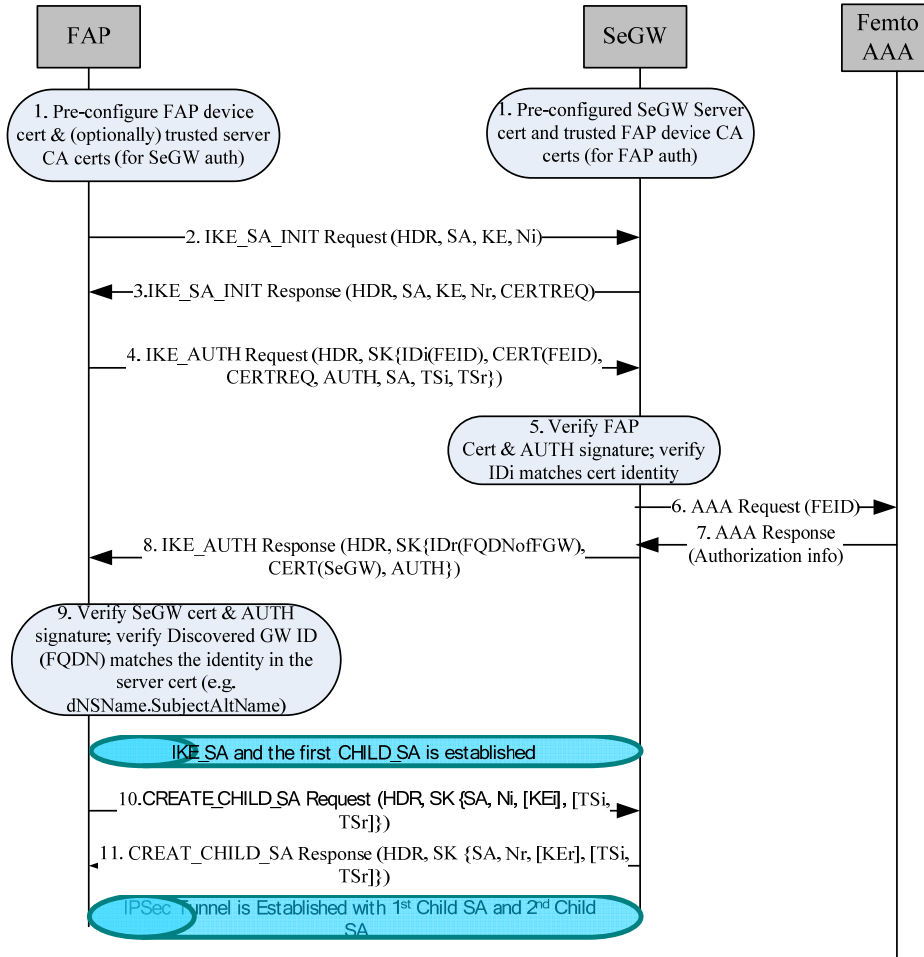
**Figure 7 SeGW Discovery**

1. The FAP sends a DNS query to the DNS Server including the FQDN of the SeGW which is preconfigured in the FAP or is built by the FAP as specified in section 3.2.1. 40
2. The DNS server responds with a DNS answer including the SeGW's IP address. 41

## A.3 FAP-SeGW IPsec Tunnel Establishment

Figure 8 shows FAP-SeGW IPsec tunnel establishment. In the call flow, as an example, a CHILD\_SA pair is created. 42

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59



**Figure 8 IPsec Tunnel Establishment**

1. The FAP is assigned a device certificate during its manufacturing. The FAP device certificate is signed by a Certificate Authority (device certificate CA) trusted by the cdma2000 operator. The private key for the certificate is stored securely at the FAP. Similarly, the SeGW is assigned a server certificate. The private key of the SeGW server certificate is stored securely at the SeGW. The SeGW is also configured with list of the root certificates corresponding to the trusted device certificate CAs. The FAP may also be configured with the list of root CA certificates corresponding to the server certificates that the FAP will accept for the SeGW.
2. The FAP initiates the IKEv2 exchange with the SeGW, known as IKE\_SA\_INIT exchange by issuing a IKE\_SA\_INIT Request to negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange with the SeGW. In addition, using the NAT Traversal procedures outlined in section 2.23 of [10], the initiator includes NAT\_DETECTION\_SOURCE\_IP and NAT\_DETECTION\_DESTINATION\_IP payloads to negotiate support for UDP encapsulation.
3. The SeGW responds with IKE\_SA\_INIT Response by choosing a cryptographic suite from the initiator's offered choices, completing the Diffie-Hellman and nonce exchange with the FAP. In addition, the SeGW includes the list of FAP CA certificates that it will accept in its CERTREQ payload. For successful FAP authentication, the CERTREQ payload has to contain at least one CA certificate that is in the trust chain of the FAP device certificate. At this point in the negotiation, IKE\_SA\_INIT exchange is complete

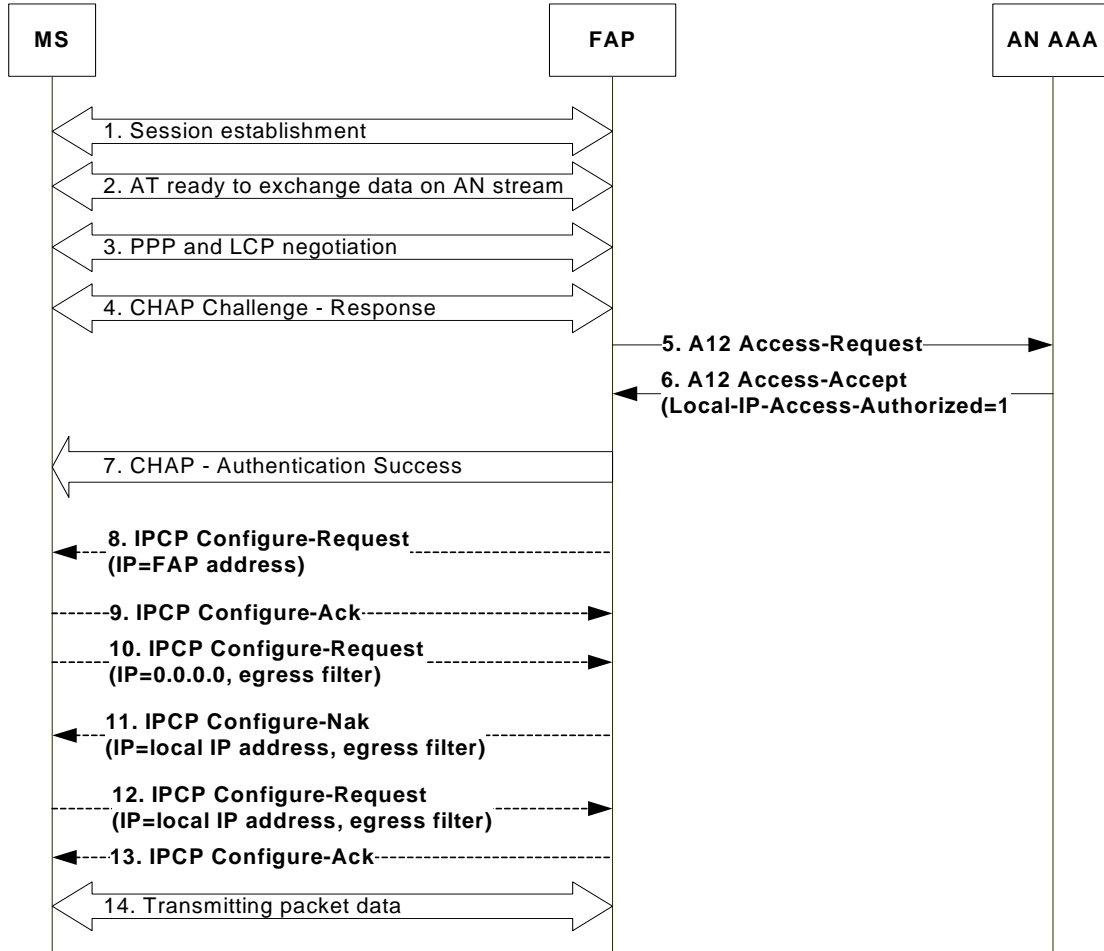
- and all but the headers of all the messages that follow are encrypted and integrity protected.
4. The FAP initiates the IKE\_AUTH exchange with the SeGW by setting the IDi payload to FEID, CERT payload set to the FAP device certificate corresponding to the FEID, and the AUTH payload containing the signature of the previous IKE\_SA\_INIT Request message (in step 2) generated using the private key of the FAP device certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload. The FAP also includes the CERTREQ payload that contains the list of CA certificates for SeGW (server) authentication. For successful SeGW authentication, the CERTREQ payload has to contain at least one CA certificate that is in the trust chain of the SeGW server certificate.
  5. Using the CA certificate corresponding to the FAP device certificate, the SeGW first verifies that the FAP device certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the FAP device certificate. If the verification is successful, using the public key of the FAP device certificate, the SeGW generates the expected AUTH payload and compares it with the received AUTH payload. If they match, then the authentication of the FAP is successful. Otherwise, the SeGW sends an IKEv2 Notification message indicating authentication failure.
  6. If the network policy requires Femtocell subscription authorization, the SeGW contacts the Femtocell AAA to verify that the FAP identified by FEID is authorized to provide service.
  7. The Femtocell AAA responds with the authorization result. If the authorization is not successful, the SeGW sends an IKEv2 Notification message indicating authorization failure. Otherwise, the SeGW proceeds with server authentication.
  8. The SeGW responds with the IKE\_AUTH Response by setting the IDr payload to the FQDN of the SeGW, CERT payload set to the SeGW server certificate corresponding to the FQDN and the AUTH payload containing the signature of the IKE\_SA\_INIT Response message (in step 3) generated using the private key of the SeGW server certificate. The authentication algorithm used to generate AUTH payload is also included in the AUTH payload.
  9. Using the CA certificate corresponding to the SeGW server certificate, the FAP first verifies that the SeGW server certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to identify in the server certificate and contains the expected SeGW value as discovered during the SeGW discovery procedures. If the verification is successful, using the public key of the SeGW server certificate, the FAP generates the expected AUTH payload and compares it with the received AUTH payload. If they match, then the SeGW (server) authentication is successful. This completes the IKE\_AUTH exchange. An IPsec SA with first CHILD\_SA pair has been established between the FAP and the SeGW. The first CHILD\_SA pair is used for best effort traffic, Tunnel management (F<sub>x</sub>3), and FAP Configuration messages.
  10. The FAP sends CREATE\_CHILD\_SA request for setting up the second CHILD\_SA pair.
  11. The SeGW responds with CREATE\_CHILD\_SA Response message. The second CHILD\_SA pair is used for SIP Signaling and (HRPD) A11 Signaling and/or 1x VoIP and HRPD (A10) VoIP bearer.

## A.4 Local IP Access Call Flows

This section describes the call flows associated with bringing up the LIPA interface at the MS.

## A.4.1 Successful LIPA Session Establishment

This scenario describes the call flow associated with session establishment for an MS that supports LIPA.



**Figure 9 Successful LIPA Session Establishment**

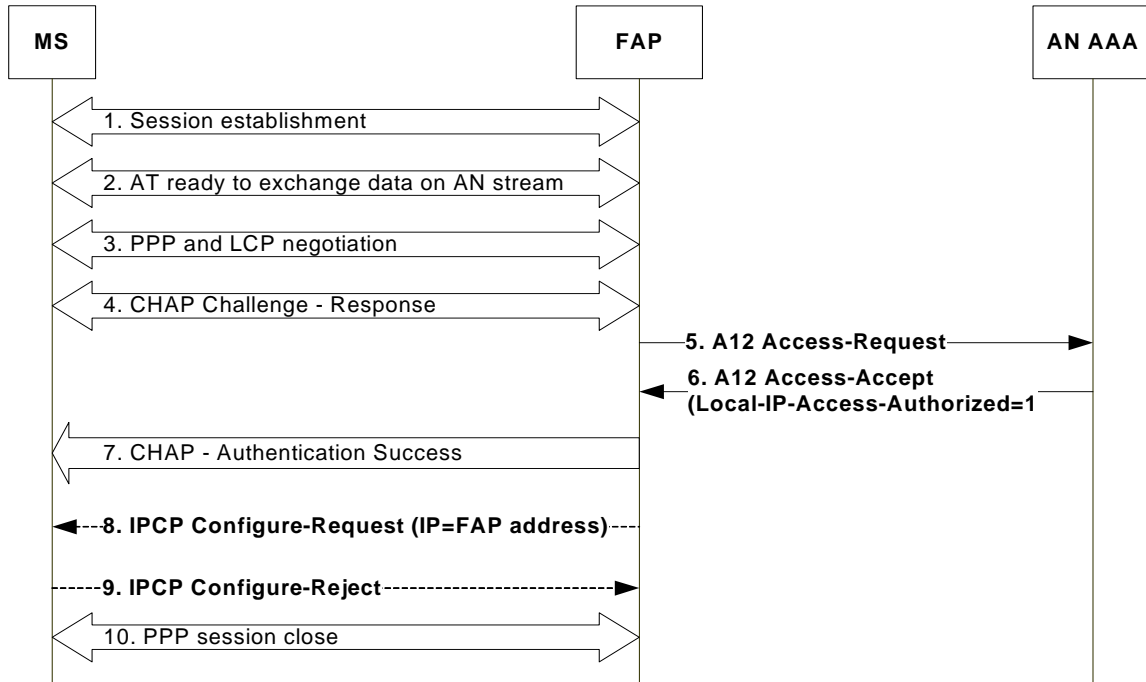
1. The MS and the FAP initiate HRPD session establishment. During this procedure, the FAP does not receive a UATI for an existing HRPD session. Since no session exists between the MS and the FAP, a session is established where protocols and protocol configurations are negotiated, stored and used for communications between the MS and the FAP. Refer to C.S0024 [9], Session Layer.
2. The MS indicates that it is ready to exchange data on the access stream (e.g., the flow control protocol for the default packet application bound to the FAP is in the open state).
3. The MS and the FAP initiate Point-to-Point Protocol (PPP) and LCP negotiations for access authentication for the architecture specified in A.S0008 (or terminal authentication for the architecture specified in A.S0009, refer to [53], [54]). Refer to RFC 1661 [36].
4. If the FAP supports access/terminal authentication and the A12 interface, the FAP generates a random challenge and sends it to the MS in a CHAP Challenge message in accordance with RFC 1994 [39].

5. When the FAP receives the CHAP response message from the MS, it sends an Access-Request message on the A12 interface to the AN-AAA, which acts as a RADIUS server in accordance with RFC 2865 [28]).
6. The AN-AAA looks up a password based on the User-name attribute in the Access-Request message and if the access/terminal authentication passes (as specified in RFC 1994 [39] and RFC 2865 [28]), the AN-AAA sends an Access-Accept message on the A12 interface in accordance with RFC 2865 [28]. The Access-Accept message contains a RADIUS attribute with Type set to 20 (Callback-Id), which is set to the MN ID of the MS. The Access-Accept message also includes a RADIUS attribute Local-IP-Access-Authorized indicating the MS is authorized to be assigned a local IP address.
7. The FAP returns an indication of CHAP access/terminal authentication success to the MS. Refer to RFC 1994 [39].
8. The FAP sends an IPCP Configure-Request message including its IP address.
9. The LIPA-capable MS sends an IPCP Configure-Ack message.
10. The MS sends an IPCP Configure-Request message to the FAP to request a local IP address. The MS may include either a NULL IP address or the non-zero IP address it wants to use for the LIPA interface. The MS also includes a vendor specific option indicating it currently has no egress packet filter criteria.
11. The FAP assigns a local IP address for the MS and sends it to the MS in an IPCP Configure-Nak message. The FAP also includes a vendor specific option that includes the egress packet filter criteria that the MS should use to determine for each packet whether it should traverse through the LIPA interface.
12. The MS sends an IPCP Configure-Request message with the local IP address assigned to it and the vendor specific option indicating the egress packet filter criteria to be use.
13. The FAP sends an IPCP Configure-Ack message in acknowledgement to the IPCP Configure-Request message received in step '12'.
14. At this point, the main connection is established and packet data can flow from the MS to the local intranet and internet through the LIPA interface at the MS without using the operator's network resources.

#### **A.4.2 LIPA not Supported at MS**

---

This scenario describes the call flow associated with session establishment for an MS that does not support LIPA.



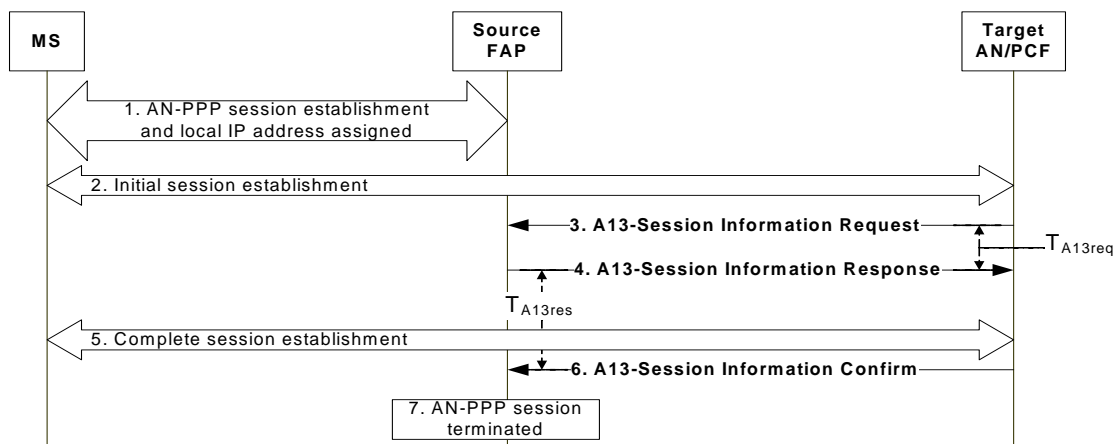
**Figure 10 LIPA not Supported by MS: Session Establishment Failure**

1. The MS and the FAP initiate HRPD session establishment. During this procedure, the FAP does not receive a UMSI for an existing HRPD session. Since no session exists between the MS and the FAP, a session is established where protocols and protocol configurations are negotiated, stored and used for communications between the MS and the FAP. Refer to C.S0024 [9], Session Layer.
2. The MS indicates that it is ready to exchange data on the access stream (e.g., the flow control protocol for the default packet application bound to the FAP is in the open state).
3. The MS and the FAP initiate PPP and LCP negotiations for access authentication for the architecture specified in A.S0008 (or terminal authentication for the architecture specified in A.S0009, refer to [53], [54]). Refer to RFC 1661 [36].
4. If the FAP supports access/terminal authentication and the A12 interface, the FAP generates a random challenge and sends it to the MS in a CHAP Challenge message in accordance with RFC 1994 [39].
5. When the FAP receives the CHAP response message from the MS, it sends an Access-Request message on the A12 interface to the AN-AAA which acts as a RADIUS server in accordance with RFC 2865[28]).
6. The AN-AAA looks up a password based on the User-name attribute in the Access-Request message and if the access/terminal authentication passes (as specified in RFC 1994 [39] and RFC 2865 [28]), the AN-AAA sends an Access-Accept message on the A12 interface in accordance with RFC 2865 [28]. The Access-Accept message contains a RADIUS attribute with Type set to 20 (Callback-Id), which is set to the MN ID of the MS. The Access-Accept message also includes a RADIUS attribute Local-IP-Access-Authorized indicating the MS is authorized to be assigned a local IP address.
7. The FAP returns an indication of CHAP access/terminal authentication success to the MS. Refer to RFC 1994 [39].
8. The FAP sends an IPCP Configure-Request message including its IP address.

9. The MS sends an IPCP Configure-Reject message back to the FAP. The MS may also drop the IPCP packet received from the FAP over the AN-PPP stream. In this case, the FAP may repeat sending the IPCP Configure-Request message multiple times.
10. The FAP terminates the AN-PPP session.

### A.4.3 LIPA Terminated after Handoff

This scenario describes the call flow associated with termination of LIPA upon completion of handoff from the source FAP.



**Figure 11 LIPA Terminated After Handoff**

1. The source FAP and the MS establish an AN-PPP session and the MS is also assigned a local IP address.
2. Upon the MS crossing a mobility boundary, the MS and the target AN/PCF initiate HRPD session establishment. During this procedure, the target AN/PCF receives the UATI of an existing HRPD session. The MS terminates its AN-PPP session as it crosses the HRPD subnet boundary.

Note: The target AN/PCF can send the A13-Session Information Request message to the source FAP via the FGW, based on the destination IP address provided for the A13-Session Information Request message. Refer to section 3.3.3.1, [1].

3. The target AN/PCF sends an A13-Session Information Request message to the source FAP to request the HRPD session information for the MS. The A13-Session Information Request message shall include the received UATI, the Security Layer Packet and Sector ID. The target AN/PCF starts timer  $T_{A13req}$ .
4. The source FAP validates the A13-Session Information Request and sends the requested HRPD session information of the MS to the target AN/PCF in an A13-Session Information Response message. The source FAP starts timer  $T_{A13res}$ . The target AN/PCF stops timer  $T_{A13req}$ .
5. The MS and the target AN/PCF complete the establishment of the HRPD session.
6. The target AN/PCF sends an A13-Session Information Confirm message to the source FAP to indicate that the target AN/PCF has received the HRPD session information. Upon receipt of the A13-Session Information Confirm message, the source FAP deletes the associated MS HRPD session information. The source FAP stops timer  $T_{A13res}$ .

7. Upon receipt of the A13-Session Information Confirm message, the source FAP also deletes the AN-PPP session.

## A.5 Remote IP Access Call Flows

### A.5.1 Redirection Based SeGW Discovery with EAP Authentication

Figure 12 shows a call flow in which the MS discovers the SeGW through redirection mechanism, in which EAP authentication is used for IPsec establishment between the MS and the SeGW. This call flow assumes the MS obtains the SeGW1 IP address through DNS discovery or other ways.

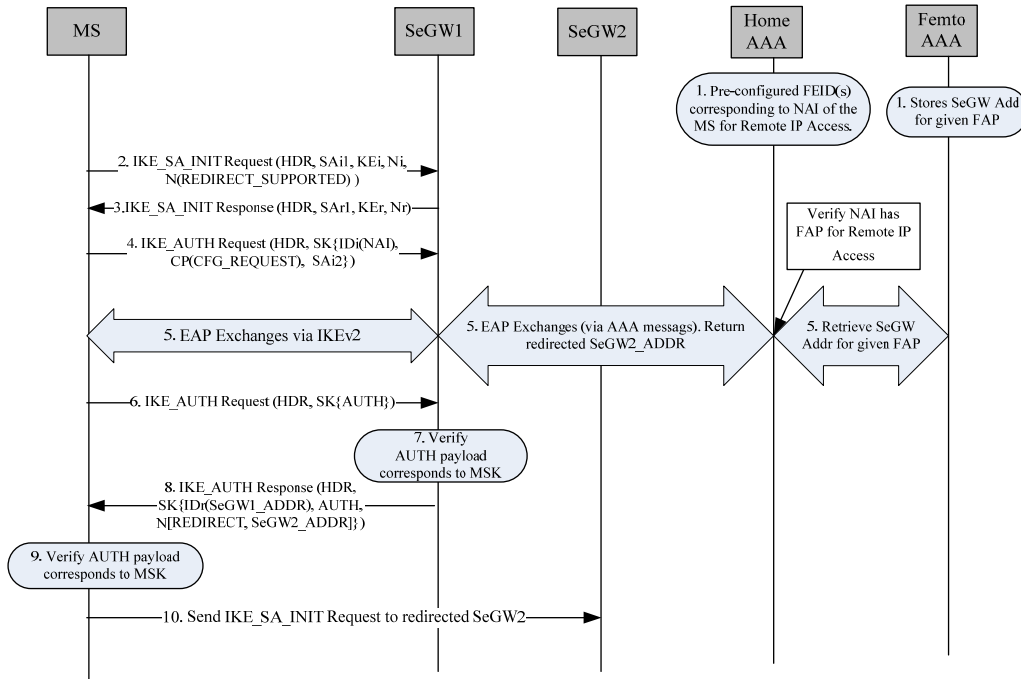


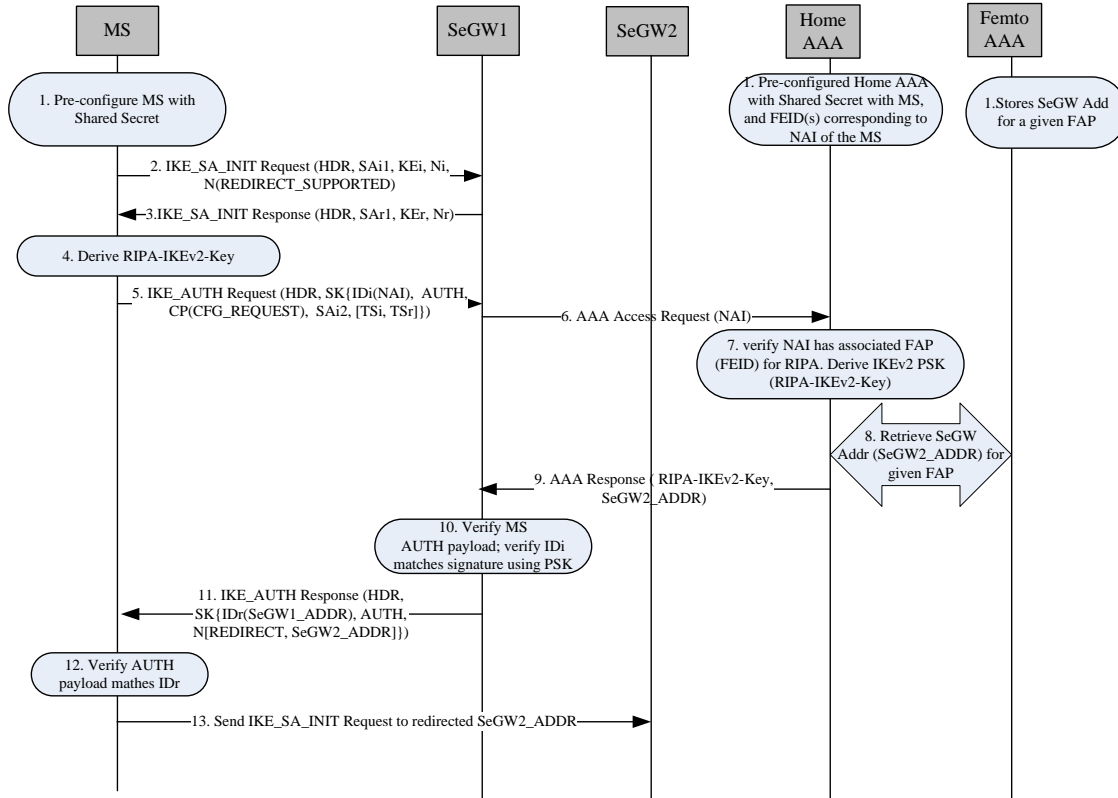
Figure 12 Redirection Based SeGW Discovery with EAP Authentication

1. The HAAA is preconfigured with the FEID(s) associated with the NAI of the MS for Remote IP Access service (RIPA). The Femtocell AAA stores the SeGW IP address for a given FAP when the FAP establishes the IP sec tunnel with the SeGW.
2. The MS obtains the SeGW1 IP address through DNS discovery or other means (not shown in this figure). The MS sends the initial IKE\_SA\_INIT request to SeGW1 to negotiate the security parameters for IKEv2 SA. The MS indicates that redirection is supported.
3. SeGW1 responds with the IKE\_SA\_INIT response message to complete the initial Diffie-Hellman key exchange.
4. The MS sends an IKE\_AUTH request message by including the NAI, but without the AUTH payload, indicating that it wants to use EAP exchange. The MS requests a dynamically assigned address at the remote FAP's local network by including an INTERNAL\_IP4\_ADDRESS or an INTERNAL\_IP6\_ADDRESS attribute (length set to 0) in the CFG\_REQUEST Payload of the IKE\_AUTH message. The MS also includes the IDi and SAi payloads to identify itself and request for RIPA service and negotiate

- IPsec SA, respectively. The IKE\_AUTH exchange is encrypted and integrity protected by the IKE SA established during the IKE\_SA\_INIT exchange.
5. EAP messages are exchanged, via the SeGW1, between the MS and HAAA for mutual authentication. Between the MS and SeGW1, the EAP messages are transported in IKE\_AUTH messages [10]. Between the HA and HAAA, the EAP messages are transported in AAA messages. The HAAA verifies that the MS has associated FAP(s) for RIPA service. The HAAA retrieves the correct SeGW address (SeGW2\_ADDR) from the Femtocell AAA that is serving the FAP associated with the MS, and returns this address (SeGW2\_ADDR) to SeGW1. Both the MS and HAAA derive the Master Session Key during EAP authentication. The HAAA sends the MSK to the SeGW1.
  6. Upon successful EAP authentication, the MS sends the IKE\_AUTH message that includes the AUTH payload. The AUTH payload is computed by the MS based on the MSK that was generated from the EAP authentication.
  7. SeGW1 verifies the AUTH payload.
  8. SeGW1 sends the IKE\_AUTH response message that includes the AUTH payload computed using the MSK. SeGW1 also includes the redirect address of SeGW2 in the IKE\_AUTH message.
  9. The MS verifies the AUTH payload.
  10. The MS sends a new IKE\_INIT\_SA request to the redirected SeGW2.

## **A.5.2 Redirection Based SeGW Discovery with IKEv2 PSK Authentication**

Figure 13 shows a call flow for an MS discovering the SeGW through redirection mechanism, in which IKEv2 PSK authentication is used for IPsec establishment between the MS and the SeGW. This call flow assumes the MS obtains SeGW1 IP address through DNS discovery or other means.



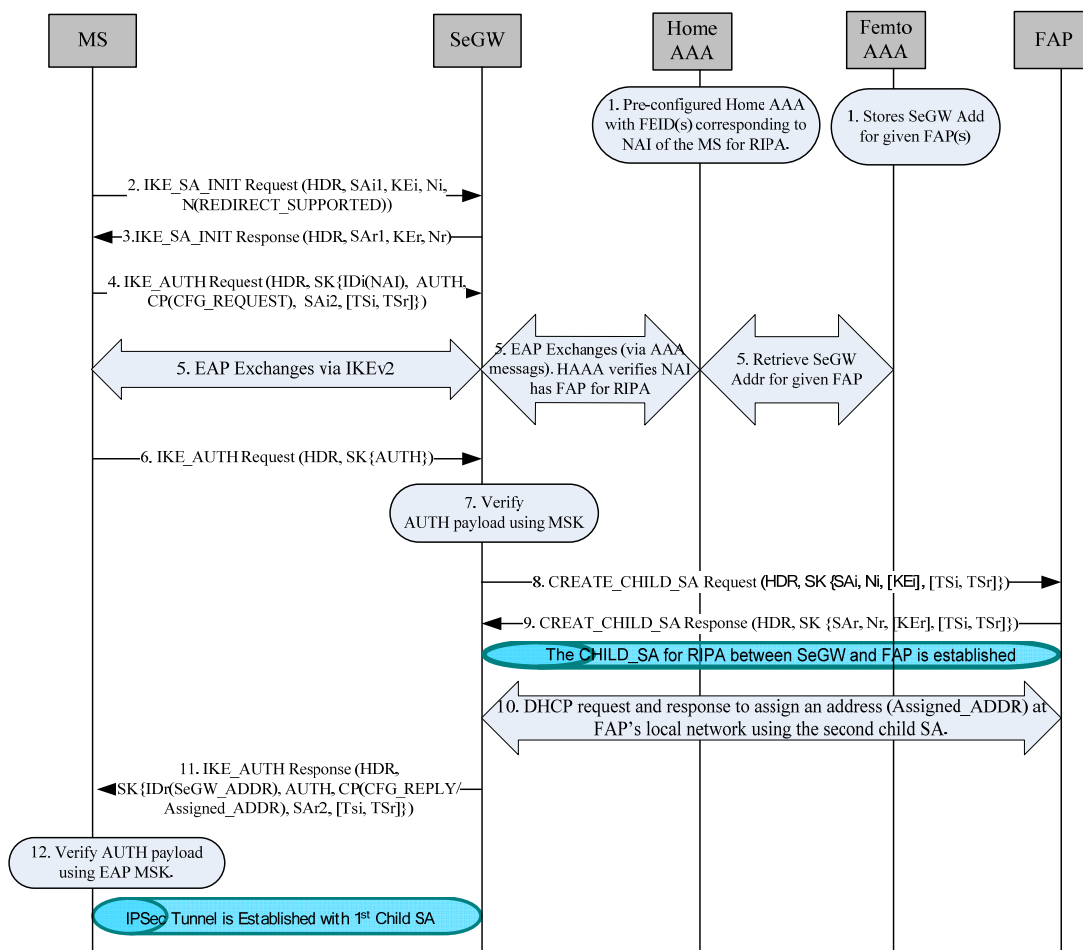
**Figure 13 Redirection Based SeGW Discovery with IKEv2 PSK Authentication**

1. The HAAA is preconfigured with the FEID(s) associated with the NAI of the MS for Remote IP Access service (RIPA). The MS and the HAAA are configured with pre-shared secret for PSK derivation. The Femtocell AAA stores the SeGW IP address for a given FAP when the FAP establishes the IPsec tunnel with the SeGW.
2. The MS sends an initial IKE\_SA\_INIT request to SeGW1 to negotiate the security parameters for IKEv2 SA. The MS indicates that redirection is supported.
3. SeGW1 responds with IKE\_SA\_INIT response to complete the initial Diffie-Hellman key exchange.
4. The MS derives the PSK (RIPA-IKEv2-Key) according to section 6.3.1.
5. The MS sends an IKE\_AUTH request message by including the NAI for Remote IP Access and AUTH payload. The AUTH payload includes the signature of the IKE\_SA\_INIT message in step 2 signed using the RIPA-IKEv2-Key.
6. SeGW1 sends an AAA access request message to the HAAA, including the MS's NAI for RIPA.
7. The HAAA verifies that the given NAI has associated FAP(s) for RIPA service, and derives the RIPA-IKEv2-Key for the given NAI.
8. The HAAA retrieves the correct SeGW address (SeGW2\_ADDR) from the Femtocell AAA that is serving the FAP associated with the MS.
9. The HAAA returns the derived RIPA-IKEv2-Key and the redirection address SeGW2\_ADDR to SeGW1.
10. SeGW1 verifies the AUTH payload using the received RIPA-IKEv2-Key.

11. SeGW1 sends the IKE\_AUTH response message that includes an AUTH payload and the redirection address SeGW2\_ADDR. The AUTH payload contains a signature of the message in step 3 signed using the RIPA-IKEv2-Key.
12. The MS verifies the AUTH payload.
13. The MS sends a new IKE\_INIT\_SA request to the redirected SeGW2.

### A.5.3 Tunnel Establishment for Remote IP Address with EAP Authentication

Figure 14 shows a call flow in which the MS establishes an IPsec tunnel with the correct SeGW that is serving the corresponding FAP. In this call flow, EAP authentication is used for IPsec establishment between the MS and the SeGW. This call flow assumes the MS obtains the SeGW IP address through DNS discovery, redirection mechanism or other means.



**Figure 14 Tunnel Establishment for Remote IP Access with EAP Authentication**

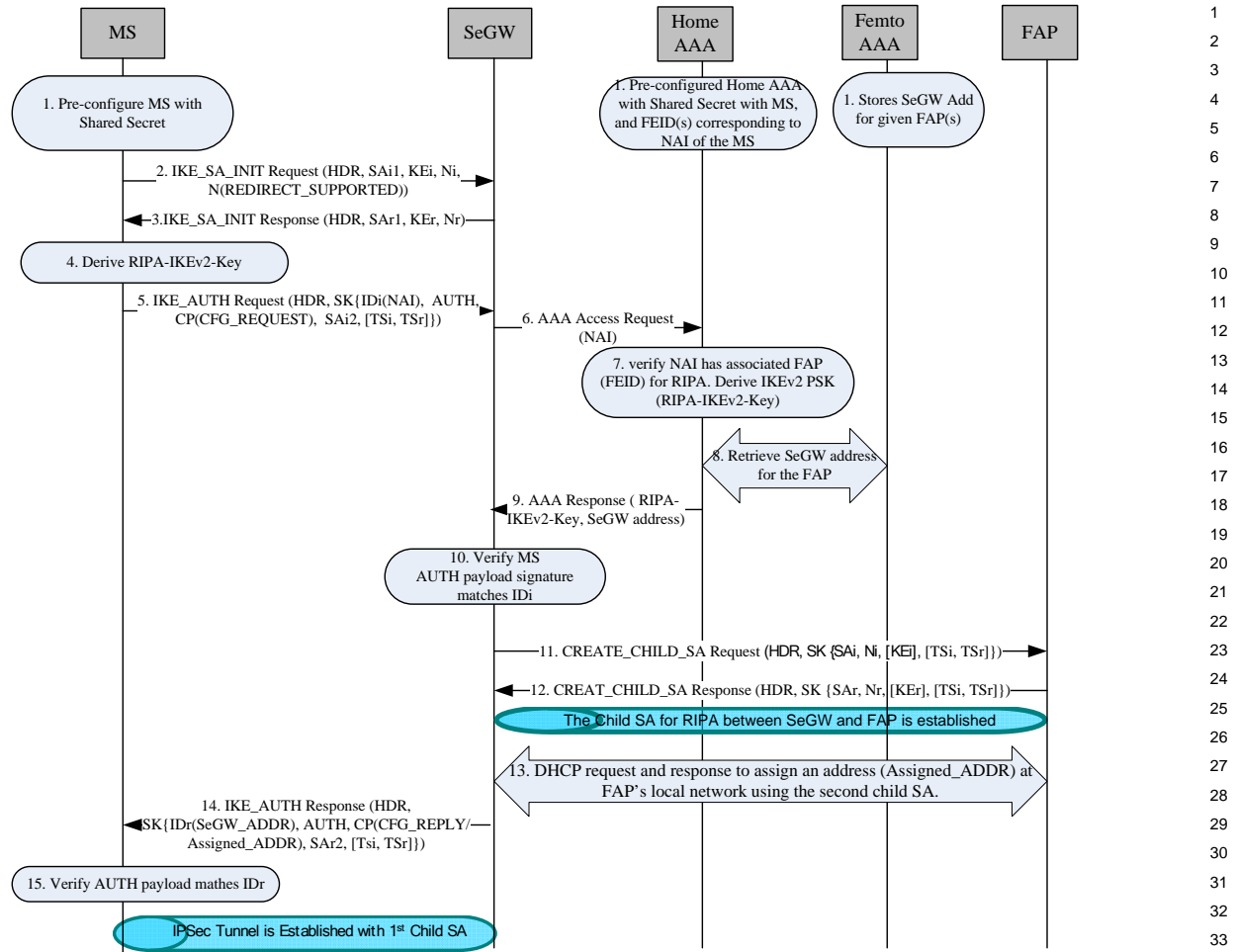
1. The HAAA is preconfigured with the FEID(s) associated with the NAI of the MS for Remote IP Access service (RIPA). The Femtocell AAA stores the SeGW IP address for a given FAP when the FAP establishes the IPsec tunnel with the SeGW.
2. The MS sends the initial IKE\_SA\_INIT request message to SeGW1 to negotiate the security parameters for the IKEv2 SA.

3. SeGW1 responds with the IKE\_SA\_INIT response message to complete the initial Diffie-Hellman key exchange.
4. The MS sends an IKE\_AUTH request message, including the NAI, but without the AUTH payload, indicating that it wants to use EAP exchange. The MS requests a dynamically assigned address at the remote FAP's local network by including an INTERNAL\_IP4\_ADDRESS or an INTERNAL\_IP6\_ADDRESS attribute (length set to 0) in the CFG\_REQUEST Payload of the IKE\_AUTH message. The MS also includes the IDi and SAi payloads to identify itself and request for RIPA service and negotiate IPsec SA, respectively. The IKE\_AUTH exchange is encrypted and integrity protected by the IKE SA established during the IKE\_SA\_INIT exchange.
5. EAP messages are exchanged, via the SeGW, between the MS and HAAA for mutual authentication. Between the MS and SeGW, the EAP messages are transported in IKE\_AUTH messages [10]. Between the HA and HAAA, the EAP messages are transported in AAA messages. The HAAA verifies that the MS has associated FAP(s) for RIPA service. The HAAA also returns the correct SeGW address for the RIPA service for the MS to the requesting SeGW, and SeGW knows that it is the correct SeGW to serve the MS (otherwise, see redirection based SeGW discovery call flow). Both the MS and HAAA derive the Master Session Key during EAP authentication. The HAAA sends the MSK to the SeGW.
6. Upon successful EAP authentication, the MS sends the IKE\_AUTH message that includes the AUTH payload. The AUTH payload is computed based on the MSK that was obtained from the EAP key exchange.
7. The SeGW verifies the AUTH payload using the MSK.
8. Upon successful authentication of the MS, the SeGW selects the existing IKE SA with the FAP associated with the MS, and sends a CREATE\_CHILD\_SA using the existing SA, including a new nonce Ni.
9. The FAP sends a CREATE\_CHILD\_SA response with a new nonce Nr. The new CHILD\_SA keys are derived by the FAP and the SeGW and the new CHILD\_SA pair between the FAP and the SeGW is established.
10. On behalf of the MS, the SeGW sends a DHCP request for an internal address at the FAP's local network. The FAP returns an assigned internal IP address (either assigned by itself or by a local DHCP server) via a DHCP message.
11. The SeGW sends an IKE\_AUTH response including an AUTH payload and a CFG\_REPLY payload. The AUTH payload contains the SeGW's credential generated using the MSK. The CFG\_REPLY payload contains the assigned internal IP address at the FAP's local network.
12. The MS verifies the AUTH payload using the MSK (derived during EAP authentication). The MS receives the assigned internal IP address. The IPsec tunnel between the MS and the SeGW is established.

#### A.5.4 Tunnel Establishment for Remote IP Access with IKEv2 PSK Authentication

---

Figure 15 shows a call flow in which the MS establishes the IPsec tunnel with the correct SeGW that is serving the corresponding FAP. In this call flow IKEv2 PSK authentication is used for IPsec establishment between the MS and the SeGW. This call flow assumes the MS obtains the SeGW IP address through DNS discovery, redirection mechanism or other means.



**Figure 15 Tunnel Establishment for Remote IP Access with IKEv2 PSK Authentication**

1. The HAAA is preconfigured with the FEID(s) associated with the NAI of the MS for Remote IP Access service (RIPA). MS and HAAA are configured with pre-shared secret for PSK derivation. The Femtocell AAA stores the SeGW IP address for a given FAP when the FAP establishes the IP sec tunnel with the SeGW.
2. The MS sends an initial IKE\_SA\_INIT request message to SeGW1 to negotiate the security parameters for the IKEv2 SA.
3. The SeGW responds with an IKE\_SA\_INIT response message to complete the initial Diffie-Hellman key exchange.
4. The MS derives the PSK (RIPA-IKEv2-Key) according to section 6.3.1.
5. The MS sends an IKE\_AUTH request message, including the NAI for Remote IP Access and AUTH payload. The AUTH payload includes the signature of IKE\_SA\_INIT message in step 2 signed using the RIPA-IKEv2-Key.
6. The SeGW sends an AAA access request message to HAAA, including the MS's NAI for RIPA.
7. The HAAA verifies that the given NAI has associated FAP(s) for RIPA service, and derives the RIPA-IKEv2-Key for the given NAI.

- 1 8. The HAAA retrieves the correct SeGW address that is serving the FAP associated with  
2 the MS.
- 3
- 4 9. The HAAA returns the derived RIPA-IKEv2-Key and the correct SeGW address to the  
5 requesting SeGW using AAA messages. The SeGW should know that it is the correct  
6 SeGW to serve the MS and associated FAP (otherwise see redirection based SeGW  
7 discovery call flow).
- 8
- 9 10. The SeGW verifies the AUTH payload in the IKE\_AUTH message received in step 5  
10 using the received RIPA-IKEv2-Key.
- 11
- 12 11. Upon successful authentication of the MS, the SeGW selects the existing IKE SA with  
13 the FAP associated with the MS, and sends a CREATE\_CHILD\_SA using the existing  
14 SA, including a new nonce Ni.
- 15
- 16 12. The FAP sends a CREAT\_CHILD\_SA response with a new nonce Nr. The new  
17 CHILD\_SA keys are derived by the FAP and the SeGW and the new CHILD\_SA pair  
18 between the FAP and the SeGW is established.
- 19
- 20 13. On behalf of the MS, the SeGW sends a DHCP request for an internal address at the  
21 FAP's local network. The FAP returns an assigned internal IP address (either assigned by  
22 itself or by a local DHCP server) via a DHCP message.
- 23
- 24 14. The SeGW sends an IKE\_AUTH response including an AUTH payload and a  
25 CFG\_REPLY payload. The AUTH payload contains the signature on the IKE\_INIT  
26 response message in step 3 generated using the RIPA-IKEv2-Key. The CFG\_REPLY  
27 payload contains the assigned internal IP address at the FAP's local network.
- 28
- 29 15. The MS verifies the AUTH payload using the RIPA-IKEv2-Key. The MS receives the  
30 assigned internal IP address. Upon successful verification of the AUTH payload, the  
31 IPsec tunnel between the MS and the SeGW is established.
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59