Reprogrammable SIMs:

Technology, Evolution and Implications

Final Report

Prepared for:

Ofcom

Prepared by:

CSMG
Descartes House
8 Gate Street
London WC2A 3HP
United Kingdom
www.csmg-global.com

25 September 2012

© 2012 Ofcom. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or means (electronic, mechanical, photocopy, recording or otherwise) without the permission of Ofcom.

ABOUT TMNG GLOBAL

www.tmng.com

TMNG Global (NASDAQ: TMNG) is a leading provider of professional services to the converging communications industry. Its companies, TMNG, CSMG, and Cartesian, and its base of over 500 consultants, have provided strategy, management, and technical consulting, as well as products and services, to more than 1,200 communications service providers, entertainment, media, and technology companies and financial services firms worldwide. The company is headquartered in Overland Park, Kansas, with offices in Boston, London, New Jersey, and Washington, D.C.

ABOUT CSMG

www.csmg-global.com

CSMG, a division of TMNG Global, is a leading strategy consultancy that focuses on the communications, digital media, and technology sectors. CSMG consultants combine a deep understanding of the global communications industry with rigorous analytic techniques to assist their clients in outmanoeuvring the competition. The organization prides itself on understanding the complex technology and financial chain that links the digital economy. CSMG serves its international client base through its offices in Boston and London.

CSMG Boston, Two Financial Center, 60 South Street, Suite 820, Boston, Massachusetts, 02111 USA
Telephone +1 617 999.1000 • Facsimile +1 617 999.1470
CSMG London, Descartes House, 8 Gate Street, London, WC2A 3HP, UK
Telephone +44 20 7643 5550 • Facsimile +44 020 7643 5555

Contact Information	
Michael Dargue *Principal* +44 207 643 5477 michael.dargue@csmg-global.com	**Hsing-Ren Chiam** *Manager* +44 207 643 5479 hsing-ren.chiam@csmg-global.com

DISCLAIMER

This report was undertaken as part of Ofcom's forward-looking technical programme. The opinions and conclusions stated within this report are those of CSMG and may not reflect the views of Ofcom or imply any future policy work by Ofcom.

csmg
A TMNG Global Company

Table of Contents

1. Executive Summary 5

Potential Consumer Pain Points 9

Evolutionary Timeline for eUICC Applications 9

Key Points for Regulators 10

2. Introduction and Methodology 12

Aims and Objectives 12

Scope and Methodology 12

Report Structure 12

3. Background and Context 14

Overview of Current SIM Cards 14

Role of the SIM in Mobile Network Systems 14

A Brief History of Subscriber Identity Technology 14

Traditional Architecture of the SIM 15

Traditional SIM Processes 18

Summary 23

4. Introduction to Reprogrammable SIMs 24

Definition of Reprogrammable SIM 24

Drivers of eUICC Demand for Industry 25

Drivers of eUICC Demand for Consumers 26

Growth in Supporting and Related Technologies 26

Summary 28

5. eUICC – M2M Applications, Technology and Processes 29

GSMA Use Cases 29

Relationships between SM-SRs 33

eUICC Standardisation Issues 33

Summary 34

6. Introduction to Consumer eUICC Applications 35

7. Handset Switching 36

eUICC Enabled Handset Distribution Models and Provisioning Processes 36

Comparison of Handset Distribution Models 36

8. National Swapping 39

Overview of SIM Swapping 39

Petitioner Samsung Ex-1027, 0003

eUICC Swapping 39
National Swapping Benefits 40
User-Driven vs. Managed Swapping 40
MNO vs. Handset Manufacturers Motives for National Swapping 41
9. International Swapping 43
Overview of International SIM Swapping 43
Implementing International Swapping with eUICC 43
Assessment of International Roaming Options 44
10. Assessments of Applications 46
Summary of Consumer Benefits and Potential Consumer Harm 46
Implications for Stakeholders for Applications 47
Likelihood of Enablers Emerging 47
Timeline for Enablers 48
Timeline for eUICC Evolution 49
Key Points for Ofcom 49
11. Conclusion 51
12. Annex 1: Conceptual Model 53
Introduction 53
References 54
Architecture and Components 55
GSMA Use Cases 59
Consumer Scenarios 68
State Models 78
Reference Architectures 82
13. Annex 2: Alternative Technologies to eUICC 84
Apple Virtual SIM Patent 84
Truphone Patent 85
Google and Apple Patents 86
Qualcomm Patent 88
Trusted Execution Environment 89
14. Annex 3: Standards Related to Reprogrammable SIMs 90
15. Annex 4: Glossary 94

Petitioner Samsung Ex-1027, 0004

1. EXECUTIVE SUMMARY

Overview

1.1 This report on reprogrammable SIM technology covers four key areas:

- A review of the current state of SIM technology and reprogrammable SIMs.
- An analysis of the applications of reprogrammable SIMs, and the likely timeline for future developments.
- An assessment of the implications for consumers and stakeholders of these applications in terms of benefits and pain points.
- Current and future considerations for regulators such as Ofcom.

Background

1.2 To understand the concept of reprogrammable SIMs it is important to understand the role of the traditional SIM in today's GSM architecture. At a conceptual level, the SIM identifies the subscriber to the network and enables this identity to be securely authenticated.

1.3 When a device connects to a network, the SIM in the device sends the network its ID (known as an IMSI), and then it passes the network a key[1]. On the network side, there is a list of IDs and a list of corresponding keys, so the network can identify and authenticate the SIM.

1.4 Traditionally a SIM has only one set of ID and keys, tying the SIM to a specific network operator. If a user wishes to change network operators, they need to physically change the SIM card in the device.

1.5 This is because traditional SIMs are not reprogrammable. For security reasons, the ID and keys, which form the credentials of the SIM, are traditionally read-only data programmed at manufacture. However, this is likely to change in future evolutions of the SIM. In a reprogrammable SIM, the credentials can be re-written in-life. This would allow the SIM to change network.

Reprogrammable SIMs: Introduction to the eUICC

1.6 The origins of the reprogrammable SIMs can be found in current SIM trends. Over time, SIM card form factors have been steadily getting smaller in size, driven in part by handset and device vendors' wishes for SIM footprints to be minimised to allow for slimmer devices. An embedded SIM, such as in Machine-to-Machine (M2M) devices, shows that the size of a SIM can be even further reduced, particularly if the SIM hardware is soldered directly onto the circuit board.

1.7 In the case where SIMs are no longer physically removable from a device, there is a clear need for these SIMs to be reprogrammable.

1.8 The GSMA has developed a requirements document for a reprogrammable SIM which has been termed the "eUICC". The GSMA defines the eUICC as "a small trusted hardware component, which may be soldered into mobile devices, to run the [SIM application] and enable the secure changing of subscription identity and other subscription data."[2]

---

[1] In reality the key (Ki) is not actually disclosed to the network by the SIM. Instead an algorithm on the SIM uses the key to compute a hash value (SRES/XRES), which is sent over the network instead. The same algorithm exists on the network side to compute an identical hash value from the relevant key. For more detail on SIM authentication, see Section 3

[2] GSMA Embedded SIM Task Force Requirements and Use Cases v1.0, Feb 2011

Petitioner Samsung Ex-1027, 0005

1.9 The eUICC is hardware agnostic, and may be a reprogrammable SIM application contained in a secure element, a surface mounted M2M SIM, or even a removable SIM card.

Benefits to Stakeholders

1.10 The eUICC brings key benefits to stakeholders in the M2M space where SIMs may be non-removable or impractical to swap.

1.11 For M2M vendors, the ability to manufacture devices with "blank" SIMs that can be provisioned in any country after they have been shipped and sold is another significant benefit.

1.12 MNOs have an interest in offering this solution as it may allow them to take a leading role in the emerging M2M solutions market.

1.13 M2M customers will also benefit from the flexibility of being able to easily change their connectivity service provider regardless of the remoteness or number of their devices.

1.14 Lastly, SIM vendors benefit from taking a new central role in the reprogrammable SIM ecosystem and from new revenue streams from the management and manufacture of reprogrammable SIMs. The new role played by SIM vendors is called the Subscription Manager (SM). It bears similarities with the role of Trusted Service Managers in mobile money platforms (e.g. CItyZi project in France). The SM modifies traditional SIM provisioning and switching, enabling the remote management of subscriptions on any mobile device with an eUICC.

Traditional SIM Provisioning Processes and Ecosystem

1.15 In order to understand the role that the SM plays in the eUICC architecture, an understanding of traditional SIM provisioning is required. Currently, SIM card vendors personalise SIM cards on behalf of MNOs. MNOs send the vendors a file with their specifications, such as the IMSI numbers of the SIM cards to produce and the authentication algorithms. SIM vendors send the personalised cards back to MNOs. The MNO is the SIM Issuer e.g. they hold the relationship with the SIM card vendor and dictate what data is placed onto the SIM.

1.16 The SIM card received by the customer is pre-provisioned with the MNO's authentication data and settings, and cannot be changed. Essentially, only two entities are involved in the supply chain: the MNO (as the network operator and SIM Issuer) and the SIM card vendor.

1.17 SIM cards are thus provisioned before the customer takes possession of the SIM card (or the device that contains it). In order for an MNO's SIM profile (with associated credentials) to be provisioned to a SIM card after the SIM is delivered to the customer, a more complex process and ecosystem is required.

eUICC Provisioning Process and Ecosystem

1.18 In the eUICC ecosystem[3], a Subscription Manager is required. The SM role fulfils two functions; Secure Routing (SM-SR) and Data Preparation (SM-DP).[4]

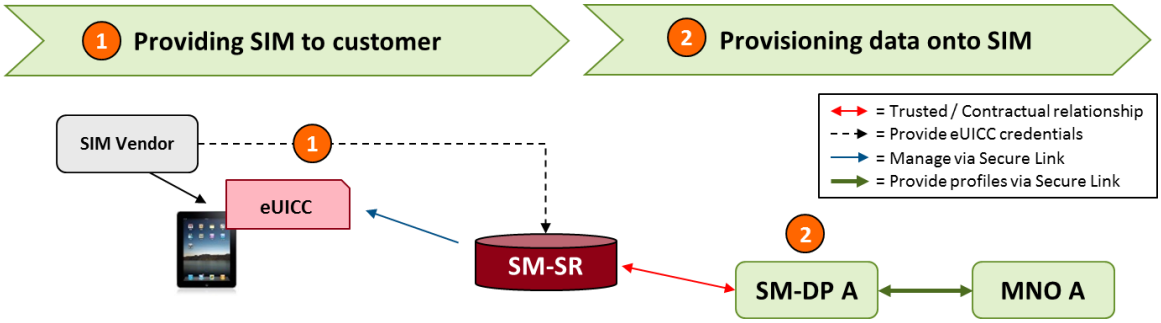
---

[3] As described by GSMA in GSMA Embedded SIM Task Force Requirements and Use Cases v1.0, Feb 2011

[4] The SM role is sub-divided into SM-SR and SM-SR in GSMA documentation on the high level architecture of eUICC. See SCPREQ(11)0113, "Embedded UICC – A high level remote provisioning architecture". However this is still an open issue for ETSI standardisation as of June 2012 – see "List of open issues in the discussions on eUICC after SCP REQ#38" ETSI documentation. For the purposes of this report, we analyse the GSMA proposed architecture

Petitioner Samsung Ex-1027, 0006

Figure 1: eUICC Provisioning Ecosystem



1.19 When an eUICC is manufactured, the eUICC Issuer will load the master keys of the eUICC into the SM-SR database. These keys allow the SM-SR to access the eUICC and download new operator profiles to the eUICC. The SM-SR interconnects with a series of SM-DPs. SM-DPs package the MNO SIM credentials (including the IMSI and Ki) for secure download. When the consumer requests an MNO profile, the SM-SR associated with the eUICC requests the profile from the relevant SM-DP and downloads it to the eUICC. Secure communications between the SM-SR and a new eUICC occurs over a "provisioning profile" or "setup bearer", which is effectively a bootstrap profile that allows the first MNO profile to be provisioned to the eUICC.[5]

1.20 Enabling eUICC functionality in an existing MNO network will require interfaces between the MNO systems and the SM. Some of these interfaces are as yet undefined. Potential integration points include the MNO provisioning systems (to trigger or allow profiles to be downloaded in the subscriber provisioning /activation process) and the Authentication Centre (to securely transfer the operator profile to the SM-DP).

1.21 This new ecosystem has important implications for switching. In a traditional removable SIM model, the consumer can change SIMs by physically removing a SIM and replacing it with another. In the eUICC model, where the SIM is embedded, the consumer may have to ask the SM to do the switch on their behalf. This example shows the importance of who controls or plays the role of the SM.

1.22 There is also a risk that this new ecosystem could potentially lead to fragmentation. If an SM does not link to all MNOs, then consumers may find themselves unable to switch to a particular operator. One solution to this issue of fragmentation is that SM-SRs are interlinked, though this will require a degree of industry cooperation and standardisation.[6]

[5] The SM in this way plays a very similar role to the Trusted Service Manager (TSM) in mobile NFC money ecosystems. In a NFC ecosystem the TSM manages the secure element on the device which contains the payment application, as well as setting up a secure connection between the application providers and the secure element. In the same way, a SM sets up a secure connection between the SM-SR and eUICC and manages the eUICC

[6] This issue is being considered by ETSI and use-cases that will allow changes of SM-SR have been detailed

Petitioner Samsung Ex-1027, 0007

Evolution of eUICC

1.23 The main focus of this technology so far has been M2M. In this area there has been significant development; M2M standards for eUICC are currently being created by ETSI and commercial deployments are expected as early as next year.

1.24 Going forwards the eUICC may develop in two ways. Firstly, it may evolve to support non-M2M devices, such as handsets. Secondly it could increase its functionality to enable swapping rather than just switching. Switching can be defined as when a customer replaces their SIM profile permanently, e.g. if a customer's contract expires and they sign up with a new MNO and do not expect to go back to their previous MNO. SIM swapping is when a customer replaces the SIM profile temporarily. Swapping can be done nationally e.g. customers may wish to swap profiles to connect to different operators within the same country. Customers may also swap profiles internationally, e.g. if the customer is going abroad and wishes to connect to a particular network when abroad but retain their subscription profile at home for when they return.

Handset Switching

1.25 The GSMA requirements document for the eUICC does not specifically exclude handset applications and could be utilised for this purpose; however it is mainly focussed on M2M solutions. When consulted as part of this research, industry experts confirmed that there is no technical reason why handsets cannot be supported. As a further proof of concept, CSMG developed a conceptual model to show how a consumer handset application might work (see Annex).

1.26 There are two ways that eUICCs might be distributed in handsets. One would be where the eUICC was pre-provisioned by the MNO. A consumer could therefore buy a handset with an eUICC in it which already had a particular MNO subscription on it. This would be quite similar to the current status quo.

1.27 An alternative option is that the consumer buys a handset which has a blank eUICC on it. The consumer would be able to select an operator at a later point in time, potentially using a menu of available operators and have that operator subscription downloaded to their SIM. The handset vendor (as the eUICC Issuer) may own this menu. This would be analogous with NFC "device-led" models e.g. Google Wallet, where Google is in control of which applications are installed. This is clearly a disruptive model and is one of the reasons why MNOs may be reluctant to bring eUICCs to handsets.

1.28 Another important point is the impact eUICCs would have on Mobile Number Portability (MNP) if used in handsets. This is not an issue for M2M devices, as these devices generally do not need to be permanently associated with a single phone number. As the GSMA requirements are focussed on M2M applications, considerations such as MNP were not included. An analysis of the current UK MNP processes and eUICC switching processes highlighted some issues which could potentially lead to the consumer losing the use of their existing number for a significant time.

National Swapping

1.29 eUICC swapping could bring coverage, cost and quality of service benefits to consumers. Swapping requires a number of pre-installed profiles to exist on a device and the ability for consumers to activate their preferred option (a "multi-profile" solution). A potential enhancement to this would be a dynamic swapping mechanism which provides automated and intelligent cost and coverage management.

1.30 As swapping is not beneficial for MNOs from a commercial perspective, it is unlikely that they will be keen to support this functionality. Handset vendors, however, have shown more interest in bringing such a solution to market. Both Apple and Google developed patents for "dynamic switching" systems in 2006 and 2007 respectively.

International Swapping

1.31 Current international roaming solutions provide a convenient and seamless way for users to connect to foreign networks abroad without needing a commercial relationship with these foreign networks. However there is a cost associated with this, and consumers currently pay higher "roaming rates" for this service.

1.32 With the eUICC, the consumer would be able to download a "local profile" over the air. The user could pick from a range of MNOs in a menu, and the credentials for that MNO would be downloaded, allowing the consumer to switch to a local connection and take advantage of local tariffs.

1.33 In a managed solution this process could be automated for a consumer, similar to how multi-IMSI solutions work today. In a multi-IMSI solution, a Managed Service Provider (MSP) forms several MVNO relationships in different countries and produces a SIM that contains multiple IMSIs. When a user travels abroad, the SIM automatically detects that it is in a new country and changes to the correct IMSI. The customer can then receive calls on both numbers and receive all their charges on a single bill. An eUICC solution would improve on this solution, as the profiles could be dynamically provisioned rather than having to be pre-loaded.

Potential Consumer Pain Points

1.34 Reprogrammable SIMs can provide a number of benefits to consumers in terms of choice, convenience, cost, and mobile coverage. However, there are also areas where this new technology could bring potential consumer harm.

1.35 As discussed above, fragmentation is a key risk which could limit a consumer's choice of network providers and have an effect on competition. Restrictions on switching may also be exacerbated simply through the adoption of embedded SIMs (rather than removable) SIMs.

1.36 Current switching and MNP processes may be unsuitable and result in a poor consumer experience. Issues could include exposing the consumer to "slamming" practices (unauthorised switches) or loss of their phone number for a significant period of time.

1.37 There is also ample scope for consumer confusion if consumers are required to adapt to new provisioning and switching processes.

1.38 Lastly, consumers may lose the subsidies they now enjoy on handsets if MNOs can no longer be guaranteed their return on subsidies. This could potentially have a negative impact on the speed of adoption of technologies such as smartphones.

Evolutionary Timeline for eUICC Applications

1.39 Stakeholder motivations are best aligned for M2M applications with clearly beneficial outcomes for MNOs and others. In the other applications, MNOs may be disadvantaged, and hence, less willing to cooperate or push the development of the application forward.

1.40 It is unlikely therefore that handset switching, national or international swapping will emerge soon as MNOs have an interest in not developing or supporting certain key enablers.

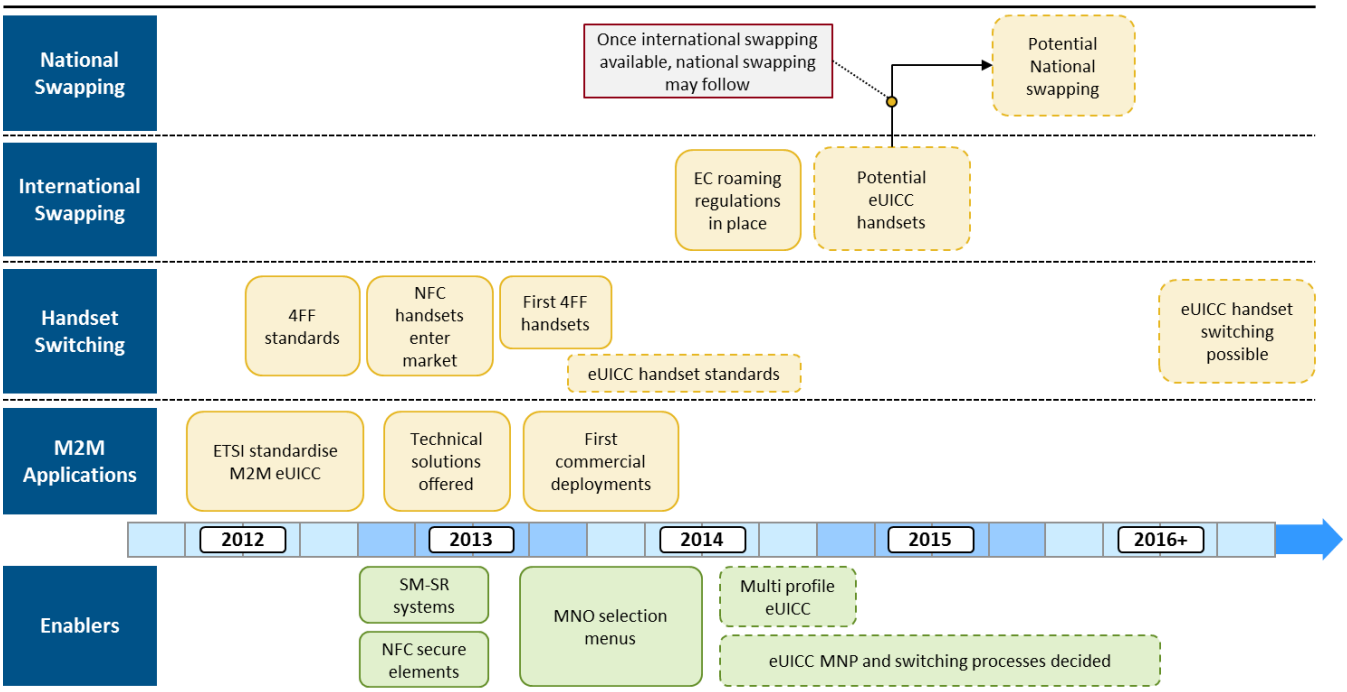
Petitioner Samsung Ex-1027, 0009

For example, MNOs may choose not to support an SM which enabled consumer eUICC-enabled handsets. MNOs may also choose not to distribute eUICC compatible handsets through their channels.

1.41 MNOs may also effectively present barriers to swapping applications by not supporting multi-profile capabilities which is a key enabler for both national and international swapping.

1.42 Commercial motivations aside, it is possible to develop a potential timeline for the emergence of these applications on the basis of the time needed for each of the enablers to be developed. In the diagram below, it can be seen that while it is fairly certain that M2M applications may emerge as soon as next year, eUICC handset standards could follow much later. International swapping applications are likely to occur at the earliest in 2015 (post European Commission roaming regulations), with national swapping and handset switching applications likely emerging in the following period. The complexity of developing and agreeing on new switching and MNP processes required in an eUICC environment is likely to delay any emergence of handset switching for some time.

Figure 2: Evolution of eUICC Timeline



Key Points for Regulators

1.43 Given these enablers, ecosystem player motivations, and the possible evolution of eUICCs, we recommend Ofcom follow eUICC developments closely.

1.44 eUICC handset standards may be drafted starting in 2014. Should this happen, we recommend Ofcom assess the potential impacts of this on MNP systems and processes. Ofcom should also ensure that suitable switching processes are in place to support eUICC switching.

1.45 Consideration should be given to the eUICC as a potential bottleneck asset. The eUICC Issuer (through its SM) controls access to the eUICC and effectively acts as a gatekeeper for service providers. New processes or governance may be needed to accommodate this.

Petitioner Samsung Ex-1027, 0010

1.46 Linked to the role of the SM is the risk of fragmentation in the ecosystem. We recommend monitoring the evolution of the eUICC handset ecosystem to determine the risk of a lack of interoperability, and the impacts this would have on consumer choice.

1.47 Depending on how handset swapping are switching are implemented, users may be presented with a menu to select an MNO. The design of this menu may favour one provider over another, similar to the EPG prominence issue in television.

Conclusion

1.48 SIM technology has evolved greatly over the last two decades, and has become a familiar part of the mobile world to consumers. While it is an invaluable tool for MNOs to provide services to these consumers, the needs of consumers have dictated the evolution towards smaller and more functional SIMs.

1.49 As SIM cards become smaller and capable of more, it is natural to speculate in what direction the technology will develop. It appears that eUICC technology is the way forward, moving the SIM as an application into a hardware-agnostic world, and potentially removing the need for a removable SIM card.

1.50 While M2M and connected devices benefit the most from eUICC technology, we foresee the potential for consumer handset applications in the future, with today's switching and swapping processes translated into the more seamless, consumer-friendly solution of tomorrow.

1.51 This, however, comes with both challenges and drawbacks around the technical and commercial implementation of such solutions, as well as the potential risks to consumer choice and cost. Several hurdles will need to be cleared and cooperation secured for a fair and comprehensive solution to arise, and thus we expect the eUICC technology to remain firmly an M2M-focused solution in the near future.

1.52 Ultimately, regulators will need to monitor the development of the eUICC. If it were to be further developed as a consumer proposition, then the regulator must understand and monitor how eUICC-based solutions will be implemented in handsets, and the necessary processes involved in switching and swapping. To this end, CSMG has developed a conceptual model of how an eUICC might differ from current M2M requirements if it is used in handsets.

1.53 Further investigation of the subject is necessary to avoid any pitfalls. Once the first industry-standardised eUICC solution is on the market, it would be wise to revisit the topic and understand the current market state and its further evolution.

Petitioner Samsung Ex-1027, 0011

2. INTRODUCTION AND METHODOLOGY

Aims and Objectives

2.1 CSMG was engaged by Ofcom's SCET (Strategy, Chief Economist and Technology) team to study SIM technology, and the implications of this technology for UK consumers and citizens.

2.2 Of particular focus were the technology and market forces behind SIM technology and development of reprogrammable SIM technology, which is being standardised within the industry (as the eUICC).

2.3 The study has three main objectives:

- Define and document the technology, standards, specifications, interoperability requirements and development environment for reprogrammable SIM technology.
- Provide an overview of potential applications and deployment models.
- Assess the implications of the anticipated evolution of the market on stakeholders and consumers and the implications for Ofcom.

2.4 This report was undertaken as part of Ofcom's forward-looking technical programme. The opinions and conclusions stated within this report are those of CSMG and may not reflect the views of Ofcom or imply any future policy work by Ofcom.

Scope and Methodology

2.5 In gathering information for the report, CSMG consulted with representatives from key stakeholders across the SIM value chain including Mobile Network Operators (MNOs), SIM technology vendors (e.g. SIM manufacturers, Subscription Management providers), handset manufacturers, standards bodies, and relevant regulatory bodies.

2.6 CSMG conducted both primary and secondary research to analyse the most significant current SIM developments, and to gain an understanding as to the key technological and commercial issues with respect to the technology.

2.7 The report primarily refers to GSM technologies that are commonly used in Europe and particularly, the United Kingdom, but also considers the similarities and differences with other wireless technologies such as CDMA and LTE where relevant.

Report Structure

2.8 The report contains sections on current SIM technology, an introduction to reprogrammable SIMs, eUICC technology and M2M use cases, consumer eUICC applications, implications of eUICC technology and a potential timeline for developments.

2.9 **Section 3: Background and Context**: This section provides an overview of SIM technologies. This includes an overview of SIM cards, their historical context, and their fundamental technology and architecture. In addition, the traditional SIM ecosystem is considered to provide background and context.

2.10 **Section 4: Introduction to Reprogrammable SIMs**: In this section an overview of the reprogrammable SIMs is provided and the significance of the eUICC (the most likely embodiment of reprogrammable SIM technology) is discussed. Recent developments are considered, as well as the key benefits and challenges of eUICCs (particularly over traditional SIM technology).

Petitioner Samsung Ex-1027, 0012

2.11 **Section 5: eUICC Technology (M2M Applications)**: This section considers the proposed architecture of eUICC for M2M applications. Included is an analysis of the key use-cases and a demonstration is provided of how these use-cases are expected to work. Finally, the section considers the significant technical issues around implementation, interoperability and backwards compatibility are discussed.

2.12 **Sections 6 to 9: Evolution of eUICC: Consumer Applications**: These sections focus on the potential future applications of the eUICC which go beyond M2M, such as: installing eUICCs in handsets; and enabling profile swapping rather than just switching. The implications of these applications for consumers and industry stakeholders are discussed.

2.13 **Section 10: Assessment of Applications and Timeline**: In the final section we discuss the likelihood of each of the future consumer applications emerging, based upon impacts on stakeholders and the status of the technical and commercial enablers. A timeline is provided for each of the applications as well as the key implications for regulators such as Ofcom.

2.14 **Annex**: In the annex, a conceptual model is provided showing how the eUICC may work in consumer handset applications. In addition, alternative eUICC technologies (including patent descriptions) are discussed. Finally we list the standards related to reprogrammable SIMs and provide a glossary of terms.

Petitioner Samsung Ex-1027, 0013

3. BACKGROUND AND CONTEXT

Overview of Current SIM Cards

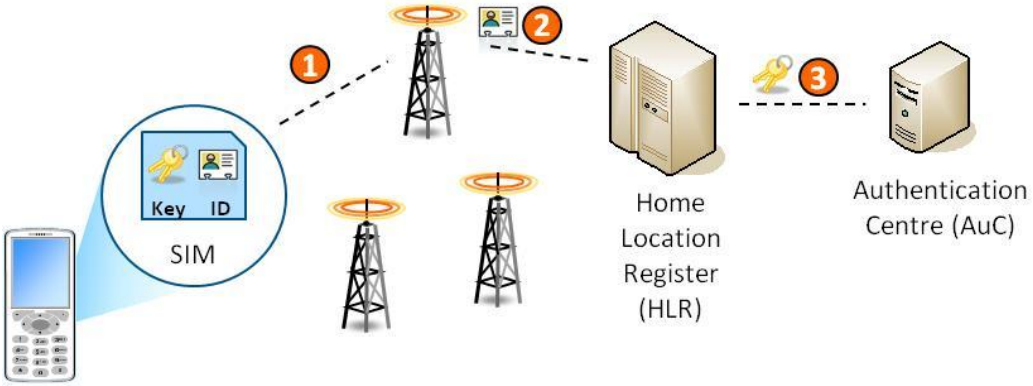
3.1 The hardware-based Subscriber Identity Module (SIM) card is central to subscriber identity and authentication for mobile services today. It provides a secure, convenient means for mobile service providers to locate, identify and provide services to their customers' mobile devices.

3.2 SIM cards are typically issued by Mobile Network Operators (MNOs) to customers when they subscribe to the MNO's mobile service.[7] A SIM card is inserted into a customer's mobile device to enable the device to connect to the MNO's service.

3.3 When a customer purchases a new mobile device and wishes to transfer an existing service subscription over to the new device, the SIM card is removed from the old device and inserted into the new device. No other set-up is necessary and the customer's original mobile number and services are carried over to the new device.[8]

Role of the SIM in Mobile Network Systems

Figure 3: SIM Authentication Mechanism



3.4 The SIM allows users to communicate with a mobile network by:

1. Helping to locate the mobile device within the cell network, as the network stores the last-known location of the SIM within its network;
2. Identifying that the SIM belongs to that network via the Home Location Register (HLR), which has a list of all registered subscriber identities;
3. Authenticating the subscriber's identity by checking the ID and keys associated with the SIM against the Authentication Centre (AuC) of the network.

A Brief History of Subscriber Identity Technology

3.5 The origin of the SIM card can be traced back to the conception and formation of the GSM in 1982 as a result of a memorandum of understanding signed by representatives from 13

[7] An exception to this is for Machine to Machine (M2M) devices (where the SIM may be pre-installed into the device) or in CDMA networks where the "SIM" is embedded into the mobile device.

[8] A caveat to this is that multiple SIM card form factors exist (covered later) and so, not all SIM cards and devices are necessarily interoperable, complicating this process somewhat.

European countries. It eventually led to the formation of the GSMA (Global System for Mobile Communications Association) in 1995, which now owns the GSM trademark and represents mobile operators worldwide.

3.6 In 1989 the responsibility for developing a standardised GSM system was passed onto the European Telecommunications Standards Institute (ETSI). Inspired by an earlier attempt at a smart card system in Germany, France Telecom and Deutsche Telekom developed a concept that used smart cards (SIM cards) with an open, standardised architecture as the basis of a common mobile telephone system.

3.7 In the late 1990s, the Third Generation Partnership Project (3GPP) was formed to develop a more advanced and secure mobile telephony system, which would eventually become the Universal Mobile Telecommunications System (UMTS). Under the 3GPP the SIM card evolved to become the Universal Integrated Circuit Card (UICC) smart card system. Within this system hardware and software components were logically separated into UICC (as hardware) and SIM (as software).

Traditional Architecture of the SIM

3.8 The architecture of a SIM card has evolved greatly since the turn of the century, with a standards-based move toward greater functionality and security, while preserving its benefits (such as size, cost, ease of use, etc.). In this section, the early SIM architecture and basics of SIM data are considered.

Early SIM Architecture

3.9 The majority of SIM cards in the world today are based on SIM card technology from the 1990s.[9] The SIM card's most common form factor (known as 2FF, and standardised as ISO 7816 ID-000) is a 15mm by 25mm strip of plastic with a chip and electrical contacts for use in GSM-based devices.

3.10 Traditional SIM cards are not normally reprogrammable as operator profile information (primarily the SIM authentication system comprising of ID, keys, algorithms, etc.) and some subscriber data is set as read-only during manufacture.[10] This is a simple way of reducing the opportunity for subscriber identity fraud by making it more difficult to modify or clone SIM cards and their credentials.

3.11 Some data (e.g. last dialled numbers, network lists) however, is reprogrammable, and can be updated by the user or remotely by the MNO. This data may require frequent updates.

3.12 Updates by the MNO are primarily accomplished over-the-air (OTA) via the OTA interface to the SIM. This allows the SIM to securely communicate (via the handset and its antenna) with the MNO's transmitters and servers and give it a secure link to the SIM's memory.

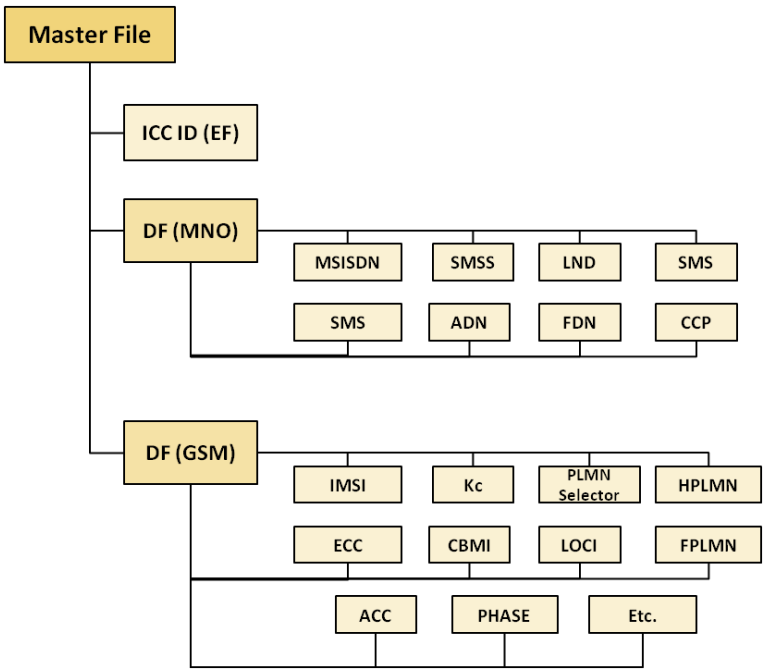
3.13 In addition, a SIM toolkit application resides on the SIM that enables applets and web services to run on the SIM card. The SIM toolkit essentially allows the SIM to initiate commands and helps enable secure value-added applications such as mobile commerce to reside on the SIM rather than on the device.

[9] ETSI (global standards body that developed SIM standards) estimates this to be approximately four billion.
[10] A number of different access right attributes are used to protect the files on the SIM card. By using these attributes, the card manufacturer can control if a file is read or write only when accessed by the mobile phone

SIM Structure and Data

3.14 SIM cards use a file system that is based on the ISO-7816 standard for smart card devices and is fully specified by the GSM 11.11 standard. A variety of MNO and subscriber information in a directory structure The root level is known as the Master file (MF), directories as Dedicated files (DF) and individual records as Elementary files (EF). Most of the records are marked as read-only by MNOs.

Figure 4: Example SIM Card Directory Structure



3.15 Every SIM card that is provisioned contains several required files that are needed in order to maintain compatibility with the GSM protocol.

3.16 Firstly a SIM Card can have three identification data fields, each with its own specific purpose. These are **IMSI** (the ID of the card that is used for identification with the network), the **MSISDN** (the telephone number that is used to route incoming calls to the device) and the **ICCID**, which is the serial number for that SIM card, often also physically printed onto the outside of the SIM card itself.

3.17 The **International Mobile Subscriber Identity (IMSI)** is a unique identifier associated with each GSM and UMTS subscription. It is stored as a 64-bit field in the SIM and is sent by the phone to the network when the device is asked to identify by the network. In order to prove the identity of the device, a secret key, "**Ki**" is also used. For greater security, Ki may be stored in a proprietary file specific to each SIM card vendor rather than in the general file structure.

3.18 In addition, **MNO-specific authentication algorithms** are also stored on the SIM and used to generate unique responses to network authentication challenges. These ensure that each MNO retains unique ownership over the SIM card and its authentication abilities.

3.19 The SIM card also contains the phone number of device, more formally known as the **Mobile Station International ISDN Number (MSISDN).** The MSISDN is allocated by the MNO and is used to route calls to the device. MSISDN country number ranges are issued to countries and monitored by the ITU-TSB (International Telecommunications Union - Telecommunication

Petitioner Samsung Ex-1027, 0016

Standardisation Bureau). The national numbering plans for each country are managed by the respective National Regulatory Authorities.

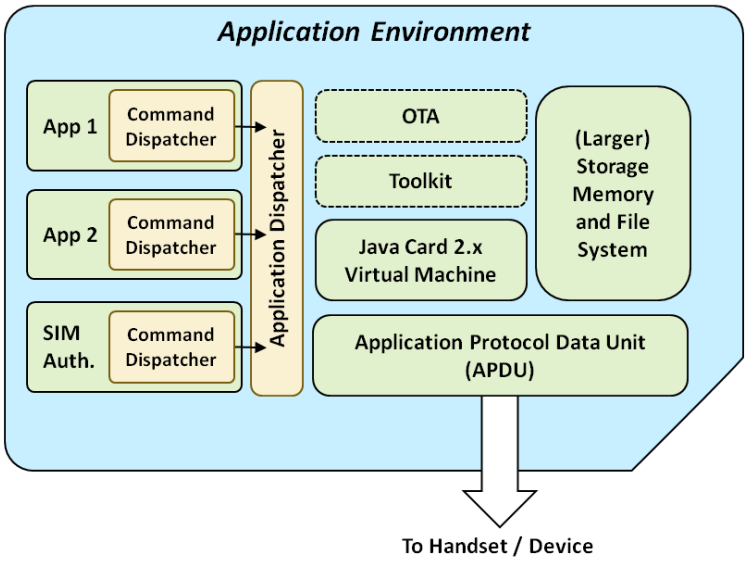
3.20 Finally, the **Integrated Circuit Card ID (ICCID)** is a 19 or 20-digit serial number for the SIM card, which is often also physically printed onto the SIM card itself. As the ICCID is printed on the outside of the SIM card and therefore does not change, the ICCID is the most constant identifier for the SIM card. In the current GSM system, the ICCID is linked to the IMSI and SIM manufacturers maintain databases mapping the two fields.

3.21 In addition to identification and authentication data, the SIM also stores additional information which helps connect and locate the SIM within the network. For example, when a SIM is outside of its home network, it is assigned a **temporary mobile subscriber identity** (TMSI); this is discussed later in this section. The TMSI and relevant **location area information** is stored (and constantly updated) in the SIM card's **Location Information (LOCI)** file, to allow tracking of the user in order to provide service when roaming between networks or service areas.

3.22 Information on the SIM card can also be used to determine which network a SIM should connect to, and in what order of preference. The **Public Land Mobile Network (PLMN) selector** is a list of MNO-preferred networks in priority order, and the **Forbidden PLMNs (FPLMN,** a list of forbidden PLMNs) allows the MNO to control which visited networks to use (i.e. when roaming or coverage is lost). The priority ordering of PLMNs is of particular use to MNOs that have roaming agreements with foreign country MNOs, as it can preferentially select a foreign network to roam onto when the user is abroad.

Current SIM Architecture

Figure 5: Current Java Card SIM Architecture

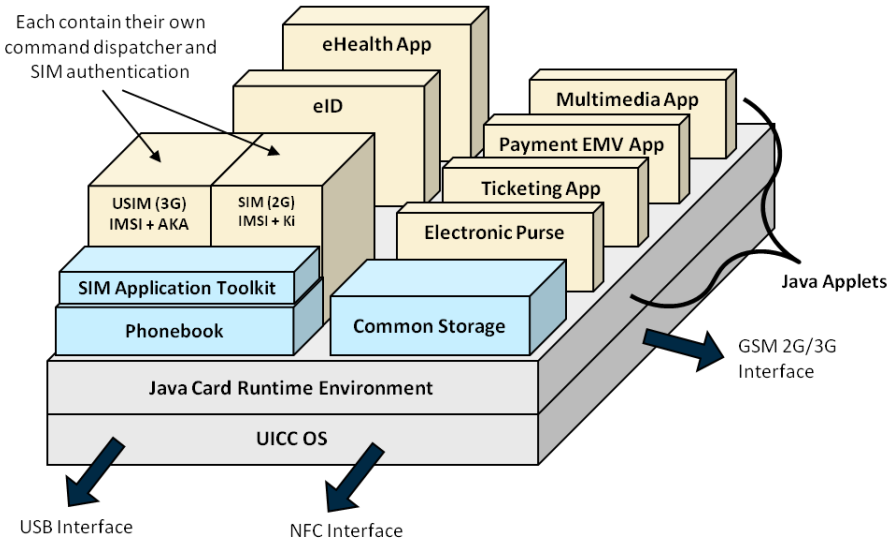


3.23 The current SIM architecture provides a more flexible environment for handling applications on the SIM versus previous SIM designs. Commands are now dispatched from Java applets running on top of the Java Card Virtual Machine (JCVM) platform. This enables interoperability across card manufacturers (for loading of Java-based applets onto the SIM card from any source) and downloading of applications post-issuance (primarily via OTA).

3.24 In the Java-based architecture the SIM card runs a separate core operating system from the device's operating system. Separation of OS and secure interfaces between each one

enables greater security for communication between the SIM and the handset and essentially allows the SIM card to act as a hardware firewall between the mobile device and the information on the SIM memory.

Figure 6: Java-Card based SIM Architecture (Stack View)



3.25 The example Java-Card-based SIM architecture stack above shows how other applications sit alongside the SIM authentication applications.[11] The USIM (3G) and SIM (2G) applications each contain the data, algorithms and credentials required for authentication on their respective networks.

3.26 Common elements shared by all applications are: the SIM/UICC Application Toolkit (which allows for manipulation of the applications on the SIM); storage for profile, status and other data; and a phonebook.[12]

3.27 The SIM architecture also provides protocols to allow the SIM to interface with device components such as OTA, USB and NFC, which are used to establish links to the 'outside world.' In newer SIMs, Remote File Management (RFM, an enhancement of OTA that allows for management of the core SIM system) and Remote Application Management (RAM, which enables the applications on a SIM to be managed securely) provide an efficient and fast way to offer value-added services via the SIM.

<u>Traditional SIM Processes</u>

3.28 Traditional SIM processes can be split into four main functions:

- SIM personalisation process - how subscriber profiles are loaded onto the SIM card.
- Registration and home network process – how the SIM card connects to its home network.
- Roaming process – how the SIM roams on other networks (normally when the user is abroad).
- Authentication processes – how the SIM authenticates with the network and how it communicates with the network in a secure manner.

[11] Sometimes called network access applications

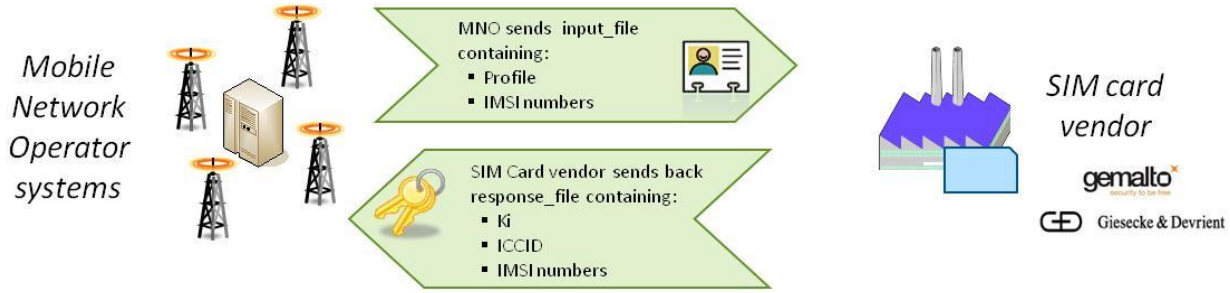
[12] However, the device itself needs to also support the use of SIM/UICC toolkit on the SIM card. Currently, a significant number of mobile handsets and devices do not fully implement the SIM toolkit standard.

3.29 It is important to discuss how these processes work today, to gain an understanding of how these processes need to change in a reprogrammable SIM environment.

SIM Personalisation Process

3.30 Currently, SIM card vendors personalise SIM cards on behalf of mobile network operators. Example SIM card vendors include Giesecke & Devrient, Gemalto and Oberthur. Personalisation data can include IMSI numbers of the SIM cards to produce; the profile settings of those SIM cards including the contents of all the files on the SIM; and the authentication algorithms used specifically by the MNO's mobile network.

Figure 7: SIM Personalisation Process



3.31 The SIM card vendor will manufacture the SIM cards based on the MNO requirements and send back all the necessary data for the operator to load into its own network systems (e.g. ICCID, Ki, and OTA keys) so that the manufactured SIM cards can be tracked, issued, authenticated and activated.

3.32 This information is sent over secure links that are set up between the SIM card vendor and MNO to ensure that critical data and key algorithms are not compromised. Integration is required between the back-end servers of each entity.

3.33 SIM cards are manufactured to operator requirements and are thus, operator-specific. SIM cards for different operators have differences in functionality and feature-sets, and may run on slightly modified core operating systems as a result of this. This has ramifications for the interoperability of applications running on SIM cards, as not all may be compatible.

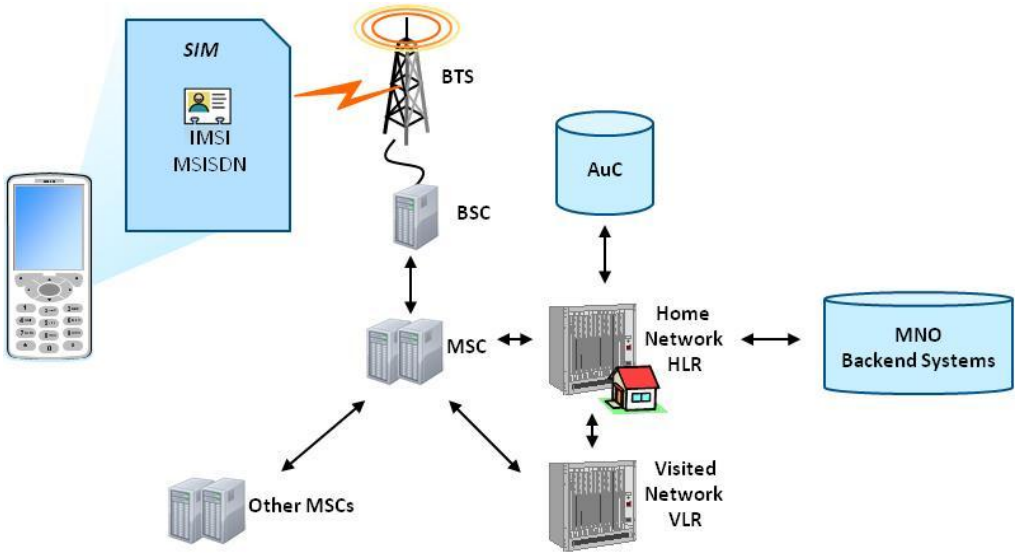
3.34 Furthermore, this allows operators to define specific algorithms for generating encryption keys used to authenticate the subscription identity with their networks.

Architecture – Home Network

3.35 To describe the processes that involve the SIM, it is useful to first review the key components of a GSM network.

Petitioner Samsung Ex-1027, 0019

Figure 8: GSM Network Architecture



3.36 **Base Transmission Station**: The BTS is a part of the Base Station Sub system and is in contact with the SIM in the handset, through the radio interface. The BTS is in charge of management of transmission and reception on the radio interface.

3.37 The BTS connects to the **Base Station Controller** which allocates and releases radio channels and manages handovers between BTSs (as the user moves from one BTS cell to another). The BTS is connected to the MSC, or **Mobile Switching Centre**.

3.38 The main function of the MSC is to co-ordinate the setting up of calls to and from GSM users and the external network. The MSC has interfaces with the BSC on one side and the **Home Location Register** and other MSCs on the other side.

3.39 The Home Location Register (HLR) together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile, and is the primary source of all subscription information and authorisations.

3.40 The HLR is connected to an **Authentication Centre** (AuC). The AuC is a database that stores a copy of the secret key stored in each subscriber's SIM card. When a SIM connects to the network the AuC is used to verify the identity of the SIM, as well as creating secure ciphering of the radio channel between the network and the device.

3.41 As well as a Home Location Register, each GSM network also contains multiple VLRs or **Visitor Location Registers**. The network of VLRs manages local subscribers as they move within the home network, as well as in-bound roamers on the network. Once the visited system detects a device, the VLR of that system sends a request to the home network HLR to make sure the device owner is a valid subscriber. It temporarily stores the last location area visited by the device and a list of the special services the device is subscribed to. The location information is updated intermittently. Each MSC has a one-to-one relationship with a VLR and in most cases the two are co-located.

Architecture – Home Network

3.42 When the device is turned on with a SIM inserted, the BTS communicates with the device via an interface known as the Um interface. The device searches for the nearest base stations (with the strongest available signal) in the MNO's frequency band.

3.43 Once it finds a BTS, it checks the BTS identifier to confirm it is the "correct" network based on information on the SIM. The SIM then attaches itself to the network by authenticating with the AuC (via the VLR and HLR) using the IMSI and Ki. This occurs over the control channel, a special communication mode for secure authentication purposes. The location of the device is then updated in the HLR.

3.44 To remove the need for constant authentication with the HLR, the VLR can subsequently be used to identify the device. After authentication, the VLR issues the device with a TMSI and creates a new record of it within its database. The TMSI is generated by the VLR and is valid only within the network domain that is covered by that VLR. When combined with the location area information (LAI), the TMSI-LAI pair is unique within the entire GSM network.

3.45 Once the VLR has issued a TMSI for a device, the VLR updates the HLR of that mobile subscriber with its location. The relationship between the IMSI and the TMSI is stored at the VLR. For all further transactions within the network area covered by the VLR (e.g. placing calls or receiving calls), only the TMSI needs to be used for identification with the network.

Architecture – Roaming

3.46 When roaming, the architecture involved is broadly similar to when at home, with the exception that certain protocols and standardised processes exist that enable the visited network's VLR to authenticate the subscription identity of the device via the home network's HLR, without the IMSI, Ki or other sensitive information being revealed to the visited network.

3.47 When the mobile device is turned on or is transferred via a handover to the network, the visited network "sees" the device, confirms that it is not registered with its own database, and attempts to identify its home network. If there is no roaming agreement between the two networks, provision of service is not possible, and service is denied by the visited network. Typically, devices will cycle through all networks in a foreign country until it finds one that has a roaming agreement with the subscriber's home network.

3.48 The visited network contacts the home network and requests service information about the roaming device (including whether or not the mobile should be allowed to roam) using the IMSI number.

3.49 If successful, the visited network maintains a TMSI for the device within its VLR. Likewise, the home network updates its information to indicate that the mobile is on the host network so that any information sent to that device can be correctly routed. This is relevant when the device needs to be "paged" so that any incoming calls can be routed to the correct BTS.

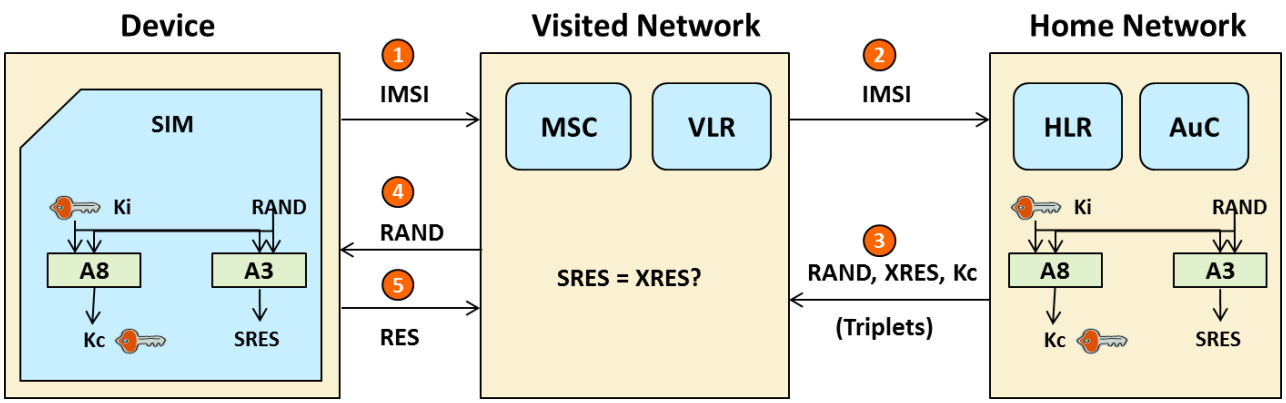
3.50 Back-end systems in the home and visited network enable subscriber usage to be monitored when roaming, such that retail billing (by the home MNO) and inter-operator settlement can be performed. Intelligent Network (IN) systems enable prepaid services to work when roaming.

Authentication Process

3.51 The authentication process for GSM uses MNO-specific encryption algorithms (A3, A8) to identify and authenticate a subscriber.

3.52 When roaming, authentication occurs in the Visited Network (with the MSC and VLR of the home operator or the visited foreign network), as shown below.

Figure 9: Authentication Architecture



3.53 The SIM identifies itself with the network (using the IMSI) and the network requests authentication from the SIM card.

3.54 The IMSI is passed through the VLR to the home network (1) which checks the IMSI against the HLR and requests authentication triplets (2).

3.55 The AuC generates the triplets, namely: RAND, a 128-bit random number; XRES, a signed response used for authentication; and the cipher key Kc, used to encrypt traffic that is passed through the network. The AuC uses the Ki and the RAND it generates to produce the XRES via an algorithm (A3). XRES is a 32-bit crypto-variable used in the authentication process.

3.56 The triplets are sent on to the Visited Network (3). The Visited Network only passes RAND to the SIM card over the air (4).

3.57 Using the RAND and its own copy of Ki and the A3 algorithm, the SIM is able to generate the signed response (called SRES) and passes this to the network (5).

3.58 The visited network checks the SRES against the XRES that was generated by the AuC, and if they match, a message is sent to the AuC that the device has been authenticated.

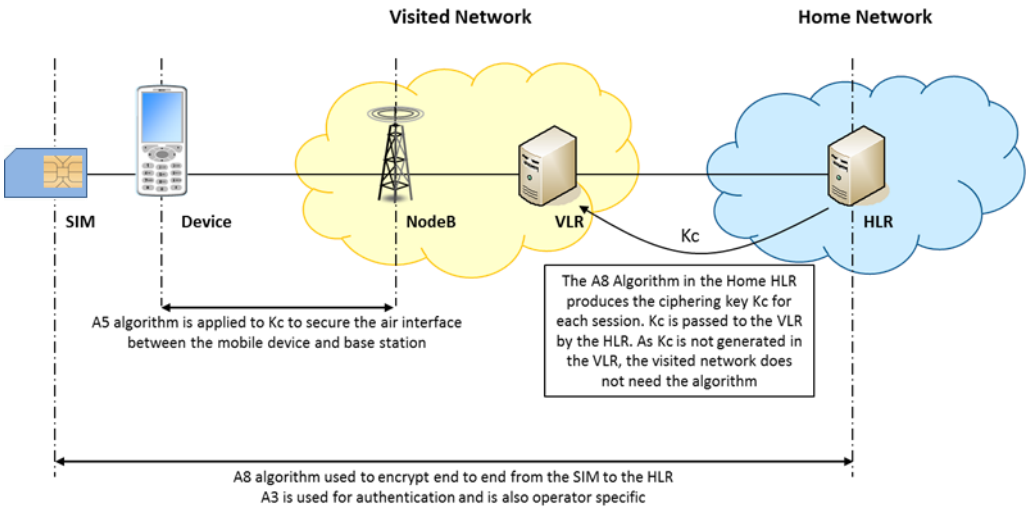
3.59 Kc is a 64-bit ciphering key generated through the use of the Ki and the A8 algorithm. The SIM is also able to generate Kc, as a copy of the A8 algorithm also resides on the SIM card.

3.60 Kc is used as the encryption key between the mobile device and the base station. This encryption is based on another algorithm, A5. Whereas the A3 and A8 algorithms can be operator-specific, the A5 algorithm is standardised, in particular, to allow roaming.

3.61 The figure below shows how A3, A5 and A8 algorithms work together when a user is roaming. In particular it shows how the A5 algorithm needs to be common across all networks to allow roaming; however the A3/A8 algorithms can be operator-specific as they only need to be consistent between an operator's SIMs and HLR.

Petitioner Samsung Ex-1027, 0022

Figure 10: Cryptographic algorithms when roaming



Summary

3.62 Current SIM technology has evolved to provide a level of flexibility and security in subscriber authentication that meets operator and user needs. The design of the SIM allows for interoperability, compatibility with multiple device types, a range of secure functionality and simplicity of use. It enables subscription profiles to be easily switched on a device, by swapping the physical SIM card. The following section discusses how changing operator and user needs may cause the SIM card to evolve further.

Petitioner Samsung Ex-1027, 0023

4. INTRODUCTION TO REPROGRAMMABLE SIMS

Definition of Reprogrammable SIM

4.1 As discussed in the previous section, the subscription identity stored in a traditional SIM cannot generally be re-written. Reprogrammable SIMs differ in this respect. Reprogrammable SIMs can be defined as a solution that enables the **subscription identity** on a connected device (e.g. mobile handset, sensor, connected car) to be **securely reprogrammed**.

Comparison of Terms Used in the Market

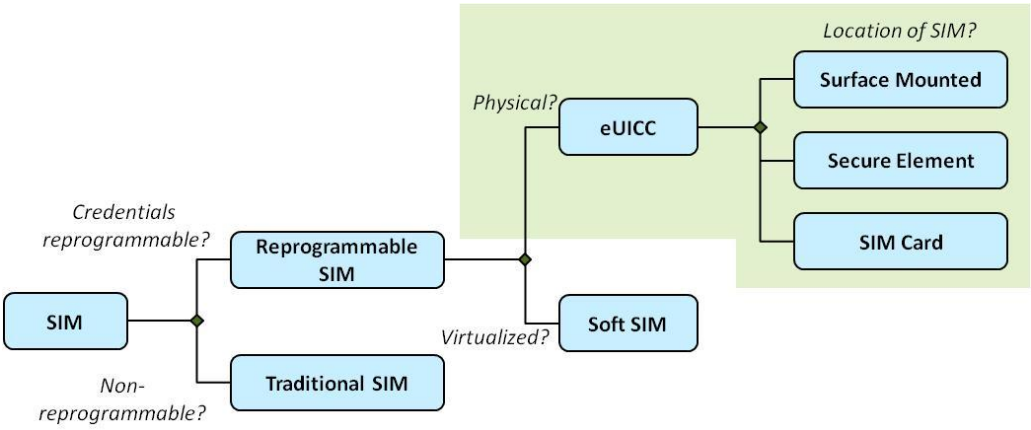
4.2 Broadly there are two forms of reprogrammable SIM; the Embedded UICC (shortened to eUICC) and Soft SIM. The term Soft SIM has a particular meaning amongst some operators and SIM card manufacturers[13], which is a virtualised SIM residing in handset memory.

4.3 However, due to widespread concerns regarding the security of a Soft SIM and the lack of MNO support for this type of SIM, the report will focus on the development and technologies of the eUICC.

4.4 GSMA defines the Embedded UICC (eUICC) as "a small trusted hardware component, which may be soldered into mobile devices (as per MFF1 and MFF2), to run the secure network access application(s) (e.g. GSM Subscriber Identity Module application) and enable the secure changing of subscription identity and other subscription data. [It] performs the role of a traditional UICC."[14]

4.5 This eUICC is hardware agnostic (e.g. the solution can sit on a UICC module, a secure element contained elsewhere on the device or any other secure hardware component).

Figure 11: Differences between SIM Types



Reprogrammable SIM in Practice

4.6 The ability of an eUICC to change its subscription credentials facilitates switching between operators.

4.7 eUICC switching works as follows:

[13] From CSMG interviews with MNOs and SIM card manufacturers
[14] GSMA Embedded SIM Task Force: Requirements and Use Cases v1.0 Feb 2011

Petitioner Samsung Ex-1027, 0024

1. A SIM is registered with MNO A, using MNO A's credentials.
2. New credentials relating to MNO B can be downloaded to the SIM from MNO B's ID database.
3. MNO A credentials are deactivated.
4. The SIM is able to connect to MNO B using its new credentials.

4.8 Provisioning new credentials on the SIM OTA, and then de-activating the previous credentials, is analogous to the current process where consumers acquire a new SIM card and swap it with their existing one.

Drivers of eUICC Demand for Industry

M2M

4.9 Reprogrammable SIMs can bring key benefits in the M2M space where SIMs may be embedded (i.e. SIM cards that cannot be removed from the device). eUICCs are likely to play a key role in enabling the expected proliferation of M2M devices (e.g. connected consumer and industrial devices such as sensors, e-readers, cars, etc.). For owners of numerous devices (e.g. utilities, or enterprises) the ability to switch a large number of devices OTA presents a significant cost saving.

4.10 ETSI are currently deciding on standards for soft switching of embedded SIM devices for M2M. As embedded SIM devices require "soft" technology to allow switching, many promoters of M2M devices and solutions (including mobile operators) are keen to drive reprogrammable SIM technology forwards.

4.11 Currently M2M solutions providers need to have multiple national and international roaming agreements to enable M2M solutions to operate worldwide. M2M solution providers attempt to simplify this by offering a contractual relationship with a single connectivity broker, which gives them access to multiple MNO relationships and allows them to remotely and dynamically manage their device subscriptions. These roaming agreements may be expensive particularly for data-heavy devices (e.g. surveillance cameras) or if they are particularly numerous (e.g. sensors). By enabling local subscriptions for these devices, reprogrammable SIMs may provide a lower cost option in terms of use and management.

Smaller Form Factor

4.12 SIMs are getting smaller as manufacturers wish to save space on devices. The most popular form factor is the mini SIM (known as the 2FF). Micro SIMs (3FF) are used by Apple in their iPhone 4 handsets and the iPad 2/3 tablets. Nokia and Sony have also adopted the micro SIM standard (for their Lumia 800 and Xperia S handsets respectively) and HTC is looking to introduce the micro SIM as standard. Recently, ETSI standardised a fourth form factor ("nano-SIM") which will be 40% smaller than the micro-SIM.[15]

4.13 eUICCs will provide even greater space-saving opportunities for handset manufacturers as SIM card holders can be completely done away with on devices and replaced by a chip on the circuit board.

[15] http://bx.businessweek.com/apple/etsi-formalizes-the-40-smaller-4ff-nano-sim-standard/11884380412730697592-a68029ef6d68189e43bf99dabda19864/

Drivers of eUICC Demand for Consumers

4.14 The eUICC can also bring a number of benefits to consumer and businesses.

Agnostic Devices

4.15 With eUICC, consumers have the ability to purchase embedded M2M devices anywhere as they can be agnostic of country or MNO. Another benefit for owners of consumer M2M devices is that reprogrammable SIM solutions may allow switching of these devices in a more convenient manner.

Facilitate Switching

4.16 With eUICC, the connectivity provider can be changed easily (OTA) without the need to source a new physical SIM to replace the old one. A simpler switching process could overcome some consumer inertia in market potentially resulting in increased competition between service providers.

Single Sign-On

4.17 Reprogrammable SIM implementations may result in a single coordinator, MVNO or "IMSI broker" function that would enable account aggregation and present consumers with a single bill for their usage across multiple networks. Apple, Google and Truphone have put forward patents (see Annex) relating to dynamic network selection. Such a mechanism could help reduce costs or improve service for users by picking the network with cheapest tariffs or best coverage at any given time.

Flexible Business Models

4.18 eUICCs open up the possibility of flexible, disruptive business models such as the potential separation of voice and data services. As more than one MNO profile can be stored on a handset, a customer may be able to consume voice services on one network, and data services on another network. This may allow consumers to take advantage of superior or cheaper data network access from one network, while maintaining their voice services from another network provider (although to do this concurrently would require two SIMs to be active at once and therefore two radios on the device).

Lower International Roaming Costs

4.19 The ability to download local SIM profiles OTA could be used to avoid international roaming costs. As such, eUICC technology provides an alternative to the options set out by EC for roaming separation such as Local Break Out.[16] This is discussed in greater detail in Section 9.

Growth in Supporting and Related Technologies

4.20 Related technologies which may support the development and introduction of eUICCs include Near Field Communications (NFC) and Multi-IMSI SIMs.

[16] http://www.wto.org/english/tratop_e/serv_e/sym_march12_e/presentation_telekomaustria.pdf

Near Field Communications (NFC)

4.21 NFC is becoming increasingly commonplace in smartphones. NFC solutions often require data (such as credit card details) to be stored in a secure element on the phone to keep this data physically separate from the handset memory and in a tamper-proof environment.

4.22 Increasingly, the SIM has become a likely candidate for the role of the secure element as it is already a separate tamper-proof chip and has additional and well-established mobile network security to layer on to the existing software and hardware security.

4.23 Alternatively, over-the-top NFC plays such as Google Wallet work with embedded secure elements that are located in secure chips on the handset circuit board.

4.24 These secure elements also provide potential locations for housing SIM credentials, as has been suggested in patents developed by Apple (see Annex). In addition, the Trusted Service Managers (TSMs - new roles created to facilitate the secure transfer of NFC data to and from these secure elements) of the NFC ecosystem could also support OTA SIM provisioning models.

Multi-IMSI SIMs

4.25 Multi-IMSI SIM cards contain two (or more) IMSIs on a single SIM card, each with its own Ki (key). Generally provided by travel SIM providers (e.g. Truphone, WorldSIM), these SIMs activate a "local IMSI" when the subscriber is abroad allowing them to save on roaming costs. T-Mobile is releasing a multi-IMSI e-reader which can register with its local networks in the UK and US, and is designed with roaming travellers in mind. However, current multi-IMSI SIMs are not reprogrammable SIMs as the IMSI and Ki are preloaded on the device rather than written to the SIM card over-the-air (OTA).

4.26 eUICCs are likely to utilise multi-IMSI technology to switch between multiple profiles on a SIM such as a provisioning profile (setup bearer) and a MNO profile, or between two operational MNO profiles.

Industry Proofs of Concept of the eUICC

4.27 A number of industry players have attempted to test and demonstrate reprogrammable SIM concepts in recent months. These solutions have all been implemented using pre-standard technology that has been developed amongst the participating parties for the purpose of the demonstration. However, they have generally been based on the proposed technical standards.

4.28 In November 2011, Telefónica managed the secure transfer of an M2M device subscription from Telefónica Spain to Telefónica UK (O2), using a pre-standard solution. The solution used custom SIM cards installed in devices that allowed for subscription management. This consisted of a subscription management platform developed by Giesecke & Devrient (G&D), and an MNO-facing management portal developed by Telefonica. The trial tested: the loading of a subscription; transfer of subscription to another device; remote loading of a second mobile operator subscription; and remote deletion. The trial utilised the subscription management platform user interface to control the SIM process. Equipment manufacturer Samsung and M2M specialists Telit Wireless were also involved.

4.29 At Cartes 2011, a proof of concept was demonstrated involving Vodafone and SFR. In this demonstration, a device's subscription information was changed from Vodafone UK to SFR (including IMSI and relevant keys) over the air.

4.30 In February 2012, Telefónica successfully demonstrated a secure solution for remotely managing M2M SIMs' subscription data (based on a pre-standard embedded SIM) by transferring an M2M device subscription to China Unicom. The solution was the result of the M2M strategic agreement signed by the two companies in October 2011 to develop M2M solutions.

4.31 Finally, most recently, in March 2012, the GSMA, Gemalto and G&D showed their OTA remote provisioning solution for eUICC at the Mobile World Congress.

Summary

4.32 It is likely that the eUICC will be the main embodiment of reprogrammable SIMs in the future. A number of proofs of concept have demonstrated the technological ability and motivation by key stakeholders in bringing an M2M solution to market. The next section will explore such a solution from a technological perspective.

Petitioner Samsung Ex-1027, 0028

5. eUICC – M2M Applications, Technology and Processes

5.1 This section reviews the current processes and technology of the eUICC as defined by the GSMA. The focus of the GSMA work so far has been in M2M applications.

GSMA Use Cases

5.2 GSMA submitted a document to ETSI detailing a number of requirements and use cases for the successful development of an eUICC industry standard. The use cases were designed to solve a problem specific to M2M devices where changing SIM cards can be difficult, either because the SIMs may be remotely located or hermetically sealed and inaccessible. The standardisation process is to support new processes whereby the remote management of embedded SIMs in M2M devices is made simpler and easier.

5.3 This standardisation process is not to define new technologies for remote management (as they already exist and can be used), but to align them across service providers in order to prevent fragmentation and security risks.

5.4 The document specifically states that these requirements are targeted at M2M and embedded devices[17], though conversations with industry players indicate that the omission of handsets is just a clarification and not an exclusionary stance[18].

5.5 There are a total of 5 use case types detailed in the document, that describe specific actions that are the constituent parts of any subscription lifecycle:

- **Use Case 1 – Provisioning of Multiple M2M Subscriptions**: An M2M Service Provider (M2M SP) sets-up M2M subscriptions for a number of connected M2M devices to start telecommunication services with a first MNO
- **Use Case 2 – Provision of First Subscription with a New Connected Device**: A subscriber purchases a connected device together with a subscription for first services to this device
- **Use Case 3 – Subscription Change**: A subscriber changes the subscription for a device to stop services with the current MNO and start services with a new MNO in accordance with policy control functions for each MNO
- **Use Case 4 – Stop Subscription**: A subscriber sells his device and stops the subscription for services from the current MNO[19]
- **Use Case 5 – Transfer Subscription**: Subscriber transfers subscription between devices

5.6 GMSA Use Cases 2 and 3 (provisioning a first subscription and changing subscriptions) are examined in more detail below as they serve to demonstrate how new roles and processes fit together in this new ecosystem.

5.7 The GSMA define two alternatives for Use Case 2 which are applicable to a consumer context. In the first, the MNO profile is provisioned to the eUICC after the customer has received it (UC2a). In the second, the MNO profile is pre-provisioned beforehand (UC2c).[20]

---

[17] As per the GSMA Embedded SIM Use Cases and Requirements document, "The primary intention of the requirements expressed in this document and any solutions that meet them, is to facilitate the M2M and Embedded Mobile [*in other words, connected devices that are not handsets*] market segments" "Embedded Mobile devices" are defined as "the emerging service category characterised by combinations of devices and services supported by an embedded 3GPP network access capability that is not traditionally considered mainstream mobile network devices"

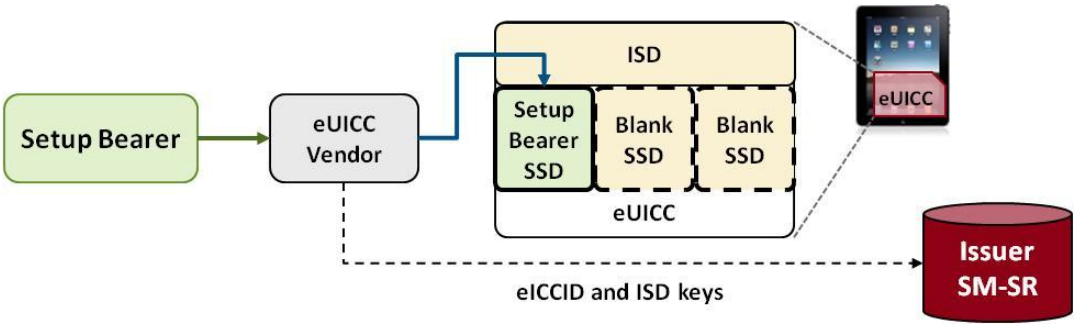
[18] CSMG Industry Interviews

[19] This use case applies to termination of subscriptions in general as well

UC2a: Post-Provisioning of an eUICC

5.8 In this use case, a consumer purchases a new device and subsequently selects the MNO. To facilitate this, the eUICC is shipped with an initial setup profile which enables the device to connect to a network (the setup bearer) and download the selected MNO profile. In the following description we assume provisioning occurs over a mobile network, although other connectivity options are possible.

Figure 12: Provisioning of Setup Bearer to eUICC by eUICC Vendor



5.9 The eUICC is divided into multiple compartments of which the primary is the Issuer Security Domain (ISD). This domain is controlled by the eUICC Issuer and allows it to create, remove or share access to secondary security domains (SSDs). It does not, however, allow access to the contents of these secondary domains.

5.10 SSDs can thus contain confidential data such as MNO subscription profiles. By compartmentalising security domains, MNOs are able to access their own domains knowing that the information (such as IMSI, Ki, network security algorithms) is secure and inaccessible to other MNOs or the eUICC Issuer.

5.11 As the device is initially MNO agnostic, this represents a departure from the traditional model in which the MNO is the only party that issues SIMs. In this model, it is likely that the eUICC Issuer would be an MNO-neutral third party, for example the device manufacturer.

5.12 In this use case, the eUICC is programmed with a setup profile which enables it to connect to a mobile network (the setup bearer) for initial OTA provisioning. The setup bearer profile would be written to an SSD. The eUICC Issuer or vendor would require a contractual relationship with the MNO providing the setup bearer.

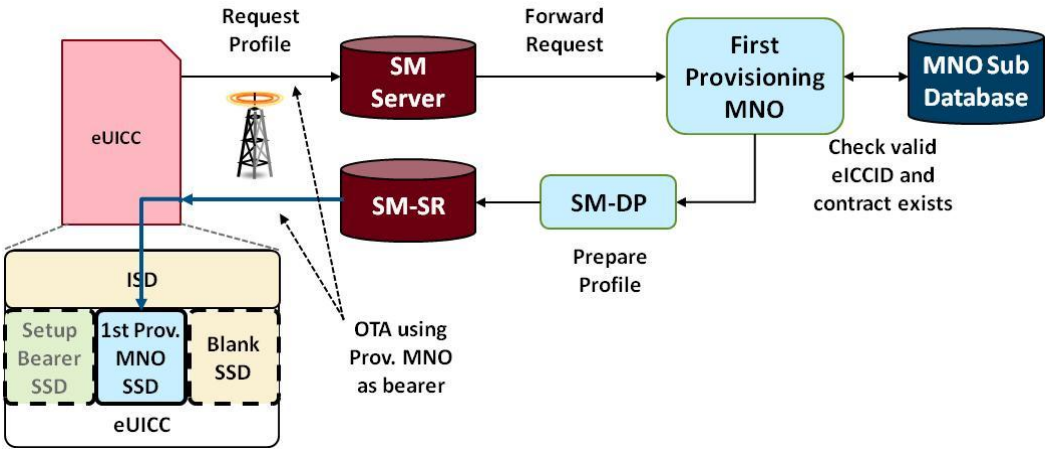
5.13 Remote access to the eUICC is managed by a Subscription Manager (SM) on behalf of the eUICC Issuer (it is possible that these two functions are combined in a single entity). The Subscription Manager – Secure Routing (SM-SR) function is responsible for management of the eUICC including the secure delivery of credentials packages.

5.14 Once the device has been distributed to the customer, the customer can set up a contractual relationship with their chosen MNO. Once in place, the first provisioning of the eUICC (shown in the diagram below) can proceed.

[20] Note that UC2b is a specific case for enterprise devices.

Petitioner Samsung Ex-1027, 0030

Figure 13: First Provisioning of Operational MNO to eUICC



5.15 The new profile request is sent from the eUICC to the Subscription Manager which forwards the request to the appropriate MNO. The MNO checks to see if the eICCID and subscriber information it has received is valid (e.g. a customer account has been setup for that eUICC). If valid, the MNO's Subscription Manager (Data Preparation), also known as SM-DP, prepares the appropriate MNO profile for the eUICC and encrypts it.

5.16 The SM-DP is responsible for the secure assembly and encryption of the package to be delivered to the eUICC via the SM-SR. The SM-DP role is thus often played by the MNO itself, or a very trusted partner such as its eUICC vendor. Once encrypted, the profile package is securely sent OTA to the eUICC using the Setup Bearer's network as the provisioning network. The encryption used by the SM-DP ensures that the MNO's secret data (e.g. Ki, authentication algorithms, etc.) cannot be seen by the SM-SR or the eUICC Issuer. This is important for providing confidence in the system to the MNOs.

5.17 The eUICC contains a Subscription Management (SM) client which then loads the package into the correct SSD. Upon being loaded into the SSD the package is decrypted to install the new MNO profile on the eUICC.

5.18 The SM client activates the operational MNO profile and deactivates the Setup Bearer profile.[21] The eUICC and device are refreshed by a UICC toolkit command, and the new operational MNO profile is used to connect the device to its network.

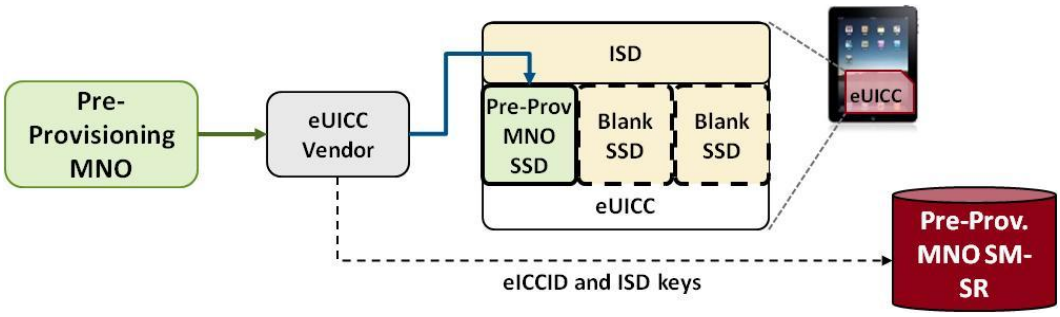
UC2c: Pre-provisioning of an eUICC

5.19 An alternative option for the provisioning of eUICCs in a consumer context, is to pre-provision them with a valid MNO profile prior to the device purchase. Under this option, the consumer would not need to select their MNO post-purchase. This has the advantage of the purchased device being ready-to-use; however it does initially tie the device to a particular MNO.

[21] Or deletes or overwrites, which is not shown here

Petitioner Samsung Ex-1027, 0031

Figure 14: Pre-provisioning of eUICC by an MNO



5.20 In this case, the MNO profile is securely written to an SSD on the eUICC during the supply chain. The process is similar to the provisioning of the setup bearer (in UC2a) as illustrated in the diagram above.

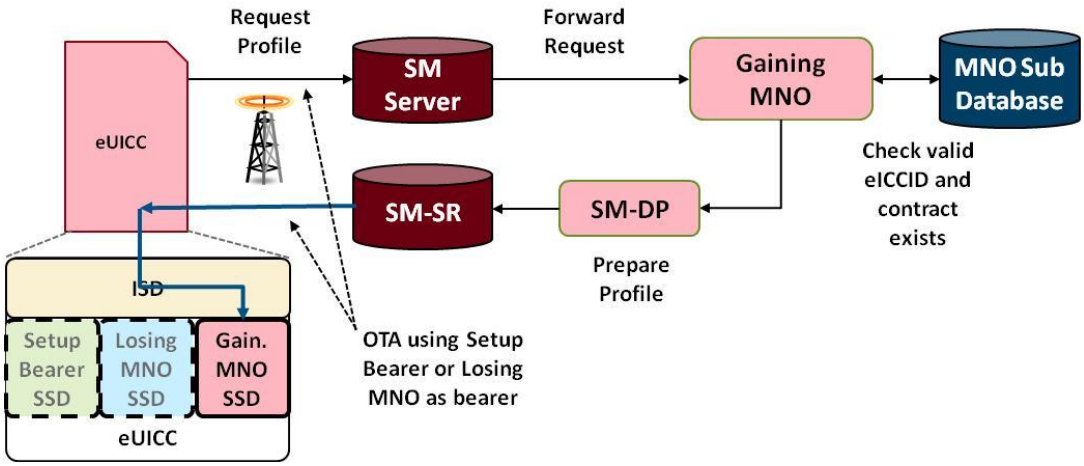
5.21 As the eUICC in this model is not MNO-agnostic at point of sale, it may be appropriate for the MNO itself to assume the role of eUICC Issuer. As in UC2a, the eUICC Issuer would use an SM to manage and control access to the eUICC on its behalf.

5.22 In this model, the operational MNO will act as the bearer if another profile is provisioned to the eUICC at a later date.

UC3: Switching of an eUICC between Operational MNOs

5.23 The switching of operational MNOs on the eUICC is similar to the First Provisioning in UC2a. However in this case, an additional Gaining MNO profile is installed on the eUICC alongside the Losing MNO's profile.

Figure 15: Switching of Operational MNOs on eUICC



5.24 The eUICC request is forwarded through the SM server first to the Losing MNO (not shown) to validate the switching action against its Policy Control Function. The request is then sent to the Gaining MNO, who checks that the eICCID is valid (e.g. a customer account has been created)[22]. If valid, it instructs its SM-DP to prepare and encrypt a profile package.

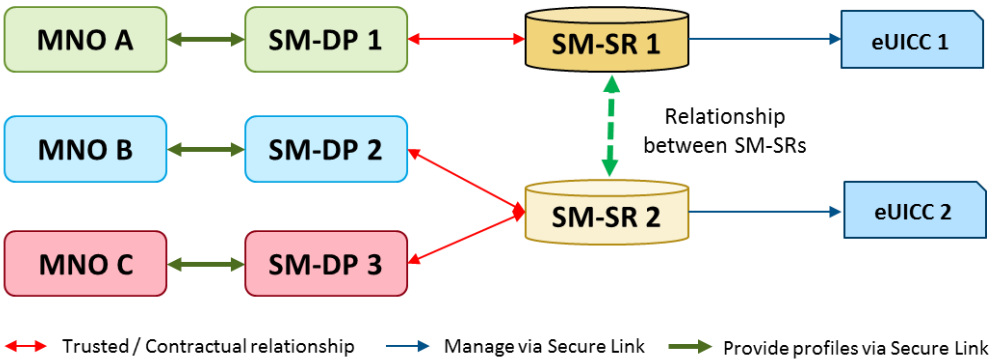
[22] Alternatively, the Gaining MNO may allow a restricted profile to be downloaded to the eUICC, and then for a customer to activate and setup the account post-download. This would most likely be for prepaid accounts

5.25 The package is routed via the SM-SR on an OTA link to a new SSD on the eUICC. The OTA is expected to occur over the Losing MNO bearer (as this would still be active, prior to the switch). Alternatively a fall-back to the setup bearer could be used. Once the new profile is installed on the SSD, the Gaining MNO profile is activated, and the Losing MNO profile is deactivated.

Relationships between SM-SRs

5.26 There is a potential issue of fragmentation if an SM-SR is not connected to all MNOs. For example, in the diagram below, consider the scenario where the customer using the device eUICC 1 wishes to provision a profile from MNO C.

Figure 16: GSMA Conceptual Architecture for eUICC Provisioning



5.27 eUICC 1's SM-SR, (SM-SR1) does not have a relationship with MNO C's SM-DP (SM-DP 3), and therefore cannot directly provision from MNO C. In this case, a relationship between SM-SR1 and SM-SR2 (MNO C's SM-SR) could facilitate this provisioning scenario. If a relationship such as this exists, SM-SR 1 could give access to a SSD on eUICC 1 to SM-SR 2, allowing the provisioning to take place.

5.28 It is therefore critical that SM-SRs develop contractual and technical relationships with MNOs and each other in order to enable broad access by market players. Any gaps in these relationships may result in a customer being unable to provision from a particular MNO.

eUICC Standardisation Issues

5.29 The technology for deploying an eUICC solution exists today and can be deployed in most places. However, for long-term viability, cooperation and progress around standards and ecosystem development are required.

5.30 At the time of writing, a number of key issues are yet to be resolved in the standardization of the eUICC by ETSI, including:

- Whether the eUICC should include consumer handset applications.
- Whether the SIM should have a single profile, or multiple active profiles.
- Security concerns regarding how the MNO authentication algorithms should be delivered to the eUICC.
- Potential interoperability issues which may result in loss of service.
- Backwards compatibility issues.

Petitioner Samsung Ex-1027, 0033

Handset Applications

5.31 The GSMA requirements document released so far has focussed on M2M and connected devices, and not consumer handsets. However, some industry players (e.g. Handset OEMs, OTT players) believe that any standards should explicitly include handsets.

Single Profile vs. Multiple Profile

5.32 The current requirement document states that the eUICC can contain multiple profiles, but "only one operational profile can be active at any point in time."[23] Multiple active profiles would allow connection to more than one network (similar to the operation of today's Dual-SIM phones). Again, some industry players are proposing that multiple active profiles should be included in the standards for the eUICC.

MNO Authentication Algorithms

5.33 Thirdly, there is debate on whether to allow the downloading of MNO authentication algorithms to unknown or unsupported hardware. MNOs are keen to protect their unique and valuable MNO-specific authentication algorithms from falling into the hands of third-parties, and are therefore less keen to have these authentication algorithms delivered over the air.

Service Interoperability

5.34 The profile manager used to switch between MNO profiles on the eUICC has been tested and shown to be interoperable across all the major SIM vendors in Europe. Few complications are expected going forward in this area.

5.35 However some MNOs are understood to have slightly different UICC operating systems from others. This may result in features and functions being lost when switching from one MNO to another. An approach must be specified and developed to deal with different operating systems. One possible option is for a minimal OS to be specified, with additional functions being downloaded as needed.

Backwards Compatibility with Existing SIM Form Factors

5.36 There has been limited effort to address backwards compatibility as the focus for eUICC has been primarily on new concept development and M2M use cases. Standards and solutions may need to be developed to ensure backwards compatibility of new embedded devices with older removable SIM cards.

5.37 The Apple Virtual SIM patent describes a Bluetooth-enabled SIM accessory to enable legacy SIM card usage with a device that has an embedded SIM on the handset secure element. It involves the use of subscription information on the legacy SIM card (over a Bluetooth connection) to enable the device to authenticate on networks.[24]

Summary

5.38 The vast majority of the technology that underpins eUICC functionality has been developed and is well-established. The proofs of concept have showed how solutions could work in practice. The major efforts now are focussed on standardisation of the solution. To this end, ETSI is trying to standardise eUICC before the end of summer 2012.

---

[23] Embedded SIM Task Force Requirements and Use Cases v1.0
[24] Figure 6, http://www.freepatentsonline.com/20110269423.pdf

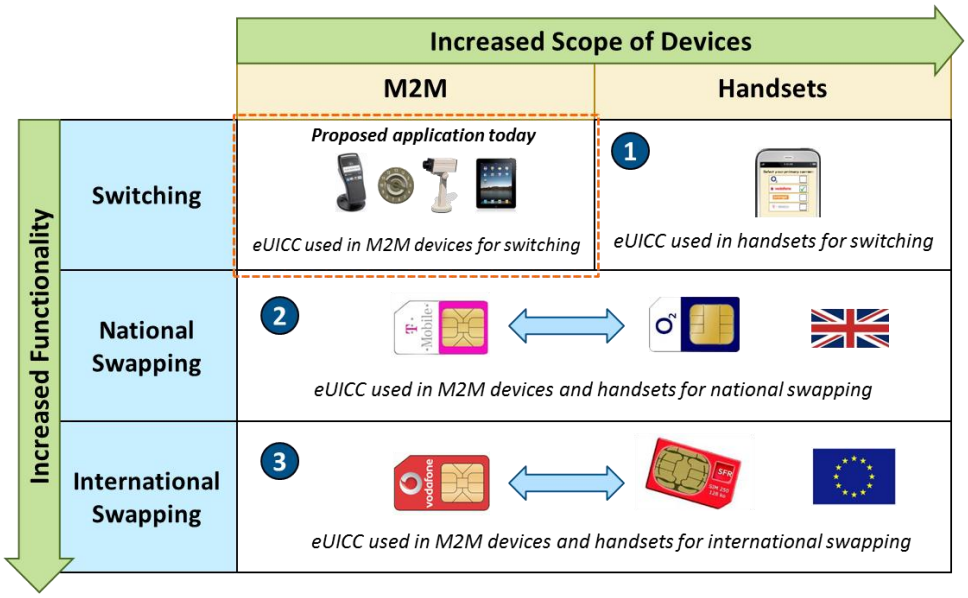
6. Introduction to Consumer eUICC Applications

6.1 Having presented an analysis of the current state of the eUICC market and technology in the M2M space, this section discusses how the eUICC might evolve to encompass consumer applications.

6.2 The eUICC could evolve in two dimensions: (i) to support more devices such as handsets (handset switching); and (ii) to include increased functionality such as subscription swapping rather than just subscription switching.

6.3 A distinction can be made between SIM switching and SIM swapping. In SIM switching, the consumer replaces the SIM profile permanently. This might be if the customer's contract expires, and if the user wishes to change their services permanently to a new provider. In SIM swapping, the SIM profile is only temporarily replaced, and the customer expects to return to their previous SIM at a later date. This might be the case when a customer goes abroad (international swapping), or if a customer has a work SIM and a personal SIM (national swapping).

Figure 17: Potential Evolutionary Applications of Reprogrammable SIM



6.4 The following sections discuss these three additional consumer applications in turn: Handset Switching, National Swapping and International Swapping.

7. HANDSET SWITCHING

7.1 Although handset applications of eUICCs have not been specifically included in the current GSMA requirements document, there does not seem to be a clear technical reason why handsets could not be supported – CSMG has developed a conceptual model to show how handset applications might work (See Annex). Industry interviews have also confirmed this understanding.[25]

7.2 Furthermore, eUICC processes for first provisioning of a SIM, a switching bearer, transferring a profile, and terminating a profile for consumer M2M devices have already been outlined. These same processes can be used for handsets (although important processes such as Mobile Number Portability have not been covered – this is discussed in this section). In addition, the same infrastructure used for M2M applications can also be utilised for handsets, such as the SM-SR, SM-DP and the eUICC. The GSMA requirements also clearly request that ETSI proposes standards which are compatible with all ETSI form factors, including the common mini-SIM form-factor which is present in nearly all handsets today.

7.3 There are also cost factors in support of adopting non-removable eUICCs in handsets. MNOs have significant costs involved in the purchasing, logistics, inventory costs and retailing costs of SIM cards. Handset manufacturer costs may also be lower if using an embedded eUICC as no SIM card holder component is required in the device design.[26]

eUICC Enabled Handset Distribution Models and Provisioning Processes

7.4 Referring to the GSMA use cases as a basis for the functionality of an eUICC-based handset solution, it can be seen that there are two potential distribution models; distributing eUICCs which are "blank" and distributing pre-provisioned eUICCs.

7.5 Handsets with blank eUICCs can be distributed to consumers by either MNOs or third parties. The consumer would purchase a handset with a blank SIM card and then choose a network operator, similar to the M2M use-cases described by the GSMA in Section 5.

7.6 Handsets could also be pre-configured with an operator SIM on the eUICC. This is again very similar to the GSMA-proposed eUICC processes previously discussed (Pre-provisioning of an eUICC). In this case, the consumer would likely buy the handset from the MNO themselves.

Comparison of Handset Distribution Models

7.7 Control of the SIM may differ depending on distribution model. A "blank eUICC" approach is potentially disruptive as it may provide handset vendors with a more influential role in the value chain than they possess currently. However, a "pre-provisioned" approach broadly maintains the status quo (or may even provide greater control to the MNOs).

7.8 In the "blank eUICC" approach, the handset vendor may control the SIM. When choosing an MNO at first start-up, a customer may be provided with a selection menu from which to choose their MNO. As a result of their ownership of the eUICC, handset vendors will likely also "own" this menu which will allow them to determine which MNOs are listed and available to the consumer. Analogies can be drawn with NFC "device-led" models (e.g.

[25] CSMG Industry Interviews May 2012

[26] However, the handset manufacturer would likely need to absorb the cost of the SIM component (i.e. chip) into their bill of materials cost.

Petitioner Samsung Ex-1027, 0036

Google Wallet, where Google "owns" the secure element and controls how open their service is to other service providers and potential partners).

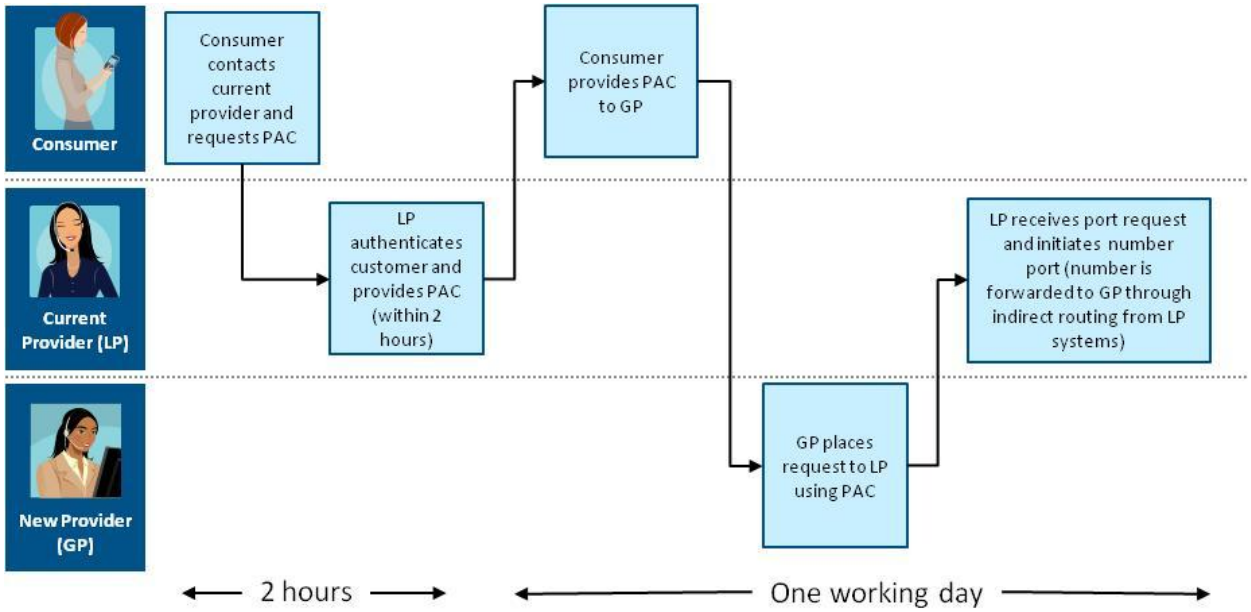
7.9 In the "pre-provisioned" model, MNOs may control the eUICC. In this position, MNOs may put in place functionality which provides greater control over how the SIM is used. For example, this may be in the form of an "enhanced SIM lock" function, which would only allow SIM switching once a consumer contract has expired. MNOs could also use this SIM lock to prevent problematic cases of pre-paid SIM switching (such as "box-breaking" – where a user, immediately upon purchase, replaces a subsidised prepaid handset).

7.10 However MNOs may see insufficient benefit in migrating to eUICCs for handsets as this technology may pose a strategic threat in terms of ceding potential control of the SIM to handset-vendors, as well as opening the door to more disruptive applications such as dynamic swapping (see Sections 8 and 9), where MNOs risk disintermediation or loss of revenues.

Consumer Issues: Mobile Number Portability and Switching

7.11 One additional implication of a handset application is the need for integration with Mobile Number Portability (MNP). Whereas in a M2M solution, this is not required (as M2M devices do not generally require a persistent phone number), this is a critical issue in handset applications of the technology.

Figure 18: Current MNP Process

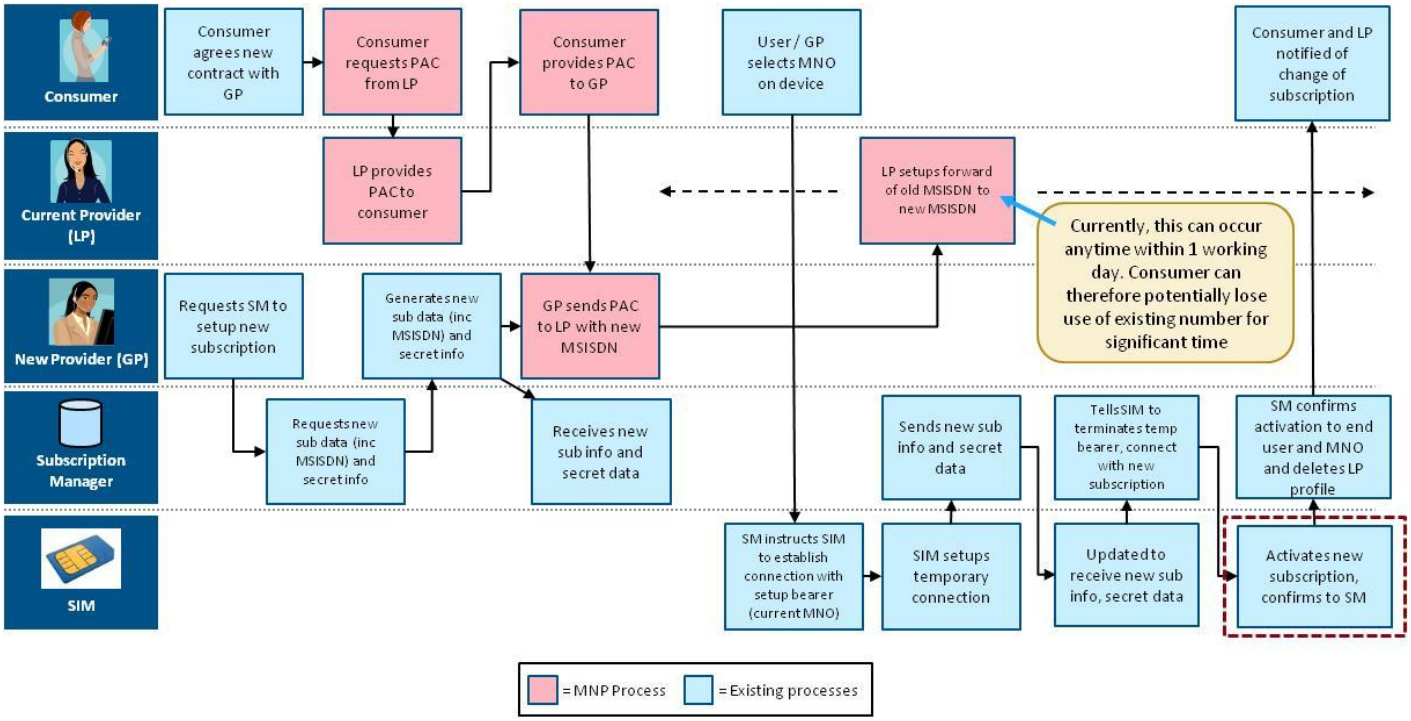


7.12 Currently MNP in the UK is Losing Provider (LP) led. The current MNP process requires users to provide a Porting Authorisation Code (PAC) to their new MNO - the Gaining Provider (GP). Upon request, the customer's existing provider needs to provide the PAC code within 2 hours. Once the customer passes the PAC code to their new provider, the new provider can pass this code to the Losing Provider. Upon receipt of the PAC code from the Gaining Provider, the Losing Provider begins the number port process. This process can happen anytime within one working day from the consumer providing the PAC to the Gaining Provider. The consumer is thus not certain when exactly the number port takes place.

Petitioner Samsung Ex-1027, 0037

7.13 In a new process, the MNP process would need to be integrated into the eUICC switch process. An example of how the MNP process could fit into the proposed GSMA eUICC switching processes is shown below. However, there are potential issues for the customer experience if current processes are used. If the new subscription profile is activated and the number is not ported immediately, it is possible that a customer may lose the ability to receive calls on their existing phone number for a significant period of time (as the MNP process can currently take up to one working day).

Figure 19: Switching with eUICC and MNP



7.14 A more tightly integrated MNP process would result in a better consumer experience. In an ideal scenario, in order to minimise the amount of time that consumers are without use of their existing number, the number port process and new subscription activation should be engineered to occur simultaneously.

7.15 Another potential consumer issue is restrictions on switching. With traditional SIMs, consumers are able to independently change SIMs between unlocked devices. With embedded SIMs, consumers would become reliant upon the MNOs and SM to perform the switching function. This could be an effective means of "SIM lock" and has impacts for switching levels and consumer choice. This is similar to the situation in the US, where the vast majority of CDMA phones have embedded chips.

Petitioner Samsung Ex-1027, 0038

8. NATIONAL SWAPPING

Overview of SIM Swapping

8.1 SIM swapping is a common practice globally through which customers switch networks. Users may SIM swap for a number of different reasons that include the arbitrage of different rates for voice and data for customers on prepay, or the selection of a network with good, reliable coverage in a specific location. Some customers may swap SIMs to separate out personal and business usage.

8.2 Various technologies facilitate SIM swapping. Dual SIM phones are one common solution (discussed later). Device features for copying contacts from SIMs to devices are also common and heavily used, which allow different SIM profiles to have access to the same contact book. Technologies such as "easy swap" also exist which enable SIMs to be swapped without restarting the device[27].

eUICC Swapping

8.3 The eUICC has potential to increase the convenience of SIM swapping as no physical SIMs are involved in the swap. Using an eUICC, consumers would select and download local subscriptions over the air without having to physically obtain a new SIM. There is no need to remove and swap the SIM in the device, and no risk of mislaying a SIM when removed.

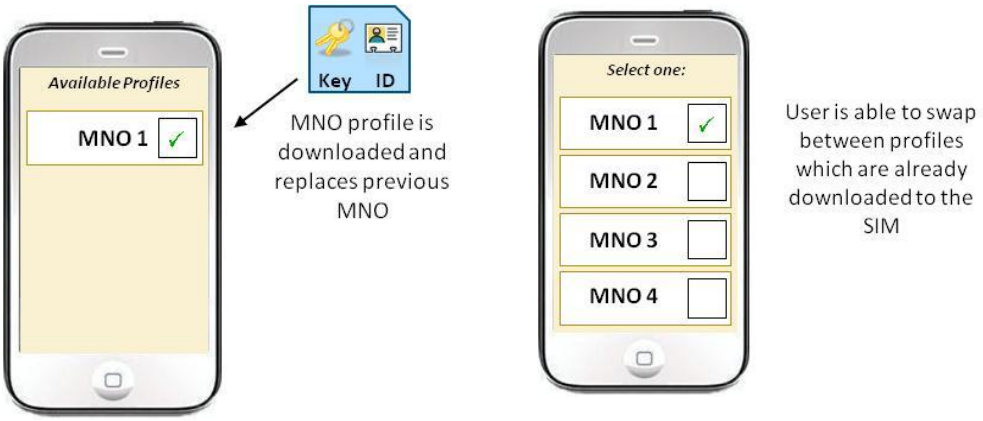
8.4 There are a number of alternative scenarios to consider:

- The eUICC could be single profile or multi-profile enabled.
- Swapping could be user-driven, or managed on behalf of the user by a service provider.

8.5 In an eUICC swapping model, a consumer is able to download multiple profiles onto the eUICC. The user could then swap between profiles as required. It is important to point out that the current GSMA use-cases, which are likely to be standardised by ETSI, do not include swapping processes. Instead they only focus on switching processes.

8.6 Two modes of swapping can be envisioned: single profile and multi-profile. These are illustrated in the diagram below.

Figure 20: Comparison of eUICC Single Profile Swapping and Multi-profile Swapping



[27] http://www.technolifestyle.com/2011/08/nokia-c2-03-dual-sim-phone-with-easy-swap/

8.7 In a single profile model (left-hand side in diagram above), each time the user "swaps" mobile operators, a new profile is provisioned and the old profile is overwritten (or deactivated) as the SIM can only hold one active MNO profile at a time. This places a burden on MNOs as the profiles need to be downloaded from their systems (or SM-DP) each time a swap is made. An analogy would be if a consumer needed to buy a new SIM each time they wished to swap their SIM.

8.8 A swapping solution based on a single profile is unlikely to emerge as requirements to allow seamless swapping may be too complex. Specifically, to allow the consumer to swap back to their original profile, MNOs would need to store profiles for subscribers that had swapped away from their networks such that these could be reapplied when a subscriber decided to swap back.

8.9 In a multi-profile system (right hand side of above diagram), more than one profile can be stored on the SIM. This allows the user to swap between profiles without needing to repeatedly download profiles from the MNO. Both old and new profiles stay active on the MNOs' systems and therefore the user can "swap back" to their old phone number and profile whenever required. Multi-IMSI SIMs are currently able to swap between multiple different MNOs in this way.

National Swapping Benefits

8.10 An eUICC swapping model could bring coverage, cost and quality of service benefits to consumers. For example, consumers could use SIM swapping to overcome coverage issues with a particular network. 900,000 households (3% of total households) in the UK are unable to receive outdoor 2G coverage from all networks while 7M households (27% of total) are unable to receive outdoor 3G signal from all networks.[28] The UK government has announced a plan to spend £150 million in improving mobile coverage for the 'not spot' areas of the UK. [29]

8.11 In theory, consumers could swap networks or tariffs depending on the offer (e.g. swap to a text prepaid tariff to send texts and swap back for voice calls). [30]

8.12 A consumer might also switch networks to improve quality if the current network is overloaded and a consumer is either unable to get a connection, or experiencing slow data speeds.

User-Driven vs. Managed Swapping

8.13 In the user-driven scenario, a consumer would use an application on their handset to manage which network they were connected to. The application would enable the user to discover available offers, setup new subscriptions with operators, and facilitate downloading of new profiles.

8.14 Assuming a multi-profile implementation, the SIM swapping application would maintain a list of the profiles available on the consumer's device and allow the user to swap between these.

---

[28] http://media.ofcom.org.uk/2011/11/01/the-state-of-the-communications-nation-2/
[29] http://www.digitalspy.co.uk/tech/news/a343599/government-announces-gbp150m-mobile-signal-boost.html
[30] http://stakeholders.ofcom.org.uk/binaries/research/consumer-experience/tce-11/3_takeup.pdf

8.15 An alternative approach would be for the swapping decision to be made on the consumer's behalf as a managed service. In this scenario, the consumer would contract with a managed solution provider (MSP) for their mobile service. The MSP would have wholesale contracts with several network operators and remotely direct the eUICC to swap between these. Swapping decisions would be made by the MSP to optimise wholesale costs and the consumer experience. In this example swaps could be made invisible to the user, providing a completely seamless experience. This is similar to how multi-IMSI solutions work today, with the advantage that new profiles could be downloaded to the eUICC over time.

8.16 A key feature of the managed service is that the customer is able to retain the same mobile number when they are switched between networks. The customer's mobile number is provided by the MSP and the MSP routes calls to the customer's device whichever network it happens to be on. This is done by the MSP intercepting calls to numbers which are not active before they get to voicemail and routing these calls to the MSISDN tied to the active IMSI.

8.17 In contrast, maintaining the same number in a user-driven swapping scenario is unlikely due to the issues it presents. The existing UK MNP process is certainly not fit for this application – the porting time is too long and the indirect routing method sub-optimal.

8.18 A user-driven swapping scenario would therefore require the user to swap numbers when they swapped networks. For some use cases (e.g. swapping between work and personal profiles) this may be advantageous, but in general it is an inconvenience. Users could setup call forwarding between numbers to overcome this however this would lead to increased costs.

8.19 A further implication is that as consumers engaging in swapping require multiple numbers, an increase in the prevalence of swapping would increase the demand for mobile numbers.

MNO vs. Handset Manufacturers Motives for National Swapping

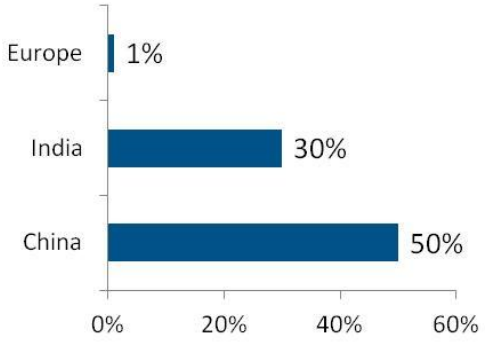
8.20 MNOs are unlikely to lead (or support) a model which allows national swapping for a number of reasons. Firstly, increased swapping may mean that the economics of handset subsidies (particularly for prepaid subscribers) would no longer work. Secondly, MNO tariffs and offers may currently benefit from cross-subsidisation (e.g. packages which bundle cheap texts and more expensive voice calls). These tariffs may not be economically viable if swapping was dynamic. Lastly, MNOs would be unable to control the end-to-end consumer experience, which would have an impact on strategic considerations, as well as potential concerns around customer care and service quality.

8.21 MNOs have historically been averse to supporting swapping models. This can be seen in the lack of MNO support for dual-SIM handsets in Europe, and the resultant low penetration (see chart below).

8.22 Dual SIM phones allow users to more easily swap between SIMs using a single handset, and still receive and make calls using both phone numbers. Dual SIM phones allow a consumer to insert two different SIM cards into one handset and to choose to make calls using either SIM, generally via a menu. The user can then receive calls on both SIM card phone numbers, which removes the need to manually switch between SIM cards.

Petitioner Samsung Ex-1027, 0041

Figure 21: Penetration of Dual SIM Handsets



8.23 High dual SIM handset penetration in China and India shows a strong demand for these products from consumers. However in Europe, there is very low penetration of dual SIM handsets. One reason for this could be that, consumers generally purchase their handsets in MNO stores or through MNO distribution channels and MNOs have an incentive not to distribute dual SIM handsets. In China and India, on the other hand, handsets are generally not subsidized and operator channels are therefore less important.

8.24 Handset manufacturers, on the other hand, are likely to be interested in developing national swapping applications. These manufacturers are well placed to install their own embedded SIM cards in devices (i.e. analogous to Google Wallet handsets). They would then be able to participate in the value chain and possibly gain control of the customer relationship. The aforementioned Apple and Google patents demonstrate the extent of the interest of these handset vendors in playing this role. Furthermore, some smartphone vendors generate revenues through on-device applications and therefore have an interest in ensuring better coverage for data services.

Petitioner Samsung Ex-1027, 0042

9. INTERNATIONAL SWAPPING

Overview of International SIM Swapping

9.1 Mobile roaming provides convenient continuity of mobile service and functionality to consumers when they travel abroad.

9.2 Mobile roaming is enabled through a commercial and technical relationship between a consumer's home network operator and the operator of the visited network. This relationship allows the home network to continue to authenticate, meter and charge subscribers when they use their devices on a visited network.

9.3 The roaming system is convenient as customers do not need to enter into multiple, separate commercial relationships with foreign networks in order to use their services abroad. However this convenience comes at a price. Roaming rates can be up to 1000 times higher than local rates (in the case of data services). [31]

9.4 To avoid roaming charges, some consumers choose to temporarily swap their home SIM for a local SIM when abroad. This enables the consumer to access local tariffs for voice and data; however it does mean that they are unreachable on their home number whilst using the local SIM.

9.5 High roaming rates have also led to regulatory intervention. The EC has introduced a series of caps on rates for consumers roaming within the EU and recently adopted a package of measures ("Roaming 3") to drive the cost down further still.

Implementing International Swapping with eUICC

9.6 eUICC handsets could facilitate international swapping in much the same way as national swapping (Section 9). The same scenarios exist in terms of support for one or more profiles and whether or not it is the user that manages the swapping.

9.7 The primary difference is that the device would need to support the swapping functionality whilst roaming on a visited network. This is because on arrival in a new country, the eUICC may not already have downloaded a local profile. The device would therefore need to temporarily roam on the visited network so that it could establish a connection to download a local profile.

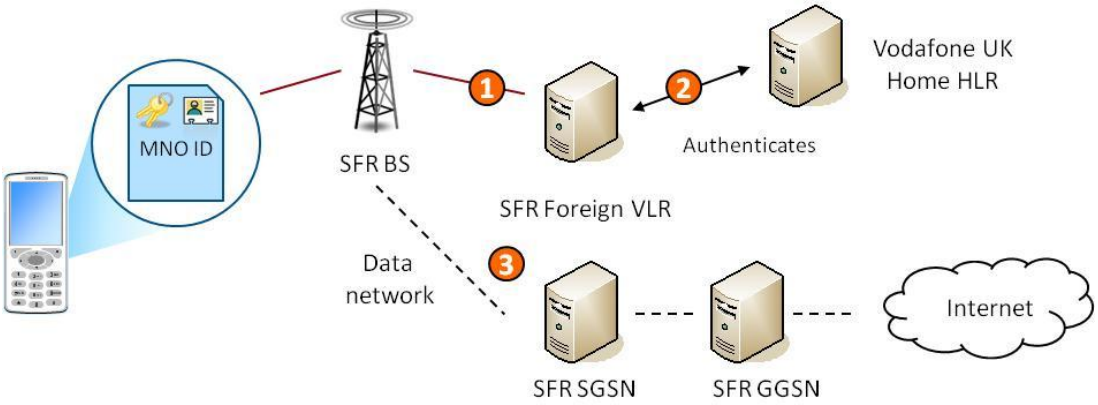
9.8 The international swapping managed solution could work in a similar way to how a multi IMSI solution works today. A managed solution provider (e.g. Transatel) signs multiple MVNO agreements in different countries and then produces a SIM that contains multiple IMSIs and subscription profiles from different MNOs. When the user travels abroad and the SIM detects it is in a new country when trying to authenticate, it changes to a local IMSI/subscription via a service provider application enabled by SIM toolkit functionality. The device then does a refresh to allow it to reconnect with a local network.

Local Break Out

9.9 The European Commission (EC) regulations have stipulated a solution which would enable selection of a local MNO independent of home operator. The Local Break Out (LBO) solution has been mandated only for local data services to be offered (not voice).

[31] According to a *Which? Group* survey: http://www.guardian.co.uk/money/2011/apr/21/ipad-roaming-charges-expensive-which

Figure 22: Local Break Out Solution – Example Vodafone and SFR Breakout



9.10 LBO gives travellers the ability to purchase local data services from foreign networks when abroad, rather than use their home network's roaming service for data. The visitor chooses from a list of available offers upon arriving in the foreign country. In the example above, the customer selects the SFR network to purchase their data services from.

9.11 The device authenticates on the home network (i.e. Vodafone UK) using the normal roaming process and throughout the process, retains access to voice roaming services. The data service, however, is provided locally by SFR without the need to go through Vodafone UK's internet gateways.

9.12 The Roaming 3 package considered other structural solutions for voice (e.g. Single IMSI, IMSI+).

9.13 An eUICC implementation would enable local break out for both voice and data, as it would allow consumers to provision and utilise new profiles when abroad. This would eliminate the need to use roaming services for voice (as well as data), as the SIM would be able to authenticate with the local network's HLR directly. However, while utilising the local network in this way, the customer would be using a local subscriber profile with a local MSISDN. This may result in a consumer being unable to receive or make calls using their original MSISDN while abroad.

Assessment of International Roaming Options

9.14 International roaming solutions were assessed on consumer-friendliness e.g. whether a consumer could receive calls on multiple numbers, cost, the hassle factor, whether the consumer could receive a single bill and whether the consumer has a free choice of MNO.

9.15 Based on this the "Managed Service" eUICC application had the most consumer-friendly features. (see table below)

Figure 23: Assessment of International Roaming Options

	Receive Calls on Multiple Numbers	Access to Local Rates	Low Hassle	Single Bill	Select Any MNO
Roaming	N/A	✗	✓	✗	✗
Physical SIM Swap	✗	✓	✗	✗	✓
Dual SIM	✓	✓	✓ Still need find local SIM	✗	✓
Multi IMSI	✓	✓	✓ Requires advanced planning	✓	✗
Local Breakout	N/A	✓ Only Data at local rates	✓ Need to manually select MNO	✗	✗
User Driven eUICC	✗	✓	✓ Need to manually select MNO	✗	✓
Managed Service eUICC	✓	✓	✓	✓	✗

9.16 For example, although the current roaming process is a highly convenient process it carries a high cost. Physical SIM swapping is technically simple and lowers costs, but involves the hassle of finding a local SIM and doing the physical swap, as well as the loss of the use of the user's home telephone number.

9.17 Dual SIM-handsets and multi-IMSI solutions both are an improvement on physical SIM swapping in terms of convenience and being able to receive calls on both telephone numbers. However both have their weaknesses. For example, the Dual SIM approach does away with the physical swapping but requires a special handset (that is not widely available) and so, severely limits customer choice. Likewise multi IMSI solutions allow for more than two IMSIs to be used, but require advanced planning to pick the correct multi IMSI before going abroad. The EC local break out (LBO) option also has limitations as it only mandates access to local rates for data.

9.18 Both eUICC solutions (user-driven and managed service-based solutions) provide benefits over existing processes. eUICC allows the customer to pick any MNO (not restricted by MVNO agreements) but the customer will not be able to receive calls on their home number while travelling. A managed service eUICC solution is the most consumer-friendly but consumers will only be able to use local networks with which the MSP has an agreement.

10. Assessments of Applications

10.1 This section will assess the implications and likelihood for each eUICC application, M2M switching, handset switching, national swapping and international swapping. To this end, for each application the section analyses:

- A summary of the major consumer benefits and potential pain points related to each application.
- The impact of each application on key stakeholders such as MNOs, Handset Vendors or alternative communication providers such as Roaming SIM providers, and therefore the motivations for each stakeholder in bringing each application to market.
- The key enablers for each application and the likelihood of the emergence of each of these enablers.
- The potential timeline for each enabler based on current status.
- Based on the timeline for each enabler, an overall timeline for each of the eUICC applications.

10.2 The section concludes with an evaluation of the potential developments and the timing of key events which regulator authorities such as Ofcom should monitor going forwards.

Summary of Consumer Benefits and Potential Consumer Harm

10.3 Each potential eUICC application brings different benefits to consumers. As discussed previously, in consumer M2M devices SIMs may be embedded. Therefore the ability to reprogram SIMs over the air provides significant benefits for M2M customers in terms of flexibility and choice. For handset switching, consumers may benefit from greater convenience if they are able to switch over the air. For national swapping, there are potential benefits in terms of increased competition and reduced cost, improved coverage and quality of service. Finally an eUICC international swapping capability could enable consumers to more easily swap SIMs to avoid roaming charges. This alternative to the single IMSI and LBO processes recommended by BEREC (Body of European Regulators of Electronic Communications) could be used beyond the European Union states.

10.4 Although eUICC functionality could be extended to achieve these consumer benefits, applications of the technology may raise concerns over potential consumer harm that may reduce the overall value of perceived benefits. These include:

- **Inflexibility**: If swapping is not allowed, or if there are greater restrictions imposed on switching (e.g. enhanced SIM lock) through adoption of eUICCs, this could reduce competition.
- **Fragmentation**: Fragmentation in the ecosystem (either for technical or commercial reasons) could result in consumers being unable to switch to particular providers or not being able to switch providers in certain countries.
- **Incompatibility with existing processes:** Existing switching Processes and MNP may need to be adapted to meet requirements of eUICC in handsets.
- **Consumer confusion**: Consumers in Europe are generally familiar with removable SIMs and the process of switching using removable SIMs; significant expense would be required to make consumers aware of new processes involving eUICCs.
- **Removal of subsidies**: If handset swapping is allowed, it may no longer be economical for operators to subsidise handsets. It is rumoured that when Apple proposed using

Petitioner Samsung Ex-1027, 0046

reprogrammable SIM technology in future iPhone models, MNOs threatened to remove subsidies for the devices.

Implications for Stakeholders for Applications

10.5 In addition to consumer concerns regarding the applications of eUICC, there are also key implications for industry stakeholders. As can be seen in the tables below, stakeholder motivations are best aligned for M2M applications with clearly beneficial outcomes for MNOs and others. MNOs may be disadvantaged in the other applications, particularly in national swapping cases where there is a large risk for operators of losing control of the customer relationship, and international swapping applications which would threaten roaming revenues.

Figure 24: Table of Stakeholder Motivations

M2M	
MNO	Others
Positive impact	**Positive impact**
• Enables MNOs to better **capitalise on growth of M2M devices**	• eUICC vendor has **potential SM role** • **M2M device vendors** in favour as it makes devices more attractive

Handset Switching	
MNO	Others
Neutral	**Positive impact**
• Could be **cost-savings** (SIM logistics) • However could **open door to swapping**	• Handset vendors can gain **greater control of customer relationship**

National Swapping	
MNO	Others
Negative impact	**Positive impact**
• Large **risk of disintermediation** for operators • Increased **competitive pressure on prices**	• Handset vendors can play **aggregating role** • **Better consumer experience** for using devices

International Swapping	
MNO	Others
Negative impact	**Positive impact**
• **Reduce roaming revenues** • Potential "roaming killer"	• Would benefit **Roaming SIM providers** • More **app usage abroad** may benefit **handset vendors / OTT players**

Likelihood of Enablers Emerging

10.6 Overall, it is likely that M2M applications will emerge. There are, however, significant commercial and strategic reasons why handset applications are unlikely to be supported.

10.7 It is unlikely that handset switching, national or international swapping will naturally emerge (in the near future at least) as these applications require technical enablers which MNOs are unlikely to help support. This is because of the negative implications of each application for MNOs which are noted above.

10.8 For example, eUICC handset switching requires: a consumer-based Subscription Manager system (which MNOs may choose to not support); availability of eUICC handsets (MNOs may choose not to sell eUICC enabled handsets); and finally modifications to existing mobile number portability processes (which MNOs may be reluctant to implement). At the moment, only handset vendors appear to have an interest in this. Therefore if the application emerges it is likely to be in a handset vendor-led ecosystem.

10.9 As for national swapping, MNOs will be highly opposed to this application. They have no incentive to support multi-profile standards (which would enable swapping). However there is potentially significant consumer benefit. Handset vendors may seek to offer this if they are

able to play an aggregator or customer-owning role and if it allows vendor to better control customer experience.

10.10 With international swapping, MNOs are again opposed to this application as it would diminish their roaming revenues. Multi-profile support is again an issue, and MNOs may have no interest in engaging in MVNO contracts for a "roaming-killer" application.

10.11 If an international swapping model emerges therefore it would likely be led by a handset vendor or ARP (alternative roaming provider / roaming SIM provider).

Figure 25: Required Enablers for Applications

	Handset switching	National swapping	International swapping
Subscription Manager	✓	✓	✓
Handset availability	✓	✓	✓
Mobile Number Portability	✓	✓	
Multi-profile / multi-IMSI		✓	✓
MVNO contracts			✓

MNO Barriers
• MNOs may not support a consumer Subscription Manager system
• MNOs may not stock handsets with reprogrammable SIM
• MNOs may be reluctant to alter existing MNP processes
• MNOs can refuse to support multiple active profiles / multi IMSI
• MNO may refuse to make MVNO deals with ACPs in some countries

<u>Timeline for Enablers</u>

Figure 26: Analysis of Status of Enablers

	M2M	International Swapping	National Swapping	Handset Switching
Subscription Manager (SM-SR, SM-DP)	In place for M2M next year	In place for M2M next year	In place for M2M next year	In place for M2M next year
Handset Availability	Not applicable to M2M	eUICC handset specs not yet available	eUICC handset specs not yet available	eUICC handset specs not yet available
Multi-profile / Multi-IMSI	Not required	Tech exists today	Tech exists today	Tech exists today
MNP and Switching Processes	Not required	Not required	May not be required	Required – may take several years
MVNO Contracts	Not required	MVNO contracts for multi IMSI	Not required	Not required

Increasing Complexity / Time required

10.12 In order to estimate the likely timeline for each application (M2M switching, handset switching, national swapping and International swapping) CSMG conducted an assessment

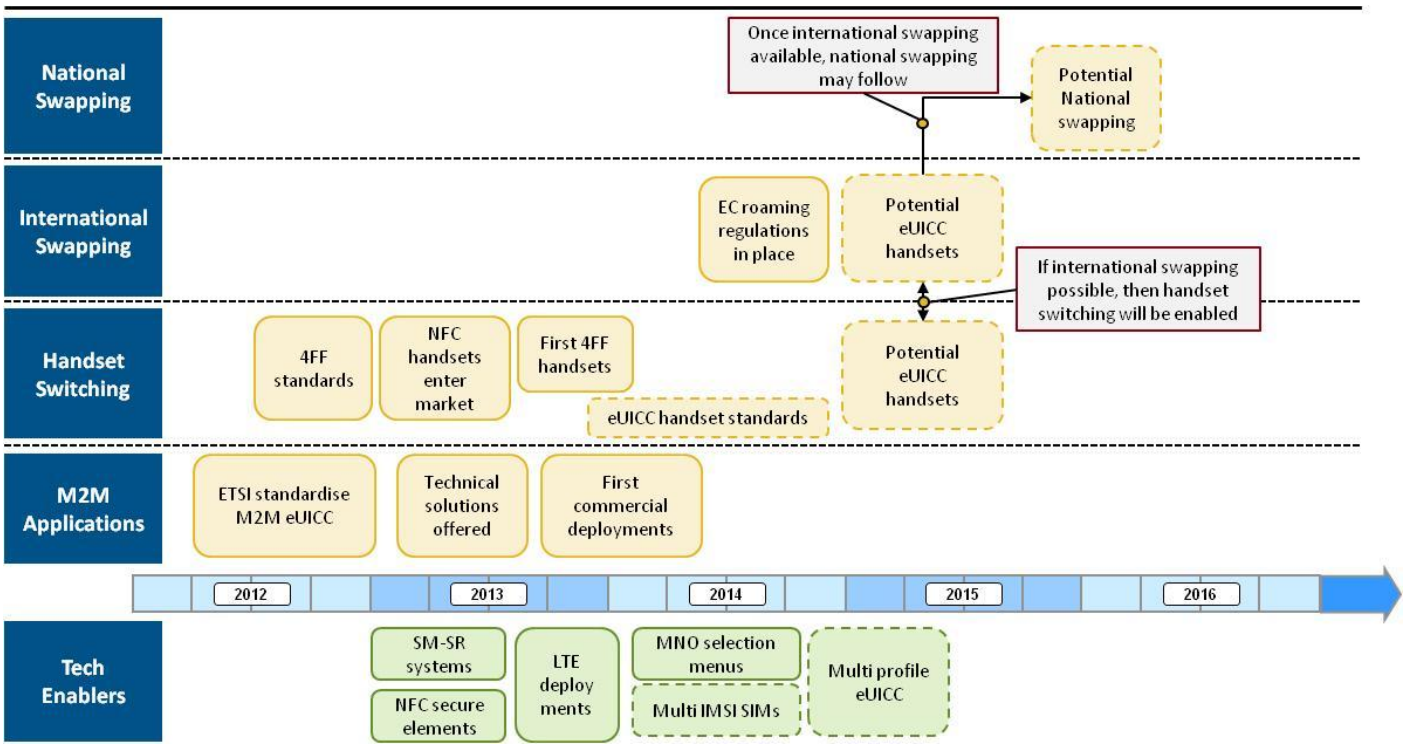
of the status of each of the key enablers required to bring these applications to market (shown in the diagram above). The assessment suggests that the handset switching application is potentially the most complex, as new mobile number portability and switching processes are required which could take years to decide upon.

10.13 Handset eUICC standards are the other enabling requirement not present today and which will clearly impact the availability of eUICC handset applications. If eUICC handset standards emerge it is likely that these will follow sometime after the agreement on eUICC M2M standards.

10.14 As the enablers for M2M exist today or are expected to be implemented in the near future, it is likely that M2M applications will emerge in 2013.

Timeline for eUICC Evolution

Figure 27: Evolution of EUICCs Timeline



10.15 As can be seen above, the earliest that non-M2M solutions can be expected is after 2014, once roaming regulations and 4FF standards are implemented, and consumer-facing eUICC requirements, use cases and standards are developed.

Key Points for Ofcom

10.16 Given these enablers, ecosystem player motivations, and the possible evolution of eUICCs, we recommend Ofcom follow eUICC developments closely.

10.17 eUICC handset standards may be drafted starting in 2014. Should this happen, we recommend Ofcom assess the potential impacts of this on MNP systems and processes. Ofcom should also ensure that suitable switching processes are in place to support eUICC switching.

Petitioner Samsung Ex-1027, 0049

10.18 Consideration should be given to the eUICC as a potential bottleneck asset. The SIM Issuer (through its SM) controls access to the eUICC and effectively acts as a gatekeeper for service providers. New processes or governance may be needed to accommodate this.

10.19 Linked to the role of the SM is the risk of fragmentation in the ecosystem. We recommend monitoring the evolution of the eUICC handset ecosystem to determine the risk of a lack of interoperability, and the impacts this would have on consumer choice.

10.20 Depending on how handset swapping are switching are implemented, users may be presented with a menu to select an MNO. The design of this menu may favour one provider over another, similar to the EPG prominence issue in television.

Petitioner Samsung Ex-1027, 0050

11. Conclusion

11.1 SIM technology has evolved greatly over the last two decades, and has become a familiar part of the mobile world to consumers. While it is an invaluable tool for MNOs to provide services to these consumers, the needs of consumers have dictated the evolution towards smaller and more functional SIMs.

11.2 As SIM cards become smaller and smaller and capable of more, it is natural to speculate in what direction the technology will develop. It appears that eUICC technology is the way forward, moving the SIM as an application into a hardware-agnostic world, and potentially removing the need for a removable SIM card.

11.3 While M2M and connected devices benefit the most from eUICC technology, we foresee the potential for consumer handset applications in the future, with today's switching and swapping processes translated into the more seamless, consumer-friendly solution of tomorrow.

11.4 This, however, comes with both challenges and drawbacks around the technical and commercial implementation of such solutions, as well as the potential risks to consumer choice and cost. Several hurdles will need to be cleared and cooperation secured for a fair and comprehensive solution to arise, and thus we expect the eUICC technology to remain firmly an M2M-focused solution in the near future.

11.5 Ultimately, regulators will need to monitor the development of the eUICC. If it were to be further developed as a consumer proposition, then the regulator must understand and monitor how eUICC-based solutions will be implemented in handsets, and the necessary processes involved in switching and swapping. To this end, CSMG has developed a conceptual model of how an eUICC might differ from current M2M requirements if it is used in handsets.

11.6 Further investigation of the subject is necessary to avoid any pitfalls. Once the first industry-standardised eUICC solution is on the market, it would be wise to revisit the topic and understand the current market state and its further evolution.

Petitioner Samsung Ex-1027, 0051

ANNEX

12. Annex 1: Conceptual Model

Introduction

12.1 This annex outlines a conceptual model in which the consumer scenarios discussed in the main document could be satisfied by the eUICC. Throughout this annex, we have aimed to remain consistent with existing documentation by GSMA and ETSI and the broad principles of the eUICC detailed within these documents. Where the discussed consumer scenarios in this report are dependent on functional use cases within the GSMA document (Ref[1]), these are also described in more detail.

12.2 The conceptual model is defined through a series of flow diagrams, state transition models and pseudo-code. These methods are intended to assist in explaining the concepts and could provide the basis for a functional design in the future.

12.3 This approach is not intended to replicate work being conducted by ETSI in producing requirements and specifications for the eUICC in M2M applications, but instead seek to build upon these. Therefore processes and technology which may be utilised in the consumer cases but which are also expected to exist in M2M applications are not outlined in this section. The purpose of this section is not to provide an end-to-end specification but instead to focus on demonstrating the incremental areas which would be necessary for the consumer use-cases to be implemented.

Consumer Scenarios

12.4 The consumer scenarios are set out in the following table.

No.	Use Case	Description
Consumer Scenario 1	Switching	SIM switching is used when a consumer switches from one operator to another. There is no requirement to switch back to the original operator on an ad hoc basis. For example, this scenario may occur when a consumer's contract expires. In this case, the consumer generally signs up with their new service provider immediately prior to the switch. After the switch, the consumer's previous SIM card is normally discarded (and may even be rendered inactive). Consumers may choose to keep their existing phone number by porting the number to their new provider. This process requires an interaction with their previous MNO in order to port the number.

Petitioner Samsung Ex-1027, 0053

Consumer Scenario 2	Swapping User initiated	User-initiated SIM swapping is used when a consumer wishes to use a single device with more than one subscription, and swap between these subscriptions at will. As the swap is temporary in nature, no number porting occurs. Examples include: • Consumer has multiple subscriptions with different MNOs to overcome coverage issues they experience while at different locations. The consumer wishes to use MNO_A when at location Y and MNO_B when at location Z • Consumer has multiple subscriptions with different MNOs to arbitrage between different tariffs. For example, the consumer may wish to use MNO_A for data and MNO_B for voice and SMS consumption.
Consumer Scenario 3	Swapping Dynamic	Dynamic SIM swapping differs from the user-initiated case in that the user is not involved in the decision to swap or the execution of the swap. Instead, the swap occurs automatically and is orchestrated by another party. An example would be a Managed Service Provider (MSP). The MSP could manage the swapping between networks to deliver a service that provides superior coverage, quality or price. To do this, the MSP may utilise multiple MNO networks and have wholesale agreements with each of the MNOs. Managed swapping by an MSP could occur between MNO networks in the same country, or between countries.

References

12.5 The following external documents are referenced throughout this annex.

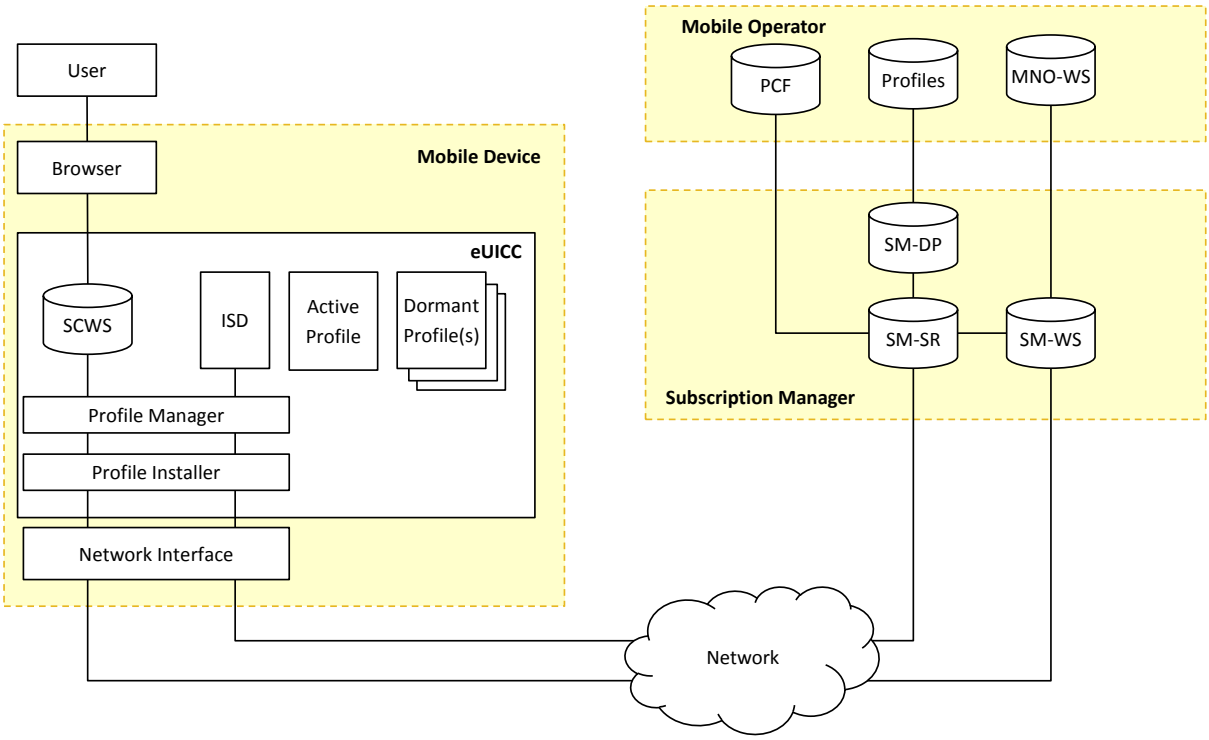
Number	Title	Author	Version – Date
Ref[1]	Embedded SIM Task Force: Requirements & Use Cases	GSMA	V1.0: 21/02/2011
Ref[2]	Draft ETSI TS 103 383 eUICC Requirements Specification	ETSI	V0.0.34: 05/2012

Petitioner Samsung Ex-1027, 0054

Architecture and Components

12.6 This section provides an overview of the ecosystem components, security credentials and prospective logical APIs that may be developed on each component. In addition it provides a list of the key assumptions that have been made in conceptualising how the consumer scenarios may work.

Figure 28: eUICC Logical Architecture



Logical Entities

Component	Description
SCWS	SmartCard WebServer: Webserver embedded on eUICC.
Profile Installer	A logical entity on the eUICC which validates decrypts & installs Profile blocks. Has a relationship with an SM-DP with "Profile Installer credentials" providing security mechanism between the two entities.
Profile Manager	A logical entity on the eUICC which manages profiles as blocks of encrypted data. Has a relationship with SM-SR with "Profile Management credentials" providing security mechanism between the two entities.
Profile	A set of applications, files & data which provide services, e.g. MNO NAA (Network Access Application) and credentials. There will generally be one active profile (unless eUICC is end-of-life) and there may be multiple inactive profiles installed on the eUICC

Petitioner Samsung Ex-1027, 0055

SM-SR	Subscription Manager - Secure Routing: Entity that securely performs functions which directly manage the operational and provisioning profiles on the eUICC. The SM-SR processes requests are received by the SM-WS. The SM-SR may check with a PCF (Policy Control Function) for authorization. The SM-SR has a relationship with the eUICC (Profile Manager) The SM-SR has a relationship with an SM-DP. A single SM-SR may have a relationship with multiple SM-DPs (see later section on Multiple SM-DP connectivity). "Subscription Management credentials" are used to provide a security mechanism between the two entities.
SM-WS	Subscription Manager Web Server: Webserver allowing trusted external entities such as SCWS and MNO-WS command access to Subscription Manager services. The SMWS would embody the SCWS Remote Administration Server
SM-DP	Subscription Manager – Data Preparation. A functional entity that prepares operational and provisioning profiles to be securely provisioned on the eUICC e.g. encryption of profile. Has a relationship with the eUICC (Profile Installer). "Profile Installer credentials" provide the security mechanism between the two entities.
PCF	Policy Control Function within the scope of this document refers to principles reflected in a set of rules that governs the behaviour of eUICC and/or entities involved in the remote management of the eUICC.
MNO-WS	MNO – WebServer: WebServer allowing command access to sub-components including SM-DP (which may be MNO owned), and (Pre-) Provisioning interfaces. For the purposes of this document it is assumed that MNO-WS will interface with other MNO sub-components such as BSS, IN and CSR.

Logical APIs

Component	Logical API	Description
Profile Installer	`PI_Install()`	Installs new MNO profile block on eUICC. API exposed to SM-DP Attributes: IMSI
Profile Manager	`Load()`	Loads the installed profile block into one of the inactive available profile slots on the eUICC. API exposed to SM-SR Attributes: IMSI
	`Enable()`	Moves an inactive profile to the active state and moves previous active profile to inactive. API exposed to SM-SR Attributes: IMSI
SM-SR	`Change_Active()`	For a given eICCID and IMSI, switch the active profile such that the given IMSI profile becomes active Attributes: eICCID, IMSI
	`SMSR_Install()`	Install a profile for a given MNO for a given eICCID Attributes: MNO_ID, eICCID

	`Get_MNO_List()`	For a given region provide all MNOs available for Profile download Attributes: eICCID, Region_ID
SM-DP	`SMDP_Install()`	For a given eICCID, Install a Profile Attributes: IMSI, eICCID

Attributes

Attribute	Description
eICCID	Electronic integrated circuit card identifier (similar to ICCID for UICCs). Used to identify a particular eUICC
IMSI	International Mobile Subscriber Identity. Used to identify a subscriber profile
MNO_ID	Mobile network operator ID
Region_ID	Region ID used to determine the availability of MNOs in a particular country / area

Assumptions

Component	Assumption	External Reference
eUICC	The eUICC supports the requirements defined by the GSMA in its submission to ETSI including the ability to be remotely reprogrammed by a Subscription Manager over a secure connection	ETSI SCPREQ(11)0113
	The eUICC supports storage of multiple subscriber profiles which may be associated with different mobile network operators; only one profile can be active at a time	
	The eUICC has the ability to notify the mobile device that changes to the eUICC configuration have occurred using the Card Application Toolkit REFRESH command	ETSI TS 102 223 V9.1.0
Smart Card Webserver	The eUICC contains a Smart Card Web Server (SCWS) as defined by the Open Mobile Alliance	OMA SCWS V1.2
	The SCWS has an Administrative Agent (also located on the eUICC) that communicates with a SCWS Remote Administration Server	OMA SCWS V1.2
	Communications between the SCWS Remote Administration Server and the Administrative Agent use HTTPS (HTTP over TLS)	OMA SCWS V1.2
Mobile Device	The mobile device has a web browser client that supports HTTPS (HTTP over TLS)	
	The mobile device supports HTTPS access from the web	OMA SCWS V1.2

	browser to the Smart Card Web Server	
	The mobile device provides external data connectivity to the Smart Card Web Server (either TCP over Bearer Independent Protocol or TCP over IP).	OMA SCWS V1.2
	The mobile device will retrieve updated subscriber profile information from the eUICC in response to a REFRESH command from the eUICC.	ETSI TS 102 223 V9.1.0
Subscription Manager	A means of federating Subscription Managers exists such that the Subscription Manager that manages the eUICC is able to load profiles for MSPs that only have relationships with other (federated) Subscription Managers	
	The SM-eUICC is able to provide a list of available MNOs for a given country; the list may include MNOs associated with other (federated) Subscription Managers	
	The Subscription Manager operates a SCWS Remote Administration Server with administrative control over the SCWS on the eUICC	
	The Subscription Manager can update SCWS content via the SCWS Remote Administration Server	
	The Subscription Manager can receive requests for updated content from the SCWS via the SCWS Remote Administration Server	

Petitioner Samsung Ex-1027, 0058

GSMA Use Cases

12.7 The consumer scenarios are dependent upon functional use cases that have been outlined by the GSMA in Ref[1]. This section references those functional use cases and illustrates their sequence diagrams. The functional use cases are:

- F2A - Download additional profile (which extends F2 to include additional profile downloads on eUICC)
- F5 - MNO Subscription Swap

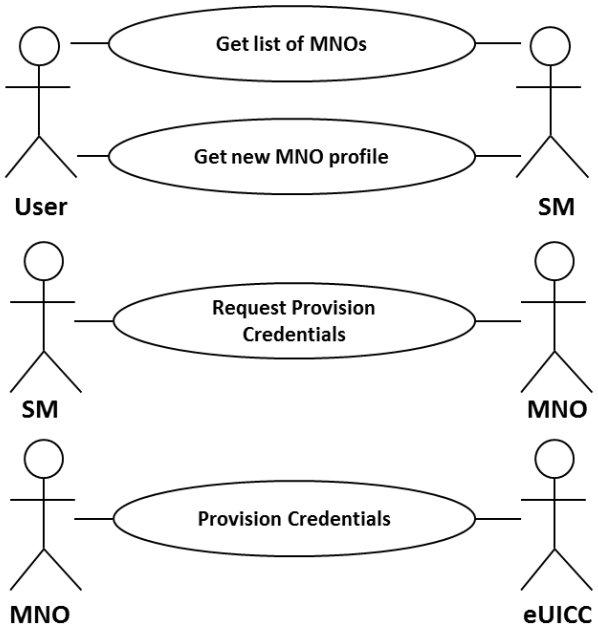
No.	Use Case	Description
F2A	Download additional profile	eUICC within a consumer device with an existing active MNO provisioned is updated with selected further MNO credentials. This functional use case elaborates on F2 which presents the initial credential download rather than an additional one. Note: For the MNO this will be linked to network/billing/CRM activation and establishing a subscription. Policy control functions as defined in LIF9 / LIF10 / SM4 of Ref[1] shall be applied.
F5	MNOs subscription swap	An inactive subscription from MNO1 becomes active, while the previous active subscription from MNO2 becomes inactive. Policy control functions as defined in LIF9 / LIF10 / SM4 of Ref[1 shall be applied.

Petitioner Samsung Ex-1027, 0059

Functional Use Case F2A – Download Additional Profile

12.8 This use case describes how a user downloads an additional profile to the eUICC.

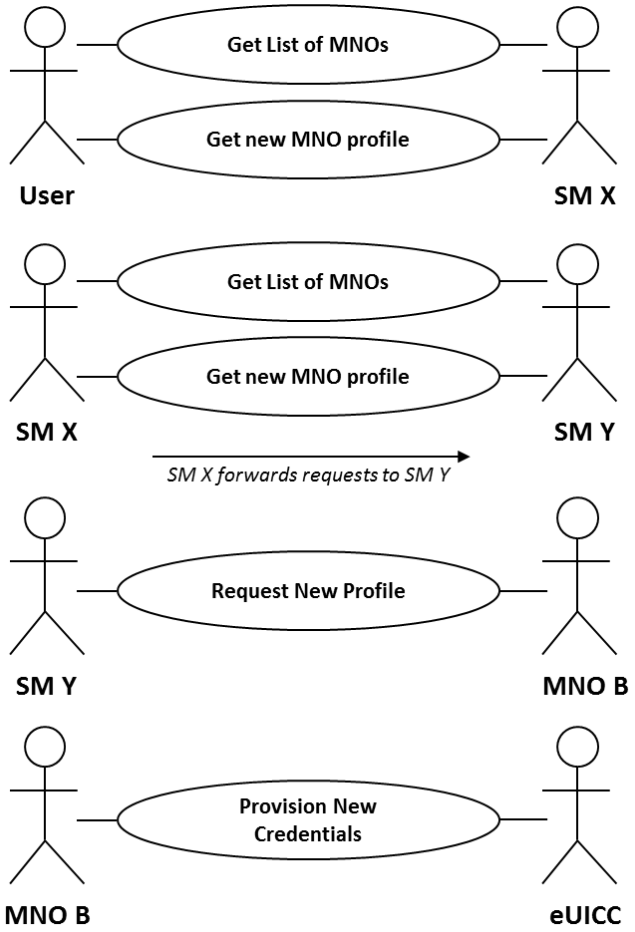
Figure 29:Functional Use Case F2A



12.9 To accommodate a multi-SM marketplace, it is desirable that an SM has the ability to download profiles for MNOs that it does not have a direct relationship with. This more complex use case is shown in the diagram below and shows how the model could work in this situation.

Petitioner Samsung Ex-1027, 0060

Figure 30:Functional Use Case F2A



12.10 The consumer has an existing subscription profile with MNO_A and wishes to download a new profile from MNO_B. The consumer's device/eUICC is managed by Subscription Manager X. However the device/eUICC does not have a direct relationship with MNO_B's subscription manager (Subscription Manager Y). The consumer's request for a subscription from MNO_B is therefore routed through Subscription Manager X to Subscription Manager Y (which has the direct relationship with MNO_B).

12.11 Further information on how SM-SRs may be linked is shown in the section on reference architectures at the end of this annex.

Petitioner Samsung Ex-1027, 0061

Functional Use Case F2A – Download additional profile	
Pre-condition	eUICC has one profile available (MNO_A) • eUICC Profile Active: MNO_A/IMSI_A
Post-condition	eUICC has two profiles[32] available: • eUICC Profile Active: MNO_A/IMSI_A • eUICC Profile Inactive: MNO_B/IMSI_B
Use Case Steps	
1	Consumer chooses to have second profile on their device. To do this consumer launches client on device which opens page on SCWS displaying user options. Consumer selects the "Profiles" menu on their device and selects "download additional profile"
2	In response to user selection, the SCWS requests a list of available MNO profiles from the eUICC's subscription manager (Subscription Manager X). This is achieved by sending a request to the SM-WS of Subscription Manager X: **Get_MNO_List(Region_ID, eICCID)** Where the Region_ID is based on the user's location.
3	SM-WS X will then return a list of available MNO profiles relevant to the user's location. This may include MNOs that do not have a direct relationship with Subscription Manager X. To obtain information on MNOs with which it does not have a direct relationship, SM-SR X can forward the Get_MNO_List command to peer SM-SRs (e.g. SM-SR Y) and act as a proxy for the return data. In this way, a user can receive a list of MNOs associated with multiple SM-SRs.
4	The user selects MNO_B on their client. SC-WS sends a request to SM-WS to provision MNO_B profile to the eUICC using: **SM-SR_Install(MNO_B, eICCID)** SM-WS sends information to SM-SR X, which checks PCF for authorisation. If okay, SM-SR X forwards the install command to the SM-WS of Subscription Manager Y (which has a relationship with MNO_B). The install command triggers SM-SR Y to request a new profile from MNO_B SM-DP

[32] The eUICC is likely to have capacity for multiple profiles. Only one will be active at any point in time, however there may be many inactive. For the purposes of this annex only one active and one inactive profile will be considered

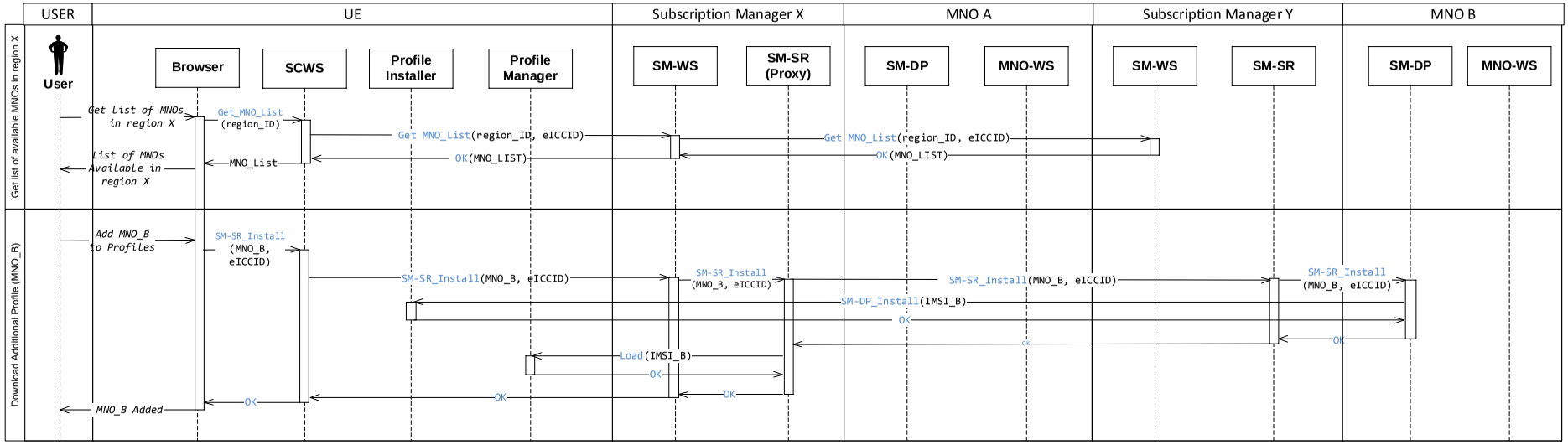
Petitioner Samsung Ex-1027, 0062

5	MNO_B SM-DP prepares the subscriber profile and sends it to the SM-SR for routing back to the eUICC Profile installer using: **SM-DP_Install(IMSI_B)** The SM-WS may also inform MNO-WS for account creation, billing etc. purposes. On the eUICC, the Profile Installer creates a new MNO profile block on the eUICC for MNO_B SM-DP using: **PI_Install(MNO_B)** Finally, the SM-SR instructs the profile manager on the eUICC to load the profile into the correct block: **Load(IMSI_B)**
6	The user now has two MNO credentials on their device: • eUICC Profile Active: MNO_A/IMSI_A • eUICC Profile Inactive: MNO_B/IMSI_B We assume MNO_B has pre-provisioned the account.[33] Upon first usage the account will be activated within the MNO's network and BSS systems. • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B Pre-provisioned, MSISDN_B

[33] Provisioning and activation processes vary between MNOs and even between account types on the same MNO. For the purposes of this document we will assume that new IMSIs will be in a pre-provisioned state on the MNO before being fully activated e.g. It may have First Call Redirect (FCR) set-up to direct user to an IVR/CSR, also browser activity may be re-directed to a subscription activation page. This will trigger activation/service provisioning. Provisioning & Activation design (including all activities relating to activation, including credit checking, network/Billing/CRM provisioning) are beyond the scope of this document.

Petitioner Samsung Ex-1027, 0063

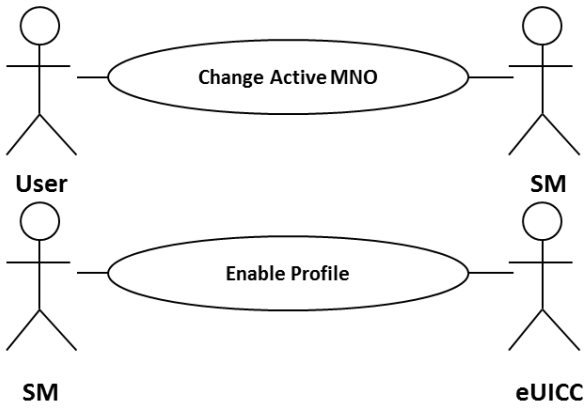
Figure 31: Sequence Diagram for F2A



Functional Use Case F5 – MNO subscription swap

12.12 Having downloaded an additional profile, functional use case F5 describes how the profiles can be changed to activate the new profile and de-activate the existing profile.

Figure 32: Functional Use Case F5



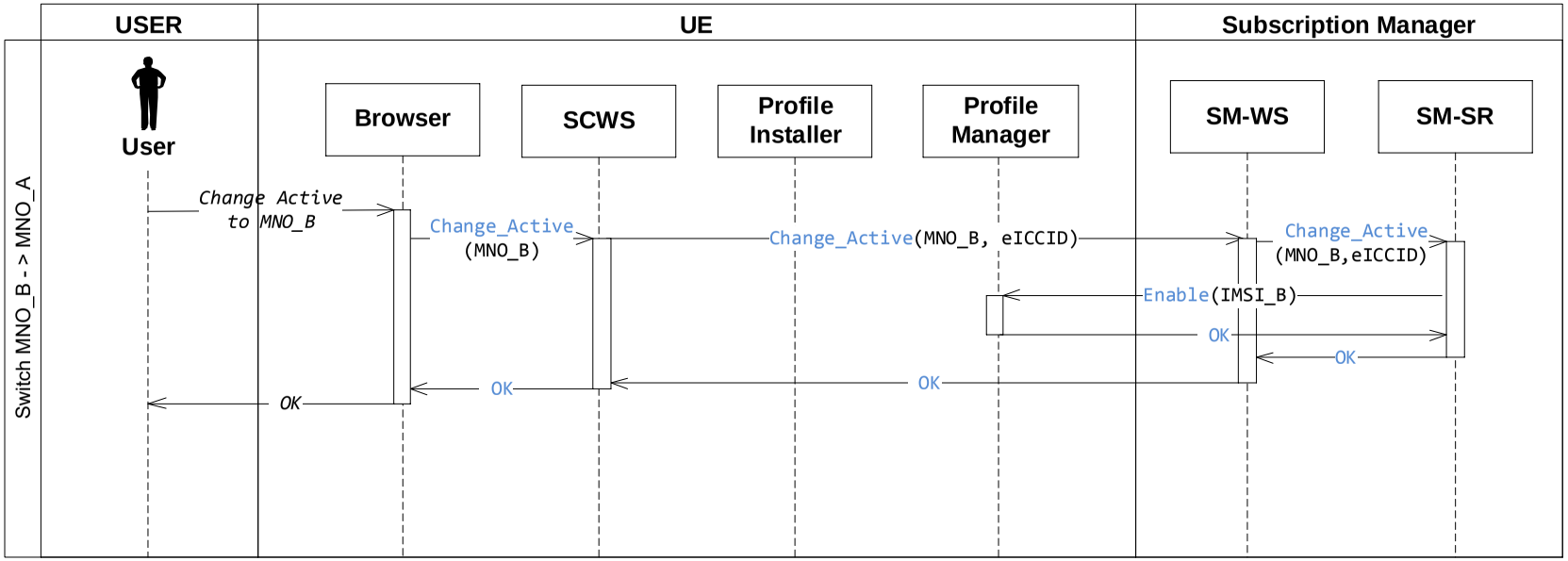
Functional Use Case 5 – MNOs subscription swap	
Pre-condition	eUICC has two profiles available MNO_A (Active), MNO_B (Inactive) • eUICC Active Profile: MNO_A/IMSI_A • eUICC Inactive Profile: MNO_B/IMSI_B Two MNOs have credentials/subscriptions associated with the eUICC • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B: Provisioned, MSISDN_B[34]
Post-condition	eUICC has two profiles available MNO_A (Inactive), MNO_B (Active) • eUICC_A Inactive Profile: MNO_A/IMSI_A • eUICC_B Active Profile: MNO_B/IMSI_B Two MNOs have credentials/subscriptions associated with the eUICC: • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B: Provisioned, MSISDN_B
Notes	None
Use Case Steps	
1	User elects to switch between MNO profiles on their device.

[34] The status could also be in pre-provisioned state meaning the eUICC has been pre-provisioned on the MNO but with FCR set waiting for activation of billing, CRM etc.

2	User launches client on device which opens page on SCWS displaying user options. User selects the "Profiles" menu on their device and sees available profiles. User selects a non-active profile and selects "Activate Profile". The device SC-WS contacts the Subscription Manager SM-WS and requests a change in active profiles using: **Change_Active(IMSI_A, IMSI_B, eICCID)**
3	SM-SR checks PCF to determine if Change_Active command is allowed for that particular eICCID (e.g. out of contract, etc.). If allowed, the SM-SR sends a command to the eUICC Profile Manager to activate IMSI_B and de-activate the previous active profile (IMSI_A). This is done using: **Enable(IMSI_B)**
4	eUICC has two profiles available MNO_A (Inactive), MNO_B (Active): • eUICC_A Inactive Profile: MNO_A/IMSI_A • eUICC_B Active Profile: MNO_B/IMSI_B Two MNOs have credentials/subscriptions associated with the eUICC: • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B: Provisioned, MSISDN_B

Petitioner Samsung Ex-1027, 0066

Figure 33: Sequence Diagram for F5



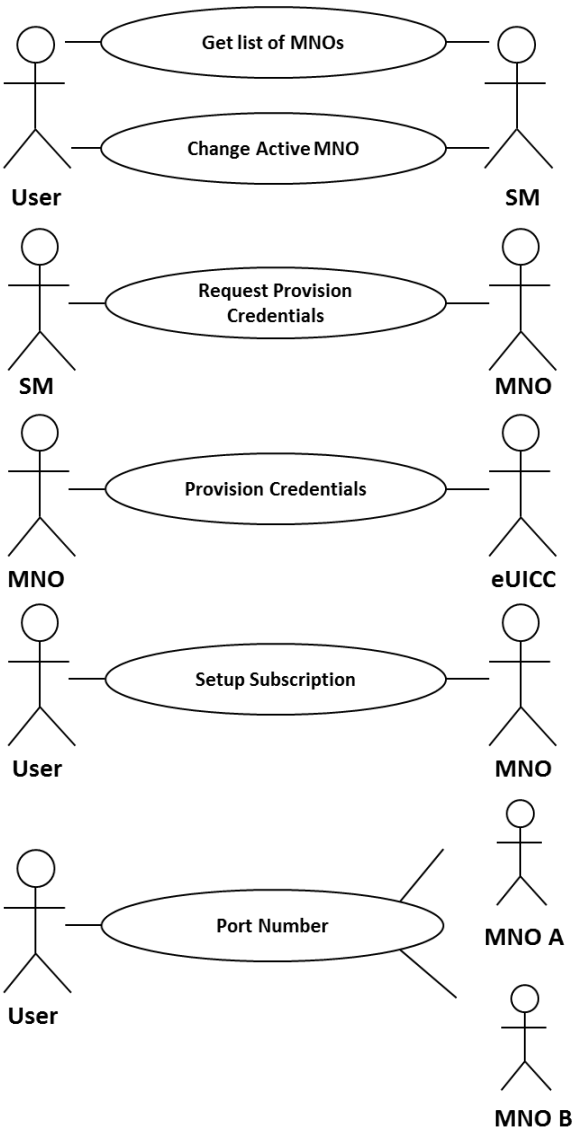
Consumer Scenarios

12.13 The following section outlines the consumer scenarios utilising the GSMA functional use cases.

Consumer Scenario 1: "Handset Switching"

12.14 The first consumer scenario considers the case where a user switches to a new MNO. The user wishes to keep their current device and port their mobile number.

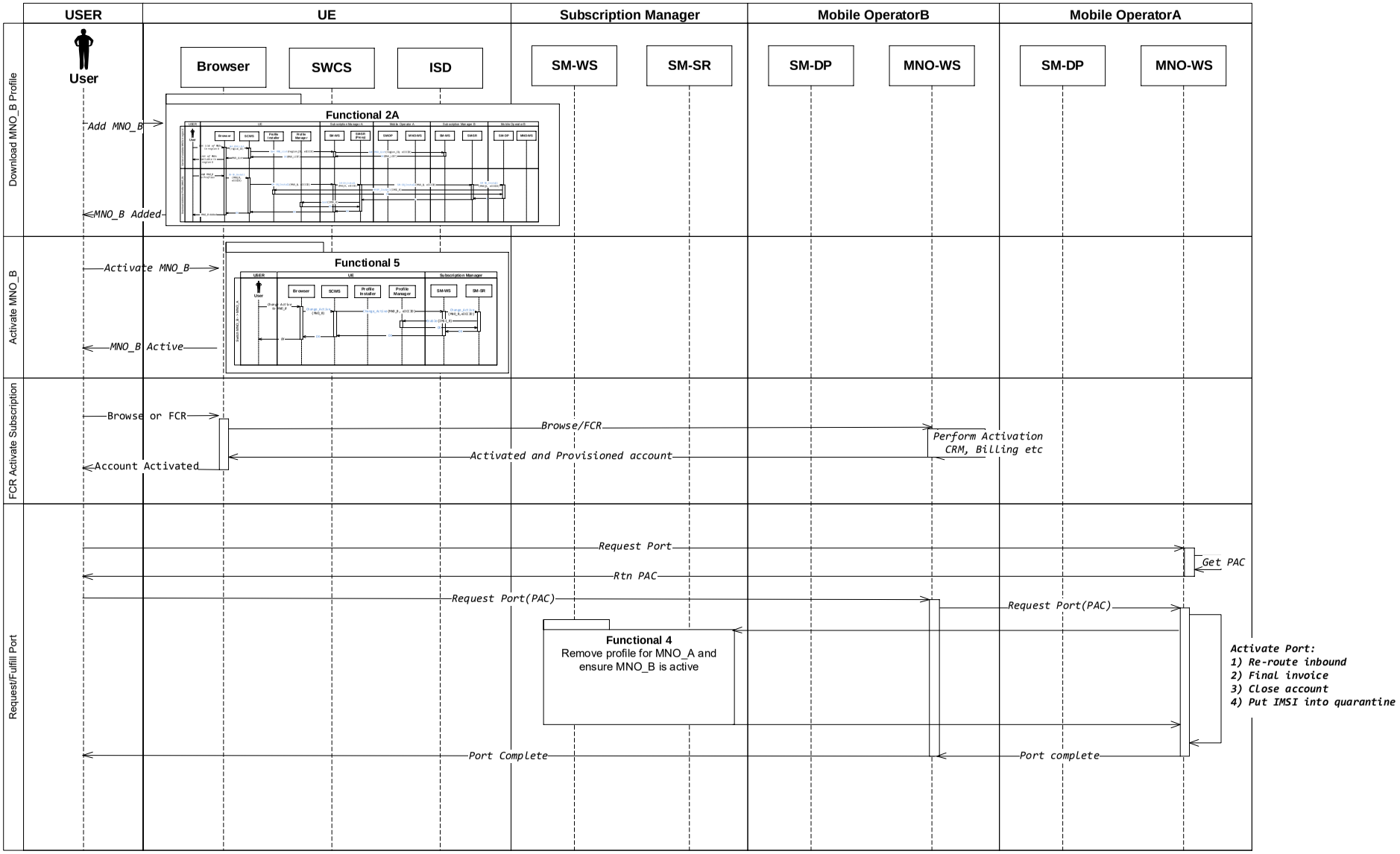
Figure 34: Consumer Scenario 1: "Handset Switching"



Consumer scenario 1	"Handset switching"
Scenario	A user's contract has expired and the user elects to join a new network and take their MSISDN with them. The user is currently using MNO_A with IMSI_A which is associated with MSISDN_A and wishes to switch to use MNO_B and take existing MSISDN (MSISDN_A) with them.

Pre-Condition	User has MNO_A credentials on eUICC and active subscription with MNO_A IMSI_A/MSISDN_A.
Post-Condition	User has MNO_B credentials on eUICC and active subscription with MNO_B IMSI_B/MSISDN_A.
Consumer Scenario Steps	
1	Assuming the user doesn't already have MNO_B credentials on their device their eUICC status will be: • eUICC Profile Active: MNO_A/IMSI_A • eUICC Profile Inactive: Null They will therefore need to download new credentials as described above in Functional Use Case F2A – Download Additional Profile.
2	The user now has two MNO credentials on their device: • eUICC Profile Active: MNO_A/IMSI_A • eUICC Profile Inactive: MNO_B/IMSI_B The MNOs' HLRs will be provisioned as follows: • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B: Pre-provisioned, MSISDN_B User now performs F5 "MNOs subscription swap" to change the active profile • eUICC Profile Inactive: MNO_A/IMSI_A • eUICC Profile Active: MNO_B/IMSI_B User makes first call or conducts browser activity on device; this will trigger activation/provisioning with the MNO. The MNOs' HLR status will be as follows: • MNO_A Profile IMSI_A: Provisioned, MSISDN_A • MNO_B Profile IMSI_B: Provisioned, MSISDN_B
3	User may then elect to perform a Port operation. User will need to contact MNO_A and MNO_B to initiate this process. Upon exchange of PAC code the MNP process can be completed as per existing processes. Upon completion of Port the MNOs' HLR status will be as follows: • MNO_A Profile IMSI_A: De-Provisioned (Quarantine), MSISDN_A: divert to MNO_B • MNO_B Profile IMSI_B: Provisioned, MSISDN_A
4	Upon completion of MNP, the MNO_A profile on eUICC may be removed. In this case, the SM-SR may send a command to the eUICC Profile Manager to remove the inactive profile. The eUICC status will therefore be as follows: • eUICC Profile Active: MNO_B/IMSI_B • eUICC Profile Inactive: Null This step is referenced as Functional use case 4 in the GSMA document (Ref[1].)

Figure 35: Sequence Diagram for Consumer Scenario 1: Handset Switching



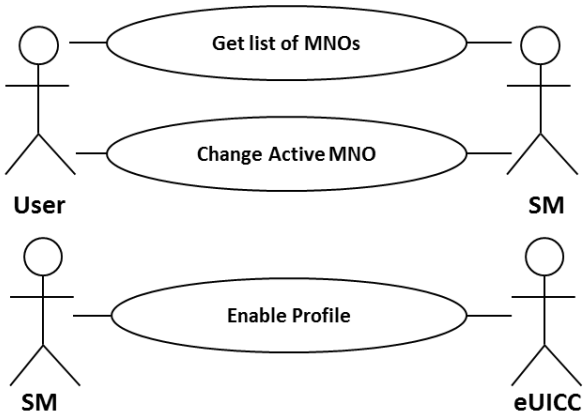
csmg
A TMNG Global Company

Consumer Scenario 2: "Swapping – User Initiated"

12.15 The second consumer scenario considers the case where a user wishes to temporarily use a different SIM in their current device. The user has the ability to revert to the original SIM at a later point in time.

12.16 For illustration purposes we use the scenario of a user travelling abroad and using a local SIM in the visited country. The use case could equally apply to a user with more than one SIM in their home country.

Figure 36: Consumer Scenario 2: "Swapping – User Initiated"

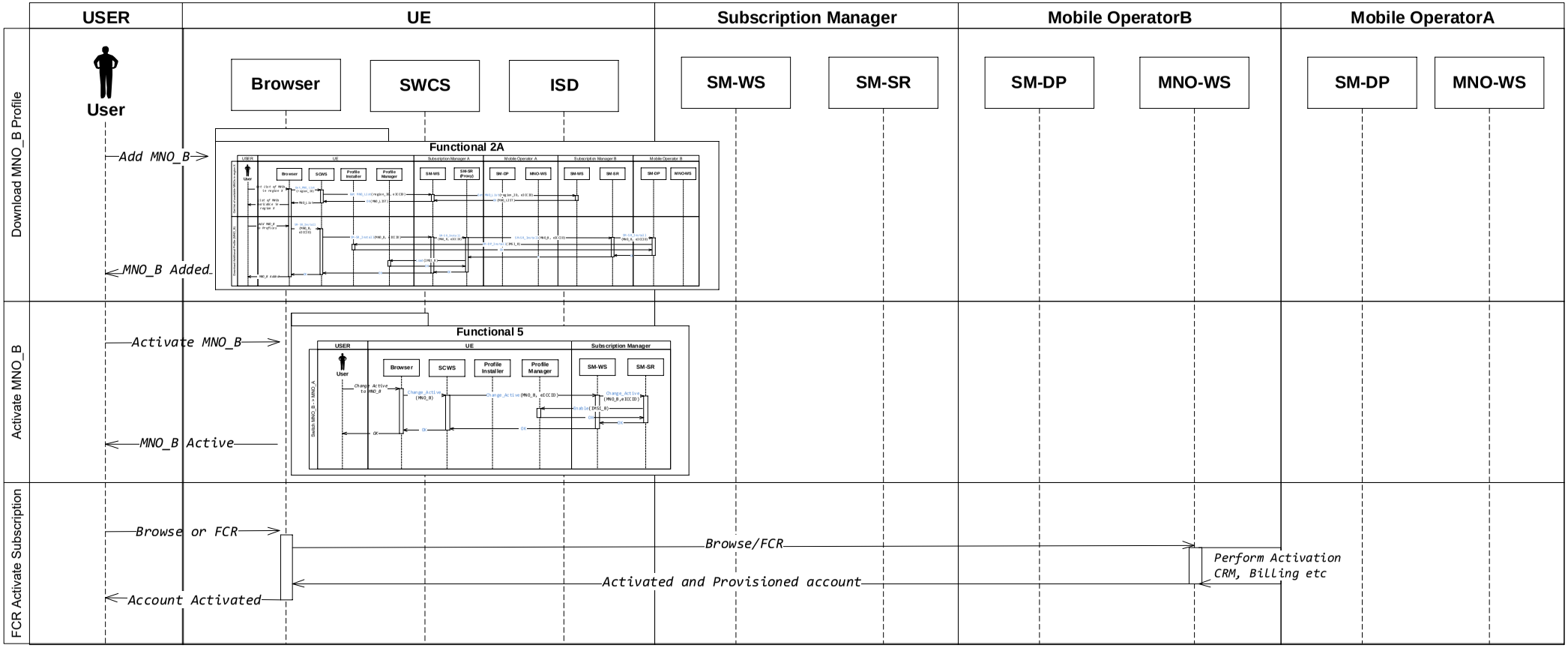


Consumer scenario 2	"Swapping – User Initiated"
Scenario	A user has a subscription with MNO_A which provides a service in their home country. The user wishes to have an additional commercial arrangement with another MNO (MNO_B) which operates in another country. The user intends to "SIM swap" whilst travelling so that they can take advantage of local rates in the visited country.
Pre-Condition	User has MNO_A credentials on eUICC and active subscription with MNO_A IMSI_A/MSISDN_A.
Post-Condition	User has MNO_A and MNO_B credentials on eUICC and a commercial relationship (Prepay or Postpay) with both MNO_A and MNO_B. The user has two MSISDNs (and IMSIs), only one of which can be active at any one time
Consumer Scenario Steps	
1	Assuming the user doesn't already have MNO_B credentials on their device their eUICC status will be: • eUICC Profile Active: MNO_A/IMSI_A • eUICC Profile Inactive: Null User begins downloading of additional profile process (F2A). As in the previous use case, the user is able to view a list of available MNOs in the country and download

	the chosen MNO profile. If the user is already present in the foreign country, the profile download procedure will occur whilst the user is roaming using their MNO_A profile.
2	The user then swaps profile (F5). In this example, as the inactive profile is not deleted (unlike in Consumer Scenario 1), the user can swap between service providers as and when the need arises. Each service provider profile is associated with its own MSISDN (no porting occurs unlike in previous example) and only one profile will be active at any given time. The MSISDNs of inactive profiles will be unreachable for inbound calls.

Petitioner Samsung Ex-1027, 0072

Figure 37: Sequence Diagram for Consumer Scenario 2 - Swapping User Initiated



Consumer Scenario 3: "Swapping – Dynamic"

12.17 This scenario builds on Consumer Scenario 2 to show how the introduction of an MSP (Managed Service Provider) in conjunction with eUICC technology devices can bring new benefits and allow dynamic and automatic swapping of profiles.

Managed Service Providers

12.18 For this scenario we consider a MSP which offers local mobile network access internationally for its subscribers. The MSP delivers this service via its partnership with a number of MVNO agreements with local MNOs in different countries. It may differentiate its service offering based on coverage, quality or price by leveraging access to local network rates. The MSP may offer users the capability to have multiple MSISDNs such that the user can have MSISDN_X for country X and MSISDN_Y for country Y therefore allowing both inbound and outbound calls to be based on local rates. In addition, the MSP may provide a call-routing service to allow users to receive calls on MSISDN_X while in country Y.

12.19 In order to deliver the service the MSP may deploy a solution containing the following high level components:

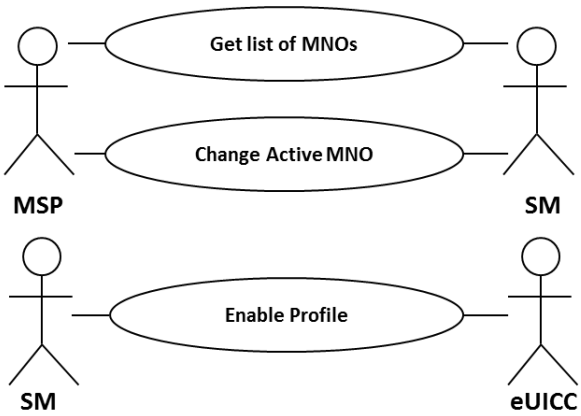
- MVNO platform consisting of mobile core and BSS capability
- MVNO wholesale agreements signed with local MNO partners in each operational country; one or many per country
- A subscription manager capable of downloading profiles for each of the MSP's wholesale network deals
- Ownership of number ranges (IMSI/MSISDN) within each of the countries managed in accordance with regional authority
- MNP platform in each region complying with the local processes and requirements of that country

12.20 The MSP may offer the following products a) SIM-only purchase b) SIM plus subsidised device. For the second option the SIM may be embedded in the device.

Consumer dynamically swaps as an alternative to Roaming

12.21 This section details the scenario where a consumer is dynamically swapping between IMSIs as an alternative to roaming.

Figure 38:Consumer Scenario 3: "Swapping – Dynamic"



Consumer scenario 3	Consumer dynamically swaps as an alternative to Roaming
Scenario	A user has previously subscribed to an MSP in country X and has a device provisioned with a profile to access the MSP's services. The user travels abroad to country Y. The eUICC dynamically swaps to a local profile as an alternative to international roaming.
Pre-Condition	User has purchased a device provisioned with a profile for the MSP and has a MSISDN for country X.
Post-Condition	User has a local MSISDN allocated for country Y and can receive calls on both home and international MSISDNs.
Consumer Scenario Steps	
1	The device will be initially provisioned to the MSP's service in country X.
2	The user switches on device which initiates full provisioning of the subscription. The eUICC will now be fully provisioned and credentials exchanged with the MSP. The user now has a fully assigned IMSI/MSISDN and the user is provisioned on the MSP MVNO BSS stack. If the user has a previous MSISDN from a Service Provider they can elect to Port this number to this subscription
3	User arrives at airport in country Y and switches on device. The MSP's HLR detects the SIM is outside home region (via the MCC). The MSP's HLR will determine whether the device should use a local service
4	The MSP automatically initiates a subscription manager session to check whether the eUICC already has a profile for the visited country (as opposed to user activation in previous use case). If a suitable profile is available on the eUICC, the process skips to step 6.
5	New profile is downloaded to eUICC using GSMA Use Case F2A – download additional profile. New profile is loaded
6	Subscription is switched using GSMA Use Case F5 – MNO subscription swap
7	Finally, the MSP HLR is configured such that incoming calls are routed and number translations are set as appropriate depending on call scenario (these are detailed below). The user may receive an SMS to welcome them to the country and provide user with local MSISDN which can be shared with local contacts.

12.22 Note that the use of roaming as the trigger in the above section is used for illustrative purposes. The trigger to swap between networks could be based on other factors as determined by the MSP's business logic, e.g. coverage, network quality, wholesale price.

Calling Scenarios

12.23 In this section, a number of calling scenarios are described, showing how a MSP may allow users to maintain multiple MSISDNs and IMSI profiles to receive calls on multiple MSISDNs as an alternative to roaming.

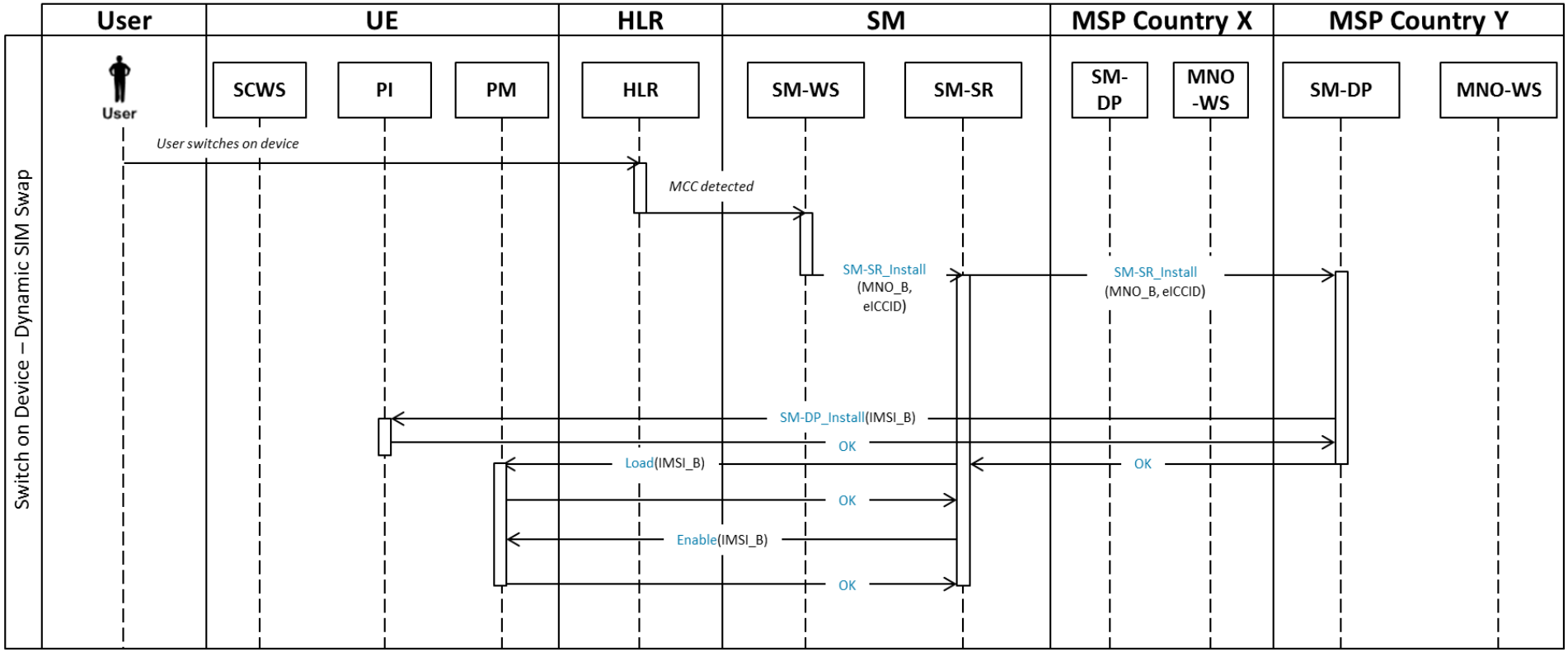
Call Scenario	High Level description

Petitioner Samsung Ex-1027, 0075

User makes call back to home country	When a user makes a call back to their home country from abroad the call is set-up via the local wholesale MNO provider to the MSP. The MSP detects that the call is destined for the home country and ensures that the CLI presented is the user's home MSISDN. The call is routed back through the MSP's global network to the home country.
User makes local call	When a user makes a call to a local number, the call is set up via the local wholesale MNO to the MSP. MSP detects that the call is local and routes call out as appropriate. The CLI presented will be the local country MSISDN.
User receives call from home country	If a user is called by a home country contact on their home country MSISDN the call is routed to the MSP network. The MSP detects that the user is abroad in another country and trunks the call to that country using the consumers "roamed" IMSI and the user connects the call by accepting the call.
User receives call from local number	When a user is called by a local contact on their local MSISDN; the call is routed to the user on their local IMSI via the MSP.

Petitioner Samsung Ex-1027, 0076

Figure 39: Sequence Diagram for Consumer Scenario 3 - Dynamic SIM Swapping



Petitioner Samsung Ex-1027, 0077

csmg
A TMNG Global Company

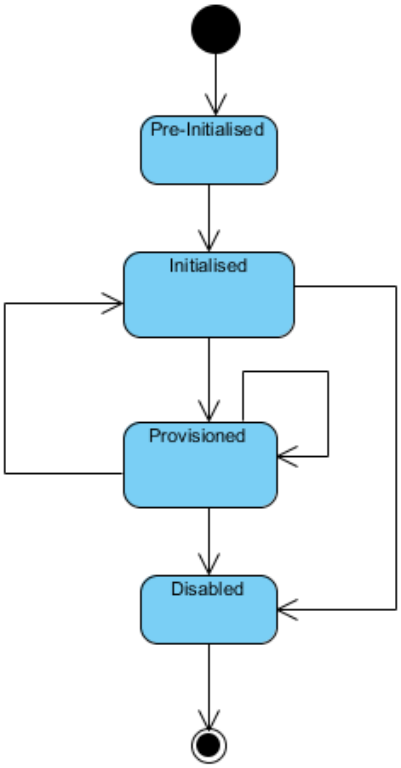
State Models

12.24 Throughout this Annex the transition state of eUICC and MNO are referenced within the use cases, the purpose of this section is to clarify and elaborate the meaning of these transition states. Ref[1] Section 3.2 presents a suggested eUICC State Transition diagram. This document further elaborates on this diagram, specifically with respect to the "provisioned" state. It takes into account that there may be multiple profiles available on the eUICC (one active and one or more inactive) and shows how these correlate to the state diagrams on MNO systems.

Ref[1] eUICC State Model

12.25 This is the eUICC state model presented in Ref[1]. It is replicated below for reference.

Figure 40: eUICC State Transition Model from Ref[1]



eUICC State		
No.	**State**	**Description**
1	Pre-Initialization	Manufactured but no credentials stored. In this state, physical presence is required to determine whether an eUICC is genuine.
2	Initialized	Initial credentials (at minimum, eUICC credentials) stored. eUICC can connect to server for purposes of further configuration in an un-trusted environment

3	Provisioned	Valid Home MNO credentials stored. eUICC has an active profile for the MNO, which is expected to enable operational connection to the network. During the transition from one MNO to another, the eUICC may move from “provisioned” state associated with one MNO to “provisioned” state with the other without going back to the “initialized” state. Note: In the situation where the subscription associated with the eUICC has been deactivated in the network, the eUICC will still be in the “provisioned” state.
4	Disabled	Presents no valid MNO credentials, but some eUICC credentials may stay valid (such as the eICCID). This state will not allow device to attach to a mobile network, since it does not have an active profile and cannot acquire one. It is thus considered to be “end of life”. The eUICC should have the capability to enter the Disabled state if removed from the device in which it was embedded. {Note: the request to go in this state has to be authenticated in order to prevent Denial Of Service attack.}

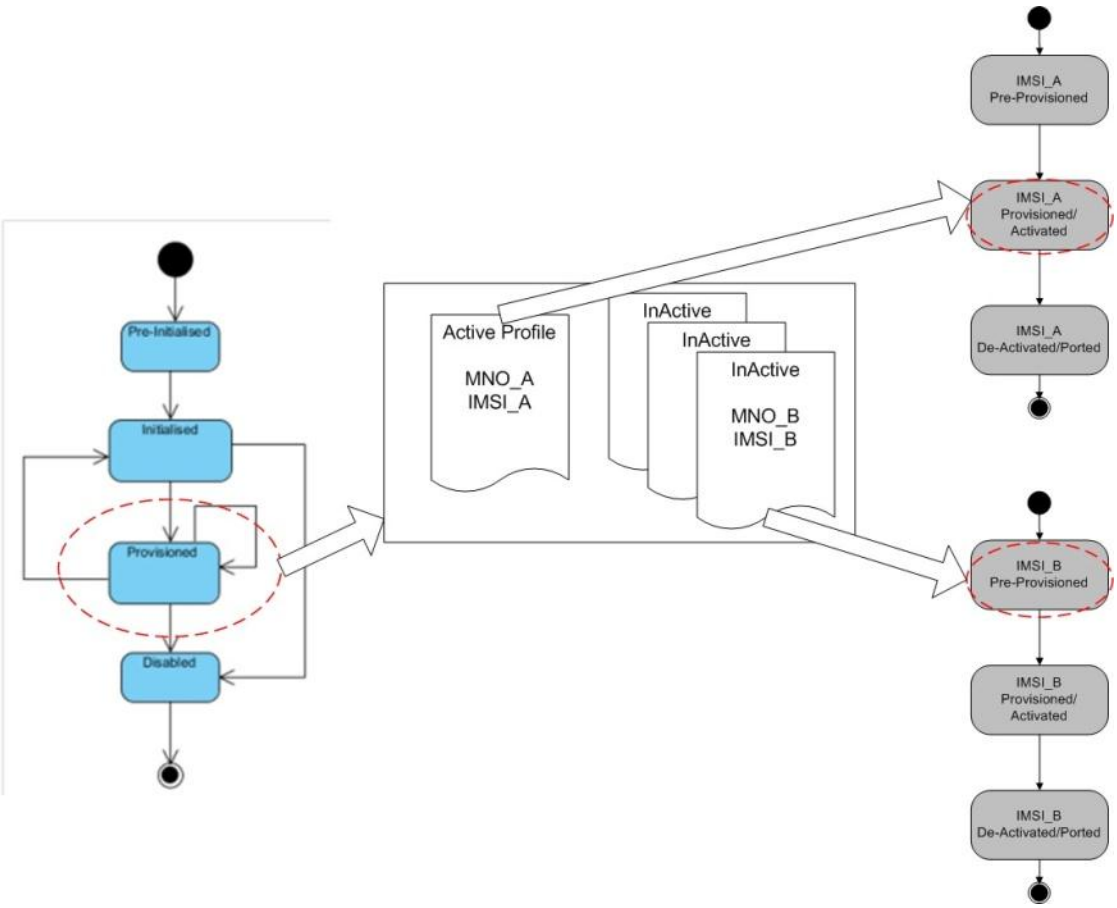
Petitioner Samsung Ex-1027, 0079

Elaborated eUICC/MNO State Models

12.26 In this section, we expand on the reference eUICC state model architecture to show how it can accommodate multiple profiles. In addition, we show how these correlate to the state models that exist on MNO systems.

12.27 Figure 38 highlights an eUICC in the "Provisioned" state with two IMSI profiles, each of the subscriptions associated with these profiles also has a transition state on their respective MNOs.

Figure 41: State Transition of eUICC and MNOs



User Downloads Second Profile

12.28 In the first instance, user has subscription with MNO_A and downloads an additional profile from MNO (MNO_B) as outlined in GSMA Use Cases F2A. The user has not yet fully activated a subscription account with MNO_B. This can be represented as the following status.

- eUICC Profile Active: MNO_A/IMSI_A
- eUICC Profile Inactive: MNO_B/IMSI_B

- MNO_A Profile IMSI_A: Provisioned/MSISDN_A
- MNO_B Profile IMSI_B: Pre-provisioned/MSISDN_B

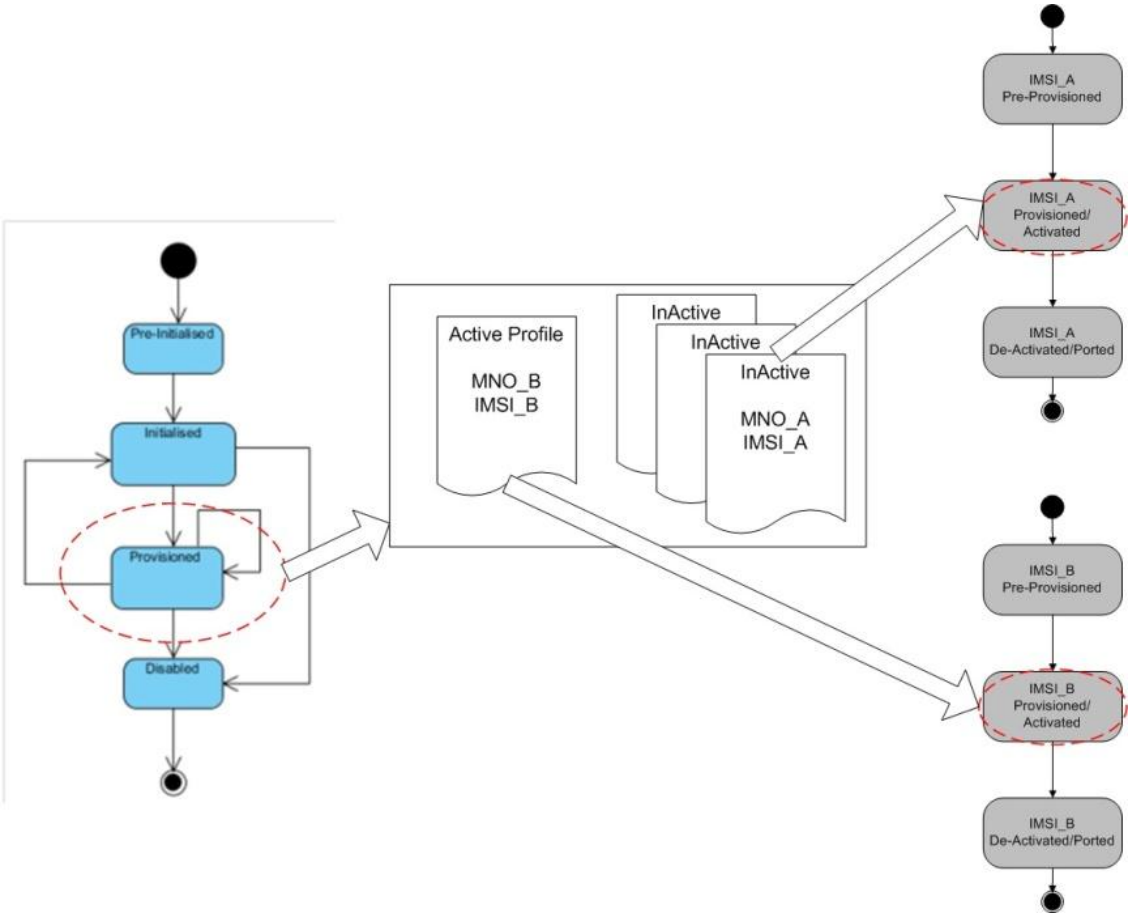
User "Swaps"

12.29 In Figure 41 below, the user has performed a swap (GSMA Use Case F5) and MNO_B profile is now active and MNO_A profile inactive. The user's MNO account has also been activated (Billing, CRM etc) i.e. the user has two subscriptions active on MNO systems and hence two MSISDNs. The status of the eUICC is therefore:

- eUICC Profile Active: MNO_B/IMSI_B
- eUICC Profile Inactive: MNO_A/IMSI_A

- MNO_A Profile IMSI_A: Provisioned/MSISDN_A
- MNO_B Profile IMSI_B: Provisioned/MSISDN_B

Figure 42: State Transition of eUICC and MNOs



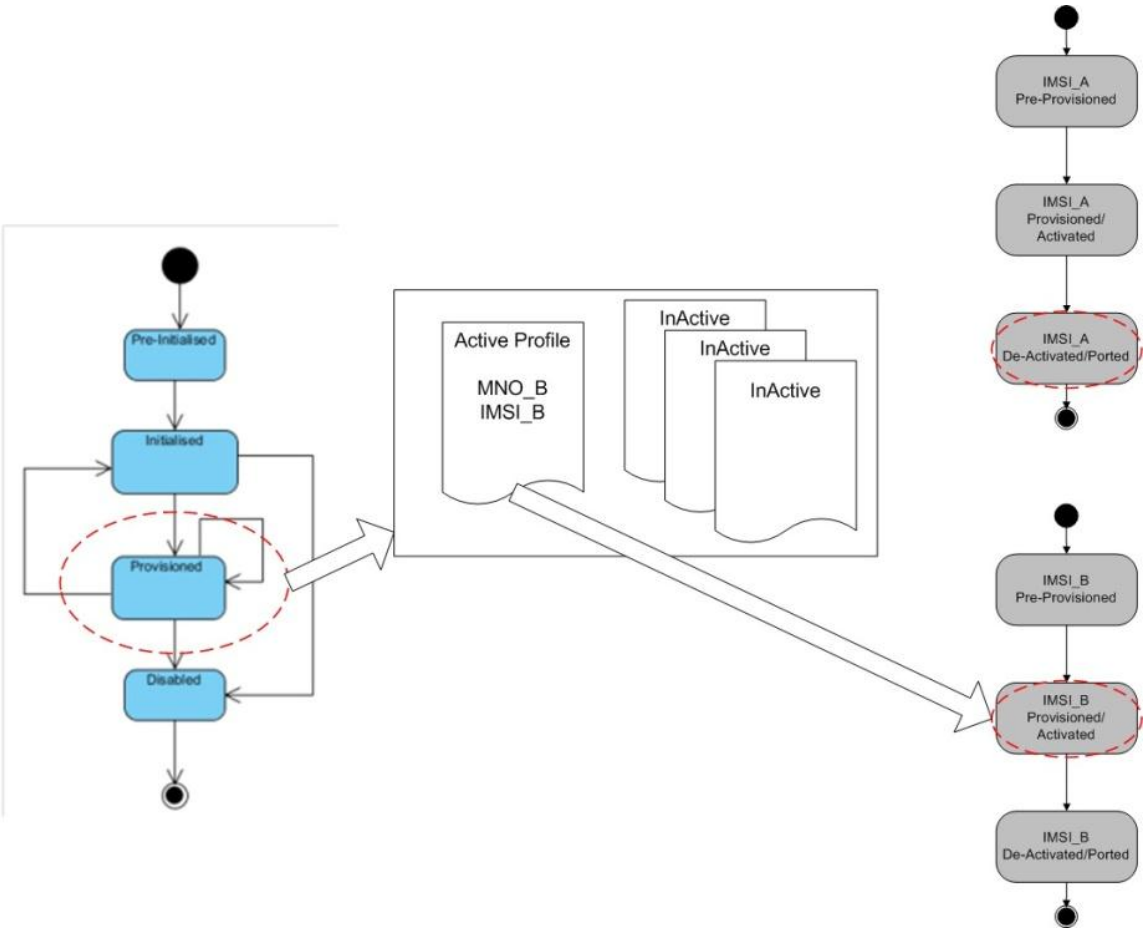
User "Ports"

12.30 User has decided to make MNO_B their main account through porting the MSISDN from MNO_A to MNO_B, the MNO_A account will now be de-activated and deleted from the eUICC. After the port, the status is as follows.

- eUICC Profile Active: MNO_B/IMSI_B
- eUICC Profile Inactive: Null

- MNO_A Profile IMSI_A: De-Activated
- MNO_B Profile IMSI_B: Provisioned/MSISDN_A

Figure 43: State Transition of eUICC and MNOs



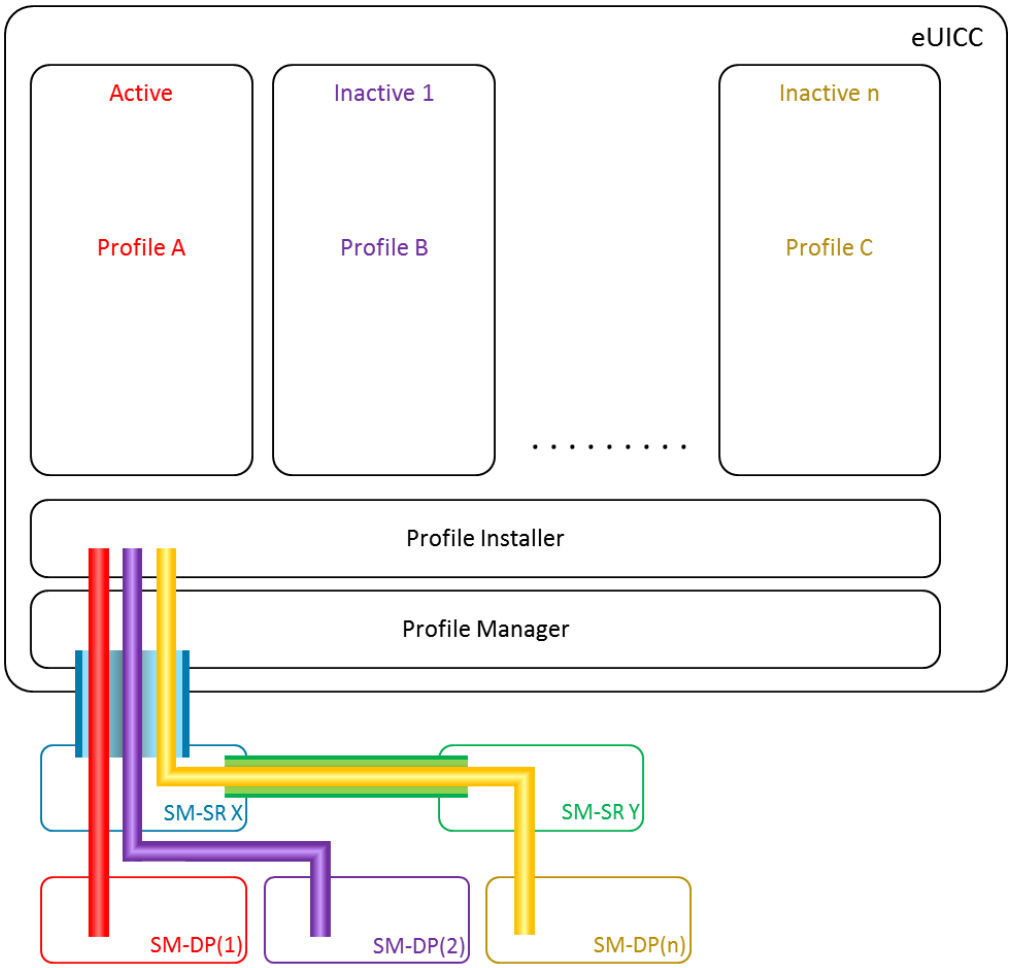
Reference Architectures

12.31 This section presents some reference architectures which further elaborate how an eUICC ecosystem might look.

Multiple SM-DP Connectivity

12.32 Within this document (See Consumer Scenario 2 and 3 and use case F2A) an assumption is made that a mechanism will be provided allowing a device to connect to any available MNO (home country or abroad) via their eUICC subscription manager. Ref[2] Annex C (reproduced as figure 43) presents a logical eUICC architecture with connectivity between eUICC, MNO, SM-SR and multiple SM-DPs.

Figure 44: Logical eUICC Architecture



12.33 It is assumed that Subscription Managers are defined such that they can be federated, i.e. the eUICC home SM-SR can also act as a proxy to allow connection to SM-DPs attached to other SM-SRs. We understand that this issue is being considered by ETSI.

Petitioner Samsung Ex-1027, 0083

13. Annex 2: Alternative Technologies to eUICC

13.1 A number of patents show how reprogrammable SIM technology may potentially evolve to encompass consumer handset applications. These patents show how the internal architecture and ecosystem may be impacted in the future. These include:

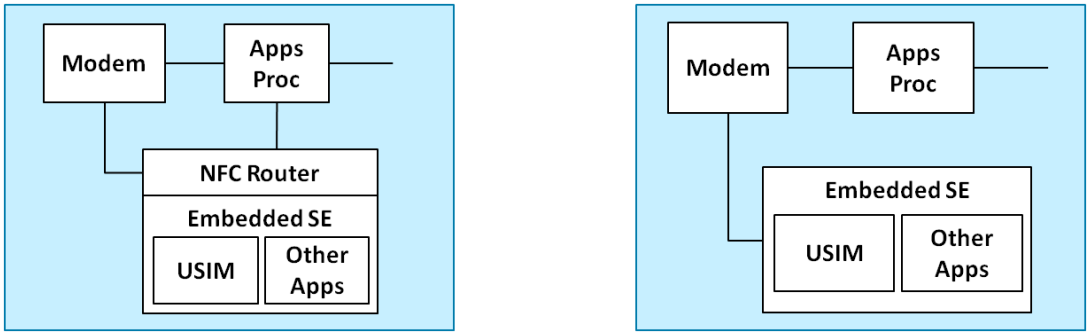
- Apple Virtual SIM patent: Potentially housing the reprogrammable SIM in a secure element used for other services (e.g. NFC).
- Truphone Patent: A system that would allow consumers to easily switch networks and download local subscription profiles when they are abroad.
- Apple and Google Dynamic Switching Patents: A system that would allow consumers to optimise their network selection based on cost, coverage and quality.

13.2 In addition there are examples that show how a virtualised SIM might work. This concept has been raised by Qualcomm in their "Virtual SIM" patent, and may potentially be enabled by advances in security technology such as the implementation of "Trusted Execution Environments". However, the GSMA has criticised the concept of "Soft SIMs" (e.g. a SIM which is located on the handset memory) as being insecure.

Apple Virtual SIM Patent

13.3 Apple's "Virtual SIM" is located on the embedded secure element of a connected device.

Figure 45: Apple Virtual SIM Architecture (with and without NFC Components)



13.4 The architecture is based on GlobalPlatform standards and a Java-based UICC, with firewalled separation of security domains (issuer and multiple secondary domains), similar to the reprogrammable SIM architecture outlined in Section 5.

13.5 The embedded secure element (SE) on the device holds the SIM application, which is provisioned by a Trusted Service Manager (TSM). Architectures are specified that integrate the secure element with or without NFC components such as the NFC router.

13.6 Although developments in eUICC standardisation may make such an implementation more feasible, this solution may require the MNOs to share certain information with the handset vendors, such as the SIM profiles (IMSIs, KIs and algorithms), which MNOs may not want to do for commercial or security reasons.

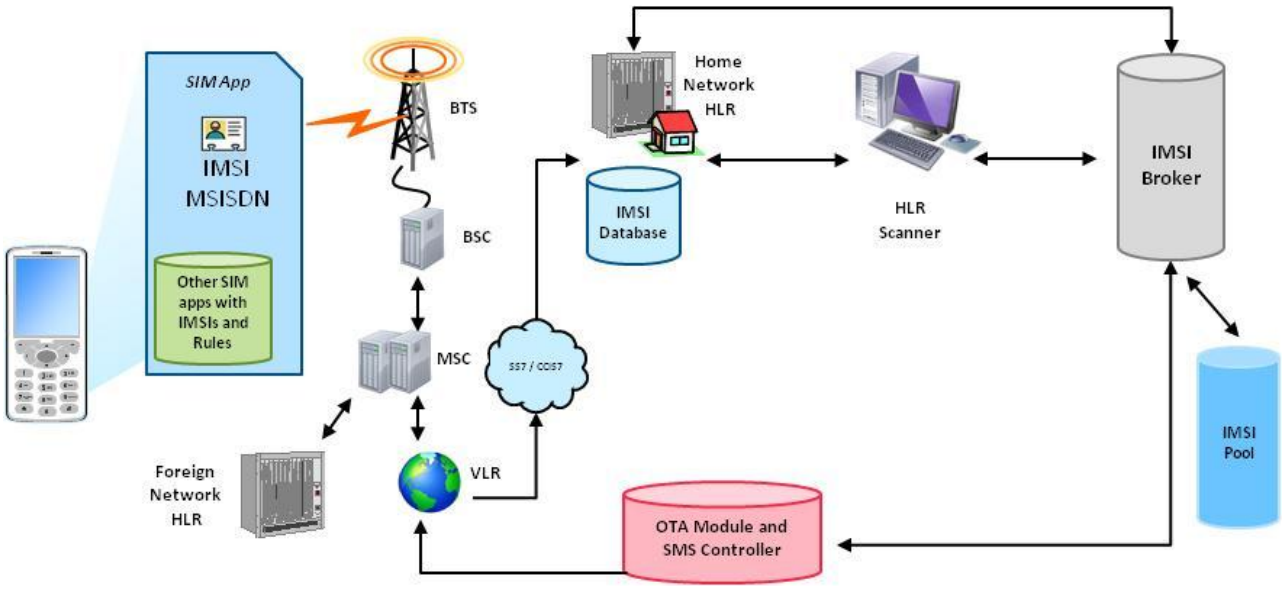
Petitioner Samsung Ex-1027, 0084

Truphone Patent

13.7 The Truphone Patent shows how an international reprogrammable SIM application might work. As discussed, one of the key benefits of the reprogrammable SIM is to enable customers to download a new IMSI if they are in a foreign country in order to avoid roaming rates. The current requirements document for the reprogrammable SIM being considered by ETSI does not outline a system which would allow customers to do this in a dynamic and intelligent manner.

13.8 Truphone have patented a means for dynamically issuing IMSIs to roaming handsets. The patent document describes an architecture for achieving this, which requires the presence of several new components, including an IMSI broker (and associated IMSI pool) and an HLR scanner.

Figure 46: Truphone Patent Architecture



13.9 The architecture relies on a new role called the IMSI broker, that a) identifies the need for a local IMSI when a subscriber is roaming, b) determines whether a new IMSI needs to be provisioned or if a previously provisioned IMSI can be reactivated, and c) initiates the provisioning of a local IMSI to the roaming reprogrammable SIM.

13.10 In the above diagram, the roaming handset connects to the VLR and sends a location update to the user's HLR. The HLR verifies the customer's identity through the SIM authentication mechanism. Once authenticated the user will typically be added to the VLR and begin 'roaming.'

13.11 In the Truphone patent, an HLR scanner is used to scan the service provider's HLR log files and from this is able to determine that a customer has begun roaming. The IMSI broker then verifies if the customer's device has an IMSI from the visited country. If not, the IMSI broker has a pool of local IMSI packages it can draw from to send OTA to the multi-IMSI SIM app in the handset.

13.12 The package is then installed and the device then refreshes and the new local IMSI and MSISDN are loaded. The original VLR and HLR recognises the device as switched off once the

new IMSI is loaded, and reroutes all calls to voicemail. The device then reregisters with the local network and the user enjoys the benefits of a local subscription.

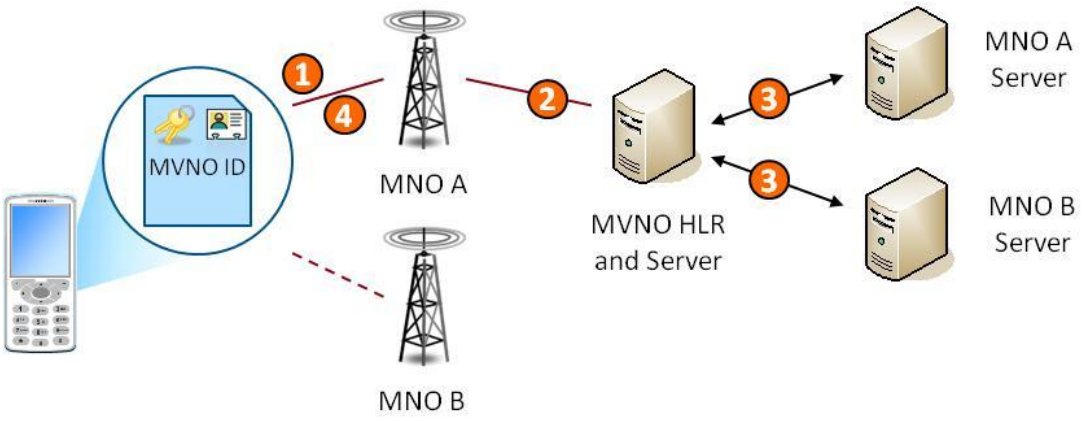
13.13 With further system integration, a temporary forwarding mechanism can exist that reroutes calls to the new MSISDN. This is not specified in the patent, however.

13.14 The standardisation of the eUICC provides a key component of the technology for the Truphone patent to be implemented. However, significant commercial barriers remain; it may prove challenging for roaming SIM providers to develop the required MVNO agreements with MNOs for a "roaming killer" solution.

Google and Apple Patents

13.15 Although not technically based on reprogrammable SIMs, both Google and Apple have produced patents that show how devices may be able to switch networks dynamically, potentially within the same country. Both patents suggest an intermediary that accepts bids from MNOs and sets up the handset dynamically with the MNO providing the best cost and/or coverage at the time.

Figure 47: Dynamic Switching Architecture



13.16 Essentially, these patents use the above architecture, with the following simplified steps followed to enable a switching of networks:

1. Handset uses MNO A network to send location or status update to MVNO HLR.
2. MVNO SIM authenticates with MVNO HLR.
3. MVNO Server requests bids based on location of SIM from MNO A and MNO B.
4. MVNO Server determines the best network for customer to be on, from a coverage or cost perspective and sends network preference to effect network steering, via MNO A's network.

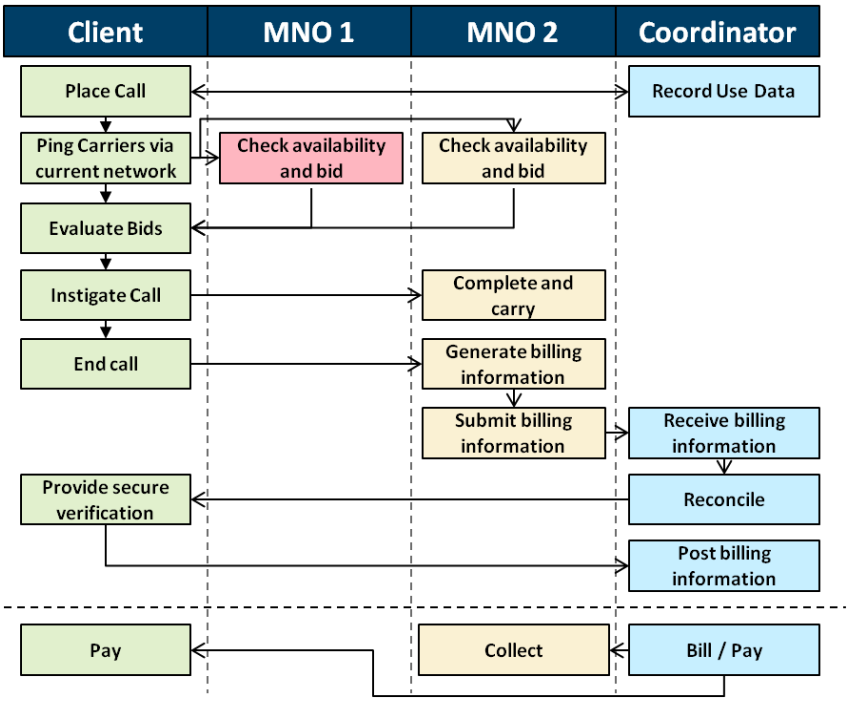
Google Patent

13.17 This patent enables the end-user to connect to different networks based on different requirements (e.g. coverage or cost). It specifies a system where a coordinator acts as a full

or partial intermediary between the MNOs and the client (end-user) when the client requires connectivity to place a call.

13.18 It does this by setting up a dynamic auction system that encourages MNOs to bid against one another for service from the end-user; an application on the device pings carriers' bid servers via the current network.

Figure 48: Google Flexible Communications System Bidding Process



13.19 The handset pings the carriers and requests bids for the best rates at which to place a call; after the call is completed, the coordinator verifies the usage and bills the end-user. In turn the MNO who carried the call, bills the co-ordinator.

13.20 For this model to work, MNOs will have to accept to provide wholesale connectivity to or through the coordinator (which may have to be formed as an MVNO). This may be challenging as many MNOs may see no benefit to themselves in losing the customer relationship.

Apple Patent

13.21 Apple's Dynamic Carrier patent is very similar to Google's patent but is specific about using an MVNO to enable network switching.

13.22 In this patent, the device is pre-programmed with an identifier (i.e. IMSI) associated with the Apple MVNO; the MVNO has an HLR, which is used to recognise the identity and needs of the end-user and initiate the bid process with multiple partner MNOs.

13.23 The handset intermittently roams on different networks as a result of the auction process and the end user benefits through cost savings and improved coverage.

Petitioner Samsung Ex-1027, 0087

13.24 In order to implement these systems, a few components are required. Firstly, an intermediary will need to be set up with an HLR and associated components (such as an AuC) to be able to register the subscriber on the network.

13.25 Then, the intermediary will need to be able to own the customer relationship, including the functions such as billing, troubleshooting, device management etc.

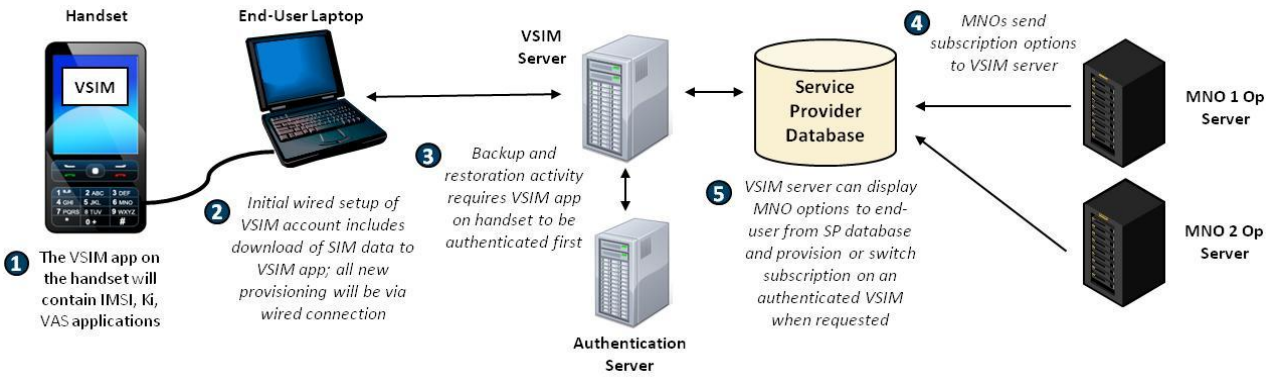
13.26 Lastly, a server that runs the auction process is required if the dynamic auction business model is used. This server will need to be integrated with the backend of each MNO it has a relationship with so that bids can be dynamically submitted and processed based on the provided cost and coverage information.

13.27 A key difference between these patents and a reprogrammable SIM implementation is that in the Apple and Google patents, the end-user maintains a single profile and switches between networks based on roaming agreements and network steering preferences. With an eUICC, an end-user could instead have multiple network operator profiles on the SIM, and swap between these profiles in order to switch between networks. In this case, a third party "co-ordinator" could still potentially manage the swapping between profiles.

Qualcomm Patent

13.28 Qualcomm's Virtual SIM is capable of reprogrammable SIM functionality, though it is positioned primarily as a subscription identity backup concept.

Figure 49: Qualcomm Patent Architecture



13.29 The Qualcomm Virtual SIM architecture enables a user to backup SIM information (e.g. the address book, messages, applications, etc.) to a VSIM server for later retrieval. The VSIM takes the place of a SIM card in GSM handsets, containing similar information used to authenticate with networks and store usage and provider data.

13.30 In operation, a mobile recalls the network provisioning information stored in the memory unit (instead of a SIM card) in order to connect to the network. The solution essentially allows consumers to download this info into a new SIM card when they change SIMs or if they lose their mobile device and replace it with a new one.

13.31 Interestingly, a use case is also mentioned where the VSIM server can be used to provision a new handset, or change network services, which would essentially make this a "soft SIM" solution with the VSIM service provider acts as the SM-SR (and possibly SM-DP).

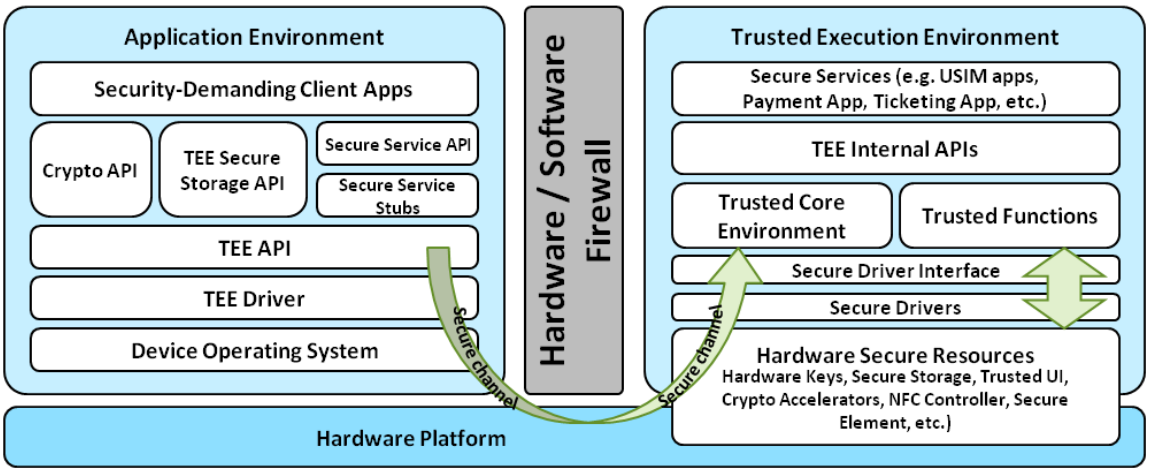
13.32 There is no real mention of security in the patent filing and functional aspects of who does what are not clearly defined.

Trusted Execution Environment

13.33 A Trusted Execution Environment (TEE) enhances the security of a reprogrammable SIM application running on the handset memory or a separate secure element. While the TEE could conceivably be used to securely store the SIM application/s (e.g. a "soft SIM" implementation), GSMA members have previously criticised the TEE as being insecure and not suitable for secure NFC and reprogrammable SIM.

13.34 To this end, none of the TEE vendors have explicitly stated that they intend to put forward TEE as a possible option for implementing reprogrammable SIM functionality.

Figure 50: Application and Trusted Execution Environments



13.35 The Trusted Execution Environment (TEE) itself is a technology offering tamper-proof, secure execution of code and also controls access to peripherals and/or data storage within a mobile device. In its current form, the TEE does not replace existing hardware security, as it is primarily a way of more deeply integrating software and hardware security.

13.36 However, one of the benefits of the TEE is that it could make SIM applications more secure, preventing the reading of credentials that might allow cloning. To do this, TEE uses secure drivers and interfaces that link hardware security features (such as secure elements which may be the SIM or an embedded chip) to the TEE environment. Internal APIs allow the trusted functions (e.g. keyboard input) to securely communicate with secure services (e.g. payment and ticketing applications).

13.37 Examples of TEE are ARM's TrustZone, GlobalPlatform's Device/Small Terminal Interoperability Platform (STIP), Intel's Trusted Execution Technology (TXT), and ST-Ericsson/Oberthur's TEE.

Petitioner Samsung Ex-1027, 0089

14. Annex 3: Standards Related to Reprogrammable SIMs

SIM Standards

14.1 There are a number of standards bodies and industry associations involved in developing standards and guidelines for SIM and reprogrammable SIM. The majority of standards for SIM technology have already been determined but how these will develop to incorporate reprogrammable SIM technology is in the early stages of standardisation.

Figure 51: Standards Related to SIM Technologies

Organisation	Standard	Description
ETSI	ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications"	Specifies the structure of Secured Packets for different transport and security mechanisms
ETSI	ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics"	Defines a generic Terminal/Integrated Circuit Card (ICC) interface; its aim is to ensure interoperability between an ICC and a terminal independently of the respective manufacturer, card issuer or operator
ETSI	ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT)"	Defines the interface between the UICC and the terminal, and mandatory terminal procedures, specifically for "NAA Card Application Toolkit"
ETSI	ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (API) for Java Card (TM)".	Defines the Application Programming Interface and Loader Requirements internal to the UICC
ETSI	ETSI TS 102 588: "Smart Cards; Application invocation API by a UICC webserver for Java Card platform"	Defines an API that allows a UICC based SCWS defined by OMA to forward Http requests to an Applet and to receive the response from the Applet
ETSI	ETSI TS 102 240/1 (Rel-9): UICC Java Card™ API - Stage 1 and 2	Defines the service description of the UICC Application Programming Interface (UICC API) internal to the UICC
ETSI	ETSI TS 102 230 (Rel-8): Smart Cards: UICC-Terminal interface; Physical, electrical and logical test specification	Specifies the tests of physical characteristics of the UICC; the electrical interface between the UICC and the Terminal; the initial communication establishment and the transport protocols; the application independent procedures
[redacted]		

Petitioner Samsung Ex-1027, 0090

3GPP	3GPP TS 23.040 (Rel-6): Technical realization of the Short Message Service (SMS)	Describes the Short Message Service (SMS) for GSM/UMTS networks
3GPP	3GPP TS 23.048 (Rel-5): Security Mechanisms for the (U)SIM application toolkit; Stage 2	Specifies the structure of the Secured Packets in a general format and in implementations using SMS Point to Point and SMS Cell Broadcast
3GPP	3GPP TS 31 102 (Rel 10): Characteristics of the Universal SIM (USIM) application	Defines the USIM application for 3GPP telecom network operation
3GPP	3GPP TS 31 111 (Rel 10): Universal SIM Application Toolkit (USAT)	Defines the interface between the UICC and the Mobile Equipment (ME), and mandatory ME procedures, specifically for "USIM Application Toolkit".
3GPP	3GPP TS 31 130 (Rel 10): (U)SIM Application Programming Interface (API); (U)SIM API for Java Card	Defines the Application Programming Interface for 2G/3G networks based on the "UICC API for Java Card"
3GPP	3GPP TS 33 105 (Rel 10): 3G Security; Cryptographic algorithm requirements	Specification that constitutes a requirements specification for the security functions which may be used to provide network access security features
3GPP	3GPP TS 43 019 (Rel 6): SIM API for Java Card; Stage 2	Describes the behaviour and limitations of the APIs used in 3G environment and description of 2G APIs and 3G APIs interworking
3GPP	3GPP TS 51 011 (Rel 4): Specification of the SIM-ME interface	Defines the interface between the SIM and the Mobile Equipment for use during the network operation phase of GSM as well as those aspects of the internal organization of the SIM which are related to the network operation phase
3GPP	3GPP TS 51 014 (Rel 4): Specification of the SIM Application Toolkit for the SIM - ME interface	Defines the interface between the SIM and the Mobile Equipment, and mandatory ME procedures, specifically for "SIM Application Toolkit".
[redacted]		
GlobalPlatform	"GlobalPlatform Card Specification", Version 2.2	Technical documentation relating to the deployment and management of multiple embedded applications on secure chip technology

GlobalPlatform	"GlobalPlatform Card UICC Configuration", Version 1.0	Implementation guide for deploying Card Specification v2.2 within the mobile services sector and managing the secure delivery over-the-air of new services
[redacted]		
Java	Java Card 3.0.1 API Specification	Defines a set of classes upon which Java Card technology-based applets can be constructed
Java	Java Card 3.0.1 Runtime Environment Specification	This specification describes the runtime environment (RE) for the Classic Edition of the Java Card Platform
Java	Java Card 3.0.1 VM Architecture Specification	This specification describes the virtual machine for the Classic Edition of the Java Card Platform
Java	JCP – JSR-000177: Security and Trust Services API for J2ME	Specify a collection of APIs that provides security and trust services by integrating a Security Element (SE)
[redacted]		
Others	SIMalliance Open Mobile API, Release v1.01	The API specified in this document enables mobile applications to have access to different Secure Elements in a Mobile such as SIMs or embedded SEs

Reprogrammable SIM-specific Documents

14.2 The GSMA and its members have published documents in recent months that seek to establish the fundamental requirements of a reprogrammable SIM solution (particularly for M2M applications). It is likely that these will feed into the final standards for reprogrammable SIM being developed by ETSI in 2012.

14.3 The documents cover the steps required for reprogrammable SIM-related processes such as provisioning and re-provisioning, as well as the shape the reprogrammable SIM ecosystem should take and the relationships between various roles.

Figure 52: Documents Related to Reprogrammable SIM Technologies

Organisation	Standard	Description
GSMA	SCPREQ(11)0113, "Embedded UICC – A high level remote provisioning architecture"	Key architecture principles, GSMA's eSIM remote provisioning eco-system architecture and what GSMA expects to be standardised in ETSI

GSMA	SCPREQ(11)0118, "GSMA and SIMalliance Collaboration on eUICC Protection Profile"	Liaison statement about GSMA & SIMalliance work to enable necessary trust relationships within the ecosystem by means of certification processes; addresses GSMA eUICC requirements not deemed to be in the scope of standardization
GSMA	"Embedded SIM Task Force Requirements and Use Cases"	Document that covers embedded SIM requirements and use cases, focused on M2M applications
Others	SCPREQ(11)0064, "High Level Components in the eUICC – First provisioning"; Vodafone Group;	This discussion document exposes what the eUICC may contain. Also it presents a high level view of how the first provisioning of operational/provisioning profiles and delivery may take place

Petitioner Samsung Ex-1027, 0093

15. Annex 4: Glossary

Abbreviation	Definition
3G	Third Generation
3GPP	Third Generation Partnership Program
AuC	Authentication Centre
BTS	Base Transmission Station
CDMA	Code Division Multiple Access
CSIM	CDMA 2000 Subscriber Identity Module (application)
DF	Dedicated File
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
eID	Electronic IDentification
ETSI	European Telecommunications Standards Institute
GSMA	Global System for Mobile Communications Association
HLR	Home Location Register
HSS	Home Subscriber Server
ICCID	Integrated Circuit Card IDentifier
IMS	Internet Protocol Multimedia SubSystem
IMSI	International Mobile Subscriber Identity
ISIM	IMS Services Identity Module
ITU - TSB	International Telecommunications Union – Telecommunication Standardisation Bureau
JCVM	Java Card Virtual Machine
Kc	Ciphering Key
LOCI	LOCation Information
LTE	Long Term Evolution
M2M	Machine-to-Machine
MCP	Mobile Communications Provider
MF	Master File
MFF	M2M Form Factor
MNO	Mobile Network Operator
MNP	Mobile Number Portability
MSC	Mobile Switching Centre
MSISDN	Mobile Station International ISDN Number

Petitioner Samsung Ex-1027, 0094

NAA	Network Access Application
NFC	Near Field Communications
OS	Operating System
OTA	Over The Air
PCF	Policy Control Function
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephony Network
RAM	Remote Application Management
RFM	Remote File Management
SCWS	Smart Card Web Server
SIM	Subscriber Identity Module
SM	Subscription Manager
SM-DP	Subscription Manager – Data Preparation
SM-SR	Subscription Manager – Secure Routing
TMSI	Temporary Mobile Subscriber Identity
UICC	Universal Integrated Circuit Chip
UMTS	Universal Mobile Telephony Telecommunications System
USIM	UMTS Subscriber Identity Module
VLR	Visitor Location Register

Petitioner Samsung Ex-1027, 0095