TECHNICAL REPORT

TR-196
Femto Access Point Service Data Model

Issue: 2
Issue Date: November 2011

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1	April 2009	Taka Yoshizawa, Technicolor John Blackford, 2Wire Heather Kirksey, Alcatel-Lucent	Original
1 Amendment 1	May 2011	Klaus Wich, Nokia Siemens Networks	Defines FAPService:1.1 with updates to Service Model for 3GPP release 9 and 10. New Theory of operations included.
2	November 2011	Klaus Wich, Nokia Siemens Networks	New Femto Access Point Service Data Model (FAPService:2) defining UMTS, LTE and CDMA2000 FAP radio models.

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor	Klaus Wich	Nokia Siemens Networks
BroadbandHome™ WG Chairs	Greg Bathrick Jason Walls	PMC-Sierra UNH
Chief Editor	Michael Hanrahan	Huawei Technologies

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

A Femto Access Point (FAP), or "Femtocell" is a small-scale cellular base station, typically designed for use in a home or small business. As such, it communicates with the user's mobile handset over the standards-based radio interface using licensed spectrum and further connects to the mobile network infrastructure over the fixed broadband connection. FAPs will be remotely managed from mobile network operators using TR-069/CWMP.

This Technical Report defines Issue 2 of the Femto Access Point Service Data Model. This version covers the 3rd Generation radio technologies for UMTS FAP, LTE FAP and CDMA2000 FAP defined by 3GPP and 3GPP2.

The complete data model for FAPs is formed from the radio technologies defined in TR-196 and common components defined in TR-262 *"Femto Component Objects"* [7] and TR-157 *"Component Objects for CWMP" [4]*.

1 Purpose and Scope

1.1 Purpose

The purpose of this Technical Report is to specify the Data Model for the Femto Access Point (FAP) for remote management purposes using the TR-069 CWMP within the scope defined in the following section.

The Femto data model is defined as a *Service Object*, and thus can be used in any CWMP root data model (both Device and InternetGatewayDevice).

1.2 Scope

TR-196 defines radio specific objects for UMTS FAP (HNB), LTE FAP (HeNB), and CDMA2000 FAP for use in CWMP managed devices with Femto Services for all root data models. Radio independent objects used for Femto Access Point data model are defined in TR-262 [7] *"Femto Component Objects"* and TR-157 [4] *"Component Objects for CWMP"*.

The current root data models are InternetGatewayDevice:1 defined in TR-098 [2], Device:1 defined in TR-181 Issue 1 [5], and Device:2 defined in TR-181 Issue 2 [6]. The current Femto service model for UMTS FAP (HNB), LTE FAP (HeNB), and CDMA2000 FAP is FAPService:2 defined in TR-196.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [14].

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

[1] **TR-069 Amendment 4,** *CPE WAN Management Protocol*, Broadband Forum, 2010

[2] **TR-098 Amendment 2,** *Internet Gateway Device Data Model for TR-069*, Broadband Forum, 2008

[3] **TR-106 Amendment 5,** *Data Model Template for TR-069-Enabled Devices*, Broadband Forum, 2010

[4] **TR-157 Amendment 5,** *Component Objects for CWMP*, Broadband Forum 2011

[5] **TR-181 Issue 1 Amendment 1,** *Device Data Model for TR-069 (Device:1)*, Broadband Forum 2011

[6] **TR-181 Issue 2 Amendment 3,** *Device Data Model for TR-069 (Device:2)*, Broadband Forum 2011

[7] **TR-262,** *Femto Component Objects*, Broadband Forum 2011

[8] **TS 29.060,** *General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface*, 3GPP

[9] **TS 32.584,** *Telecommunication management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HNB to HNB Management System (HMS)*, 3GPP

[10] **TS 32.594,** *Telecommunication management; Home enhanced Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HeNB to HeNB Management System (HeMS***),** 3GPP

[11] **TS.32.111-5,** *Telecommunication management; Fault Management; Part 5: Alarm Integration Reference Point (IRP): eXtensible Markup Language (XML) definitions*, 3GPP

[12] **TS32.300,** *Telecommunication management; Configuration Management (CM); Name convention for Managed Objects*, 3GPP

[13] **TS33.102,** *Technical Specification Group Services and System Aspects;3G Security; Security architecture*, 3GPP

[14] **RFC 2119,** *Key words for use in RFCs to Indicate Requirement Levels*, IETF, 1997

[15] **RFC 1305,** *Network Time Protocol (Version 3) Specification, Implementation and*

Analysis, IETF, 1992,

[16] **RFC 2960,** *Stream Control Transmission Protocol*, IETF, 2000

[17] **RFC 3550,** *RTP: A Transport Protocol for Real-Time Applications*, IETF, 2003

[18] **IEEE-1588,** *Standards for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, IEEE, 2003

[19] **ITU-X.733**, *Information Technology Open systems Interconnection systems Management: Alarm Reporting Functions*, ITU, 1992

2.3 Definitions

The following terminology is used throughout this Technical Report.

ACS	Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
CPE	Customer Premises Equipment.
CWMP	CPE WAN Management Protocol (TR-069)
Root Object	The top-level object of a CPE's Data Model that contains all of the manageable objects. The name of the Root Object is either "Device" or "InternetGatewayDevice" – the latter is used only for the TR-098 [2] InternetGatewayDevice:1 Data Model
Service Object	The top-most object associated with a specific service within which all Objects and Parameters associated with the service are contained. (see TR-106 [3])

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
CDMA	Code Division Multiple Access
CN	Core Network
FAP	Femto Access Point (generic name for Femtocell)
FAPGW	Femto Access Point Gateway
GPRS	General packet radio service
GSM	Global System for Mobile
GTP	GPRS Tunneling Protocol
HNB	Home NodeB (UMTS FAP)

HeNB	Home eNodeB (LTE FAP)
IP	Internet Protocol
IPsec	Internet Protocol Security
LTE	Long Term Evolution
PSTN	Public switched telephone network
RAN	Radio Access Network
RGW	Routing Gateway
SecGW	Security Gateway
SA	Security Association
TR	Technical Report
UMTS	Universal Mobile Telecommunication System
URN	Uniform Resource Name
WCDMA	Wideband Code Division Multiple Access
WG	Working Group

3 Technical Report Impact

3.1 Energy Efficiency

TR-196 has no impact on Energy Efficiency.

3.2 IPv6

TR-196 has no direct impact on IPv6, because it uses the IP connectivity defined on the underlying root device. It is possible to use the FAPService:2 with a root data model supporting IPv6, so that all connections are IPv6 connections.

3.3 Security

The FAPService:2 object defined in TR-196 uses IPsec tunnels to secure the Femto traffic from the device to the mobile network in essence extending the mobile network to a device in the house.

4 Data Model Definition

Figure 1 below shows the general overall view of the Femtocell system. Both standalone and integrated FAP product types are shown.

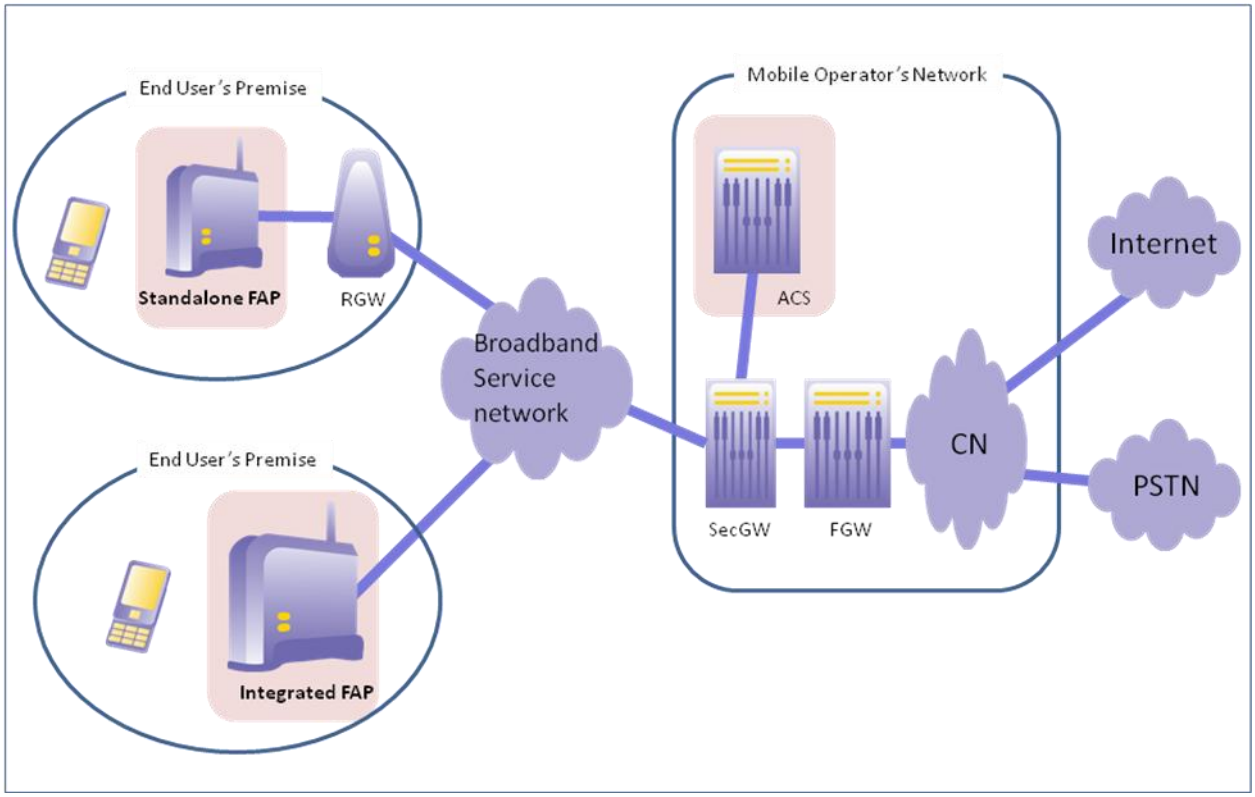

Figure 1 – General Overall View of the Femtocell System

Figure 2 below illustrates the internal structure of the FAPService:2 object.

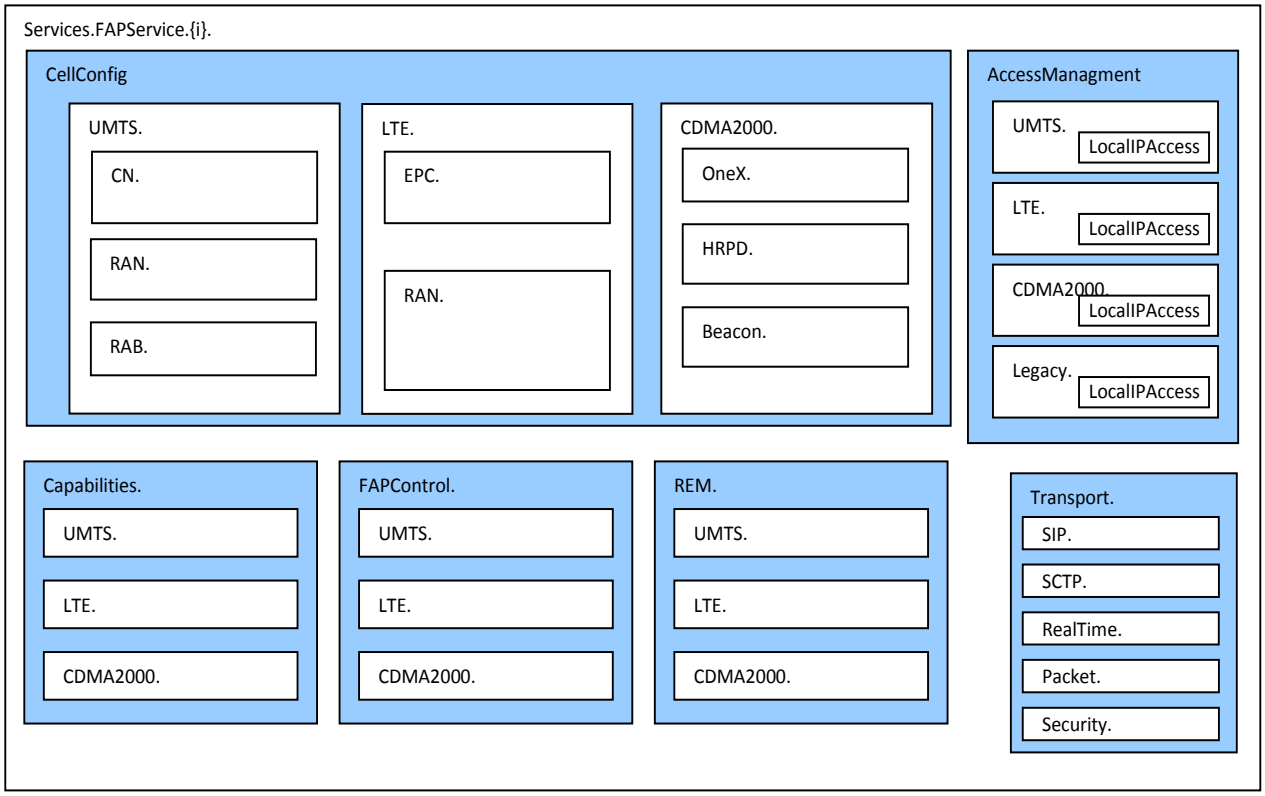

Figure 2 – Services.FAPService.{i}.Structure

5 FAPService:2 Parameter Definitions

The normative definition of the FAPService:2 data model is split between several DM Instance documents (see TR-106 [3] Annex A). Table 1 lists the data model versions and DM Instances that had been defined at the time of writing. It also indicates the corresponding Technical Reports and gives links to the associated XML and HTML files.

Note that, because new minor versions of the FAPService:2 data model can be defined without re-publishing this Technical Report, the table is not necessarily up-to-date. An up-to-date version of the table can always be found at http://www.broadband-forum.org/cwmp.

Table 1 – FAPService:2 Data Model Versions

Version	DM Instance	Technical Report	XML and HTML[1]
2.0	tr-196-2-0.xml	TR-196 Issue 2	http://broadband-forum.org/cwmp/tr-196-2-0.xml
			http://broadband-forum.org/cwmp/tr-196-2-0.html

[1] For a definition of the naming conventions used in the XML and HTML files refer to TR-106 [3].

Annex A: Required CPE Method in Optional RPC Messages

Section A.4.1/TR-069 [1] describes the optional CPE Methods in RPC messages. By definition, they are optional for individual CPE vendors. However, among them, at least one of them is required for the FAP operation. Therefore, all FAP vendors that comply with this specification MUST support the following optional CPE method RPC message:

- Upload

Annex B: Vendor Specific Type Definitions

B.1 Vendor Specific File Type

Note: These definitions only apply for UMTS and LTE FAP implementations.

The following vendor specific file type is defined for this version of the FAP data model. All FAP vendors that comply with this specification MUST support this file type to be used in the Upload CPE method.

- "X 00256D 3GPP Performance File"

The format is based on the vendor specific file type extension per Section A.4.1.5/ TR-069 [1]. By inserting "3GPP" in the beginning of the vendor-specific identifier field, it uniquely identifies the file types to be specific for the 3GPP specification per TS 32.584 [9] for UMTS FAP and TS 32.594 [10] for LTE FAP. The <OUI> field is replaced with the Broadband Forum OUI value of 00256D.

B.2 Vendor Specific Event Types

Note: These definitions only apply for UMTS and LTE FAP implementations.

The Event Type indicates the reason why a CPE establishes the TR-069 session with ACS, and is included in the Inform RPC method sent by the CPE. Section 3.7.1.5, Table 7 in TR-069 [1] defines the Event Types. However, some FAP specific scenarios represent a situation where FAP needs to establish a TR-069 session with the ACS due to a reason not covered by the existing Event Types.

The FAP MUST use new Event Types specifically defined specific for TR-196 in an Inform RPC method when it establishes the TR-069 session with the ACS after one of the following conditions occurred and request for re-provisioning:

1) FAP failed to establish the secure tunnel connection with all of the SecGWs previously provided by the ACS, or

2) FAP failed to establish the Iuh connection with all of the FAPGWs previously provided by the ACS.

This version of the FAP data model defines the following vendor specific event types. All FAP vendors that comply with this specification MUST support these event types if in the Inform ACS method.

Table 2 – Vendor Specific Event Types

Event Code	Cumulative Behavior	Explanation	ACS Response for Successful Delivery	Retry/Discard Policy
"X 00256D 3GPP Reprovision Required: SecGW"	Single	Indicates that the FAP failed to establish the secure tunnel connection with all of the SecGWs previously provided by the ACS	InformResponse	The CPE MUST NOT ever discard (except on BOOTSTRAP) an undelivered ***"X 00256D 3GPP Reprovision Required: SecGW***" event. (except on BOOTSTRAP)
"X 00256D 3GPP Reprovision Required: FAPGW"	Single	Indicates that the FAP failed to establish the Iuh connection with all of the FAPGWs previously provided by the ACS	InformResponse	The CPE MUST NOT ever discard an undelivered "***X 00256D 3GPP Reprovision Required: FAPGW*** "" event. (except on BOOTSTRAP)

This format is based on the vendor specific event type per Table 7 in TR-069 [1]. By inserting "3GPP" in the beginning of the vendor-specific identifier field, it uniquely identifies the event to be specific for the 3GPP specification. The <OUI> field is filled with the Broadband Forum OUI value of 00256D.

Annex C: URN Definitions for App and Flow Tables

The root data models (TR-098 [2], TR-181 [6]) define a set of URNs for the App and Flow tables in the QueueManagement mechanism.
An additional set of URNs has been defined to associate traffic arriving over the FAP air interface with the *QueueManagement.Classification.{i}* (for TR-098 [2]) or-the *QoS* object (for TR-181 [6]).

C.1 Protocol Identifier

The root data models (TR-098 [2], TR-181 [6]) define a set of URNs for the Protocol Identifier parameter in the App table. The following URNs are additional values that are applicable to the FAPService object.

Table 3 – FAP Service URN definitions

URN	Description
urn:broadband-forum-org:iuh.control	SCTP as defined in RFC2960 [16]
urn.broadband-forum-org:gtp	GTP protocol as defined in 3GPP TS 29.060 [8]
urn:broadband-forum-org:iuh.rtp	RTP as defined in RFC3550 [17] or multiplexed RTP
urn:broadband-forum-org:time	Network Time Protocol (NTP) as defined in RFC1305 [15] or IEEE1588 Precision Time Protocol (PTP) [18]

C.2 Flow Type

A URN for the *FlowType* parameter in the Flow table of the QueueManagement service for the GTP protocol as defined in 3GPP TS29.060 [8] is formed as follows

For the Protocol Identifier urn:broadband-forum-org:gtp, the following QoS-related flow types are defined:

```
urn:broadband-forum-org:gtp-conversational
urn:broadband-forum-org:gtp-streaming
urn:broadband-forum-org:gtp-interactive
urn:broadband-forum-org:gtp-besteffort
```


Appendix I. Structure of Femto Data Model

I.1 Structure

The figure below shows from which TRs a Femto device data model is built:

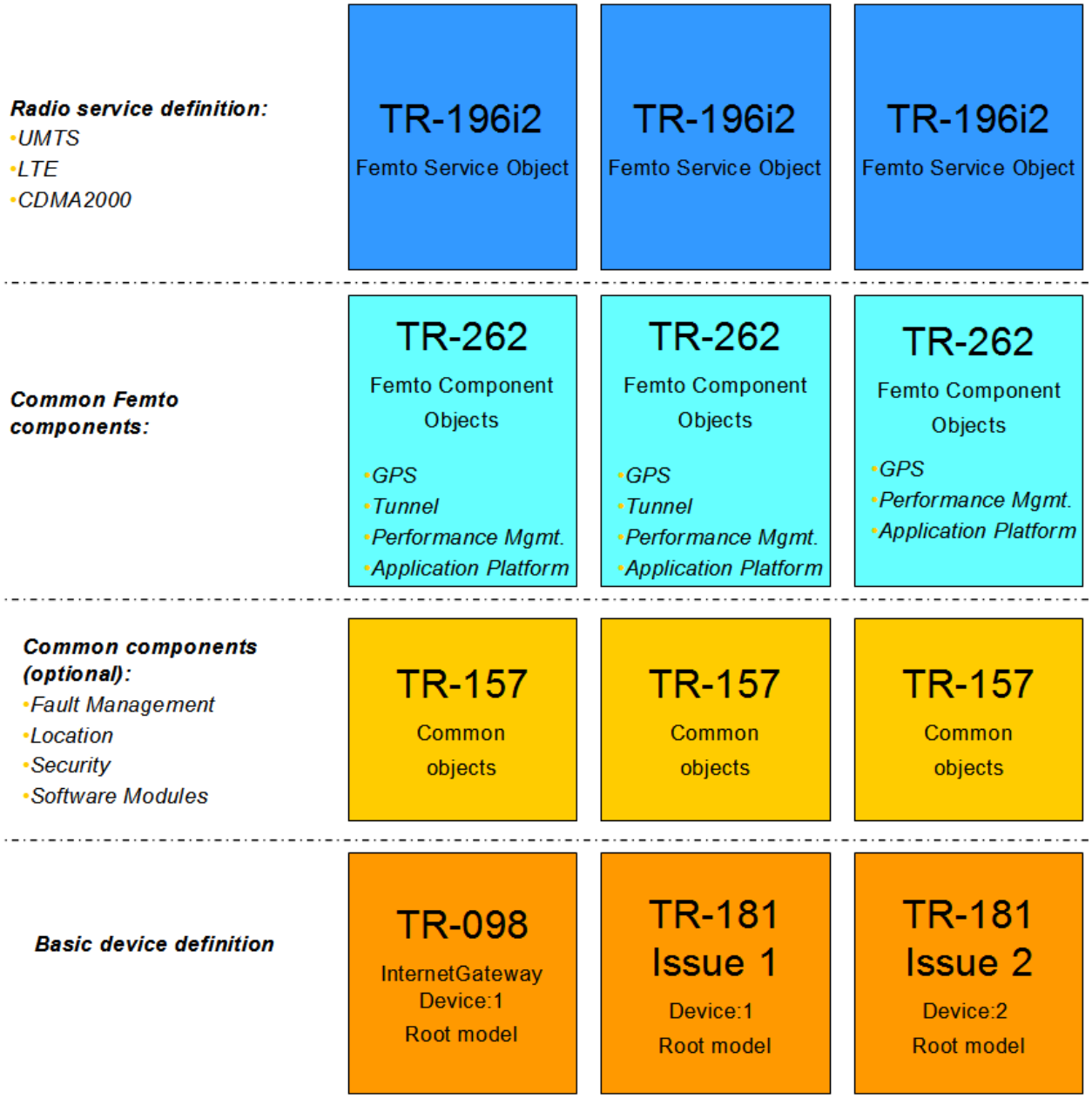

Figure 3 – Femto data model structure

I.2 Examples

I.2.1 Single radio UMTS FAP device based on TR-098

The data model for an older device based on the InternetGatewayDevice model (TR-098 [2]), would look like:

InternetGatewayDevice.	(from TR-098)
InternetGatewayDevice.DeviceInfo.	
InternetGatewayDevice.ManagementServer.	
InternetGatewayDevice.Time.	
InternetGatewayDevice.FaultMgmt.	(from TR-157)
InternetGatewayDevice.Security.	
InternetGatewayDevice.Services.FAPService.1.	(from TR-196i2)
InternetGatewayDevice.Services.FAPService.1.Capabilities.	
InternetGatewayDevice.Services.FAPService.1.Capabilities.UMTS.	
InternetGatewayDevice.Services.FAPService.1.FAPControl.	
InternetGatewayDevice.Services.FAPService.1.FAPControl.UMTS.	
InternetGatewayDevice.Services.FAPService.1.AccessMgmt.	
InternetGatewayDevice.Services.FAPService.1.AccessMgmt.UMTS.	
InternetGatewayDevice.Services.FAPService.1.CellConfig.	
InternetGatewayDevice.Services.FAPService.1.CellConfig.UMTS.	
InternetGatewayDevice.Services.FAPService.1.REM.	
InternetGatewayDevice.Services.FAPService.1.REM.UMTS.	
InternetGatewayDevice.Services.FAPService.1.Transport.	
InternetGatewayDevice.Services.FAPService.1.Transport.SCTP.	
InternetGatewayDevice.Services.FAPService.1.Transport.Realtime.	
InternetGatewayDevice.Services.FAPService.1.Transport.Packet.	
InternetGatewayDevice.FAP.	(from TR-262)
InternetGatewayDevice.FAP.Tunnel.	
InternetGatewayDevice.FAP.GPS.	
InternetGatewayDevice.FAP.PerfMgmt.	

Note: Root device specific objects, which are not Femto specific, like network interface, firewall, etc. are not shown.

I.2.2 Single radio LTE FAP device based on TR-181i2

The data model for an LTE FAP device based on the Device:2 root data model (TR-181i2 [6]) which also supports additional Femto applications would contain the following areas

Device.	(from TR-181i2)
Device.DeviceInfo.	
Device.ManagementServer.	
Device.Time.	
Device.IPsec.[2]	
Device.QoS.	
Device.FaultMgmt.	(from TR-157)
Device.Security.	
Device.Services.FAPService.1.	(from TR-196i2)
Device.Services.FAPService.1.Capabilities.	
Device.Services.FAPService.1.Capabilities.LTE.	
Device.Services.FAPService.1.FAPControl.	
Device.Services.FAPService.1.FAPControl.LTE.	
Device.Services.FAPService.1.AccessMgmt.	
Device.Services.FAPService.1.AccessMgmt.LTE.	
Device.Services.FAPService.1.CellConfig.	
Device.Services.FAPService.1.CellConfig.LTE.	
Device.Services.FAPService.1.REM.	
Device.Services.FAPService.1.REM.LTE.	
Device.Services.FAPService.1.Transport.	
Device.Services.FAPService.1.Transport.SCTP	
Device.Services.FAPService.1.Transport.Realtime	
Device.Services.FAPService.1.Transport.Packet	
Device.FAP.	(from TR-262)
Device.FAP.GPS.	
Device.FAP.PerfMgmt.	
Device.FAP.ApplicationPlatform.	

Note: Root device specific objects which are not Femto specific like network interface, firewall, etc. are not shown

[2] IPsec objects for Device:2 are not part of the current Device:2 specification and are planned to be defined in a future Amendment (> Amendment 4)

I.2.3 Multiple radio UMTS/CDMA200 multiple service FAP device based on TR-098

The data model for an FAP device which supports UMTS and CDMA2000 in parallel radio instances based on the InternetGatewayDevice model (TR-098 [2]) would look like:

InternetGatewayDevice.	(from TR-098)
InternetGatewayDevice.DeviceInfo.	
InternetGatewayDevice.ManagementServer.	
InternetGatewayDevice.Time	
InternetGatewayDevice.FaultMgmt.	(from TR-157)
InternetGatewayDevice.Security.	
InternetGatewayDevice.Services.FAPService.1.	(from TR-196i2)
InternetGatewayDevice.Services.FAPService.1.Capabilities.	
InternetGatewayDevice.Services.FAPService.1.Capabilities.UMTS.	
InternetGatewayDevice.Services.FAPService.1.FAPControl.	
InternetGatewayDevice.Services.FAPService.1.FAPControl.UMTS.	
InternetGatewayDevice.Services.FAPService.1.AccessMgmt.	
InternetGatewayDevice.Services.FAPService.1.AccessMgmt.UMTS.	
InternetGatewayDevice.Services.FAPService.1.CellConfig.	
InternetGatewayDevice.Services.FAPService.1.CellConfig.UMTS.	
InternetGatewayDevice.Services.FAPService.1.REM.	
InternetGatewayDevice.Services.FAPService.1.REM.UMTS.	
InternetGatewayDevice.Services.FAPService.1.Transport.	
InternetGatewayDevice.Services.FAPService.1.Transport.SCTP	
InternetGatewayDevice.Services.FAPService.1.Transport.Realtime	
InternetGatewayDevice.Services.FAPService.1.Transport.Packet	
InternetGatewayDevice.Services.FAPService.2.	
InternetGatewayDevice.Services.FAPService.2.Capabilities.	
InternetGatewayDevice.Services.FAPService.2.Capabilities.CDMA2000.	
InternetGatewayDevice.Services.FAPService.2.FAPControl.	
InternetGatewayDevice.Services.FAPService.2.FAPControl.CDMA2000.	
InternetGatewayDevice.Services.FAPService.2.AccessMgmt.	
InternetGatewayDevice.Services.FAPService.2.AccessMgmt CDMA2000.	
InternetGatewayDevice.Services.FAPService.2.CellConfig.	
InternetGatewayDevice.Services.FAPService.2.CellConfig.CDMA2000.	
InternetGatewayDevice.Services.FAPService.2.REM.	
InternetGatewayDevice.Services.FAPService.2.REM.CDMA2000.	
InternetGatewayDevice.Services.FAPService.2.Transport.	
InternetGatewayDevice.Services.FAPService.2.Transport.SIP.	
InternetGatewayDevice.Services.FAPService.2.Transport.Realtime	
InternetGatewayDevice.Services.FAPService.2.Transport.Packet	
InternetGatewayDevice.FAP.	(from TR-262)
InternetGatewayDevice.FAP.Tunnel.	
InternetGatewayDevice.FAP.GPS	
InternetGatewayDevice.FAP.PerfMgmt.	

Note: Root device specific objects, which are not Femto specific, like network interface, firewall, etc. are not shown.

I.2.4 Multiple radio UMTS/CDMA2000 single service FAP device based on TR-181i2

The data model for an FAP device which supports LTE and CDMA2000 with one radio instance based on the Device:2 root data model (TR-181i2 [6]):

Device.	(from TR-181i2)
Device.DeviceInfo.	
Device.ManagementServer.	
Device.Time	
Device.IPsec.[3]	
Device.FaultMgmt.	(from TR-157)
Device.Security.	
Device.Services.FAPService.1.	(from TR-196i2)
Device.Services.FAPService.1.Capabilities.	
Device.Services.FAPService.1.Capabilities.UMTS.	
Device.Services.FAPService.1.Capabilities.CDMA2000.	
Device.Services.FAPService.1.FAPControl.	
Device.Services.FAPService.1.FAPControl.UMTS.	
Device.Services.FAPService.1.FAPControl.CDMA2000.	
Device.Services.FAPService.1.AccessMgmt.	
Device.Services.FAPService.1.AccessMgmt.UMTS.	
Device.Services.FAPService.1.AccessMgmt CDMA2000.	
Device.Services.FAPService.1.CellConfig.	
Device.Services.FAPService.1.CellConfig.UMTS.	
Device.Services.FAPService.1.CellConfig.CDMA2000	
Device.Services.FAPService.1.REM.	
Device.Services.FAPService.1.REM.UMTS.	
Device.Services.FAPService.1.REM.CDMA2000.	
Device.Services.FAPService.1.Transport	
Device.Services.FAPService.1.Transport.SIP.	
Device.Services.FAPService.1.Transport.SCTP	
Device.Services.FAPService.1.Transport.Realtime	
Device.Services.FAPService.1.Transport.Packet	
Device.FAP.	(from TR-262)
Device.FAP.GPS	
Device.FAP.PerfMgmt.	

Note: Root device specific objects, which are not Femto specific, like network interface, firewall, etc. are not shown.

[3] IPsec objects for Device:2 are not part of the current Device:2 specification and are planned to be defined in a future Amendment (> Amendment 4)

Appendix II. Theory of Operation for UMTS Femto Access Points

This informative appendix describes the theory of operation of the Femto Access Point Data Model for UMTS, explaining the intended usage of the objects and parameters to achieve the desired operation of the UMTS FAP.

Note that the actual implementation are influenced by factors external to the data model itself – such as operator policy, vendor implementation decision, variations of FAP products, etc. Therefore, variations of implementations will exist and there is no single right answer to accomplish the desired end-goal (i.e. self-configuration). However, objects and parameters in the FAP data model defined in TR-196i2 and TR-262 are complex enough to warrant some explanations of the intended usage. Under this circumstance, this appendix illustrates, as a guideline, the intended usage of objects and parameters to achieve such goals. It is certainly possible for a FAP vendor to invent and implement mechanisms beyond the existing objects and parameters. However, this is outside the scope of this appendix.

Note 1: In all of the figures in this appendix, arrows pointing to the ACS indicate the "get" action (GetParameterValues) and arrows pointing away from the ACS indicate the "set" action (SetParameterValues) by the ACS.

Note 2: This theory of operation is based on the data model for UMTS (3G) Femto Access Points. For other radio technologies the theory has to be adapted. The general concept presented in this theory of operation for UMTS Femto is partly applicable to other radio technologies. However, specific parameter names and object path names will differ for other radio technologies.

Note 3: If not specified otherwise, all objects names starting with a dot are relative to the "<rootobject>.Services" object. In all other cases the whole path is specified.

II.1 Management Connection Establishment

There are two possible scenarios how an UMTS FAP establishes a TR-069 CWMP session with the ACS:

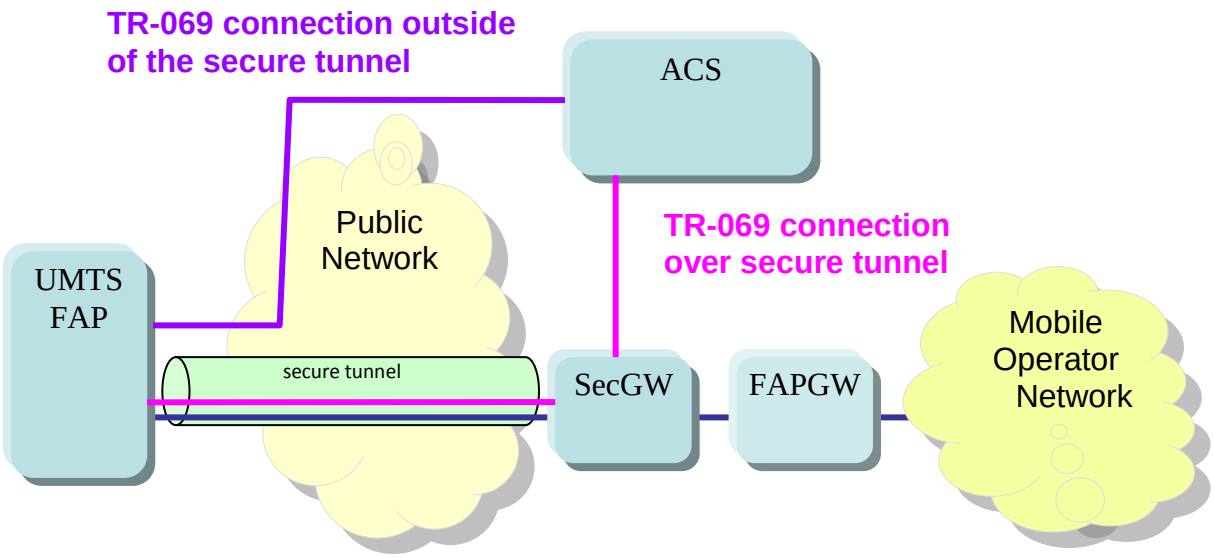

Figure 4 – FAP to ACS connections

If the connection is established outside the IPsec tunnel, no specific explanation is needed. TLS/SSL as the TR-069 native method provides the security of the management connection. The <rootobject> already defines the ACS identity, and is expected to exist as the factory-default setting of the FAP:

- ACS identify and associated parameters:
  - <rootobject>.ManagementServer.URL
  - <rootobject>.ManagementServer.Username (if used)
  - <rootobject>.ManagementServer.Password (if used)

If the ACS connection is established through the IPsec tunnel, first the IPsec tunnel needs to be established with the SecGW before the TR-069 session is established with the ACS. In this case, in addition to the parameters listed above, the SecGW identity and associated security parameters are expected to exist as the factory-default setting of the FAP:

- SecGW identity
  - .FAPService.{i}.FAPControl.UMTS.Gateway.SecGWServer1

- Object and subtending sub-objects and parameters necessary to establish the IPsec tunnel are part of the underlying root data model. Their location vary depending on the used root data model:
  - For the Device:1 (TR-181 Issue 1 [5]) or the InternetGatewayDevice (TR-098 [2]) root data models, which use the Femto Tunnel Component object defined in TR-262 [7] :
    - <rootobject>.FAP.Tunnel.
    - .FAPService.{i}.Transport.Security
  - If Device:2 (TR-181 Issue 2 [6]) is used:
    - Device.IPsec.[4]
    - Device.FAPService.{i}.Transport.Security.

The FAP's decision whether to use the IPsec tunnel for initial configuration or not depends on the existence of the SecGW parameters in the factory defaults and an indication in the parameter <rootobject>.FAP.Tunnel.UseForCWMP. The table shows the possible decisions for root data models using the Femto Tunnel Component object defined in TR-262 [7] :

Table 4 – IPsec Tunnel selection Decision for FAP.Tunnel component

	<rootobject>.FAP.Tunnel.UseForCWMP		
SecGW parameters	*Not implemented*	*False*	*True*
Not implemented	Direct connection	Direct connection	Direct connection
defined	Use Tunnel	Direct connection	Use Tunnel

[4] IPsec objects for Device:2 are not part of the current Device:2 specification and are planned to be defined in a future Amendment (> Amendment 4)

II.2 SecGW, FAPGW Discovery and Connection Establishment

Connection Establishment without SecGW:
Figure 6 below illustrates the process used by the FAP to establish the signaling connection with FAPGW over the IPsec connection with SecGW when the ACS is outside of the IPsec tunnel.

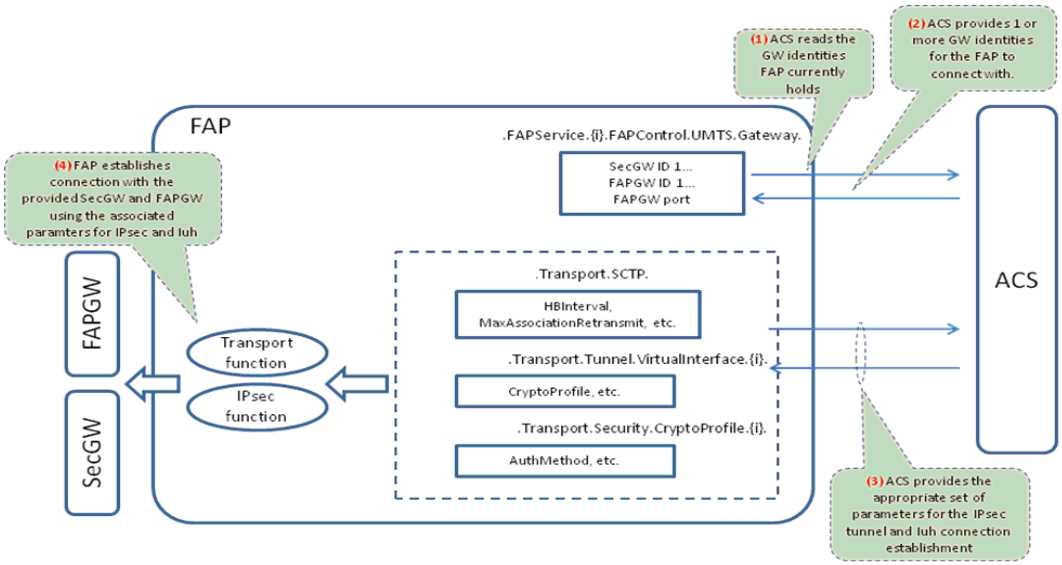

Figure 5 – SecGW, FAPGW connection establishment

During this process the FAP is configured with the necessary information about the SecGW.

Connection Establishment with SecGW:
If the initial TR-069 session with the ACS is established through the IPsec tunnel, then the necessary IPsec related parameters are expected to be already set in the FAP as factory-default. In this case, the ACS can modify the IPsec and SecGW related parameter values anytime if needed.

Selection of SecGW:
If the FAP is provided with more than one identity for SecGW, it tries to establish an IPsec tunnel with them in the sequential order they are provided (SecGWServer1, SecGWServer.2…). In case the IPsec tunnel is not successfully established, FAP tries the next on the list. After the FAP successfully establishes an IPsec, it moves on to establish signaling connection with the FAPGW similar to the establishment of the SecGW connection.

If ACS decides that the FAP should establish a connection with a SecGW that is different from what it is currently connected, then the ACS can overwrite the SecGW identity. Then the FAP first tears down the existing IPsec tunnel and re-establishes with the new one.

When FAP fails to establish connection with either SecGW or FAPGW for all of the identities provided, then the FAP tries to connect to the ACS directly for re-provisioning of SecGW and/or FAPGW.

IPsec Tunnel Status

An IPsec tunnel is established between FAP and SecGW so that FAP and FAPGW can communicate to each other over the secured connection. Within the FAP the status of the tunnel is visible in the appropriate root data model parameter:

- For the Device:1 (TR-181 Issue 1 [5]) or the InternetGatewayDevice (TR-098 [2]) root data models, which use the Femto Tunnel Component object defined in TR-262 [7] the parameter is:
  - <rootobject>.FAP.Tunnel.IKESA.{i}.Status
- If the Device:2 (TR-181 Issue 2 [6]) root data model is used, the parameter is part of the IPsec[5] object.

Table 5 below shows as an example the description of the values of this status for tunnels based on the Femto Component object in TR-262 [7]. If one or more of this multi-instance object pre-exists in FAP, the values in the table apply to reflect the current status of the IKE SA. If individual multi-instance object is dynamically created/deleted by FAP based on the IPsec tunnel establishment/tear-down, only a subset of the values may be supported to indicate the current status of the IKE SA.

Table 5 – IKE SA Status

Status	Description
Disabled	This IKE SA is not active.
Active	This IKE SA has been successfully created.
Completed	This existing IKE SA has been terminated/deleted.
Progressing	This IKE SA is in the process of being created.
Error	This value MAY be used by the CPE to indicate a locally defined error condition. OPTIONAL

For the Device:2 (TR-181 Issue 2 [6]) root data model the same applies in principle, even if the values definition is different.

II.3 Location Verification

For Location verification one or more of the following type of information is used:

1. REM process using macro cell information
2. GPS
3. Others (e.g. fixed broadband related information)

The figure below shows the list of objects available for this purpose.

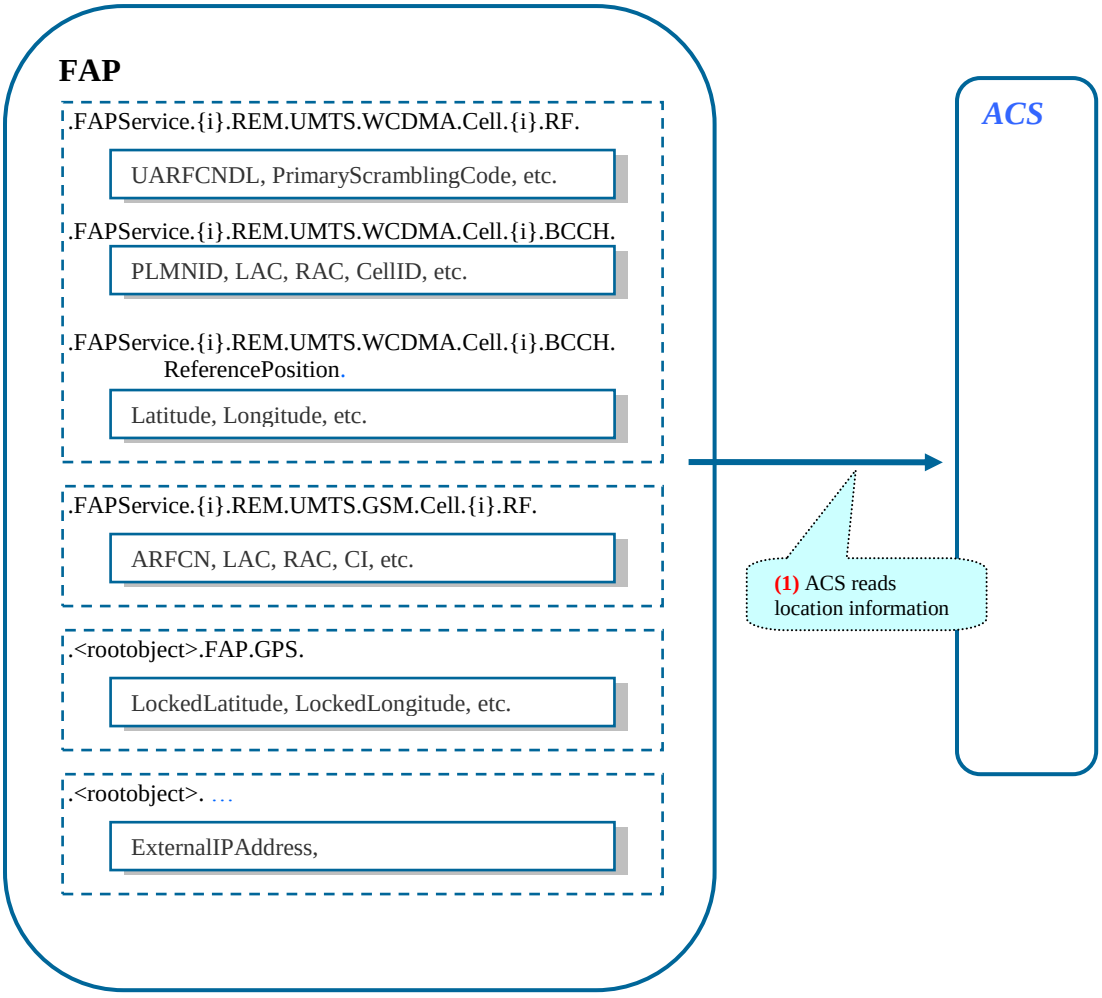

Figure 6 – Location information for UMTS FAP

II.4 Self-Configuration

II.1.1 General Description

This section describes the self-configuration aspect of the FAP. This topic includes multiple aspects and can mean different things to different people. Even for the same aspect, (e.g. configuration of radio related parameters or neighbor list), it is possible to design more than one way to accomplish the goal. In this respect, even though there is no "right" or "wrong" way in an absolute sense, it is desirable to define a model on which the mechanism is based. To this end, the section illustrates the fundamental concept and approach to the self-configuration.

Note that Radio Environment Measurement (REM) and Neighbor List (NL) configuration require special attention. Therefore, these two topics are discussed separately.

II.1.2 General Approach to Self-Configuration

Self-configuration is a process in the CM where the FAP determines a specific parameter value among multiple possible choices under the guidance of the ACS as opposed to the latter providing a specific parameter value to the former. The following is the general high-level "theory" of self-configuration of FAP:

1. The ACS acts as the master of the overall self-configuration behavior of the FAP and explicitly instructs the FAP which aspect of the self-configuration it has to perform (or not to perform).
2. FAP behaves under the guidance of the ACS for self-configuration and performs self-configuration for the aspect it is requested to perform within the limitation and boundary set by the ACS.
3. The ACS can provide more than one possible choice of value (or range of values) from which the FAP selects one based on criteria including its local knowledge (e.g. environmental information).
4. The ACS can query the choice made by the FAP and may override the value that the FAP has selected during this process.
5. Once the ACS overrides any specific parameter in the FAP, the FAP accepts the new value unconditionally (as long as the value is valid).

II.1.3 General Process Flow

Figure 7 illustrates an example of the general process flow for the self-configuration. Note that this is a "general" flow and variations exist depending on the exact type of self-configuration. For example, in step (3) in the figure, the ACS provides a list of choices from which the FAP selects. However, in the case of neighbor list configuration, this does not necessarily apply; see the separate section for the self-configuration of the neighbor list.

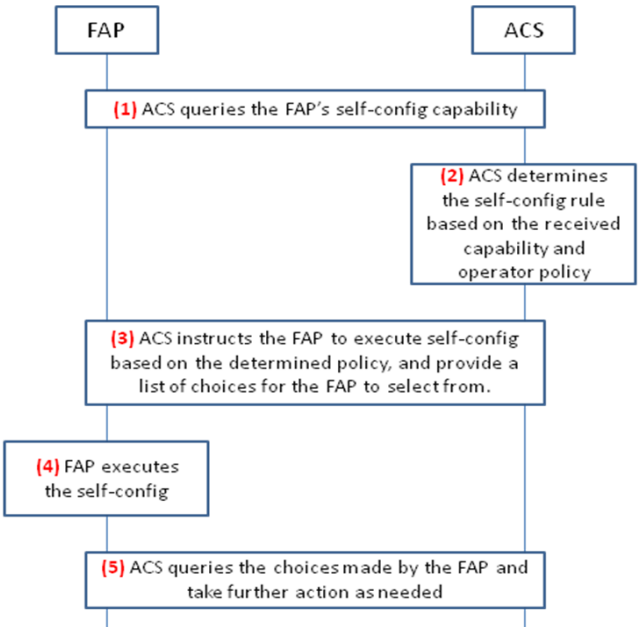

Figure 7 – General process flow of self-configuration

II.1.4 Use of "Active Notification"

In some cases, self-configuration activity can take a period beyond a single TR-069 session. In this case, self-configuration process continues within the FAP independent from the TR-069 session. This implies that a new session needs to be re-established when the FAP is ready to continue with the self-configuration process but no TR-069 session exists at that time.

In this case, one way to facilitate this is to use "active notification." for the self-configured parameters. This is done via setting the "active notification" attribute with an SetParameterAttributes RPC like described in TR-069 [1]. For all parameters with a turned on "active notification" attribute a TR-069 session establishment is triggered when its value changes, and the value change is communicated to the ACS (e.g. self-configuration status change to indicate that the FAP is ready to continue to the next step). This implies that a certain set of parameters needs to have the "notification" attribute to be set appropriately.

The example of parameters that can utilize this mechanism includes the followings:

Table 6 – Example Parameters for Active Notification

Parameter	Description
.*FAPService*.{i}.REM.UMTS.WCDMA FDD.ScanStatus	Indicates the current REM status of the UMTS cells (FDD). The change of value from *"InProgress"* to *"Success"* or *"Error_TIMEOUT"* indicates that the FAP has completed the REM process and is ready to proceed to the next step with the FAP.
.*FAPService*.{i}.REM.UMTS.GSM.Sca nStatus	Indicates the current REM status of the GSM cells. The change of value from *"InProgress"* to *"Success"* or *"Error_TIMEOUT"* indicates that the FAP has completed the REM process and is ready to proceed to the next step with the FAP.

II.1.5 Default Values

There are writable parameters to enable the self-configuration function in the FAP. Typically these writable parameters are set to *"disabled"* when shipped from the factory implying that no self-configuration is allowed until the ACS explicitly sets them to enable them.

This applies to all parameters located under:

- .FAPService.{i}.FAPControl.UMTS.SelfConfig.

II.1.6 Discovery of Device Capabilities and Activation of Self-Configuration

Figure 8 below shows the activation of self-configuration. The ACS first reads what self-configuration functionalities the FAP supports by reading *…Config* parameters under *.FAPService.{i}.Capabilities.UMTS.SelfConfig*. Based on this information, the ACS enables the appropriate *…ConfigEnable* parameters under *.FAPService.{i}.FAPControl.UMTS.SelfConfig* to activate that specific aspect of the self-configuration. The FAP in turn starts the internal self-configuration function.

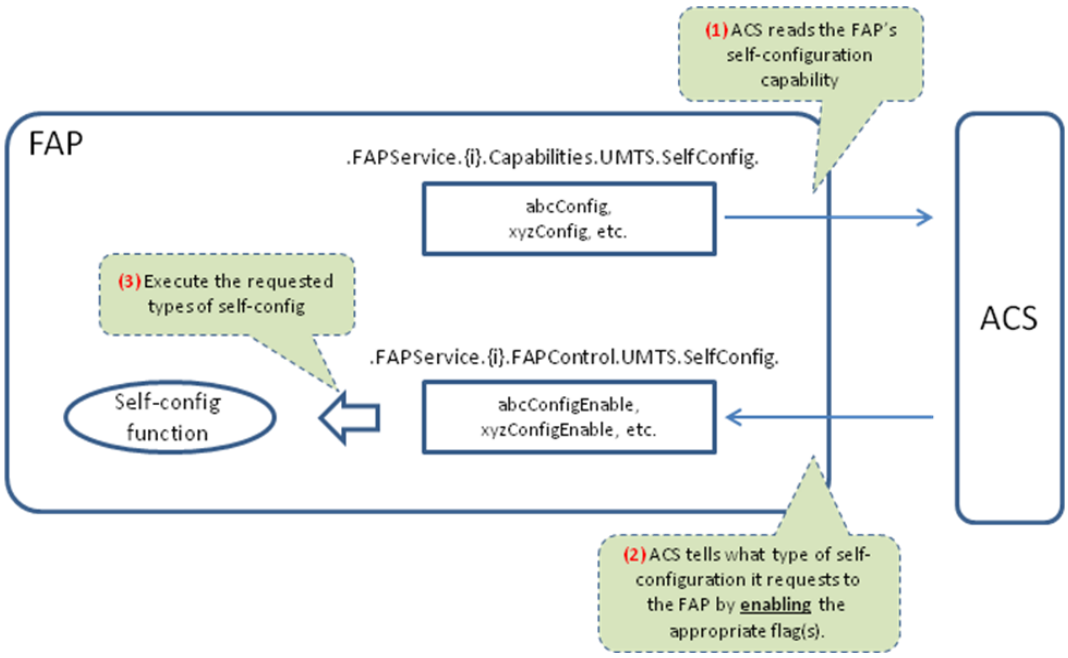

Figure 8 – Discovery of device capabilities and activation of self-configuration

II.1.7 Deactivation of Self-Configuration

Deactivation of self-configuration is done in the following way as shown in Figure **9** below. The ACS disables the appropriate *…ConfigEnable* parameter under

.FAPService.{i}.FAPControl.UMTS.SelfConfig

to de-activate that specific aspect of the self-configuration. FAP in turn stops the internal self-configuration function.

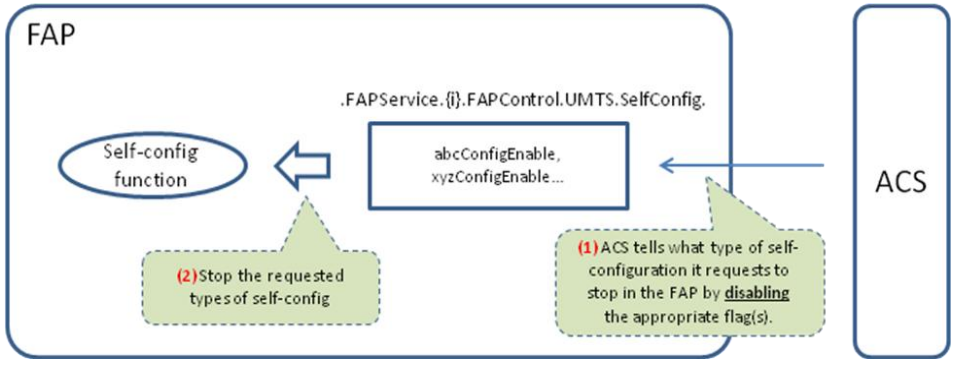

Figure 9 – Deactivation of self-configuration

II.1.8 Self-Configuration Operation

There are two types of self-configuration operation. The first type applies to individual parameter and the second type applies to a group of parameters. In Figure 10 below shows these as two horizontal groups. In addition, the figure also displays the relationship of objects and parameters to illustrate the process or flow of events with four columns moving from left to right.

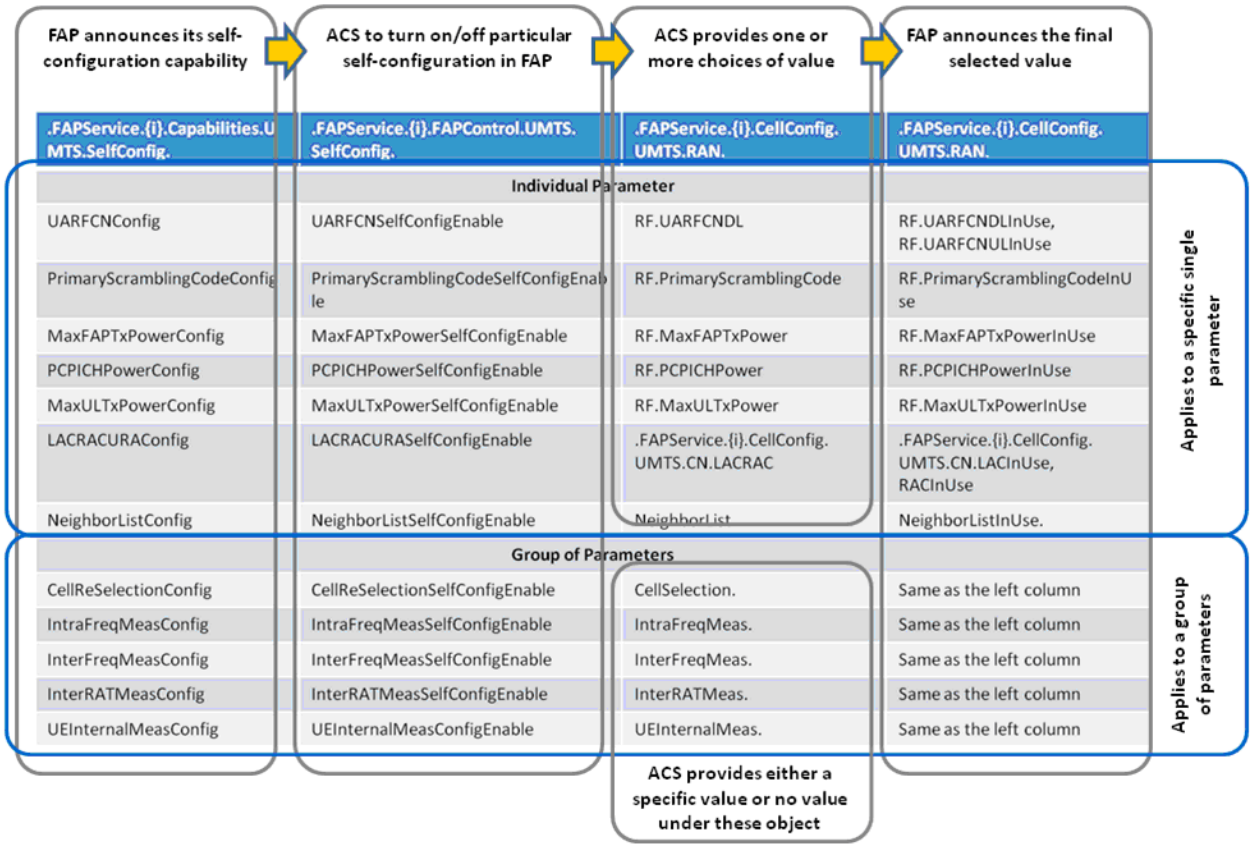

Figure 10 – Self-configuration operation – object relationship

For the first type that applies to the individual parameter (the upper horizontal group in the figure), the self-configuration operation is simple – the respective …ConfigEnable flag turns on or off the self-configuration of that particular parameter (e.g. UARFCN).

For the second type that applies to a group of parameters (the lower horizontal group in the figure), the self-configuration operation works as follows:

1. If the ACS explicitly provides a value to a particular parameter in the group during configuration, the FAP takes it as is and considers that self-configuration action of that parameter is not requested.

2. If the ACS does not explicitly provide a value to a particular parameter in the group during the configuration, the FAP considers it as a request by the ACS that those

"missing" parameters require self-configuration. The FAP initiates the self-configuration action for those "missing" parameters.

II.5 Radio Environment Measurement (REM) Process

There are three main purposes for the REM process and they are functionally separated:

1. Location verification
   The surrounding cell information (e.g. macro cells) can be used as a "fingerprint" of the area the FAP is located in order for the O&M system to verify its location against the location the FAP owner subscribed the service with (e.g. street address of the owner). The previous section that discusses location verification covers this.

2. Neighbor list (NL) configuration
   The scanning of the DL information (physical radio level information and broadcast information) is gathered from the nearby cells to build the neighbor list. This is a part of the FAP configuration so that it can broadcast appropriate set of NL to the UEs. The next section will cover this.

3. Parameter value selection
   The scanning of the DL information (both physical radio level and broadcast information) from the nearby cells is useful for the parameter selection process within the FAP. If the FAP is provided with a choice of multiple values or range of values, the nearby cell information can be used to avoid collision or to minimize interference in the area. Some of the examples are as follows:
   - Primary Scrambling Code
   - Maximum FAP Transmit Power
   - Maximum UL Transmit Power
   - PCPICH Power
   - LAC, RAC

This section discusses the general aspect of the REM process to facilitate these two purposes.

II.5.1 Execution of REM

The REM process is expected to be executed at the following timings:

- Very first (I.e. "out-of-the-box") initialization
- Subsequent initialization (i.e. reboot/reset)
- At periodic interval during the normal operation

II.1.9 Configuration of Periodic Measurement

The ACS configures the periodic interval of the REM process by setting one or more of the parameters shown in Figure 11 below.

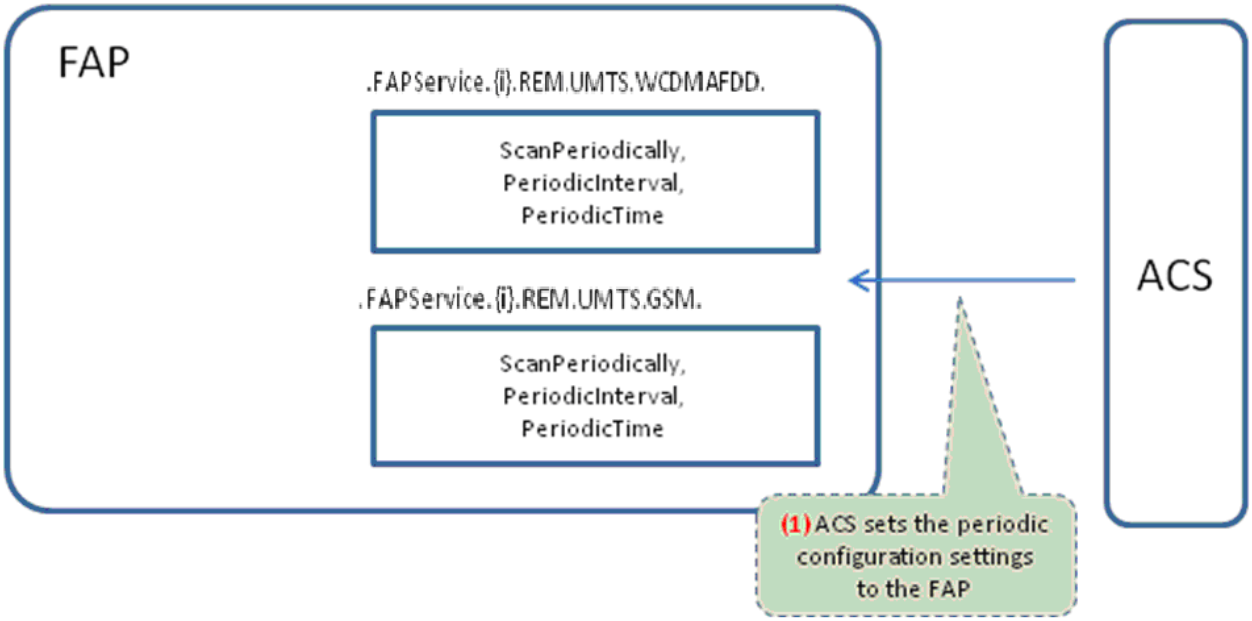

Figure 11 – REM Periodic Configuration

II.1.10 Configuration of Selective Measurement

The REM activity can be setup so that only a selected subset of the possible measurements is to be done. This helps to optionally speed up the REM process in the FAP by possibly ignoring other cell(s) that the system operator chooses not to consider (e.g. cells that belong to other PLMNs, or cells under a specific UARFCN, or other Femto cells). This can be done by using one or more of the following parameters shown in Figure 12 below. Typically, no selective measurement is assumed by the FAP with factory defaults. In other words, all parameter values in Figure 12 are *"<empty>"* when shipped from the factory.

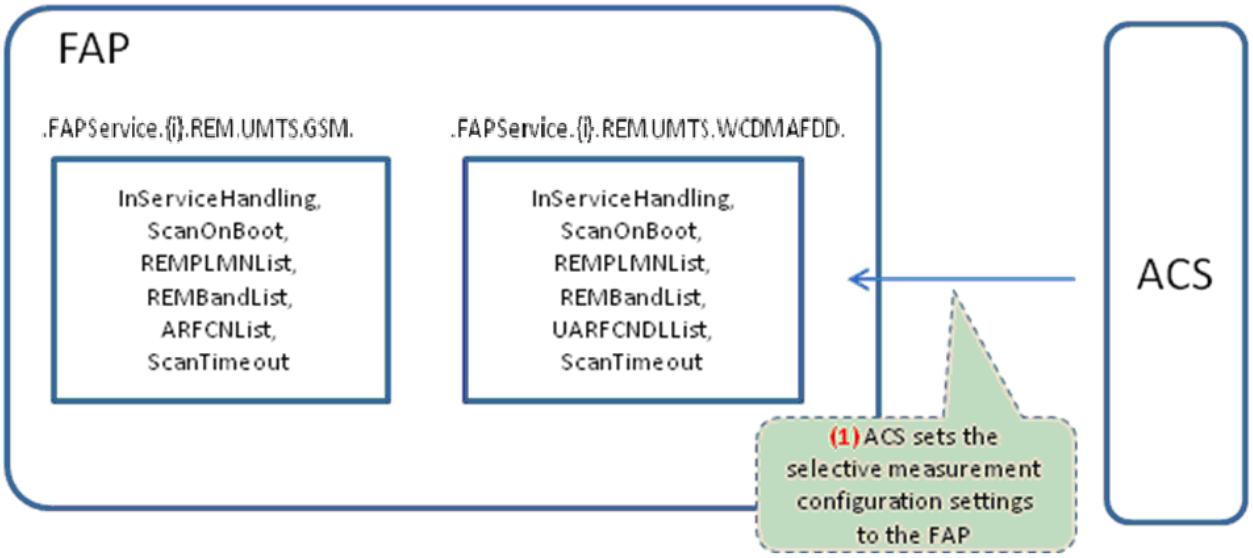

Figure 12 – REM Selective Measurement Configuration

II.1.11 Storage and Retrieval the Measurement Result

Figure 13 below shows the storage and retrieval of the REM information. When the FAP indicates that the information is available (*ScanStatus*), ACS can read the content. See Table 6 for the use of "Active Notification" attribute discussed earlier in this appendix.

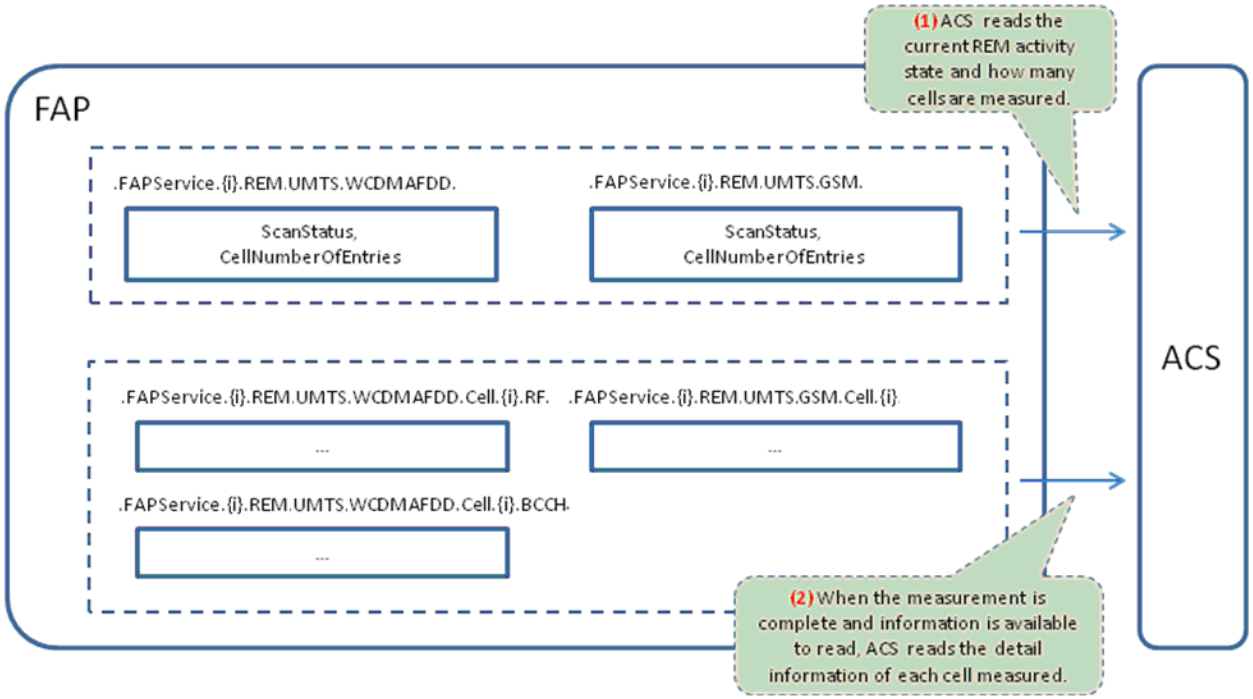

Figure 13 – Retrieval of REM Result

Two *ScanStatus* parameters shown in the above figure indicate the current REM status as defined in Table 7 below (this applies to both WCDMA-FDD and GSM cells).

Table 7 – *ScanStatus* Definition

Value	Description
Indeterminate	REM has not been executed and there are no valid scan results available, or REM has been executed but no neighbor cells have been detected. This is also the initial (default) value (i.e. out-of-the-box state).
InProgress	REM process is currently in progress and the corresponding *"...Cell.{i}."* objects are not yet ready to be read.
Success	REM process has completed successfully and corresponding *"...Cell.{i}."* objects are ready to be read. At least one valid entry can be found in the "...Cell.{i}." objects.
Error	REM process has resulted in error and corresponding *"...Cell.{i}."* objects is either empty or does not contain valid information.
Error_TIMEOUT	REM process was terminated due to timeout set by the ScanTimeOut parameter. CellNumberOfEntries indicates the number of the valid entries in the corresponding "…Cell.{i}." objects and are ready to be read.

II.6 Neighbor List Configuration

There are two methods for the neighbor list configuration:

- Fixed-configuration
- Self-configuration

II.1.12 Fixed-configuration

In fixed-configuration, the entire neighbor list configuration is provided by the ACS without consideration of the detected neighbors by the FAP as a result of the REM process. In this case, the detected neighbor list from the REM process can be used specifically for the location verification purpose only, but not for the neighbor list configuration purpose. Or ACS can, if so desired, optionally turn-off the entire REM process by setting for UMTS the following parameters to *"false":*

- *.FAPService.{i}.REM.UMTS.WCDMA.ScanOnBoot*
- *.FAPService.{i}.REM.UMTS. WCDMA .ScanPeriodically*

For GSM these parameters have to be set to *"false":*

- *.FAPService.{i}.REM.UMTS.GSM.ScanOnBoot*
- *.FAPService.{i}.REM.UMTS.GSM.ScanPeriodically*

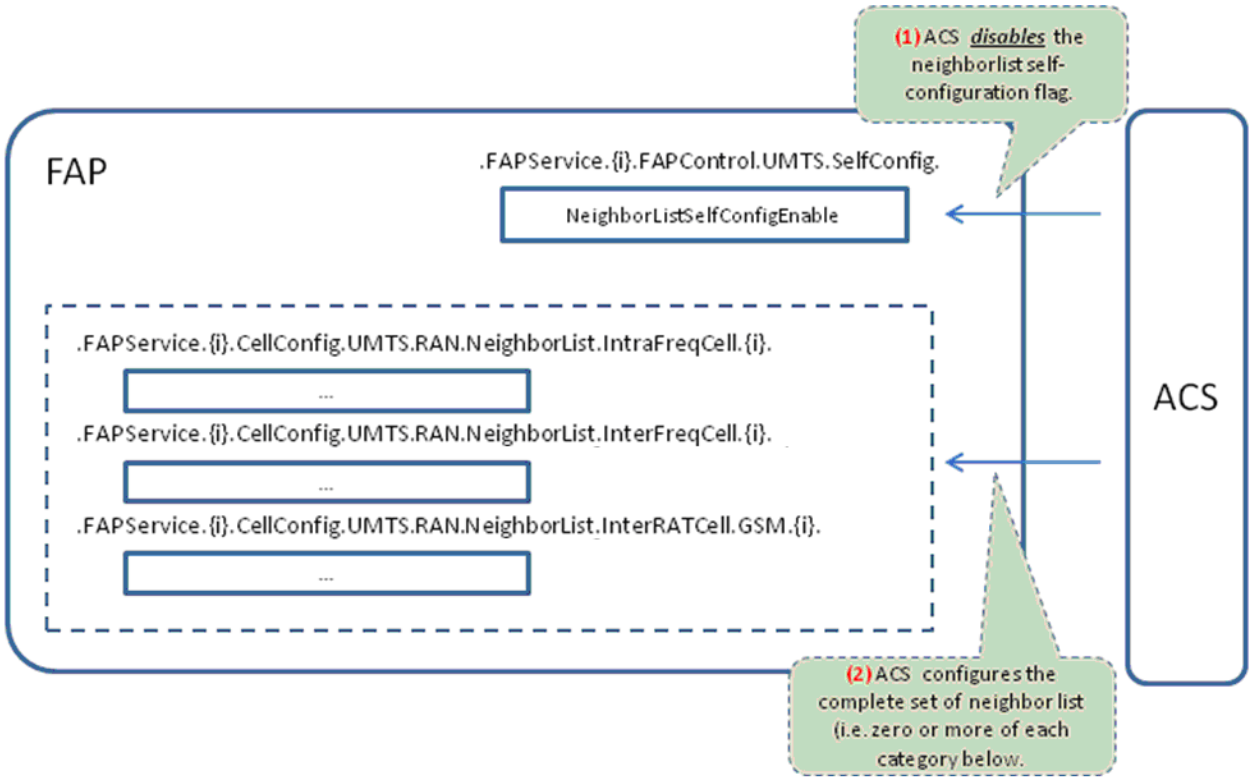

Figure 14 – Neighbor List – Fixed-configuration

II.1.13 Self-configuration

In self-configuration, the result from the REM process is taken into account for the final neighbor list configuration. Based on the REM result, the ACS takes additional step to configure the neighbor list.

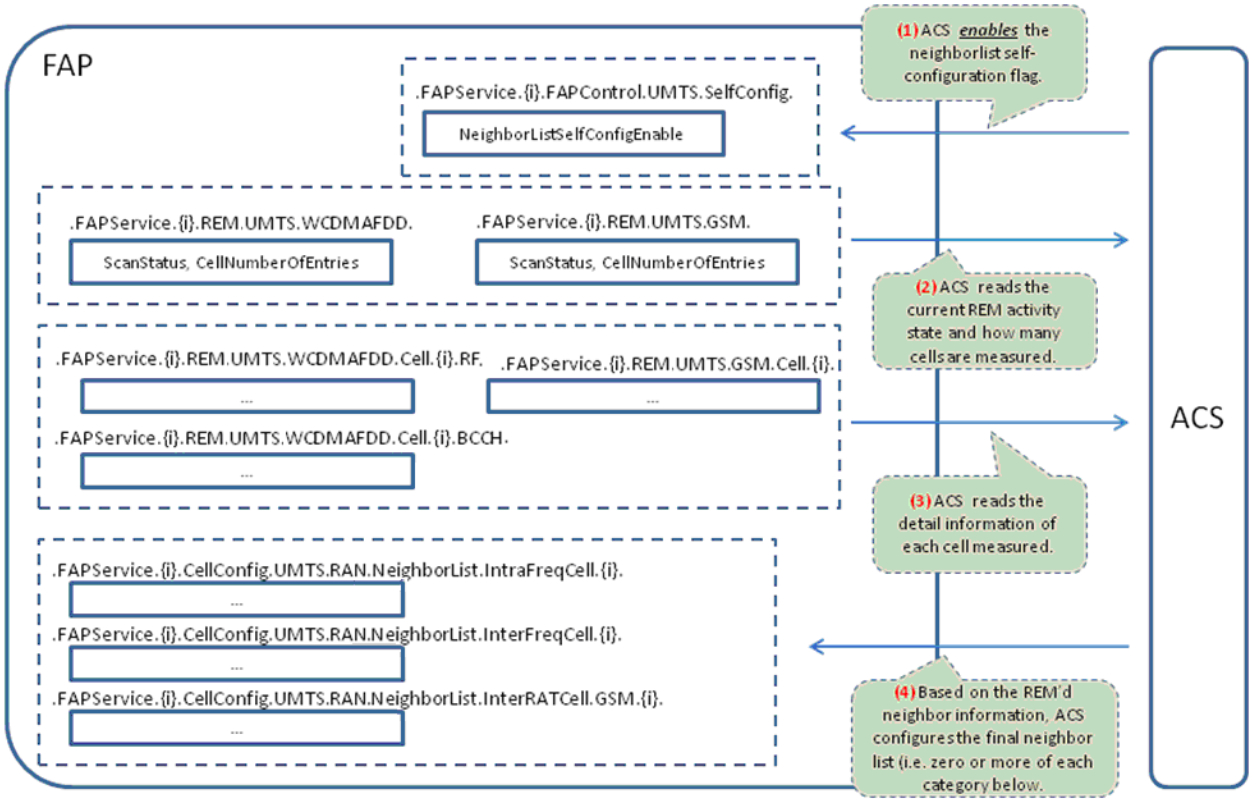

Figure 11: Neighbor List – Self-configuration

Upon obtaining the detected neighbor list through the REM process, the ACS has two options to take for each detected neighbor in order to derive the final neighbor list configuration:

1. Keep it.
2. Remove it (ignore it).

In addition, if the ACS wishes to add any cell that is not in the reported neighbor list, it can add it to the final neighbor list.

The decisions made by the ACS mentioned above are communicated to the FAP by *MustInclude* parameters under the following objects:

- .FAPService.{i}.CellConfig.UMTS.RAN.NeighborList.IntraFreqCell.{i}.
- .FAPService.{i}.CellConfig.UMTS.RAN.NeighborList.InterFreqCell.{i}.
- .FAPService.{i}.CellConfig.UMTS.RAN.NeighborList.InterRATCell.GSM.{i}.

Upon receiving the neighbor list in the above object, the FAP obeys the request by the ACS expressed in MustInclude parameters (see next Table).

Table 8 – *MustInclude* Definition

MustInclude value	Description
True	ACS requests FAP to include this particular neighbor in the final neighbor list.
False	ACS requests FAP to exclude this particular neighbor from the final neighbor list.

II.7 State Management

The following Figure 15 shows the State Management.

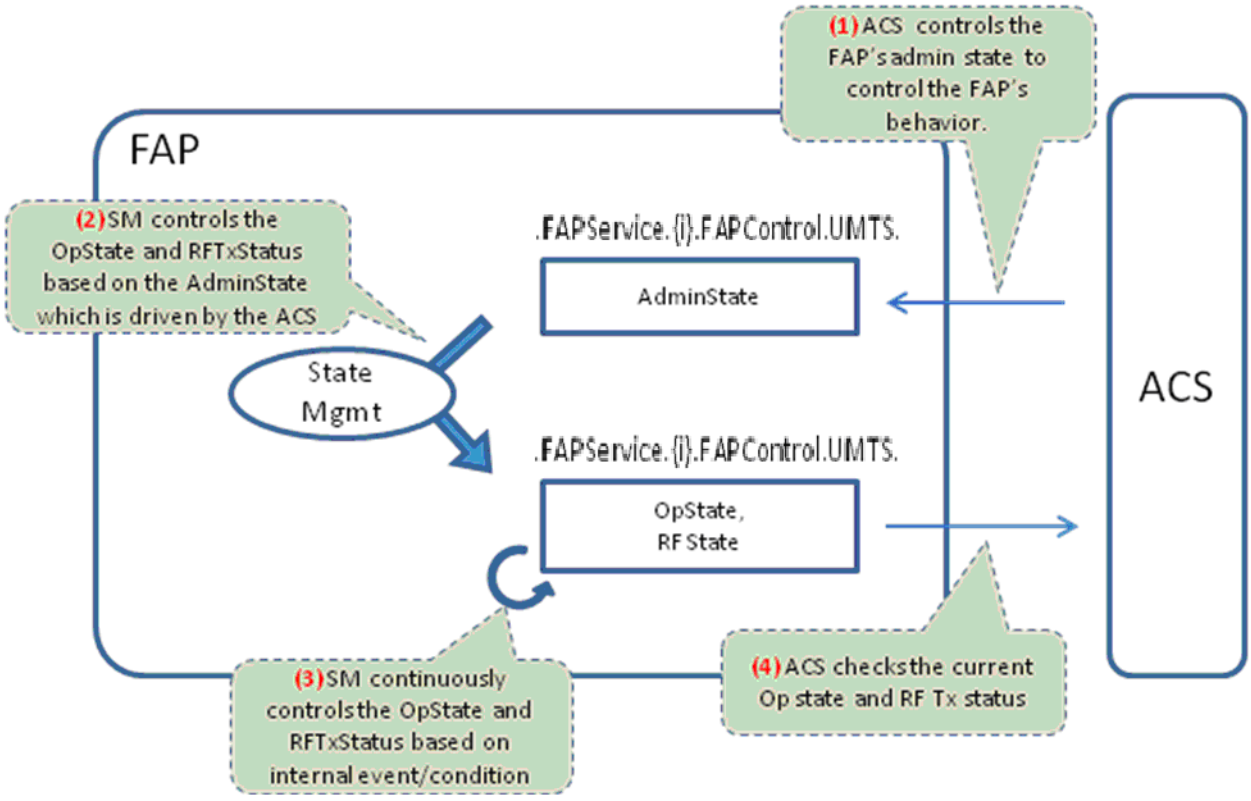

Figure 15 – State Management

There are 3 parameters that controls the UMTS FAP state and operation.

1. Administrative State (.FAPService.{i}.FAPControl.UMTS.AdminState)

2. Operational State (.FAPService.{i}.FAPControl.UMTS.OpState)
3. RF Tx Status (.FAPService.{i}.FAPControl.UMTS.RFTxStatus)

When the FAP (re-)initializes, it changes the status of these parameters to the following value as default regardless of the current value (see Table 9).

Table 9 – SM parameter Definition

Parameter	Default value
Administrative State	false (i.e. locked)
Operational State	false (i.e. disabled
RF Tx Status	false (i.e. RF off)

Appendix III Fault Management for Femto Access Points

The Fault management objects are defined as general component objects in TR-157 [4]. This section describes the following behaviors required for FAPs to manage faults. Specifically FAP devices behave differently for the following items:

- Use of Indeterminate Severities for the *PerceivedSeverity* Parameter
- Definition of which Probable Causes and Event Types values are supported by FAPs
- Event Tables Behavior Across Reboot of the FAP
- ManagedObjectInstance Encoding Formats and Domain Name Prefix Values

III.1. Use of Indeterminate Severities for the PerceivedSeverity Parameter

TR-157 [4] fault management objects permit a value of "Indeterminate" for the following parameters:

- <rootobject>. FaultMgmt.SupportedAlarm.{i}.PerceivedSeverity
- <rootobject>. Device.FaultMgmt.CurrentAlarm.{i}.PerceivedSeverity
- <rootobject>. FaultMgmt.HistoryEvent.{i}.PerceivedSeverity
- <rootobject>. FaultMgmt.ExpeditedEvent.{i}.PerceivedSeverity
- <rootobject>. FaultMgmt.QueuedEvent.{i}.PerceivedSeverity

Although *Indeterminate* is defined in ITU-X.733 [19] the value SHOULD NOT be used by FAP device as a *PerceivedSeverity*.

III.2. Probable Causes and Event Types

FAP devices utilize event (alarm) types and probable causes defined in 3GPP-TS.32.111-5 [11] for the following objects:

- <rootobject>. FaultMgmt.SupportedAlarm.{i}.EventType, ProbableCause
- <rootobject>. Device.FaultMgmt.CurrentAlarm.{i}.EventType, ProbableCause
- <rootobject>. FaultMgmt.HistoryEvent.{i}.EventType, ProbableCause
- <rootobject>. FaultMgmt.ExpeditedEvent.{i}.EventType, ProbableCause
- <rootobject>. FaultMgmt.QueuedEvent.{i}.EventType, ProbableCause

III.3. Event Tables and Reboot Functionality

FAP devices MUST retain data in the following tables across reboots of the device:

- <rootobject>. FaultMgmt.HistoryEvent.{i}.
- <rootobject>. FaultMgmt.ExpeditedEvent.{i}.
- <rootobject>. FaultMgmt.QueuedEvent.{i}.

III.4. ManagedObjectInstance Parameter Encoding

FAP devices should pre-pend the *.FAPService.{i}.DNPrefix* parameter to the local DN to create the value of the *ManagedObjectInstance* parameter. In addition, the *ManagedObjectInstance* parameter should be encoded according to 3GPP-TS.32.300 [12].

This affects the *ManagedObjectInstance* parameter for the following objects:

- <rootobject>. Device.FaultMgmt.CurrentAlarm.{i}.ManagedObjectInstance
- <rootobject>. FaultMgmt.HistoryEvent.{i}.ManagedObjectInstance
- <rootobject>. FaultMgmt.ExpeditedEvent.{i}.ManagedObjectInstance
- <rootobject>. FaultMgmt.QueuedEvent.{i}.ManagedObjectInstance

End of Broadband Forum Technical Report TR-196

