VIRTUAL ROAMING SYSTEMS FOR GSM, GPRS AND UMTS
OPEN CONNECTIVITY IN PRACTICE

Arnaud Henry-Labordère
Professor at Ecole Nationale des Ponts et Chaussées, France
Contents

Preface xiii

By the Same Author xviii

Abbreviations and Acronyms xix

1 ‘Virtual Roaming’ Purpose and Principles 1

1.1 Mobile Services Affected by Virtual Roaming 1

1.2 Virtual Roaming Hub for Inbound Visitors’ Service (Single IMSI) 2

1.2.1 Registration Principle for a Virtual Visitor 2

1.2.2 CAMEL Prepaid Outgoing Call of a Virtual Visitor 3

1.2.3 SMS-MO Sending for a Virtual Visitor 3

1.2.4 GPRS Access (Data Services) for a Virtual Visitor 4

1.2.4.1 Billing Principle 4

1.2.4.2 Business Model: Data Services of the Roaming Hub 5

1.2.5 Incoming Call 7

1.3 Virtual Roaming Hub for Outbound Subscribers: Multi-IMSI 7

1.4 Brief Introduction to Standard Bilateral Roaming Procedures 9

1.5 Principles of the SS7 Protocol Layers Used in Roaming Procedures 10

1.5.1 Need to Have Standardized Messages: the MAP and CAMEL Protocols 10

1.5.2 Need to Exchange Them with Transactions: the TCAP Protocol 12

1.5.3 Packet Protocol to Transfer Data between Two Different Networks: SCCP 12

1.5.4 Packet Protocol to Transfer SCCP Blocks between Equipment: MTP or SIGTRAN 12

1.5.5 The Lower Layers, not a Concern for Virtual Roaming Systems 13

2 Architecture of Virtual Roaming Systems 15

2.1 SCCP, MAP, CAP and GTP Transformation Principle in the Roaming Hub 15

2.1.1 Setup of Virtual Visitor Roaming in the VPLMN 16

2.1.2 Required SCCP Address Transparency of the MAP, CAMEL and TCAP Layers of the SS7 Stack 16

2.2 Procedures for the Virtual Roaming Visitors’ Service (Single IMSI) 16

2.2.1 The UPDATE LOCATION Registration Procedure (MAP Sent to the HLR) 17

2.2.2 Outgoing Calls for Post-paid Visitors 18

2.2.3 Reception of Calls while Roaming (MAP Sent to the VLR) 18

2.2.4 Outgoing SMS-MO (MAP to the SMSC) 19
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.5</td>
<td>Reception of SMS-MT while Roaming (MAP Sent to MSC)</td>
<td>19</td>
</tr>
<tr>
<td>2.2.5.1</td>
<td>Case of ‘Reply Path’ Setting</td>
<td>20</td>
</tr>
<tr>
<td>2.2.6</td>
<td>READY FOR SM Procedure (MAP to the HLR)</td>
<td>20</td>
</tr>
<tr>
<td>2.2.7</td>
<td>Outgoing USSD (MAP to the HLR)</td>
<td>20</td>
</tr>
<tr>
<td>2.2.8</td>
<td>Reception of USSD ‘Push’ while Roaming (MAP Sent to MSC)</td>
<td>21</td>
</tr>
<tr>
<td>2.2.9</td>
<td>Outgoing Supplementary Services (Call Forwarding or Barring) (MAP to</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>the HLR)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2.9.1 Without Get Password</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>2.2.9.2 Get Password Request by the HLR</td>
<td>21</td>
</tr>
<tr>
<td>2.2.10</td>
<td>PURGE MS Procedure (MAP to the HLR)</td>
<td>22</td>
</tr>
<tr>
<td>2.2.11</td>
<td>2.5G and 3G: UPDATE LOCATION GPRS (MAP to the HLR)</td>
<td>22</td>
</tr>
<tr>
<td>2.2.12</td>
<td>2.5G and 3G: Outgoing Create PDP Context (GTP to the HPLMN GGSN)</td>
<td>25</td>
</tr>
<tr>
<td>2.2.13</td>
<td>Extended Service: Optimal Call Reception Routing (MAP to the HLR)</td>
<td>26</td>
</tr>
<tr>
<td>2.2.14</td>
<td>Extended Service: Optimal Routing to VMS (MAP to the GMSC)</td>
<td>26</td>
</tr>
<tr>
<td>2.2.15</td>
<td>Extended Service SMSeXchange: Visitor Receiving SMS-MT from All the</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>VPLMN Subscribers</td>
<td></td>
</tr>
<tr>
<td>2.2.16</td>
<td>Extended Service: Allowing the VPLMN to ‘Push’ USSD to the Virtual</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Visitors</td>
<td></td>
</tr>
<tr>
<td>2.2.17</td>
<td>Extended Service: Providing the Control of Stolen Handsets in the VPLMN</td>
<td>28</td>
</tr>
<tr>
<td>2.2.18</td>
<td>Outgoing Call, SMS or GPRS for Prepaid Visitors (CAMEL to the SCP)</td>
<td>28</td>
</tr>
<tr>
<td>2.2.19</td>
<td>Reception of Calls while Roaming for a Prepaid Subscriber</td>
<td>29</td>
</tr>
<tr>
<td>2.3</td>
<td>Restriction of Virtual Roaming by the Roaming Hub</td>
<td>29</td>
</tr>
<tr>
<td>2.3.1</td>
<td>GPRS Barring</td>
<td>30</td>
</tr>
<tr>
<td>2.3.2</td>
<td>SMS Interworking Barring</td>
<td>30</td>
</tr>
<tr>
<td>2.3.3</td>
<td>CAMEL Roamers Barring</td>
<td>30</td>
</tr>
<tr>
<td>2.4</td>
<td>Procedures for the Virtual Roaming Visitors’ Service (Multi-IMSI)</td>
<td>31</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Setup for the Roaming Hub in the ‘Auxiliary Mobile Network’</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>2.4.1.1 Connecting the Virtual Roaming Hub in the Auxiliary Network:</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>E214 and E164 Incoming Route Table Creation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4.1.2 Manufacturing the Dual IMSI Cards (if the STK Solution is Used)</td>
<td>32</td>
</tr>
<tr>
<td>2.4.2</td>
<td>Setup in the Roaming Hub of the Correspondence ‘Auxiliary IMSI →</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Nominal IMSI’</td>
<td></td>
</tr>
<tr>
<td>2.4.3</td>
<td>The SEND AUTHENTICATION Procedure</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>2.4.3.1 Difference between 2G and 3G</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>2.4.3.2 Segmented TCAP Dialogues</td>
<td>34</td>
</tr>
<tr>
<td>2.4.4</td>
<td>The UPDATE LOCATION Registration Procedure (MAP Sent to the HLR</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Nominal)</td>
<td></td>
</tr>
<tr>
<td>2.4.5</td>
<td>Reception of Calls while Roaming (MAP Sent to the VLR)</td>
<td>34</td>
</tr>
<tr>
<td>2.4.6</td>
<td>Outgoing SMS-MO (MAP to the SMSC): Generalization of SMSeXchange</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>2.4.6.1 No MNP in the Country of the Outbound Roaming Subscriber</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>2.4.6.2 MNP in the Country of the Outbound Roaming Subscriber:</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Mandatory ‘Address Resolution’ by the Roaming Hub</td>
<td></td>
</tr>
<tr>
<td>2.4.7</td>
<td>Reception of SMS-MT while Roaming (MAP Sent to MSC)</td>
<td>37</td>
</tr>
<tr>
<td>2.5</td>
<td>IS 41 ↔ MAP GSM Inter-standard Roaming Hubs</td>
<td>37</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Initial Registration Procedure GSM Network → IS 41</td>
<td>37</td>
</tr>
<tr>
<td>2.5.2</td>
<td>Reception of Calls while Roaming (IS 41 Virtual Visitor) and VMS Forwarding</td>
<td>37</td>
</tr>
<tr>
<td>2.6</td>
<td>Various MAP and CAMEL Transformation Methods</td>
<td>39</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Called SCCP Address from Transparent MAP Parameters</td>
<td>40</td>
</tr>
<tr>
<td>2.6.2</td>
<td>MAP and SCCP Translations from Tables</td>
<td>40</td>
</tr>
</tbody>
</table>
3 Connecting the VPLMN MNOs to a Virtual Roaming Supplier 51

3.1 MNO Configuration vs Roaming Hub Supplier Configuration 51

3.2 Connection to the Roaming Hub Service, MNO Point of View: Using the ‘Alias GT’ Method 51

3.2.1 Basic Services: Voice and SMS 51

3.2.1.1 CC-MGT of HPLMNs Must Be Translated to the Roaming Hub GT 52

3.2.1.2 E212 → E214 of HPLMNs Created to Route to Roaming Hub 52

3.2.1.3 Prepaid Virtual Visitors’ Configuration (CAMEL) 53

3.2.1.4 Setting up the ‘SMSeXchange Service’ if it is Provided by the Roaming Hub Supplier 53

3.2.1.5 Control of Stolen Handsets: Checking of the IMEI Service 53

3.3 Details of E212 → E214 MNO Configuration with the GT Translation Methods 53

3.3.1 Alias GT E214 53

3.3.2 Alias GT E164 54

3.4 Connection to the Roaming Hub Service, MNO Point of View: Using the ‘MTP Transparent Tunnelling’ Method 54

3.5 Roaming Hub Supplier Point of View: Different Modes of Connection of the MNO Clients 54

3.5.1 GT Translations 55

3.5.2 MTP Transparent Tunnelling 55

3.5.2.1 MTP Level 56

3.5.2.2 SCCP Level 56

3.5.3 National Point Code <-> International Point Code Routing 56

3.6 Implementation of a Roaming Hub with Several Point Codes 57

3.6.1 Architecture Principle for Multiple Point Codes 57

3.6.2 Details of Operation 58

3.6.2.1 Outgoing SCCP (Roaming Hub → Distant Mobile Network) 58

3.6.2.2 Incoming SCCP (Roaming Hub ← Distant Mobile Network): Impossibility of Using a Standard SCCP 59

3.6.2.3 Correct Solution: Bypass of SCCP from MTP3 → TCAP 60

3.6.2.4 Case of SST and SSA 60

3.6.3 Origin Point Code Substitution to Avoid Creating MTP Routes to all the MNOs 61

3.7 SS7 Stack Architecture for a Robust Integrated System with Several Point Codes 61

3.7.1 Layered Architecture Diagram 61

3.7.2 Intermediate Layer MTP3-SCCP 62

3.7.3 Intermediate Layer TCAPuser 62

3.8 SIGTRAN Introduction and Practical Configuration 63

3.8.1 SIGTRAN the all IP SS7 Signalling Connection for 2.5G, 3G and 4G 63

3.8.2 Example of an E1 (TDM) Connection Configuration with Dialogic Software 63

3.8.3 SCTP (Stream Control Protocol): Principle [3.2] 64

3.8.4 Example of MTP3/M2PA/SCTP Configuration with the Dialogic SIGTRAN Software 65
3.8.5 Example: M3UA/SCTP Configuration with the Dialogic SIGTRAN Software 65
3.8.5.1 Config File: AS Side 65
3.8.5.2 Config File: SG Side 66

3.9 Standard MTP3 Load Distribution Algorithm 66
3.9.1 Distribution of Traffic on the Various Links of a Given Linkset 66
3.9.2 Load of the Most Loaded Link(s) 66

3.10 SCCP Class 1 (Sequenced Connectionless Protocol) 68
3.10.1 The ‘Sequence Control’ Number 68
3.10.2 Messages between the SS7 Protocol Layers when SCCP Class 1 is Used 69

References and Further Reading 69

4 Networks of Roaming Hubs and SMSeXchanges 71
4.1 Cooperation of Several Roaming Hubs 71
4.2 Problem Raised by Mobile Number Portability (MNP) 71
4.2.1 Reminder: Example of MNP Implementation 71
4.2.2 Implementation of the Network Search with Distributed Roaming Hubs 73

4.3 Use of the TCAP Dialogue Part to Provide an End-To-End Routing Capability 74
4.3.1 TCAP Dialogue and Component Parts 74
4.3.2 Example of Use of the ‘Destination Reference’ 75
4.3.3 Example of Use of the Origin_Reference 76
4.3.4 Avoiding Unnecessary MAP (or CAMEL) Version Negotiations 76
4.3.5 Compatibility with Roaming Hubs not Capable of ‘End-to-End’ Routing 77

References and Further Reading 77

5 Hosted Roaming Hubs with Virtual GTs 79
5.1 Purpose 79
5.2 TCAP Dialogue Implementation Constraints 79
5.2.1 TCAP Protocol Reminder 79
5.2.2 TCAP Dialogue ‘Segmentation’ 80
5.2.3 Different Methods for GT Address Translation in Roaming Hub Partners 82
5.2.3.1 First Method: Straight Address Translation to Real GT Roaming Hub 82
5.2.3.2 Use of the ‘Prefix’ Method (Hub Indicator HI) 82
5.2.3.3 Comparison of the Two Methods 83
5.2.3.4 Capabilities Required with the TCAP Programming Interface 83

References and Further Reading 84

6 Location-based Services and Virtual Roaming 85
6.1 Traces Show How an SMLC Really Works 85
6.2 ‘Spyware Measurements’ in the Handset 86
6.2.1 Spyware in the Handset (Java Applet or Proprietary OS) 87
6.2.2 How a Location Server Can ‘Automatically’ Learn the Map of the Cells 87
6.2.3 Spyware in the SIM Tool Kit Methods for MT-LR 87
6.2.4 Syntax of the AT Command Sent by the STK or the Java Applet for the ‘Cell Environment’ 88
6.2.4.1 Syntax (Wavecom Modem GSM) 88
6.2.4.2 Result of Direct Handset-based Measurements with AT Commands 88
6.2.4.3 Comparison with Network-based Measurements Made through the BSC 88
6.2.4.4 Computation of Mobile Location Estimate with TA and Measurement Reports
6.2.4.5 Use of Timing Advance (TA) Only

6.3 Network MAP-based Location Obtaining Methods: Prerequisites
6.3.1 Location Alerts and Mobile Originating Location Request (MO-LR)
6.3.1.1 Location Preparation Procedure
6.3.1.2 Positioning Measurement Establishment Procedure
6.3.1.3 Location Calculation and Release Procedure
6.3.2 Network Initiated Location Request (MT-LR)
6.3.2.1 Location Preparation Procedure
6.3.2.2 Positioning Measurement Establishment Procedure
6.3.2.3 Location Calculation and Release Procedure
6.3.3 Changes in the VLR Profile for LBS for Virtual Roaming
6.3.4 Explanations of the LCS Parameters in the Mobile Profile to be Provisioned in the HLR
6.3.4.1 GMLC List
6.3.4.2 LCS Privacy Exception List

6.4 Simple BSS-based SMLC Architecture Using the Mobile TA and Measurements
6.4.1 The MAP Location Service Enquiry is Required in the MSC
6.4.2 Detailed Data Flow
6.4.3 NSS-based SMLC Alternative: Possibility of Using an External Hosted SMLC
6.4.4 Detailed Traces: What Connection Oriented SCCP (SCCP Class 2) is
6.4.4.1 MAP Dialogue Initial Part
6.4.4.2 BSSAP-LE Dialogue: between BSC and SMLC
6.4.4.3 MAP Dialogue End Part between MSC and GMLC

6.5 Details of a More Accurate Positioning Method: A-GPS
6.5.1 Signalling Layers between the SMLC and the Handset (Target MS)
6.5.2 Trace of BSSAP-LE Dialogue between the SMLC and the Handset

6.6 The Enhanced Time Difference (E-OTD) Method: Hyperbola Intersections
6.6.1 Understanding E-OTD Method in GSM Networks
6.6.1.1 Why the Intersection of Hyperbolas?
6.6.1.2 How a ‘Burst’ of the Neighbouring BTS is Triggered by the Measurement Position Request
6.6.1.3 How the Calibration RTDi are Obtained by the SMLC
6.6.2 Content of the E-OTD Assistance Data
6.6.3 Content of the MS POSITION COMMAND for E-OTD

6.7 Annex: Execution of the Algorithm for Position Computation with the ‘Measurement Reports’ or E-OTD

7 Roaming Costs or Inter-operator Traffic Charge Suppression Systems, and Other Service Improvements
7.1 VMS Anti-tromboning: Large Financial Savings in GSM and UMTS
7.1.1 ‘Optimal Routing’ (OR) and Other Methods
7.1.2 Active CAMEL Logic in the Service Control Point
7.1.3 ISUP and MAP Call Transfer Package
7.1.4 Passive CAMEL Monitoring and MAP Call Transfer Package
7.1.4.1 MAP Roaming Number Enquiry Package V3 Available
7.1.4.2 How It Works for the Case PROVIDE ROAMING NUMBER
Is ≤ MAP V2
7.1.4.3 For the Developers: All the Trace Details
7.2 Call Back and Local Calls Optimization
7.2.1 Classical Call
7.2.2 Call Back: Ergonomics Improvement with a SIM Tool Kit
7.2.3 Call Back: Ergonomics Improvement with a CAMEL Platform
7.2.4 Implementing Call Back: Use an IVR or Simply CAMEL?
7.2.5 Fully Transparent Ergonomics: Local Roaming Number System
7.3 Dialled Number Correction with CAMEL
References and Further Reading

8 SIM Cards ‘Over The Air’ Provisioning
8.1 Principles of SIM OTA Using SMS: Download and Upload
8.1.1 Applications and Different OTA Methods: for Handsets and for SIM Cards
8.1.2 The SMS SIM OTA: How It Works for Download and Upload
8.1.2.1 PoR by SMS-MO ‘SUBMIT’
8.1.2.2 PoR by SMS-MT Ack ‘DELIVER REPORT’
8.1.2.3 OTA with a Chain of Hubs
8.1.3 Checking the Result of a SIM Download with the Handset
8.1.4 Uploading Large SIM Files with Concatenated SMS: Single PoR
8.1.5 Security in OTA
8.1.6 SIM Download/Upload: Different Type of Applications
8.1.6.1 On Request General SIM Downloads
8.1.6.2 Regular (2–3 months) General SIM Downloads
8.1.6.3 Real-time Individual SIM Uploads (Read the Content of the Handset)
8.1.7 Integrated vs External OTA SIM Servers
8.1.7.1 Downloaded File Size and Performance Issue When Using OTA by SMS-PP
8.1.7.2 External OTA SIM Servers from Card Vendors
8.1.7.3 Integrated (with SMSC) OTA SIM Servers
8.1.8 Bi-IMSI SIM Tool Kits for Virtual Roaming
8.2 OTA SIM Provisioning Interface Examples
8.2.1 SIM Card Profiles
8.2.2 Customer Information
8.2.3 Read/Update a SIM Card
8.2.3.1 Read a SIM Card
8.2.3.2 Update a SIM Card
8.3 Coding the Binary Payload to Download (Write) and Upload (Read) Files of the SIM Card (Access with Remote File Manager)
8.3.1 Different Types of File in the SIM Card
8.3.2 File Download Examples Using the Remote File Manager
8.3.2.1 Example of Service Provider Name (SPN) Download (‘Transparent File’)
8.3.2.2 Example of ‘Address Book’ (Abbreviated Dialling Number) and Download (‘Linear Fixed’ File)
8.3.2.3 Example of SMS Parameters Download (‘Linear Fixed’ File)
8.3.3 Example of SIM File ‘Upload’ (Remote Reading by the SMSC) Using the Remote File Manager
8.3.3.1 Reading the Serial Number (‘Transparent File’)

CONTENTS

7.1.4.2 How It Works for the Case PROVIDE ROAMING NUMBER Is ≤ MAP V2 123
7.1.4.3 For the Developers: All the Trace Details 123
7.2 Call Back and Local Calls Optimization 124
7.2.1 Classical Call 124
7.2.2 Call Back: Ergonomics Improvement with a SIM Tool Kit 124
7.2.3 Call Back: Ergonomics Improvement with a CAMEL Platform 125
7.2.4 Implementing Call Back: Use an IVR or Simply CAMEL? 127
7.2.5 Fully Transparent Ergonomics: Local Roaming Number System 127
7.3 Dialled Number Correction with CAMEL 128
References and Further Reading 129

8 SIM Cards ‘Over The Air’ Provisioning 131
8.1 Principles of SIM OTA Using SMS: Download and Upload 131
8.1.1 Applications and Different OTA Methods: for Handsets and for SIM Cards 131
8.1.2 The SMS SIM OTA: How It Works for Download and Upload 132
8.1.2.1 PoR by SMS-MO ‘SUBMIT’ 132
8.1.2.2 PoR by SMS-MT Ack ‘DELIVER REPORT’ 133
8.1.2.3 OTA with a Chain of Hubs 133
8.1.3 Checking the Result of a SIM Download with the Handset 133
8.1.4 Uploading Large SIM Files with Concatenated SMS: Single PoR 134
8.1.5 Security in OTA 134
8.1.6 SIM Download/Upload: Different Type of Applications 135
8.1.6.1 On Request General SIM Downloads 135
8.1.6.2 Regular (2–3 months) General SIM Downloads 135
8.1.6.3 Real-time Individual SIM Uploads (Read the Content of the Handset) 135
8.1.7 Integrated vs External OTA SIM Servers 136
8.1.7.1 Downloaded File Size and Performance Issue When Using OTA by SMS-PP 136
8.1.7.2 External OTA SIM Servers from Card Vendors 136
8.1.7.3 Integrated (with SMSC) OTA SIM Servers 136
8.1.8 Bi-IMSI SIM Tool Kits for Virtual Roaming 136
8.2 OTA SIM Provisioning Interface Examples 137
8.2.1 SIM Card Profiles 137
8.2.2 Customer Information 138
8.2.3 Read/Update a SIM Card 138
8.2.3.1 Read a SIM Card 138
8.2.3.2 Update a SIM Card 139
8.3 Coding the Binary Payload to Download (Write) and Upload (Read) Files of the SIM Card (Access with Remote File Manager) 139
8.3.1 Different Types of File in the SIM Card 139
8.3.2 File Download Examples Using the Remote File Manager 139
8.3.2.1 Example of Service Provider Name (SPN) Download (‘Transparent File’) 140
8.3.2.2 Example of ‘Address Book’ (Abbreviated Dialling Number) and Download (‘Linear Fixed’ File) 142
8.3.2.3 Example of SMS Parameters Download (‘Linear Fixed’ File) 143
8.3.3 Example of a SIM File ‘Upload’ (Remote Reading by the SMSC) Using the Remote File Manager 145
8.3.3.1 Reading the Serial Number (‘Transparent File’) 145
8.3.3.2 Reading the Location Information (‘Transparent File’) 145
8.3.3.3 Reading the SMS Parameters (‘Linear Fixed File’) 146
8.3.3.4 Reading the SIM Service Table (‘Transparent File’) 147
8.3.3.5 Reading the Phase Identification File (‘Transparent File’) 148
8.3.3.6 More Complicated: OTA Reading and Updating the PLMN Selector Table (‘Transparent File’ Variable Length) for the ‘Steering of Roaming’ 148
8.3.3.7 Get the Length of the File 150
8.3.3.8 Read the PLMN Selector File 150
8.3.3.9 Update the PLMN Selector File to Set the Preferred PLMN 151
8.3.3.10 You Want to be Sure? Read the Updated PLMN Selector File Now 152
8.3.3.11 Improving the Efficiency of the Registration of Your Subscribers While in Your HPLMN: Avoid Scanning Your Competitors by Setting the Forbidden PLMN File 152
8.3.3.12 Changing the ‘Auxiliary IMSI’ of a Dual IMSI Virtual Roaming SIM Tool Kit 153

8.4 Coding the Binary Payload to Download (Write) and Upload (Read) Data of the SIM Card (Access with Applet File Manager) 154
8.4.1 Data Upload (Reading) 154
8.4.2 Reading the SIM Card Resources 154

8.5 Coding a Binary Payload Which Triggers the Execution of a Remote SIM Tool Kit (Using the Applet File Manager) 154

8.6 More Details on OTA Formats 155
8.6.1 Detailed Analyser: See the Cryptographic Checksum 155
8.6.2 Details of Optional Ciphering 159

8.7 Details for the Upload of a Big SIM Address Book (Multiple Entries) Using Concatenated SMS 160

8.8 Security Keys, How to Use the Card Vendor Provided Data 163
References and Further Reading 164

9 Handset ‘Over The Air’ Provisioning of GPRS Profiles, Automatic Device Management 167
9.1 The Data Access Path in GSM: Purpose of GPRS Profile Settings 167
9.1.1 Creation of a Data Connection 167
9.1.2 Two Standards for GPRS Profiles: Which One to Set? 168

9.2 Obtaining the IMEI of a Handset for Device Management 168
9.2.1 Static Method: Use of Billing Files 169
9.2.2 Automatic Detection of Handset Model Using Signalling from Mobile
9.2.2.1 SIM Tool Kit 169
9.2.2.2 HLR Alerting the Device Management Centre 170
9.2.2.3 EIR Checks 170
9.2.2.4 Roaming Hub Case: Extraction in the MAP UPDATE LOCATION Messages 170
9.2.2.5 Roaming Hub Case with the GPRS Virtual Data Service: Use of GTP 171
9.2.2.6 Roaming Hub Case: Use of CAMEL Initial DPs 171
9.2.3 On Request from the OTA Server Method 171

9.3 Method to Remotely Check that a Loaded GPRS Profile Works 172
9.3.1 Example of MMS Notification Sent by SMS-MT to the Handset to Get its Model Type 172
9.3.2  Corresponding HTTP GET Sent by the Handset and Providing
the Model Type 172

9.4  Architecture of a Classical OTA GPRS Server 173
  9.4.1  Integrated or SMPP-connected GPRS Server 173
  9.4.2  Security 174

9.5  Stochastic Automatic GPRS Profile Type Learning OTA Server 174
  9.5.1  Extracting the Origin Number from the MMS Notification 175

9.6  Stochastic Convergence 176
  9.6.1  Convergence Time 176

9.7  Best Order to Try an Unknown Handset GPRS Profile Type 177

References and Further Reading 178

10  Current Developments and Directions: GSM-UMTS ↔ VoIP Roaming 179

10.1  Pirate Techniques? 179

10.2  Seamless ‘Free Roaming’? GSM-UMTS with SS7 ↔ VoIP Gateways 180
  10.2.1  Business Case and Usable Terminals for VoIP ↔ GSM Service 180
  10.2.2  System Architecture GSM and UMTS Using an SS7-VoIP Gateway 180
  10.2.3  Receiving Calls or SMS 181
  10.2.4  Making Calls or Sending SMS 182
  10.2.5  Charging VoIP Calls Based on Location: Use of IP Address Resolution 183
  10.2.6  Visio Calls SIP ↔ UMTS 184

10.3  Attracting the Visitors and Forcing Them to Roam Immediately in
      a Given VPLMN 184
  10.3.1  Offering the GSM-UMTS ↔ VoIP to Lock Visitors into One’s Network 184
  10.3.2  Erasing the SIM Card Localization Information (Last LAC) 185
  10.3.3  Erasing the SIM Card GPRS Localization Information (Last RAC) 186

10.4  IMS, the all IP Network Architecture 186
  10.4.1  Origin of IMS 187
  10.4.2  Principles Claimed for IMS 187
  10.4.3  Fixed/Mobile Convergence 187
  10.4.4  IMS vs UMA (Unlicensed Mobile Access) 187

10.5  Making a 4G ‘IP Call’ to a Mobile 187
  10.5.1  Paging through the GTP Protocol 188
  10.5.2  Paging for Data Service Connection through the MAP Protocol 189

References and Further Reading 189

11  Worked-out Examples 191

11.1  Examples of Chapter 1 191
  11.1.1  Example 1: SMSeXchange Behaviour 191
  11.1.2  Example 2: Mobile Subscriber Purge 191
  11.1.3  Example 3: Change of Password 199

11.2  Examples of Chapter 3: Roaming Hub with Several Point Codes 215

11.3  Examples of Chapter 4 221
  11.3.1  Example 1: Update Location – Post-paid Subscriber 221
  11.3.2  Example 2: SMS-MO 236
  11.3.3  Example 3: CAMEL Subscriber Call 251
  11.3.4  Example 4: CAMEL Call with Number Correction Service 272

Index 303