Embedded SIM Task Force Requirements and Use Cases

1.0

21 Feb 2011

Security Classification – NON CONFIDENTIAL WHITE PAPER

Table of Contents

1 Introduction 3
- **1.1** Overview 3
- **1.2** Problem Statement 3
- **1.3** Approval 4
- **1.4** Scope 4
- **1.5** Definition of Terms 4
- **1.6** Interchange of terms: UICC / USIM 6
- **1.7** Document Cross-References 7

2 Assumptions & Principles 8
- **2.1** Assumptions 8
- **2.2** Principles 9

3 eUICC State Model 11
- **3.1** Valid eUICC States 11
- **3.2** State Transition Diagram 12

4 Role and Trust Definitions 13
- **4.1** Role Definitions 13
- **4.2** Trust Relationships 13
- **4.3** eUICC Certification 14

5 Use Cases 16
- **5.1** Vertical Use Cases 16
- **5.1.1** Overview of the use cases 16
- **5.1.2** UC1: Provisioning of multiple M2M subscriptions 16
- **5.1.3** UC2: Provision of first subscription with a new connected device 18
- **5.1.4** UC3: Change of subscription for a device 19
- **5.1.5** UC4: Termination of a subscription for a consumer device 19
- **5.1.6** UC5: Subscriber transfers subscription between devices 21
- **5.2** Functional Use Cases 22

6 Processes 23
- **6.1** UC1: Processes for (multiple) M2M use cases 23
- **6.1.1** UC1 a) Provisioning an M2M subscription on a new device 23
- **6.1.2** UC1 b) Process for changing a M2M subscription 24
- **6.1.3** UC1 c) Process for fallback to a previous subscription 25
- **6.2** UC2: Provision of first subscription with new device 25
- **6.2.1** UC2 a) Provision of device consumer selects MNO 25
- **6.2.2** UC2 b) Provision of enterprise devices 26
- **6.2.3** UC2 c) Device with first subscription pre-loaded 27
- **6.3** UC3: Change of Subscription for a Consumer Device 28
- **6.4** UC4: Termination of a Subscription for a Consumer Device 29
- **6.5** UC5: Subscriber transfers subscription between devices 30

7 Requirements 31
- **7.1** Lifecycle requirements table 31
- **7.2** Service Management Requirements Table 32
- **7.3** Communications Requirements Table 33
- **7.4** Robustness Requirements Table 33
- **7.5** Liability Requirements Table 33
- **7.6** Market Requirements table 34
- **7.7** Security requirements table 35
- **7.8** Certification Requirements Table 36

8 Ongoing Topics 37

9 Document Management 38

1 Introduction

1.1 Overview

The GSMA Embedded SIM Task Force created this document. It develops Use Cases and Requirements for the “enhanced, remote management” of a UICC, which is embedded in a communication device, i.e. where the UICC is not easily accessible and replaceable. This type of UICC is compatible with Machine-to-Machine (M2M) applications. The UICC may be embedded at the manufacturing site in advance depending on the country and network operator, and is compatible in a variety of end-user equipment. In these scenarios, there may be a requirement to change a subscription easily, this is currently achieved by physically changing the UICC.

The purpose for defining these requirements is to provide ease of use and deployment benefits for end users/consumers and thereby stimulate the M2M device sector. A further intent is to enable the creation of common standards and processes for remote management of subscriptions on UICCs, such that fragmentation across the industry is effectively discouraged and prevented.

The use cases will describe a technical solution for “enhanced remote management” for the future of embedded UICCs. This includes reusing established international standards to maximise acceptance worldwide.

1.2 Problem Statement

Since the inception of GSM, the UICC/SIM card has successfully provided Authentication and Authorisation capability to allow user devices access to networks. This illustrates users accepting the use of UICC/SIM cards to transfer their network subscriptions from one device to another. The creation of higher capacity cards in terms of memory and processing power, work is underway to increase the scope of the UICC card and to provide additional services supported by technologies such as Smart Card Web Server, InterChip USB, and Single Wire Protocol (NFC).

It is noted that new business models and usage scenarios, primarily driven by M2M, struggle when supported by the traditional UICC/SIM card. For example:

- By installing physical UICC/SIM cards, the user is connected to a specific network, as the card only provides access to one network. Should the user wish to (or need to) use another network, then they or the M2M service provider has to fit another card in his/her device.
- Changing UICC/SIM cards maybe problematic, noting that M2M equipment may be remotely located, and/or hermetically sealed. It should be noted that where the UICC/SIM is not intended to be sealed and inaccessible, the portability of traditional form factor UICC/SIM cards is perceived to be a user benefit.
- Non-standard provisioning and re-provisioning methods are being defined and used. These present security implications and a risk of fragmentation within the industry.

New remote provisioning / re-provisioning mechanisms are required to support the new business models and usage scenarios.

Fragmentation of solutions leads to additional complexity, further costs within the industry and inhibits user choice. To prevent fragmentation across the industry the new mechanisms should be standardised by appropriate Standards Developing Organisations. These should comply with and be auditable against relevant security standards.

The intention of this document is to enable the development of solutions combined with any appropriate standards necessary that will permit remote provisioning and remote re-provisioning of credentials to a UICC in a secure manner without necessarily having to transport the UICC back to a secured and accredited physical location.

1.3 Approval

This document has been approved by the GSMA Strategy Committee for submission to ETSI SCP.

1.4 Scope

The primary intention of the requirements expressed in this document and any solutions that meet them, is to facilitate the M2M and Embedded Mobile (see Definition of Terms) market segments.

The scope of solutions is intended to cover requirements for the complete provisioning ecosystem.

1.5 Definition of Terms

Note definitions taken from 3GPP 21.905 V10.2.0. Following the completion of a review, any duplicates with 3GPP 21.905 V10.2.0 shall be removed.

Term	Description
Administration Profile	Profile enabled to allow a recovery point during a transition should failure occur. This profile shall be able to coexist with an operational profile but shall not be used for purposes other than administration of the eUICC by the SM. .
Credentials	Combination of data required to provision a eUICC so that it can be authenticated by an MNO or other service provider e.g. a Subscription Manager. Such credentials may additionally support mutual authentication and confidential communications. MNO credentials may include algorithms, Ki/K, and IMSI stored within a network access application such as a SIM/USIM/ISIM. (Note: this definition covers neither contractual nor billing activities nor all aspects of the MNO's subscriber administration.)
CSIM	CDMA 2000 Application on UICC. An application residing on the UICC used for accessing CDMA network services.
Device/Terminal	Device, which is capable of providing access to 3GPP System services to users, either alone or in conjunction with an UICC. Can cover embedded modules and other device form factors.
Donor Operator	The operator/MNO whose credentials were active in the device, but are no longer active after the provisioning process.
Embedded Mobile or Embedded Device	Used to denote 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.
Embedded UICC (eUICC)	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. Performs the role of a traditional UICC. Term used for clarity within this document and does not necessarily introduce a new component. .
Embedded UICC (eUICC) Credentials	A set of information provided by the eUICC supplier to allow future provisioning of the eUICC. This shall contain at least the following: - A persistent identifier for the eUICC (see also ICCID). - A secure association between the persistent identifier and lifetime characteristics of the eUICC (e.g. Operating System version, cryptographic and downloading software) - A means for at least one Subscription Manager to authenticate the eUICC against this persistent identifier

	Any specific Subscription Manager will also need its own cryptographic keys to establish confidentiality and mutual authentication between the eUICC and the SM (see Credentials). Such credentials have to be securely delivered to a specific SM e.g. by the eUICC supplier, or by secure handover mechanisms between SMs.
EMP	GSMA Embedded Mobile Programme
first subscription	Subscription provided by an MNO used for operational purposes (network access providing connectivity to telecom and value added services) after issuance of the eUICC.
Form Factor	Manifestation of UICC. Specified in references 1 and 15.
Host Equipment	Equipment in which the module is inserted during assembly. Examples include: Meter, Car and Camera.
ICCID	Unique number for the UICC hardware that is stored on the UICC and – for a conventional UICC - also engraved upon it. Defined according to ITU-T recommendation E.118. Note: An example solution for the eUICC is to have an ICCID file that is associated with the current active MNO, but this may change if the active MNO changes. Regardless of solution, the eUICC shall also have a standardised unique persistent identifier. The numbering scheme used for this purpose should be encoded such that data about the eUICC can be derived in a similar manner to the existing E.118 scheme.
IMSI	International mobile subscriber identity (IMSI). Unique identifier owned and issued by Mobile operators to SIM applications to enable devices to attach to a network and use services.
Initial Credentials / Provisioned State	Either a first set of valid MNO credentials for immediate use or a set of credentials for a trusted service provider (Subscription Manager) who can then download selected MNO credentials.
ISIM	IMS Services Identity Module
M2M	Machine to Machine, normally applied to services such as Utility metering where no traditional user or user interface is provided. Such services are expected to operate stand-alone and physical access by MNOs and Service Providers is often limited.
Module	Form of device/terminal manufactured for embedding within larger host equipments.
MNP	Mobile Number Portability
NAA	Network Access Application
OTA	over the air
Operational Profile	Combination of MNO credentials, data and applications to be provisioned on to a eUICC. This may include MNO, third party and user applications and data. Only one operational profile can be active at any point in time.
Personalisation	The act of loading credentials onto a UICC/eUICC. For UICC typically undertaken in Personalisation centres (see Trusted Environment). Note: Provisioning and Personalisation have been used interchangeably in this document.
PIN	Locks the UICC and SIM applications until the correct code is entered. If the PIN is entered incorrectly 3 times in a row, the UICC will be blocked requiring a PUK.
Policy Control Function / PCF	A set of rules defined by the MNO that controls the usage of its own credentials. Policy Control consists of determination of the rules to apply and enforcement of those rules. Each MNO is responsible for its own rules, although an SM can execute these on a MNOs behalf. SM is responsible for enforcement on behalf of the MNO.
Protection Profile	Set of security and functional objectives, for the eUICC. To allow SMs to perform their function there needs to be alignment on common agreed protection profile(s) across MNOs. Note there may not be a single unique protection profile across all operators.
Provisioning	Within this document, provisioning typically refers to the loading of profiles, credentials, data and applications into a eUICC/USIM. This does not remove

	the need for 'classical' provisioning of network elements e.g. HLR and in general the requirements for provisioning of network elements is not described in this document. Note: Provisioning and Personalisation have been used interchangeably in this document.
provisioning subscription	The provisioning subscription enables a device access to a mobile network for the purpose of management of MNO subscriptions on the eUICC. An administration profile could be used for this purpose. Note: a provisioning subscription may not be required where provisioning is executed using an alternative access e.g. tethering or direct-wired access.
PUK	PIN Unblocking Key.
Recipient Operator	The operator/MNO whose credentials become active in the device after the provisioning process.
Services	Portfolio of choices offered by operators and service providers to a user, functionality offered to a user.
SIM	SIM application contains the unique identifier of the mobile user (IMSI), security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to and two passwords (PIN for usual use and PUK for unlocking)
SIM Portability	Ability to move UICC/USIM between devices
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorised to enjoy these services, and also to set the limits relative to the use that associated users make of these services
Subscription	Describes the commercial relationship between the subscriber and the service provider.
Subscription Manager(s) (SM)	Entity managing credentials and data on eUICCs on behalf of specific / multiple MNOs; as described in 4.1 (Roles and Trust definitions).
Trusted Environment	Environment specifically constructed for the personalisation of UICCs on behalf of MNOs. Should be certified by the GSMA SAS accreditation scheme plus additional MNO validation based on contractual relationships. {Note: eUICCs are expected to receive their Initial Credentials in a Trusted Environment}
UICC	A smart card that conforms to the specification written and maintained by the ETSI Smart Card Platform project. Recent definitions (Ref 1) permit soldered versions of UICCs.
Un-trusted Environment	Everything that is not a Trusted Environment.
USIM	Universal Subscriber Identity Module. Application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security

1.6 Interchange of terms: UICC / USIM

The terms UICC and USIM have specific meaning as given in the definitions. In 3GPP markets to date, the distinction between UICC and USIM (essentially that of hardware/OS as distinct from software application) has not been significantly relevant, as mostly a combination of the two has been delivered to market as a package from SIM vendors, in the same way as previously for 2G SIM cards. Furthermore, colloquial marketing language has often not accurately used the terms.

If there is an evolution to "eUICC", the use of the appropriate terms will become important. There may be a requirement to develop further terms defining differing combinations of layers within the "eUICC"; e.g. Java and Global Platform as OS and management layers respectively on top of the native card OS and Security domains. These will become clear when business, ownership models and technical solutions become developed to support the use cases and requirements given in this document.

It should be noted that the varying use of terms UICC and USIM throughout this document are indicative at an early stage of the split in the "eUICC" of hardware and application software functionality, but should not be taken as rigid requirements in the future development of architecture and technical specifications.

1.7 Document Cross-References

Ref	Document Number	Title
1	ETSI TS 102.671	Smart Cards; Machine to Machine UICC; Physical and logical characteristics
2	ETSI SCP TS 102.221	Smart Cards; UICC-Terminal interface; Physical and logical characteristics
3	TS 22.101 (§13)	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles
4	TS 21.111	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM and IC card requirements
5	TS 102.224	Security mechanisms for UICC based Applications - Functional requirements
6	TS 102.225	Secured packet structure for UICC based applications
7	TS 102.226	Remote APDU Structure for UICC based Applications
8	3GPP CT6 TS 31.101	3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristic
9	ETSI TS 122.038	USIM application toolkit
10	3GPP TS 31.111	USIM application toolkit
11	ETSI TS 102.223	Card Application Toolkit
12	3GPP TS 31.102	Characteristics of USIM Application
13	3GPP TS 31.103	Characteristics of ISIM Application
14	3GPP2 C.S0065	CSIM application on UICC
15	ISO 7816-1	Physical Characteristics of Integrated Circuit Cards

2 Assumptions & Principles

2.1 Assumptions

The following assumptions are made in this work.

No.	Assumption
A1	Any solutions implemented supporting these requirements are intended to be used in addition to existing UICC/SIM standards rather than replace them. The eUICC in which the (U)SIM application will be installed shall comply with UICC standards contained in the References listed, with the exception of the removable aspects.
A2	The use of a eUICC shall limit the need for any change in existing personalisation and distribution models.
A3	Any solution will be applicable to all international agreed standards for Form Factors. Currently this means ID1, 2FF, 3FF, MFF1, MFF2.
A4	The owner of the eUICC shall have an appropriate obligation to preserve the physical and logical integrity of the eUICC in such a way that its suitability for secure storage is maintained, and shall ensure that a similar obligation is imposed on any subsequent owner during any transfer of ownership of the eUICC. {Note1: Issued UICC and SIM cards are currently owned by MNOs, it is understood that eUICCs may introduce new ownership models.} {Note2: An ‘appropriate obligation’ as described above may be legal, contractual, regulatory or of some other form.}
A5	Any switch from MNO A to MNO B may be limited by the functionality of the eUICC feature set in accordance to MNO A donor and MNO B recipient roles. {Note1: This is not referring to any mechanism to prevent switching, but to note that switches may occur with subscribers losing some services.} {Note2: This issue should be minimised (hopefully eliminated) by an agreement between all operators on the set of features the eUICC has to support.}
A6	A new Trust model between entities will need to be established due to the necessary business processes resulting from the eUICC. This is likely to introduce liability changes.
A7	Any remote provisioning mechanisms must make use of requisite protocols implementing at least an agreed minimum required security level. Any UICCs that are incapable of being upgraded to the required level for such protocols and algorithms are deemed to be outside the scope of any solution and will not be subject to any of the mechanisms described in this document. {Note1: This will lead to specific technical requirements in terms of security.} {Note2: Agreement shall be required on the necessary security levels described above. In general, the minimum level of security must be at least as good as the current industry best practise for UICCs.}
A8	Not all personalisation may be performed at the same time, and there may remain a split whereby some or all personalisation will continue to be undertaken prior to the eUICC leaving the eUICC supplier environment, or combination of the eUICC supplier and Subscription Manager (SM) entities.
A9	It shall be possible for the SM to manage network access and applications/services on behalf of the MNO on the eUICC in accordance with the defined policy control functions.
A10	Modifications to the eUICC OS during the in-field lifecycle of the eUICC are out of scope for this document. However, it is anticipated that any solution to the requirements in this document may require modifications to existing UICC OSs.
A11	It is not presumed that any deployed solution based on the requirements embedded within this document should be compliant with all use cases. All described functions; are an example, of

No.	Assumption
	smart metering devices and may not require the implementation of 'transfer subscription', or 'provisioning of a first subscription with a new connected device' use cases, which may permit to offer a cost effective solution, satisfying level of required features in this particular environment and keeping the required security level.
A12	Existing regulatory requirements (when apply) should continue being supported as today.
A13	It shall be possible for SMs to manage eUICC Credentials and manage their own credentials in order to permit Assumptions A9. Noting that: • All eUICC vendors must be able to securely distribute credentials to one or more SMs; • SM is not a mandatory organisation, it is a mandatory role that can be performed by many types of organisation; • Depending upon business models and commercial relationships MNOs may use more than one SM and SMs may interconnect in an appropriate way to permit management of an eUICC to swap between SMs; • MNOs policies may include which SMs to operate with based on commercial and quality assurance considerations.

2.2 Principles

The following principles are made in this work:

No.	Principle
P1	Traditional UICC/SIM models will not be affected and will continue to work on existing networks.
P2	Provisioning credentials are always the property of the MNO that supplied them.
P3	Solutions to these requirements shall retain existing or improved levels of user friendliness. {Note1: Where the device has a human end user, the user’s experience of first choice or change of an MNO shall not be less convenient than the current experience of inserting or removing a UICC/SIM card.} {Note2: An explicit notification and/or request for action on the part of the human user should be required prior to the execution of changes on the UICC/SIM card.}
P4	The implementation of any solution to these requirements shall re-use and profile existing international standards wherever possible minimising the need for additional standardisation.
P5	Current levels of fraud prevention and tamper resistance shall be retained.
P6	The eUICC shall be a component accredited against agreed industry criteria for the secure storage and management of security-critical data. {Note: In this context, data means data and applications.}
P7	Issuance and maintenance of all forms of credentials will require trust between the individual actors involved. {Note1: Such trust has legal and liability implications that will need to be embodied in formal relationships.} {Note2: Accreditation shall be required to support the trust between actors.} {Note3: Credentials shall only be stored by trusted entities. Operators shall not be obliged to

No.	**Principle**
	store their credentials where trust does not exist.}
P8	Any solution to these requirements shall maintain existing levels of trust and security in the GSM/3G/LTE systems.
P9	An MNO should need to maintain only a small number of interfaces to the entities, which manage personalisation of eUICCs on behalf of that MNO.
P10	Any solution to these requirements shall meet applicable regulatory requirements in relevant jurisdictions
P11	The goal of the technical implementation is to re-use existing procedures to provision the eUICC and HLR data wherever possible.
P12	Any solutions to these requirements should be cost effective for all stakeholders.
P13	Any solution to these requirements must be open and equally available to all industry participants.
P14	Any solution to these requirements shall be globally acceptable, independent of a particular MNO, country, or region.
P15	Any solution to these requirements must be available to all (including non-members of GSMA) on FRAND terms.
P16	Any solution to these requirements must meet tests for anti-competitive practises.
P17	As soon as a specific MNO profile (including the relevant (U)SIM application) is active on the eUICC, this active element must comply with the security policy of the relevant MNO. {Note: A relevant generic security policy would be provided for MNO consideration by the GSMA Security Working Group}
P18	There shall be only one active Operational profile on the eUICC during the provisioned state at any stage in the lifecycle of the eUICC.
P19	There should be an obligation of interoperability for every solution to these requirements, in order to prevent any disruption in the resulting ecosystem and to preserve the consumer friendliness of devices and services for every mobile user in all their daily activities.

3 eUICC State Model

Describes the states in which a eUICC can exist..

Note that the states described are for the eUICC only, not the eUICC in conjunction with any other entities (e.g. Subscription, which can also describe also the state of entities within network elements).

3.1 Valid eUICC States

Not all the states will need to be accessed and defined, depending on the lifecycle of the SIM/USIM applications in the eUICC.

No.	State	Description
1	Pre-Initialisation	Manufactured but no credentials stored. In this state, Physical presence is required to determine whether eUICC is genuine.
2	Initialised	Initial credentials (at minimum, eUICC Credentials) stored. eUICC can connect to server for purposes of further configuration in an un-trusted environment. Optionally, the eUICC credentials become linked to the device's IMEI.
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 Initialised state. Note: In the situation where the subscription associated with the eUICC has been deactivated in the network, the eUICC will still be in Provisioned state.
4	Disabled	Presents no valid MNO credentials, but some eUICC credentials may stay valid (at least the eUICC persistent identifier) 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.}

3.2 State Transition Diagram

This is included for guidance and not a firm requirement on valid / invalid state transitions.

Transition between states is equivalent to processes such as activate, suspend and delete.

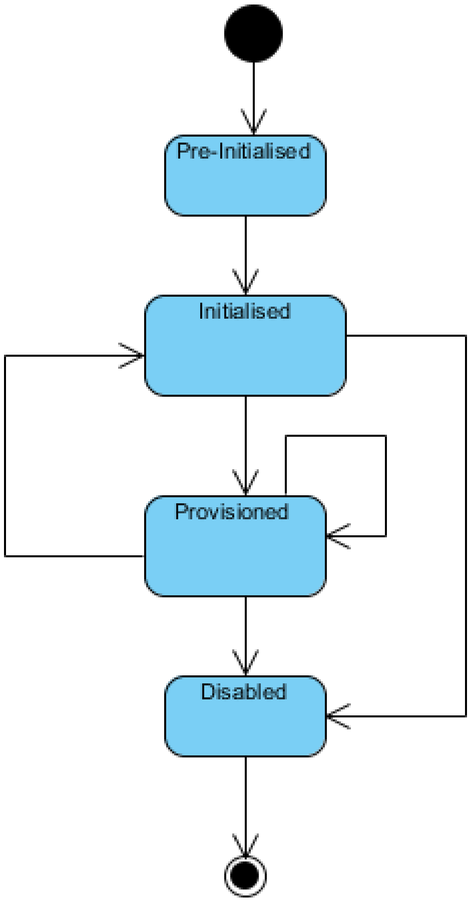

Figure 1: Suggested eUICC State Transition Diagram

4 Role and Trust Definitions

4.1 Role Definitions

No.	Role	Description
1	Device Vendor	A supplier of devices; these devices include wireless modem functionality to communicate over wide area networks run by MNOs, thus requiring a form of UICC (traditional UICC or eUICC).
2	eUICC supplier	A supplier of the secure eUICC modules and resident software (such as firmware and operating system). The hardware, software and production processes are expected to be certified to meet a specified level of security. This role may be performed by two entities – one of which delivers the hardware and the other supplying the lifetime resident software. However, even if the role is performed by a combination of entities, accreditation shall be applied as if the eUICC is provided by a single entity. The eUICC supplier provides the necessary credentials for managing the eUICC to at least one SM.
3	Machine-to-Machine Service Provider (M2M SP)	A type of enterprise subscriber, which provides machine-to-machine services for business customers and consumers.
4	Mobile Network Operator (MNO)	Provides communication services to their customers through wide area wireless networks. Where the SM role is not performed by the MNO, the MNO shall be connected to at least one Subscription Manager.
5	(Trusted eUICC) Subscription Manager (SM)	An organisation trusted by MNOs to manage the active profile and other profiles within the eUICC. The role of the SM minimises the changes for the subscription management for MNOs. Several Subscription Managers may exist; an accredited process of eUICC handover and associated credential exchange has to be established between them. The Subscription Manager role may be performed by any organisation that meets the necessary standardisation requirements, including MNOs. The necessary relationships between an SM and an MNO required for the SM to perform its role are to be defined (see Ongoing Topics).

4.2 Trust Relationships

The following trust relationships are required.

No.	Description
1	It is essential that the party which performs the transition from the pre-initialised to the initialised state (see Functional Use Case F1) is trusted by all MNOs and service providers which ever use the eUICC to store credentials.
2	Associated obligations and liabilities in relation to fraud management must be agreed.
3	The current primary contractual and trust relationship between the UICC/SIM vendors and any other 3rd parties that are involved in provisioning the UICCs/SIMs must remain between these parties and the operator. {Note1: Must end up with a model that maintains the obligations of SIM vendors to support

No.	Description
	required security levels.} {Note2: The Operator must be ultimately responsible for the security and proper functioning of its network and the SIM plays a vital role in this. For this to happen, any players with a critical role in the security of the SIM must be acting under both contractual and financial responsibilities to the Operator. In addition to the safety and security arguments, the Operator is the regulated entity, and the SIM plays a key role in allowing the operator to meet its regulatory obligations.}
4	Evaluation and qualification protocols have to be executed by independent and agreed MNOs qualified Laboratories.

4.3 eUICC Certification

The SIM/UICC is the security element chosen by mobile operators to ensure maximum protection, based on a physical component hosting industrial secrets that cannot be fraudulently modified. Currently the qualification of each element of the chain, as well as the qualification of the whole, is undertaken by mobile operators and their business partners. Any eUICC solution that will be agreed on will have to include and implement qualification processes and criterion acknowledged by all actors, specifically MNOs providing industrial secrets. Maintaining a formal certification for the overall eUICC (including USIM), as new profiles (including applications) are downloaded, is theoretically possible. However, covering the whole range of profiles would seem ambitious, and more than is required. However, with only self-certification and commercial trust relationships there is a risk that assurance is not robust enough. For example, a manufacturer claims compliance, and the Subscription Manager only does business with manufacturers making such claims. However, no one has confirmed the specification of the eUICC provided.

What is recommended is an approach that sits between self-certification (based on recommended criteria) and formal certification:

- A formally evaluated certification under a Protection Profile for the initial eUICC, covering hardware, OS and secret keys management;
- An SAS-like accreditation for the eUICC supplier, particularly covering its processes for key management and initial provisioning;
- An SAS-like accreditation for the Subscription Manager, particularly covering its processes for key management and OTA provisioning.

The following trust relationships are then required.

Then the MNO only deals with accredited SMs; and the MNO has a contractual relationship with the SM whereby an MNO's profile is only ever sent to certified eUICCs from accredited eUICC suppliers. In addition, MNOs and SMs between them get the message across to eUICC suppliers that, to succeed in the market, they have to have the eUICC certification and manufacturer accreditation.

This should enable an informal security composition and with all the elements in place, the end result should provide sufficient assurance for a secure ecosystem. An intended outcome of this approach is that when a device is bought into a region from a different “region” (e.g., country); additional re-certification should not be needed.

Currently, it is unclear which body should do the eUICC certification. In addition, a Protection Profile will need to be defined (see Open Issues). The alternatives are:

- Find an existing standard profile that fits the purpose; or

- The scheme is not about certification against standard profiles, but rather certification against claimed profiles - and then we can define our own "minimum claimed profile" without having to get it standardised.

None of the above shall preclude a formal security composition being achieved where required, for example some financial NFC cases.

5 Use Cases

A range of use cases is identified in this section to derive requirements for the development of a trusted framework for the management of an embedded UICC (eUICC). This is not intended to be an exhaustive list of use cases and applications, but a set of examples to ensure requirements will be flexible enough to support securely both current and future use cases.

The use cases are divided into vertical and functional use cases, where the vertical use cases define usage scenarios and functional use cases define logical operations. Each functional use case needs to be supported by at least one vertical.

Use cases are provided as a means to understand and add context to the overall requirement.

5.1 Vertical Use Cases

5.1.1 Overview of the use cases

No.	Use Case	Description
UC1	Provisioning of multiple M2M subscriptions.	A Machine-to-Machine Service Provider (M2M SP) sets-up M2M subscriptions for a number of connected M2M devices to start telecommunication services with a first MNO. Optionally, the M2M SP may later change subscriptions to a subsequent MNO.
UC2	Provision of first subscription with a new connected device	A subscriber purchases a new type of communications or connected device from a device vendor together with a subscription to provide first services to this device.
UC3	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.
UC4	Stop Subscription	A subscriber sells his device and stops the subscription for services from the current MNO.
UC5	Transfer Subscription	Subscriber transfers subscription between devices.

It should be noted that all Use Cases above are required to support M2M / embedded service usage. UC1 explicitly describes a role for an M2M Service Provider.

5.1.2 UC1: Provisioning of multiple M2M subscriptions

A Machine-to-Machine Service Provider (M2M SP) sets-up M2M subscriptions for a number of connected M2M devices to start telecommunication services with a first MNO. While it is expected that there will be a very great range of M2M applications, and many of these will have different parties and business models, it is likely that the key technical requirements will become clear through examining a few examples of this use case; the following examples are considered further in this section:

a) Provision of first subscription, and optional later change of subscription, for communication services for automated reading of utility (electricity, water, gas) meters; a M2M Service Provider will contract these subscriptions.

b) Provision of first subscription and optional later change of subscription for a security camera.

c) Provision of first subscription, and optional later change of subscription for communication services to vehicles (e.g. telematics); the vehicle vendor will provide the automotive services.

5.1.2.1 UC1a) Utility Meters

The Meter Reading M2M SP has a commercial contract to both supply meters and – once they have been installed – to provide regular meter readings of these meters to the utility company. The M2M SP selects the preferred MNO to provide a number of subscriptions after completing a tender process for the communication services as part of a defined service level agreement.

Once the MNO is selected, the M2M SP arranges for the utility meters to be installed, and as part of the installation process for the communication services to start. While the physical installation is a manual process, the subscription management required for the communication services will be automated.

Contracts for communication services should be negotiated to last for a period of several years; when / if a change of contract is negotiated, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period.

5.1.2.2 UC1b) Security Camera

A consumer purchases a security camera for monitoring his house. The security camera is supplied with a subscription for communication services so that recorded data is uploaded and stored as part of the service from a security (M2M) SP. The consumer (or M2M SP) installs the camera and sets up access to the security services online.

The M2M SP selects the MNO for the video camera service; the subscription management will be automated for the contracted number of subscriptions between the M2M SP and the MNO.

Contracts for communication services should be negotiated to last for a period of several years; when / if a change of contract is negotiated, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period. Noting that the level of MNO coverage within individual properties can be different, an automated check of coverage for the target MNO may form part of any subscription update.

5.1.2.3 UC1c).Telematics

A consumer purchases a new vehicle and this includes a number of vehicle manufacturer provided services delivered over wide area wireless communications to the vehicle and its occupants. The services will be delivered whether the vehicle is mobile or stationary, and whether or not the vehicle is in the country in which it was purchased. The vehicle manufacturer himself or a subcontractor acts as M2M SP, providing both vehicle related services (such as engine monitoring) and being a broker for services supplied by other SPs (such as infotainment).

The subscription will be activated at vehicle purchase to be operational as the customer drives the vehicle away; the subscription management will be automated for the contracted number of subscriptions between the M2M SP and the MNO. The M2M SP agrees to the commercial contract with MNO(s) in either the same or different countries for subscriptions for the communication services; the vehicle customer may not know which MNO is providing communication services.

Contracts for communication services should be negotiated to last for a period of several years; when / if a change of contract is negotiated by the M2M SP, the change is likely to apply to multiple subscriptions. The changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period.

5.1.3 UC2: Provision of first subscription with a new connected device

An end user purchases a new type of communications or connected device from a device vendor together with a subscription to provide first services to this device. While it is expected that there will be a range of consumer purchased devices for communication, media and Internet applications and more, and many of these will have different parties and business models, it is likely that the key technical requirements will become clear through examining a few examples; the following examples are considered further in this section:

a) Provision of a new device; the consumer will select the MNO to provide communication services.

b) Provision of multiple connected new device for an enterprise workforce; the enterprise will select the MNO to provide the subscriptions.

c) Purchase of a new device with the first subscription already pre-loaded.

5.1.3.1 UC2a) Provision of a new device

A consumer purchases a new device with a eUICC and then selects an MNO for communication services. The MNO might be selected at the same or another retailer, with an MNO shop or online and will be activated within a short period. First use of the new device will be with the first subscription already set-up, or if no subscription is set-up, the user will select an MNO and, if required, after appropriate authorization a subscription will be set-up. Subscription set-up may happen via the mobile network using either a pre-loaded first subscription or a provisioning subscription or via any other connectivity mechanism provided by the device and the eUICC SM, subject to required end-to-end security being provided e.g. LAN, WLAN, Bluetooth, or USB.

The subscription management will be automated for this single consumer subscription between the consumer and the MNO. The consumer agrees to the contract with the MNO for the subscription for the communication services.

5.1.3.2 UC2b) Provision of multiple devices for an enterprise

An enterprise (Purchasing Manager) purchases new devices for a set of employees. Contracts for multiple subscriptions will be negotiated for communication services, which enable a range of telecommunication and enterprise applications. The subscriptions will be activated as new employees start, at the latest on their first use of the device. Subscription activation may happen via the mobile network using a pre-loaded subscription or via any other connectivity mechanism provided by the devices and the eUICC SM, subject to required end-to-end security being provided e.g. LAN, WLAN, Bluetooth, or USB.

The subscription activation may be followed by device management to configure enterprise specific applications and directories.

The subscription management will be automated for the contracted number of subscriptions between the enterprise and the MNO. The enterprise agrees to the commercial contract with MNO(s) for subscriptions for the communication services; the enterprise employees will be aware of which MNO is providing communication services.

5.1.3.3 UC2c) Purchase of device with subscription pre-loaded

A consumer purchases a new device with a eUICC with a pre-loaded subscription for communication services from a specific MNO.

Subscription management is set up so that it is possible for the consumer to change the subscription at a later point in time, for example at the end of a contract period in accordance with the relevant policy control functions.

5.1.4 UC3: Change of subscription for a device

A subscriber changes the contract and thus subscription for the device to stop services with the current MNO and start services with a new MNO.

a) Change of a subscription for a device by the consumer.

b) Change of the subscriptions of multiple connected new devices for an enterprise workforce to a new MNO; the enterprise will select the MNO to provide the subscriptions.

c) Change of the subscription by the consumer for a device, which had the first subscription already pre-loaded. This is expected to be the same as UC3a therefore is not considered further.

5.1.4.1 UC3a) Change of subscription by consumer

A contract for communication services of a device is expected to last for a period of one or more years; when / if a change of contract is decided upon by the consumer, the change is likely to apply to a single subscription, or possibly a few subscriptions the consumer has for connected devices. The changeover is expected to be managed seamlessly in an automatic fashion at an agreed date. The changeover shall be undertaken in accordance with relevant Policy Control Functions as defined by the Donor Operator first and the Recipient Operator second. In addition to new MNO subscription data, the change of subscription may involve provisioning of a new eUICC network access application as well as MNO specific applications, and the movement of consumer data stored within the eUICC. In parallel, there may be management for telephone number portability.

5.1.4.2 UC3b) Change of subscriptions for devices for enterprise workforce

Contracts for communication services for the workforce are expected to be negotiated to last for a period of one or more years. When / if a change of contract is negotiated by the enterprise, the change is likely to apply to multiple subscriptions, and the changeover is expected to be managed in an automatic fashion at an agreed date over a relatively short period. The changeover shall be undertaken in accordance with relevant Policy Control Functions as defined by the Donor Operator first and the Recipient Operator second. In addition to new MNO subscription data, the change of subscription may involve provisioning of new eUICC applications, and the movement of enterprise and individual employee data stored within the eUICC. In parallel, there may be device management for enterprise applications as well as the management of telephone number portability.

5.1.5 UC4: Termination of a subscription for a consumer device

A consumer sells his mobile device and stops usage of the services from the current MNO. Note that some form of settlement between MNOs and consumers may be needed when devices with upfront paid subscription fees change subscription before the end of the contract period. It is expected that there will be a range of consumer purchased devices and business models and it is likely that the key technical requirements will become clear through examining a few examples.

The following examples are considered in this section:

a) Removal of a subscription and related services from a device.

b) Termination of a device contract with an MNO.

c) Termination of a contract for multiple connected new devices for an enterprise workforce where the enterprise selected the MNO.

d) Termination of the contract by the consumer for a device, which had the first subscription already pre-loaded. This is expected to be the same as UC4b so is not considered further.

e) Termination of service by MNO to prevent fraud or network damage. Device is not allowed to connect to any MNO without some physical intervention. (Note in the description we may have to have caveats about supporting emergency calls – maybe national regulatory issues)

5.1.5.1 UC4a) Removal of a subscription from a device

A consumer wants to sell his device. Before selling the device, he wants to remove the subscription and related services from the device while keeping the device contract with the MNO.

To remove the subscription, the consumer leaves his device connected to the network or reconnects, allowing the eUICC MNO to request the SM to send a command, the eUICC is switched to the eUICC provisioned state.

The buyer can then set-up a new subscription in the same way as for a new device.

The subscription management will be automated for the removal of this single consumer subscription between the consumer and the MNO.

5.1.5.2 UC4b) Termination of a device contract with an MNO

A consumer wants to sell his device. Before selling the device, he terminates the contract with the MNO. This will trigger the removal of his subscription and related services from the eUICC.

If the consumer leaves his device connected to the network or reconnects, allowing the eUICC MNO to request the SM to send a command, the eUICC is switched to the eUICC provisioned state.

If the consumer does not reconnect before selling his device, then the eUICC is switched to the eUICC provisioned state possibly triggered as a result of a network error code or user interaction.

The buyer can then set-up a new subscription in the same way as for a new device.

The subscription management will be automated for the removal of this single consumer subscription between the consumer and the MNO.

5.1.5.3 UC4c) Termination for multiple connected enterprise devices

An enterprise wants to take multiple devices out of use and hand them over to employees for private use or to a company that sells used company equipment. Before handing the device to employees or another company, the enterprise will terminate the contract with the MNO, and thus trigger the removal of the related subscriptions. The eUICCs are switched to their provisioned state and any buyer can set-up a new subscription in the same way as for a new consumer device.

The subscription management will be automated for the removal of these enterprise subscriptions between the enterprise and the MNO.

5.1.6 UC5: Subscriber transfers subscription between devices

A number of scenarios can arise where credentials are required to be moved from device A to device B. Examples are listed below:

a) Due to Fault.

b) Customer requires change.

c) Move subscription from a eUICC to a traditional UICC or vice versa (need to be consistent with definitions – applications etc).

5.1.6.1 UC5 a) Transfer due to Fault

Following identification of a fault on a previously supplied device, a second device is supplied and the subscription and related services transferred from the original device to the replacement device.

In addition to all the subscription parameters, also all the related eUICC services (e.g. NFC applications etc.) may be removed from the device with a wipe command avoiding the misuse of specific applications by third parties for fraudulent scope. The wipe command shall be authenticated by the eUICC before being executed to prevent remote denial-of-service attack. As the customer will perform the subscription transfer, the pre-existing activated services will be downloaded on the new eUICC.

As the original device cannot be assured to be operational, the subscription must be deleted in the MNO systems (including HLR/AUC) and a new subscription has to be installed into the eUICC of the replacement device.

This may imply a loss of data for the customer, unless a backup of the whole “package” is secured somewhere at MNO (or SM) premises.

5.1.6.2 UC5 b) Transfer requested by Customer

A consumer transfers usage from one device that supports eUICC to another for some reason. The user will want to transfer the subscription and related services from the device while keeping the device contract with the MNO.

To remove the subscription, the consumer leaves his device connected to the network or reconnects, allowing the eUICC SM to send a command, the eUICC is switched to the eUICC provisioned state. The transfer shall be undertaken in accordance with relevant Policy Control Functions as defined by the MNO.

For the replacement device, the subscription set-up may happen via the mobile network or via any other connectivity mechanism provided by the device and the eUICC SM, subject to required end-to-end security being provided e.g. LAN, WLAN, Bluetooth, or USB.

5.1.6.3 UC5 c) Transfer between eUICC and UICC

A consumer transfers usage from a device that supports eUICC to one where eUICC support is not available for some reason. The user will want to transfer the subscription from the device while keeping the device contract with the MNO.

To remove the subscription, the consumer leaves his device connected to the network or reconnects, allowing the eUICC SM to send a command, the eUICC is switched to the eUICC provisioned state.

The user and MNO can then use traditional methods to set-up a subscription for the replacement device.

The subscription management will be automated for the removal of this single consumer subscription between the consumer and the MNO.

Note that in the opposite case "UICC to eUICC", existing MNO policies and procedures should apply.

5.2 Functional Use Cases

No.	Use Case	Description
F1	Pre-Provisioning (within a trusted environment)	Takes various components, un-provisioned eUICC, Device, (optionally) Host Equipment and provisions the eUICC with the necessary Initial Credentials to enable connection to a 3GPP access network (or via any other connectivity mechanism provided by the device and the eUICC SM, subject to required end-to-end security being provided e.g. LAN, WLAN, Bluetooth, or USB) for subsequent re-provisioning.
F2	Post Sale (initial) Provisioning (outside a trusted environment)	Initially provisioned eUICC within a device or host equipment and module is updated with a selected MNO credentials. {Note 1: May (or may not) include MNO selection} {Note 2: For the MNO this will be linked to network/billing/crm activation and establishing a subscription}. {Note 3: What happens when no user interface on the device?}
F3	Life-cycle Management	Enables remote re-configuring of the MNO credentials. {Note 1: Care required to avoid scenarios that create, for example, a signalling thrashing scenario within the network without the ability to create an authenticated and authorised connection in cases where volumes could be incredibly high.} {Note 2: There would exist a need for a contractual mechanism, to define the period whereby a eUICC can be disabled.}
F4	Re-Provision	Remove subscription associated with MNO A and replace with subscription for MNO B. Donor Operator and subscriber must give permission for a new subscription. However, an existing subscription can be removed without subscriber permission; typically, this would be due to non-fulfilment of contractual obligations. At all times, there shall be some credentials within the eUICC that permit radio access.
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 shall be applied.
F6	Device Transfer	Transfer an existing subscription (including data/applications) from one device to another within a single MNO. {Note: Need to understand if there is a use case that requires the transfer of other data/applications associated with the subscriber identity, e.g. replicate experience of moving UICC containing SIM+banking application from one device to another device.}

6 Processes

Describes processes and how they relate to roles etc. the different processes phases are given as examples to illustrate steps of processes that may be considered to resolve the embedded requirements but do not mandate any particular added requirement; Therefore, not all steps will need to be supported by the solution.

The requirement to minimise the changes for MNO subscription management processes leads to the introduction of a new role: the Subscription Manager (SM). The introduction of this role will minimise the number of interfaces required by an MNO to manage the personalisation of a eUICC. The SM shall provide interfaces to the MNOs for subscription data in the same manner as done by UICC manufacturers today. The SM shall enforce the Policy Control Functions defined by each MNO the SM acts on behalf of, noting that an MNO may manage the policy control function in its own right. The processes described below takes the SM role into account.

Within the examples below the service providers (for example SP for metering, security or vending machines) and the affected devices (for example utility meter, security camera..) are different. However, the processes for the provisioning or changing of an M2M subscription are the same. They are described below in a generalised way.

The processes below describe individual steps as being triggered by specific actors in the system (e.g. being triggered by eUICC). The process steps do not imply that any technical solution must follow these steps or use the actors in this way.

6.1 UC1: Processes for (multiple) M2M use cases

6.1.1 UC1 a) Provisioning an M2M subscription on a new device

Pre-conditions	an M2M SP has established a commercial contract for the provisioning of certain devices
	M2M SP has selected device vendor to supply devices with integrated modems
	M2M SP has selected MNO to provide first communication services
Start of Process	the M2M SP requires new devices
	The M2M SP requests the M2M device vendor to supply a batch of devices
	The M2M device vendor requests the eUICC supplier to supply a batch of eUICCs
	The eUICC supplier produces and provisions each eUICC with secret data
	For each eUICC, the eUICC supplier sends secret data to the eUICC SM. This secret data enables the eUICC SM to uniquely identify and authenticate the eUICC
	The eUICC supplier ships the eUICCs to the M2M device vendor, who integrates them in the devices. {Note: This may also be a multi-step integration process involving MNO or other manufacturers, e.g. a modem manufacturer, who will integrate the eUICC into a modem that is then integrated into the device. During or after the integration, the M2M device vendor may wish to test device, possibly using either the provisioning subscription or a pre-loaded MNO subscription to access a network.} eUICC may optionally include MNO credentials
	The M2M device vendor ships the devices to the M2M SP
	At each device installation, the eUICC requests the device to set up a data bearer. (Note: In the case that a mobile data bearer is used, this requires a provisioning subscription to be present, e.g. with the eUICC SM acting as providing connectivity through an appropriate agreement MVNO.) SM is responsible for

	whatever access is used for provisioning linked to above comments
	The eUICC generates a request for a first subscription and forwards this request via a data bearer to the eUICC SM
	The eUICC SM looks up the M2M SP that is associated with the device. (Note: The required mapping to M2M SP may have been provisioned with the eUICC SM; or can be part of the request.)
	The eUICC SM verifies the validity of the request with the M2M SP and requests the identity of the MNO that will handle the subscription
	The eUICC SM contacts the MNO to exchange the subscription information including associated secret data
	The eUICC SM sends updates to the eUICC to activate the MNO's subscription
	The eUICC instructs the device to terminate the temporary data bearer that was used for establishing the first subscription
	The eUICC instructs the device to setup a data bearer to the eUICC SM using the new subscription
	The eUICC confirms to the eUICC SM that the new subscription has been established
	The eUICC SM confirms new subscription is active with the M2M SP
Post-conditions	a first subscription is established for the device

6.1.2 UC1 b) Process for changing a M2M subscription

Pre-conditions	The M2M SP requires activation of new subscriptions to already deployed devices.
	The M2M SP knows identities of the devices for subscription change, or, at least, knows basic information for the eUICC SM to determine the identities.
	The M2M SP has already negotiated commercial contracts for the provision of an agreed number of subscriptions with the new MNO and agreed the termination of existing contracts, and thus subscriptions, with the current MNO.
Start of Process	The M2M SP requests the eUICC SM to update subscriptions for a specified batch of devices for the new MNO within an agreed time schedule. Note: The M2M SP may also contact the current MNO or the new MNO to initiate the subscription change, thereafter the MNO will forward the request to the eUICC SM.
	The eUICC SM contacts the new MNO to exchange the subscription information including associated secret data.
	For each individual eUICC within the batch; the eUICC SM sets up a temporary data bearer to the eUICC; this may be using the current MNO communication services.
	The eUICC SM sends updates to the eUICC to activate the new MNO's subscription
	The eUICC SM terminates the temporary data bearer that was used for changing the subscription
	The eUICC instructs the device to setup a data bearer to the eUICC SM using the new subscription
	The eUICC confirms to the eUICC SM that the new subscription has been established

	For the batch of devices; the eUICC SM confirms old subscriptions terminated with the previous MNO and new subscriptions active with the M2M SP
Post-conditions	the subscriptions are changed for the batch of devices

6.1.3 UC1 c) Process for fallback to a previous subscription

It is possible to provision a first subscription or change a subscription using a mobile network. During this process there is a risk that the M2M device cannot connect to the new network (e.g. due to lack of coverage). In order for the M2M device not to get lost, the following process is initiated by the eUICC:

- In the processes described above, if at the step where "*The eUICC instructs the device to setup a data bearer to the eUICC SM using the new subscription*" setting up of the data bearer fails, the process continues as follows:
    - The eUICC retries to set up a data bearer for a number of times at defined time intervals.
    - If all retries fail, the eUICC re-activates the previous (operational) subscription and notifies the eUICC SM that activation of the new subscription has failed. Note 1: This requires the old subscription to be held active in the network until a successful change is confirmed by the eUICC SM. Note 2: Switchback could also happen to the provisioning subscription.
    - Corrective actions are initiated by the eUICC SM.

6.2 UC2: Provision of first subscription with new device

A consumer purchases a new type of communications or connected device from a device vendor that includes a subscription to provide first services to this device. While it is expected that there will be a range of consumer purchased devices for communication, media and Internet applications and more, and many of these will have different parties and business models, it is likely that the key technical requirements will become clear through examining a few examples; the following examples are considered further in this section:

a) Provision of a new device; the consumer will select MNO to provide communication services.

b) Provision of multiple connected new devices for an enterprise workforce, and the later change of the multiple subscriptions to a new MNO for communication services; the enterprise will select the MNO to provide the subscriptions.

c) Purchase of a new device with the first subscription already pre-loaded.

While there are a number of similarities for many parts of the processes for the example use cases, there are also sufficient differences such that a single general process to cover these examples is not clear. The processes for each use case example are described below.

6.2.1 UC2 a) Provision of device consumer selects MNO

Pre-conditions	Retailer has agreed the commercial terms for the supply of new devices.
	Retailer has selected device vendor to supply devices with eUICCs.
Start of Process	The retailer requires a new batch of devices to sell.
	The retailer requests the device vendor to supply a batch of devices.

	The device vendor requests the eUICC supplier to supply a batch of eUICCs.
	The eUICC supplier produces and provisions each eUICC with secret data.
	For each eUICC, the eUICC supplier sends secret data to the eUICC SM. This secret data enables the eUICC SM to uniquely identify and authenticate the eUICC.
	The eUICC supplier ships the eUICCs to the device vendor, who integrates them in the devices.
	The device vendor ships the devices to the retailer.
	A consumer purchases and takes delivery of a new device from the retailer – either directly at a retailer shop or on delivery after an online purchase.
	The consumer then selects and agrees a personal contract for an MNO subscription; this may be in the shop where the device was purchased, another shop or online.
	At power-up of the new device, an application running on the device and / or the eUICC, and / or a connected PC with Internet connectivity, initiates the provisioning of a first subscription.
	The eUICC requests the device to set up a data bearer. (Note: In the case that a mobile data bearer is used, this requires a provisioning subscription to be present.)
	The eUICC generates a request for a first subscription, possibly including the MNO and new subscription contract reference, and forwards this request via a data bearer to the eUICC SM.
	Via the MNO policy control, the eUICC SM verifies the validity of the request with the consumer who purchased the device and if not already included, requests the identity of the MNO and reference for the first subscription contract.
	In accordance with the MNO policy control the eUICC SM confirms validity of reference for a new subscription; if this is valid, the SM requests to exchange the subscription information including associated secret data.
	The eUICC SM sends updates to the eUICC to activate the MNO's subscription.
	The eUICC instructs the device to terminate the temporary data bearer that was used for establishing the first subscription.
	The eUICC instructs the device to setup a mobile data bearer to the eUICC SM using the first subscription.
	The eUICC confirms to the eUICC SM that the first subscription has been established.
	The eUICC SM confirms the first subscription is active with the MNO and the consumer who purchased the device and agreed the MNO contract.
Post-conditions	A consumer selected first subscription for communication services is established for the purchased device.

6.2.2 UC2 b) Provision of enterprise devices

Pre-conditions	An Enterprise (Purchasing Manager) has agreed the contract to purchase multiple new devices for new employees over a given period.
	The Enterprise (Purchasing Manager) has selected, negotiated and agreed a contract for communication services, which enable a range of telecommunication and enterprise applications.

	The MNO or retailer that supplies the devices has sufficient numbers of the selected model in stock. For each eUICC within these devices, the eUICC supplier has sent the secret data to the eUICC SM.
Start of Process	The Enterprise orders a new batch of devices and communication services for a group of new starters.
	Enterprise orders and takes delivery of a batch of new devices from the MNO or retailer.
	Enterprise IT and Communications department activates the agreed MNO subscription within the device, and provides this working device to the new starter; alternatively, the IT and Communications department provides a device and subscription set-up instructions to the new employee.
	At power-up of the new device, an application running on the device and / or the eUICC, and / or a connected PC with Internet connectivity, initiates the provisioning of a first MNO subscription for the Enterprise.
	The eUICC requests the device to set up a data bearer. (Note: In the case that a mobile data bearer is used, this requires a provisioning subscription to be present.)
	The eUICC generates a request for a first subscription, possibly including the MNO and the Enterprise new subscription contract reference, and forwards this request via a data bearer to the eUICC SM.
	Via the MNO policy control, the eUICC SM verifies the validity of the request with the Enterprise that purchased the device and, if not already included, requests the identity of the MNO and reference for the Enterprise first subscription contract.
	The eUICC SM contacts the MNO to confirm validity of reference for a new subscription; if this is valid, eUICC SM requests to exchange the subscription information including associated secret data.
	The eUICC SM sends updates to the eUICC to activate the MNO's subscription.
	The eUICC instructs the device to terminate the temporary data bearer that was used for establishing the first subscription.
	The eUICC instructs the device to setup a mobile data bearer to the eUICC SM using the first subscription.
	The eUICC confirms to the eUICC SM that the first subscription has been established.
	The eUICC SM confirms the first subscription is active with the MNO and the Enterprise.
	The MNO may use device management to configure the device for the contracted set of Enterprise services.
Post-conditions	The new employees in the Enterprise have devices with an active subscription for communication services.

6.2.3 UC2 c) Device with first subscription pre-loaded

Pre-conditions	An MNO has decided to offer a pre-loaded subscription with a device package.
	The MNO has contractual agreement with a device vendor to supply particular models of devices with eUICCs pre-configured with the first MNO subscription.

Start of Process	The MNO requires a new batch of devices to sell.
	The MNO requests the device vendor to supply a batch of devices with pre-loaded MNO subscriptions.
	The device vendor requests the eUICC supplier to supply a batch of eUICCs with pre-loaded MNO subscriptions.
	The eUICC supplier produces and provisions each eUICC with secret data.
	For each eUICC, the eUICC supplier sends secret data to the eUICC SM. This secret data enables the eUICC SM to uniquely identify and authenticate the eUICC. The eUICC supplier also requests the first subscription data to be pre-loaded from the eUICC SM.
	The eUICC SM contacts the MNO to confirm validity of a reference for a new batch of first subscriptions; if this is valid, eUICC SM requests the MNO to provide the subscription information including associated secret data to the eUICC supplier. (Note: this may be via the eUICC SM which is a trusted entity.)
	The eUICC supplier ships the pre-loaded eUICCs to the device vendor, who integrates them in the devices.
	The device vendor ships the devices to the MNO.
	A consumer purchases and takes delivery of a new device from the MNO – either directly at an MNO shop or on delivery after an online purchase from the MNO. This device already has an active MNO first subscription and is ready for use.
Post-conditions	The first subscription for communication services is active for the device the consumer purchased.

6.3 UC3: Change of Subscription for a Consumer Device

A consumer, enterprise or retailer / device vendor changes the contract and thus subscription for the device to stop services with the current MNO and start services with a new MNO.

a) Change of a subscription for a device by the consumer.

b) Change of the subscriptions of multiple connected new devices for an enterprise workforce to a new MNO; the enterprise will select the MNO to provide the subscriptions.

c) Change of the subscription by the consumer for a device, which had the first subscription already pre-loaded.

UC3b will follow the same general process as described for the change of multiple M2M subscriptions in section 6.1.2, with the only change that the Enterprise will request the change of subscriptions instead of an M2M SP. For the remaining use cases, the consumer initiated change follows the same general process as follows.

Pre-conditions	The consumer is using a connected device with a eUICC and a subscription for telecommunication services. Where the subscription is part of a bundled service, e.g. with a tablet PC, it is assumed that the consumer seeks the new MNO subscription directly from the new MNO.
Start of Process	The consumer seeks to change the MNO subscription with an existing connected device.

	The consumer selects and agrees a commercial contract for the provision of a subscription with the new MNO in a shop or online, and agrees the termination of existing contracts with the current MNO (or retailer).
	The consumer requests the new MNO to update the subscription for a specified device. In accordance with policy control functions, the MNO requests the eUICC SM to update the subscription for this specified device.
	The eUICC SM exchanges the subscription information including associated secret data with the new MNO.
	The eUICC SM sets up a temporary data bearer to the eUICC; this may be using the current MNO communication services.
	The eUICC SM sends updates to the eUICC to activate the new MNO's subscription.
	The eUICC SM terminates the temporary data bearer that was used for changing the subscription.
	The eUICC instructs the device to setup a data bearer to the eUICC SM using the new subscription.
	The eUICC confirms to the eUICC SM that the new subscription has been established.
	The eUICC SM confirms that the old subscription is terminated with the previous MNO, that the new subscription is active with the new MNO and that relevant policy control has been applied.
Post-conditions	The subscription is changed for the consumer device.

6.4 UC4: Termination of a Subscription for a Consumer Device

A consumer sells his mobile device and stops the contract for services from the current MNO. Note that some form of settlement between MNOs (or retailers if they manage the subscription) and consumers may be needed when devices with upfront paid subscription fees change subscription before the end of the contract period. While it is expected that there will be a range of consumer purchased devices and business models, it is likely that the key technical requirements will become clear through examining the following few examples:

a) Removal of a subscription, services and sensible data from a device.
b) Termination of a device contract with an MNO.
c) Termination of a contract for multiple connected new devices for an enterprise workforce where the enterprise selected the MNO.
d) Termination of the contract by the consumer for a device, which had the first subscription already pre-loaded.

The above consumer and enterprise use cases follow the same general process as follows.

Pre-conditions	The consumer or enterprise end user is using a connected device with a eUICC and a subscription for telecommunication services.
Start of Process	The consumer or enterprise seeks to remove the subscription and optionally terminate the MNO contract for an existing connected device, or batch of devices.
	The consumer or enterprise agrees any commercial implications for the termination of the contract(s) with the MNO if known, or with provider of the

	connected device (retailer) if the contract is bundled.
	The consumer or enterprise requests the current provider of the subscription to remove the subscription. The subscription provider contacts the MNO to advise of the removal of the subscription (if not the MNO itself).
	The provider of the subscription contacts the eUICC SM to remove the subscription for a specified device or batch of devices.
	The eUICC SM sends an update to the eUICC to remove the current MNO's subscription and the eUICC switches to provisioned state. In the case, that the contract is terminated, the next time the device connects, the eUICC is switched to the eUICC provisioned state possibly triggered as a result of a network error code or user interaction.
	The eUICC confirms to the eUICC SM that the subscription has been removed.
	The eUICC SM confirms that the old subscription is removed with the MNO, and if different, the provider of subscriptions who confirms the removal and optionally termination with the consumer or enterprise.
Post-conditions	The subscription is removed from the specified consumer device(s).

6.5 UC5: Subscriber transfers subscription between devices

A number of scenarios can arise where credentials are required to be moved from device A to device B. Examples are listed below:

a) Due to Fault.

b) Customer requires change.

c) Move subscription from a eUICC to a traditional UICC or vice versa (need to be consistent with definitions – applications etc).

No specific process flows have been created for these use cases.

7 Requirements

The following requirements are provisionally categorised into groups for ease of reading. These groups are only suggested and should not be considered as final categorisation. Importantly, all Requirements tables should be considered when deriving any solutions to these requirements.

7.1 Lifecycle requirements table

No.	Requirement
LIF1	There shall be a mechanism to install a provisioning subscription onto the eUICC.
LIF2	There shall be a mechanism to install a first subscription onto the eUICC pre-issuance.
LIF3	There shall be a mechanism to install a first subscription onto the eUICC post-issuance.
LIF4	There shall be a mechanism to change the current installed profile from one MNO to another MNO.
LIF5	It shall be possible to configure the eUICC that it needs to seek the first subscription on power-up.
LIF6	It shall be possible to load profile data and applications in the same session or in a different session as for the loading of the subscription.
LIF7	It shall be possible to securely delete the MNO subscription and data including credentials, profile and applications, without assigning a new MNO subscription identity.
LIF8	Provisioning and re-provisioning should be possible without removing the UICC or the device from its operating environment during the lifetime of the device
LIF9	Provide for more than one ‘profile’ within a eUICC at any stage in its lifecycle but only permit a single profile to be active at any point in time. Any action on the active profile shall be subject to validation, which shall include among other considerations, reference to the Policy Control Functions (PCF) of the MNO that owns the active profile on the eUICC. The PCF may be undertaken by the MNO or the SM acting on its behalf. {Note that an active profile may contain multiple applications if desired.}
LIF10	The provisioning of multiple profiles on a eUICC shall be subject to control of individual MNOs administered through policy control functions. (E.g., an MNO should have the ability to declare whether it permits a eUICC to hold its credentials alongside those of other MNOs when its credentials are not active, or in the case where it is the active MNO, whether other credentials can be stored.)
LIF11	The provisioning of the eUICC (whatever this is in detail) shall be triggered by the subscriber or by (personnel of) the recipient operator. Where there is a donor operator then the provisioning shall be done in accordance with policy control functions of the donor operator, followed by the policy control functions of the recipient operator.
LIF12	It shall be possible a) transfer subscription to another device, or b) delete the subscription or c) store the subscription in a secure way to reuse it later; a ‘profile’ cannot be active in more than one device in any case.
LIF13	Policy control functions may impose specific requirements on the process of subscription change to ensure that it is genuinely under subscriber control. For example, where the subscriber is a human end user of the device, the policy may require that change requests are initiated through the UI, that the device reboots after any such change and the change is clearly visible through the UI.
LIF14	A device no longer containing a valid operational profile may be assigned new profiles and MNO credentials.
LIF15	Personalisation may include identities, keys, algorithms, and applications. Not all personalisation may be performed at the same time, and there will remain a split whereby

No.	Requirement
	some or all personalisation will continue to be undertaken prior to the eUICC leaving the vendor environment, or combination of the vendor and Subscription Manager entities.
LIF16	The eUICC should be able to be de-activated (e.g. locked and its memory wiped clean). {Note 1: An example of the use of this facility is when a device is stolen. Such an event would also be expected to cause an update in the GSMA IMEI database.}
LIF17	It shall be possible for the Device Vendor to test the device before shipment using the provisioning subscription or pre-loaded MNO subscription.
LIF18	There shall be a clear specification of which credentials can be changed at which lifecycle state of the eUICC and the associated security with these changes. (E.g. Algorithm can be loaded into the eSIM at the personalisation of the eSIM at the factory, crypto libraries cannot be changed as built into the OS etc...)
LIF19	The eUICC must contain a minimum set of credentials to allow the device/eUICC to attach to a network and be updated with an Operator's data, irrespective of the type of network it is allowed to connect to.

7.2 Service Management Requirements Table

No.	Requirement
SM1	There shall be a mechanism of provisioning an operational profile onto the eUICC in a secure way. {Note: depending upon device characteristics, market, and other considerations the mechanism for installing an operational profile may vary and cover 'wired' and 'wireless' (and other) connectivity.}
SM2	These requirements shall support the management of any type of NAA subscription, e.g. SIM, USIM, CSIM, and R-UIM
SM3	It shall be possible to manage MNO specific profiles and applications on the eUICC in accordance with LIF9 and LIF10.
SM4	Solution should allow for remote provisioning (and de-provisioning) of additional eUICC based services during lifetime of subscription and device.
SM5	Bulk re-provisioning should be supported where under the control of a single subscriber. {Note: to enable bulk switching for M2M scenarios}
SM6	Before changing MNO credentials on a eUICC a check needs to be performed that the new profile will fit on the destination eUICC. {Note: appropriate checks required to ensure that this is transparent and doesn't introduce unfair practises blocking transfer}
SM7	The donor operator shall be able to provide SIM usage guarantees to the recipient operator before activation of provisioning phase; this may include lifetime counters, additional counters…
SM8	The donor operator and/or the corresponding SM shall be able to provide to recipient operator sufficient information level before activation of provisioning phase; such information may include memory space available, hosted algorithms, OTA capabilities
SM9	The mobile network operator retains the ability and the right to update elements of its profile, e.g. setting configurations or adding new applications, without needing user intervention or consent. {Note: see note in SM1}
SM10	There may be application mechanism on the eUICC that identifies a change of device.

No.	Requirement
SM11	It shall be possible for the consumer data stored on the eUICC to be transferred during the change of the current subscription from one MNO specific profile to another MNO specific profile.
SM12	In the same way as traditional UICCs, the eUICC shall continue to allow MNOs to deploy custom / proprietary applications using for example SIM Toolkit applications.
SM13	Memory availability for MNO profiles on the eUICC shall not be restricted beyond that necessary to provide the eUICC capability.

7.3 Communications Requirements Table

No.	Requirement
COM1	All remote provisioning shall employ secure standardised communications mechanisms.
COM2	The provisioning mechanism shall also be able to run over other connectivity mechanisms: Internet (fixed or wireless), local connectivity (e.g. Bluetooth), NFC using the security mechanism specified for COM1. Subject to equivalent end-to-end security being provided.

7.4 Robustness Requirements Table

No.	Requirement
ROB1	The mechanism to install a subscription in a secure way should be allowed for the life-time of the eUICC.
ROB2	Mechanisms shall exist that safeguard against mis-application of provisioning changes on the eUICC that result in erroneous states or devices being unintentionally left without connectivity. {Note: the specific cases and procedures when fallback would be applied need to be defined.}
ROB3	The use of safeguard mechanisms shall be set at the time a eUICC provisioned state is to be changed.
ROB4	The SM shall be available 24 x 7 with extremely high reliability.

7.5 Liability Requirements Table

No.	Requirement
L1	The eUICC shall be specified, tested and approved by the operators approved body. {Note: Specification to include features to cover protection from attack etc.}
L2	SIM profile shall be specified, tested and approved by the operator.
L3	It must be possible to accredit the manufacture and provisioning of any solution in a similar manner to the current SAS provided by GSMA
L4	The provider of the subscriptions shall be the operator or a trusted party on behalf of the operator
L5	The SM shall notify MNOs of changes to status of their subscriptions in a device.
L6	Transfer of secure data (e.g. Ki and authentication algorithm) must be over agreed mechanisms which meet agreed common security requirements and where suitable trust relationships are in place.

No.	Requirement
	{Note: ETSI and Global Platform have prior work in this area that can be re-used.}
L7	After migration between MNO A to MNO B, each operator shall receive a proof of the subscription migration procedure execution; this proof shall be compatible with each legal courts able to represent each operator; In case this proof has not being received, the SIM shall be able to come back to the previous MNO A

7.6 Market Requirements table

No.	Requirement
MAR1	The eUICC shall comply with all standardised form factors, as per Ref 1.
MAR2	Any compliant solution to these requirements shall be able to be multi-sourced for competition and business continuity.
MAR3	If licensing is required for a solution to these requirements, any such licence must be granted on a FRAND basis. {Note: Ideally, solutions shall not require licensing and FRAND is seen as a maximum and not a necessity.}
MAR4	Any element of a solution to these requirements that needs to be used across or between ecosystem players shall be standardized and open.
MAR5	A compliant solution to these requirements should be commercially deployable in short timescales; guideline is 18 months from publication of this document.
MAR6	As far as possible, the solution should be based on existing standards for deploying (U)SIMs on UICCs - as per References to this document.
MAR7	As many as possible existing logistics, interfaces and processes should be retained in any solution to these requirements.
MAR8	The use of a eUICC must not mandate the need for any change in existing personalisation and distribution models.
MAR9	The solution should enable device manufacturing without pre-determination of either the operator network, or the geographic location where the device shall be used.
MAR10	Any MNO shall be able to choose from a range of trusted parties to provision a SIM profile to any given eUICC, rather than operators being “locked in” and forced to use the original supplier of the eUICC hardware. {Note: Several Subscription Managers may exist, and then an accredited process of eUICC handover and associated credential exchange has to be established between them (§4.1.5).}
MAR11	The solution has to support all existing business processes and provide the flexibility to enable new ones
MAR12	The entire MNO profile, including any eUICC authentication algorithms and associated data, remain the property of the mobile network operator, even when provisioned into a eUICC hardware device not supplied by the operator.
MAR13	There needs to be a cross-industry agreement on the base specification (or specifications) for a eUICC (e.g. memory size, OS, APIs, which standards realise compliance).
MAR14	Any solution to these requirements must be compatible with MNO strategies for third party services: GSMA PBM, GSMA digital signature and identity, NFC services.
MAR15	The solution must not preclude an MNO to play the role of the Subscription Manager.

7.7 Security requirements table

No.	Requirement
SEC1	The eUICC shall have a unique, constant and secure hardware identity.
SEC2	The hardware identity in SEC1 shall be in a secure way remotely accessible, for example to correlate the eUICC with a specific customer.
SEC3	Any process for loading credentials to the eUICC shall ensure that the plain text form of those credentials is only available within the destination eUICC.
SEC4	It shall be possible for the eUICC to provide an additional level of confidentiality between the MNO and the eUICC for subscription and secret data.
SEC5	Overall security shall be at least equivalent to that achieved with current removable UICC implementations, processes and OTA management.
SEC6	Current levels of resistance to Fraud within Provisioning processes must not be reduced.
SEC7	The SIM application must be at least as resilient to attack as current SIM application solutions.
SEC8	The embedded UICC arising from these requirements and any applications that reside upon it as part of a solution must also be as resilient to attack as current solutions.
SEC9	End to end protection needs to be provided when personalisation data is sent between trusted entities and where un-trusted entities form part of the data transmission.
SEC10	All data transmitted towards the eUICC under these requirements shall be integrity protected.
SEC11	It should be possible to upgrade the security of the SIM remotely (for example against new attacks on the authentication algorithm and if possible against new side-channel attacks). {Note: this is a desirable and not mandatory as currently written. Also, this requirement should be subject to eUICC capability.}
SEC12	Private data of an operator shall never be disclosed to another operator without his agreement.
SEC13	Any solution to these requirements shall define conditions in which security conditions data can or cannot be updated
SEC14	Under no circumstances shall a device be allowed to use a mobile channel (for provisioning) unless the device is authenticated for mobile access. In particular, provisioning may only take place over a mobile channel if there is already a credential in place allowing authentication to an MNO so that the device can use that mobile channel.
SEC15	eUICC provisioning shall be done in such a way that a provisioning message created for one eUICC cannot be misused to provision or modify any other eUICC; nor can it be recorded and later misused to modify the target eUICC a second time. Cryptographic means may be used to achieve these requirements.
SEC16	Authentication of a eUICC and SM shall be mutual in both directions.
SEC17	Any MNO or SM should be able and allowed to check that the new remote candidate eUICC is compatible with their minimum secure, operational and functional requirements. This check may be performed remotely in a secure way. {Note: The results of such a check are likely to form a part of policy control decisions.}
SEC18	Any solution to these requirements shall be no more vulnerable to large scale denial of service attacks than current provisioning systems

7.8 Certification Requirements Table

No.	Requirement
CERT1	Certification to include a formally evaluated certification under an agreed Protection Profile for the eUICC.
CERT2	Certification to include an SAS-like accreditation for the eUICC manufacturer, covering, at least, its processes for key management and initial provisioning.
CERT3	Certification to include an SAS-like accreditation for the Subscription Manager, covering, at least, its processes for key management and OTA provisioning.

8 Ongoing Topics

To enable Embedded SIM to reach the market, the GSMA intend to continue their work on a number of areas connected with the introduction of Embedded SIM, especially on topics where ‘standardisation’ bodies are not typically active / involved or where it is too soon to undertake work in a standards body. A non-exhaustive list of such topics is provided below. This work will be conducted as part of a GSMA project and within the appropriate GSMA Working Groups.

No.	Issue	Description
1	eUICC Ownership	Introduction of the eUICC within M2M and Embedded Devices is likely to introduce changes to UICC ownership from the current solution of being MNO owned. The consequences of changes and how they are addressed need to be resolved.
2	eUICC Certification	Currently, it is unclear which body should do the eUICC certification. In addition, a Protection Profile will need to be defined. See section 4.3 eUICC Certification.
3	Trust and Liability Models / Role of the SM	The necessary relationships between SMs and MNOs.

9 Document Management

9.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0	28 Nov 2010	Initial version		Ian Pannell / GSMA
0.61	10 Jan 2011	Update incorporating comments provided on version 0.6.		Ian Pannell / GSMA
0.62	14 Jan 2011	Post meeting version for final Task Force review prior to sending to GSMA EMC, SG, SC.		Ian Pannell / GSMA
0.63	17 Jan 2011	Final version for EMC, SG review		Ian Pannell / GSMA
0.7	2 Feb 2011	Final Draft Version		Ian Pannell / GSMA
0.8	4 Feb 2011	For SC Approval		Ian Pannell / GSMA
1.0	21 Feb 2011	SC Approved		Ian Pannell / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org
Your comments or suggestions & questions are always welcome.