Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries

Concept and processes for MCIM management

Harald Bender, Gerald Lehmann
Nokia Siemens Networks
Research
Munich, Germany
harald.bender@nsn.com, gerald.lehmann@nsn.com

Abstract—

The fast growing market for wireless Machine-to-Machine (M2M) communication services is facing specific challenges which do not exist comparably in the traditional cellular subscriber market. The challenges are emerging around the changed ecosystem and value chain and dealing with different traffic and load profiles in the network. The significantly reduced ARPDs (average revenue per device) are calling for increased operational efficiency and flexibility and tangible cost reductions. With regard to the requirements arising in this context this paper focuses on new concepts for SIM management (SIM: Subscriber Identity Module) in the M2M domain from a subscription management perspective in order to develop an economic MCIM provisioning process (MCIM: M2M communication identity module).

Three technical concepts were addressed and described with a look on the critical features. Essential items are the circle of trust, the grade of flexibility, the complexity of the solution and the impact on security. A further evolution of the Embedded UICC (Universal Integrated Circuit Card) proposal currently handled in standardization is presented and discussed, which gives the device owner and the M2M service provider a more active role and responsibility in the process. This approach enables full flexibility for change of operator and subscription and requires less administrative effort from MNOs (Mobile Network Operators), in particular for devices currently not requiring an active subscription.

The respective business processes for MCIM management are presented as blueprints and discussed with regard to the lifecycle phases. There is a need for an increased grade of automation and integration of these workflows going beyond the boundaries of a particular stakeholder participating in the value net.

Keywords – M2M; SIM; MCIM; eUICC; provisioning process; subscription management; circle of trust;

I. Challenges of the M2M market

Today, the cellular market arena has huge expectations and hopes regarding the growth and volume of the new Machine-to-Machine (M2M) segment. It is currently seen as one of the very promising growth segment of the future which is also reflected by the fact that continuously new players are entering the scene.

End of January 2012 the OECD (Organization for Economic Co-operation and Development) has published the report “Machine-to-Machine Communications, connecting billions of devices” as part of the series of “Digital Economic Papers” (No. 192) [1] where they have analyzed the M2M market with a particular focus on mobile wireless networks. They have looked at a number of analyst reports with regard to the market development and came to the forecast that over 50 billion devices will be connected by the end of 2020. That is roughly ten times the number of nowadays cellular subscribers, but certainly with significantly different and diverse traffic profiles.

The M2M services are characterized by industry specific solutions with embedded cellular connectivity. From a big picture perspective these services can be structured into two tracks with three categories each (ref. McKinsey Quarterly 2010/2 [2]), namely *Information and Analysis* with the categories *tracking behavior*, *enhanced situational awareness*, and *sensor driven decision analytics* and secondly *Automation and Control* with the categories *process optimization*, *optimized resource consumption,* and *complex autonomous systems.*
More concretely Harbor Research [3] has identified 10 industry segments where M2M services will emerge, which are Buildings/ Facilities/ Homes, Energy & Power, Industrial, Healthcare, Retail, Security & Infrastructure, Transportation, Information Technology & Network Infrastructure, Resources, Consumer/ Professional. This shows that it’s really about a cross-industry domain when talking about M2M.

When looking at the broad range of M2M services, each service will have its own specific functionality and requirements. In terms of the underlying connectivity layer there are significant commonalities regarding functions and capabilities. We are discussing those capabilities with a specific focus on the provisioning process of M2M. The new requirements for this process are caused by the business challenges described below.

978-1-4673-1526-5/12/$31.00 ©2012 IEEE

A. Business challenge 1: Low ARPDs (average revenue per device).

In many of those services the bandwidth demand and therefore the data volume transferred is rather low compared to personal communication services, i.e. also the average revenue per device will be significantly lower than for cellular subscriber services. This is certainly true in the initial phase of the mass market of M2M services. The situation will change once multi-media rich services emerge (e.g. thinking of the healthcare sector where surgeries could be supported remotely by experts if an appropriate image or video quality is available).

B. Business challenge 2: Change of UICCs("SIM cards") during lifetime is not feasible.

One of the characteristics is that for many M2M services the lifetime is much longer with up to 30 years compared to the five to seven years of traditional wireless communication [1]. This calls clearly for the capability to change the operator during lifetime without swapping the UICC (Universal Integrated Circuit Card), also colloquially named "SIM card". In most cases the UICC can't be exchanged since it would be by far too costly to send service personnel to the dispersed devices and machines and in addition the UICCs embedded in devices are not removable as they are soldered in the communication module (form factor MFF2: Machine-to-Machine Form Factor 2).

The above listed different industries show that there are additional roles and players in the M2M ecosystem, e.g. the role of an M2M Service Provider who is supposed to get wholesale access to the mobile network (B2B: business-to-business) and offers industry specific services.

Conclusively that means that there are more and new stakeholders joining the value chain. It seems to be a key factor of success for this new market and a prerequisite for the fast growth that the provisioning, activation, and life-cycle management of the cellular connectivity has to be standardized and automated at the highest possible degree. The preventive provisioning of wireless connectivity into all kind of equipment, devices, and appliances creates the playground and basis for the agile development and deployment of new M2M services at mass scale.

In the following chapters this paper outlines alternatives for the subscription change during the device lifetime and the supporting business processes specific for the M2M market. The respective challenges were initially identified and analysed in a collaboration project between the GSM Association (GSMA) and Nokia Siemens Networks conducted in the 2nd half of 2010. The results of this project were also presented on last year's poster session of the ICIN conference. (ICIN 2011) [4].

The objective of the described and discussed concepts for MCIM provisioning is the contribution to an ecosystem in order to enable fast growth of this new market segment with its fascinating new perspectives and to prepare benign frame conditions for it.

Prerequisite for a broad penetration of cellular connectivity is certainly that the provisioning and commissioning of the embedded communication capabilities is transparent for the end-customer. A key requirement for a good user acceptance is that he doesn't have to run a dedicated setup procedure each time he is switching on the device.

A Smart Metering service deployed by an utility is a good example to understand the urgency to change a subscription during lifetime: One scenario is that the Service Provider of the Smart Metering service is ceasing his contract with the operator, which means that all deployed smart meters must be updated with a new SIM respectively MCIM and related subscription data. But also in case an owner or tenant of an apartment is changing the utility he has a contract with, the MCIM and subscription data for this particular Smart Meter needs to be updated. Both cases emphasize the necessity to automate this process to the highest degree.

II. SOLUTIONS ADDRESSING THE CHALLENGES

The discussion around concepts and solutions addressing these challenges of a subscription change is ongoing already for a longer time. E.g. in a technical report issued two years ago by 3GPP standardization titled "*Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment*" [5] the different opportunities were listed and discussed. This report differentiates between the alternatives "TRE based" (TRE: trusted environment) and "UICC based" solutions. As often "TRE based" is colloquial, but not correctly translated into "Soft SIM", this structure might have hindered the objective view and discussion of the different features each solution brings in. It is of value to decompose each solution in its features, and to assess, how one feature contributes to ***security***, ***flexibility*** and ***costs*** of the whole solution. NSN reviewed the concepts proposed by various parties and extracted their relevant features. May be not astonishing for insiders very often the same or similar features were used in different concepts, also in UICC and non-UICC based concepts. We discuss the following ones more in detail:

- **A shielded, protected, separated and trusted area at the device** for hosting credentials and for providing mechanism for mobile networks access and credential management. In the following we name this area more neutrally *Protected & Trusted Device Area (PTDA)* – This area is able to hold IDs, algorithms, device authentication credentials and network access credentials. This could be either an eUICC or a Trusted Environment (TrE). The functionality and relevant features of this PTDA need to be standardized and every manufacturer has to certify, that a specific chircuit component is compliant to that standard. An important security-related feature is the strong physical binding of the PTDA holding the network access credentials to the device. This is necessary, because often devices are unattended and can be a target for manipulations. This tight binding can be achieved by using a resistant housing or shielding and by using integrated circuit form factors directly soldered on a Printed Circuit Board (PCB). A very high integrated option is to place this entity on the same ASIC (Application Specific Integrated Circuit) together with other elements of the embedded system of the device, so that a separation of the device's embedded system and his network authentication part becomes much harder. However, this totally integrated solution requires a new trustful cooperation of MNOs with device vendors producing such components.

- **A central entity hosting credentials**. These credentials were generated during the early phase of manufacturing of the PTDA and then assigned to a device. These credentials need to be stored also outside the device, so that the device can be securely addressed later on. These primary credentials can be used for (first) device authentication and/or for the encryption of MNO-specific credentials. Also subsequent subscriptions (or MCIMs) can be securely downloaded to the device only with the help of these credentials. In consequence, this common entity has to host the primary credentials during the whole lifetime of the device and subscriptions cannot be changed, when this entity or the access to this entity is not available anymore. Since one global entity seems to be not feasible and not accepted by all stakeholders, it is likely, that several entities will exist, which need to federate for providing global operation. Business-wise, this entity is a new role in the subscription provisioning process with need to be financed. This entity has to host credentials also for devices with integrated wireless connectivity which might not into operation during lifetime.
- One characteristic for enabling security needs to be highlighted, that is the **Small Circle of Trust**. In fact, this feature is one major pillar of secure SIM and subscription management incl. secure authentication in UMTS/GSM networks. The trustful exchange of keys and algorithms between an MNO and his selected UICC vendor is a major warrantor that keys do not leak to other parties or fraudsters. One target for a new concept for MCIM provisioning is certainly to keep a minimized number of parties handling with credentials in this circle of trust.
- **The (delayed) download of MCIMs**, or other credentials, parameters and control information over the air to the device is a must, when the requirement of a subscription change in the field should be supported. This feature introduces a new potential vulnerability compared to the credential handling in the conventional UICC case. However, this vulnerability is common to all concepts supporting an over-the-air MCIM change. Therefore, this feature needs to be hardened with up-to-date encryption techniques and related measures.

We take now a closer look to these concepts or solutions:

A. "Handover"of credentials

A more or less obvious option is a "handover" of credentials from MNO A to MNO B, so that at the device side only minimum changes need to be applied. In principle, only the IMSI (International Mobile Subscriber Identity), which indicates the home network, needs to be exchanged at the device. The credentials for network access and device access remain the same, and this avoids the download of these credentials to the device. Of course, after a change, the corresponding credentials have to be removed from the MNO A's network (and this means securely deleted) and forwarded to MNO B. MNO B has to provision the credentisls to his network. The charming aspect of this approach is that this is already feasible with today's UICC cards, since the IMSI is in most cases rewritable by using existing OTA (over the air) mechanisms. This approach was already discussed for a longer time, e.g. also in the 3GPP study [5]. Besides the prerequisites, that both MNOs have to agree on a minimum set of UICC features and algorithms to be supported, it is very essential that both trust each other. In particular, the overtaking MNO B has to trust the former MNO A that he has securely deleted the network access credentials and OTA keys after the change, because this information paired with the new IMSI enables UICC control and network access to MNO B's network. In case of series of handovers during the device lifetime, the current MNO needs to trust also the whole chain of former MNOs. In order to overcome this drawback, another variant introduces a list of credentials already pre-stored on the UICC during manufacturing. Here, in case of an MNO change, the device is only instructed via OTA to take the next credentials from the list. MNO B needs to obtain the new credentials from a central entity, who hosts the corresponding list outside the device. The operator of such a managing and hosting entity could be the UICC manufacturer, a global acting MNO or another 3rd party. With this variant, the extension of the circle of trust comes only in another configuration: All potential MNOs have to trust this central entity managing the list of credentials.

B. GSMA/ ETSI eUICC proposal

Under the headline „Embedded UICC (eUICC)" a work item was created, which is handled by the ETSI Smart Card Platform (SCP) standardization body. This item was initiated by the GSMA under the name "Embedded SIM" and is supported by some MNOs and smart card vendors. In a first step, requirements from an MNO's point of view were defined, which were mostly taken from the GSMA proposal [6]. The basic requirement that a device owner/subscriber can in principle change the subscription from operator A to operator B is included, but without the definition what the minimum prerequisites are, so that a device owner can change to *any* operator B. Does this solution enable a device owner to switch from A to B (and back) as fast as he likes, as long as respective subscription contracts are valid? A closer look to the current discussion in ETSI SCP reveals, that this proposal represents basically an extension to the usual UICC card provisioning and handling, which is enabling a more or less restricted change of MNOs during the device lifetime. This concept supports Embedded UICCs (eUICC), which are mounted (e.g. as a soldered chip using the form-factor MFF2) during M2M device production. Also an eUICC contains a first set of credentials, which are neither removable nor re-writable. Outside the device the related credentials are hosted the whole device lifetime by a new entity named subscription manager (SM). Main tasks of the SM are the creation of an MNO-specific profile using these credentials (subscription manager data preparation (SM-DP)) and the secure provisioning of these to the device (subscription manager secure routing (SM-SR)). The way how the encryption of the download and the authentication is done in detail (cryptographic details) is not standardized yet.

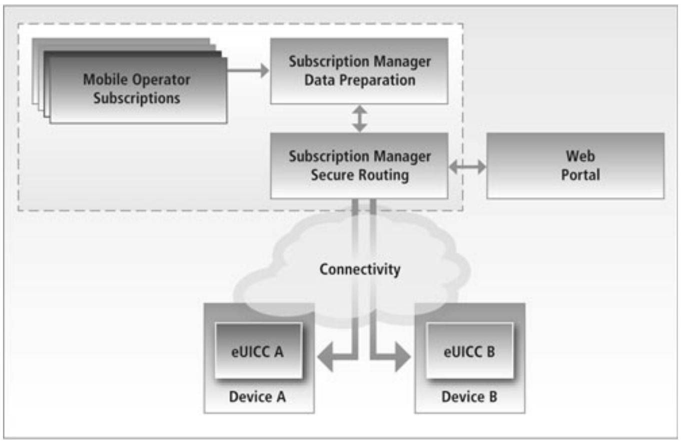
Mobile Operator Subscriptions
Subscription Manager Data Preparation
Subscription Manager Secure Routing
Web Portal
Connectivity
eUICC A
Device A
eUICC B
Device B

Figure 1. "Embedded SIM" Remote Provisioning Outline [7]

If the SM-SR holding the device access credentials does not belong to the MNO selected by the device owner, different SMs can cooperate by using an SM to SM interface and protocols to be standardized by ETSI SCP. This enlarges the circle of trust, at the end all potential MNOs have to trust the common instance and the network of SMs. If there is no trust and no cooperation to one MNO (e.g. because this operator doesn't belong to the specific circle of trust supporting the change), this MNO cannot be chosen by the device owner. As we highlighted earlier, a small circle of trust is essential for security and fraud resistance, but the outlined concept requires that all potential MNOs trust the central SM entity holding the device access information, and every MNO needs to trust all MNOs to which the device owner is enabled to change. This is quite different and more complex when compared to the small circle handling the conventional UICC provisioning. A globally present MNO could consider minimizing this risk by only cooperating with his national subsidiaries, but this of course would not fit to the original requirement of a free choice.

Also a more or less quick change of the MNO is not in scope of this proposal. Given examples assume always a change after years and the requirement that there "shall be only one active profile on an eUICC" was indicated as essential by major MNOs and smart card vendors [8]. This might be not acceptable for M2M applications with high mobility or in regions, where one MNO provides only moderate coverage outdoors and/or indoors.

In order to have initial wireless connectivity for the first provision a provisioning profile, which is installed on the eUICC during manufacturing, is needed for a later over-the-air (OTA) provisioning. Another option is to use another IP connection of the device.. But for low-cost devices having no other interfaces a provisioning profile stored during manufacturing is mandatory. In this case one MNO supporting global roaming needs to be involved in the first configuration of the eUICC anyhow and has to supply a first subscription in this early phase of the device lifecycle.

The concept of keeping the subscription manager (SM) in control of the device's subscriptions brings also advantages to the device owner. As the operator of the SM (e.g co-operating MNOs and/or smart card vendors) takes at the same time the responsibility for network connectivity availability, secure device authentication and secure access to the PTDA, the device owner does not need to care about this. This "care-free" packet includes providing initial and continual connectivity for the whole device lifetime and security measures independent from the rest of the device (achieved by introducing certified and trusted eUICCs). M2M applications in the security domain might welcome the benefit from this.

C. Further concept evolution

When compared to the requirements discussed in chapter I, a further evolution of the Embedded UICC proposal needs to cover the following points:

- Raise the attractiveness of cellular M2M connectivity seen by M2M service providers and device vendors by offering a more flexible solution.
- Minimize the costs of MNOs for subscription and credential management of devices, also considering devices where the cellular connectivity is not used during lifetime.

This leads to following key questions:

- Who takes the responsibility for the mobile network access option when the device is produced, but not put into wireless operation?
- What is the business model for central entities like the SM, i.e. who operates it and pays for it over the whole lifetime of the device and guarantees at the same time, that a device can get wireless access as long the device exists?

One option is the device owner, who should manage the device operation incl. wireless connectivity. Only he knows when a device lifetime ends and he should provide all needed device information so that a device can be connected to the network. So why not giving him an active role in this process? In particular in the M2M domain it can be assumed that the device owners are mostly companies like M2M service providers who are able to fill this role in a dependable way.

The MNO needs to trust and to accept the device owner (his customer) and the device, for which the customer applies for wireless connectivity. Both need to be identified and authenticated. But it is beneficial, to see the two identification procedures together.

For device authentication it is indispensable to have a protected and trusted area (PTDA) for storing the credentials as mentioned before, e.g. in an eUICC. But instead of keeping related credentials in a common entity like the Subscription Manager, those keys will be forwarded to the device owner together with the device. Asymmetric cryptography should be used here, and only the public part of the keys is forwarded or made accessible to the device owner, while the private half of the asymmetric keys resides in the device only.

The device owner can use the initial or already existing connectivity to the device to prepare the access for a newly selected MNO, e.g. by assigning a new MNO access key. In a second step, the device owner applies for a mobile subscription for his device at selected MNO. When the MNO accepts the device, he gets the public device access key, his specific access key (the one generated and downloaded by the device owner) and PTDA information (e.g. which type and certification) directly from the device owner together with the current device access information. With these keys the MNO is able to access, identify and authenticate securely the device and to download an encrypted MCIM to the device, which can only be decrypted by the device itself. But is this secure enough? How can a download to a compromised or non-certified device be prevented?

Since network access security is of course essential, we draw an example of an attempt to defraud in the following: Let us assume that a fraudster wants to get hold of network access credentials and he has no certified device, but an open software platform implemented with relevant key handling procedures. So he could generate his own asymmetric key pair and forward this together with other needed information to the MNO during subscription application process. For getting a subscription contract, the fraudster needs to identify himself or has to use a stolen identity. If accepted by the MNO, a download of a valid MCIM could take place to this compromised open platform, and the fraudster is able to decrypt the network access key, since in this case he is also aware of the private key generated by him. He could also clone this key and use it for further purposes in multiple devices. But what is the potential damage to MNO in this case? First of all, if the customer is known to the MNO, he is able to evaluate, if this is a regular professional business partner, may be already known from former subscription contracts. So the identification and authentication of the device owner should be seen as a relevant part of the whole process, which is done anyhow. Second, it is recommended to follow a pre-paid model, so that a fraudster has to invest here. Third, fraud detection measures in the network can detect concurrent subscription use and other fraud cases. Fourth, the potential financial damage to the MNO is anyhow always limited to the connection costs, as the MNO does not take anyway responsibility for risks caused by devices on application level.

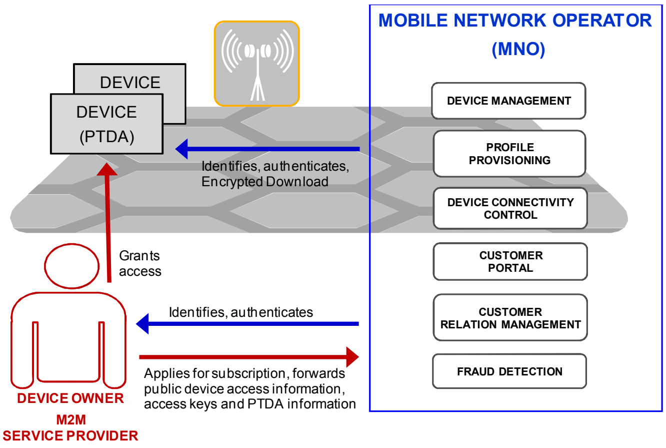
MOBILE NETWORK OPERATOR
(MNO)
DEVICE MANAGEMENT
PROFILE PROVISIONING
DEVICE CONNECTIVITY CONTROL
CUSTOMER PORTAL
CUSTOMER RELATION MANAGEMENT
FRAUD DETECTION
DEVICE
DEVICE
(PTDA)
Identifies, authenticates, Encrypted Download
Grants access
Identifies, authenticates
Applies for subscription, forwards public device access information, access keys and PTDA information
DEVICE OWNER
M2M
SERVICE PROVIDER

Figure 2. Outline Revised Concept

With this simplified customer-centric provisioning model, the device owner can choose any operator he wants, but he has to take the responsibility for the secure subscription management for his device(s), e.g. he has to host the keys and protect them against unauthorized access. He has to ensure and be responsible, that the device is certified, follows certain standards, and is not compromised. For example, this can be assumed for the automotive industry, as the embedded systems mounted in a car have their own security and reliability requirements.

The circle of trust is kept small here, since the MNO has to trust his customer (e.g. the M2M service provider or the device owner) and the integrity of the device.

The MNO is unburdened from administration tasks, does not need to maintain additional interfaces to other entities than the customer and the device itself. He can do this with extensions to his already existing Customer Relation Management (CRM) and Device Management (DM) systems. This concept benefits also from the re-use of existing systems at the network side as fraud detection and the direct interface to customers via portals.

D. Summary of solution characteristics

The handover of credentials solution could be a fast stop gap solution, however the required enlargement of the circle of trust seems to hinder the wide application. The Embedded UICC proposal follows the approach that the subscription management is handled by MNOs and trusted partners autonomously, taking the whole responsibility for secure device authentication and connectivity. This might provide a higher level of security, it comes inherently with the drawback that only these trusted partners can be chosen for an operator change. A revised variant puts the device owner in a more responsible role, and therefore the MNO has to trust in a certain way his customer. Such a trustful relation can be assumed for commercial M2M service providers bringing bulks of devices into the networks. It addresses the flexibility needs of M2M service providers paired with remarkable less administrative effort assigned to network operators.

III. Business Process for a Flexible MCIM Provisioning Concept

As already outlined in the first chapter, the characteristics of the M2M ecosystem require more flexible procedures for the provisioning of MCIMs. This significantly impacts the composition of the business process which is steering the e2e workflow divided in (1) the initial provisioning resp. bootstrapping (preassignment and initial activation) of the MCIMs, (2) the lifecycle operations (e.g. use case "change of operator") and finally also for (3) end-of-life and market phase out of machines and appliances with embedded connectivity.

The top-level constraints from current perspective are certainly the expected lower ARPD (average revenue per device) and the more fragmented value chain where new players especially from the vertical industries are emerging. Additionally it needs to be considered that the lifetime of a device or machine with embedded cellular connectivity is in most cases significantly longer than the typical contract term of end-user communication services like voice or SMS.

These constraints call for the highest possible degree of automation and integration of the related business processes. An additional challenge in that scope is that the workflows related to MCIM provisioning are executed by multiple parties of the M2M value chain who are often represented by different companies.

On the top level the MCIM provisioning process can be structured into 3 main phases (figure 3) which are ***(1)*** the ***Preassignment***, ***(2)*** the ***Initial Activation***, and ***(3)*** the ***Operation Lifecycle*** which also includes the phase out of a particular machine [4].

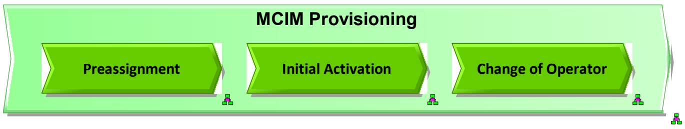

Figure 3. MCIM provisioning process

The described process flow relates to the 3rd solution approach as elaborated in detail in the previous chapter (utilizing the asymmetric encryption to download a new MCIM to the PTDA). This enables the Service Provider to directly download the MCIMs to the concerned device.

The design of the process and the documentation was done using the ARIS method [9]. Beside the process model also the associated data model was defined using UML (Unified Modeling Language).. The data model is not further explained in this paper.

The decomposition of the process phases into the particular actions and steps reveals the interaction between the different roles resp. parties participating in the M2M value chain.

The provisioning process is typically triggered by the ***Service Provider*** when ordering new devices resp. communication modules for a dedicated service or application. This request goes to the ***OEM Device Integrator*** who is either delivering the ordered devices from stock or has to start the production of new ones. This in turn might require to order modules from the ***Communication Module Supplier*** with integrated Protected and Trusted Device Areas (PTDA), where this area might be either an integrated trust zone or a separate chip (eUICC) which can be mounted (soldered) in the communication module. The **PTDA Supplier** will generate the device specific key material, where only the private part is stored in the device. The Service Provider is then capable to provision the first connectivity (provisioning profile) to the devices he ordered.

The preassignment (figure 4) decouples the production of the communication module from the provisioning of the connectivity. This differs significantly from the traditional established workflow for UICC provisioning where the key material and credentials needed for network access are already at production time provisioned into the UICC.

In the further course of the preassignment the Service Provider will order an MCIM (or MCIM batch) from the Initial Operator for the download of the encrypted MCIM data to the device, in particular to the target PTDA. The Initial Operator is the operator who delivers the provisioning profile. The Service Provider can then download the provisioning MCIM via a local (wired) I/F which meets also stronger security concerns.

It is presumed that a contract relationship exists between Service Provider and MNO for these subscriptions. This touches an open issue as there is no clear view yet on how the business model of the Initial Operator is working.

In order to activate the associated subscription a related entry must also be administered in the Home Location Register (HLR). With the activation of the MCIM of the provisioning profile on the PTDA the device is prepared for the over-the-air the download of the first operational MCIM which is part of the Initial Activation process step (figure 5).

The next phase of MCIM provisioning deals with the Initial Activation of a device to be put into operation. Some segments of the work flow sequence are similar resp. almost the same as the Preassignment part, different is basically the ordering and manufacturing part which can be omitted here.

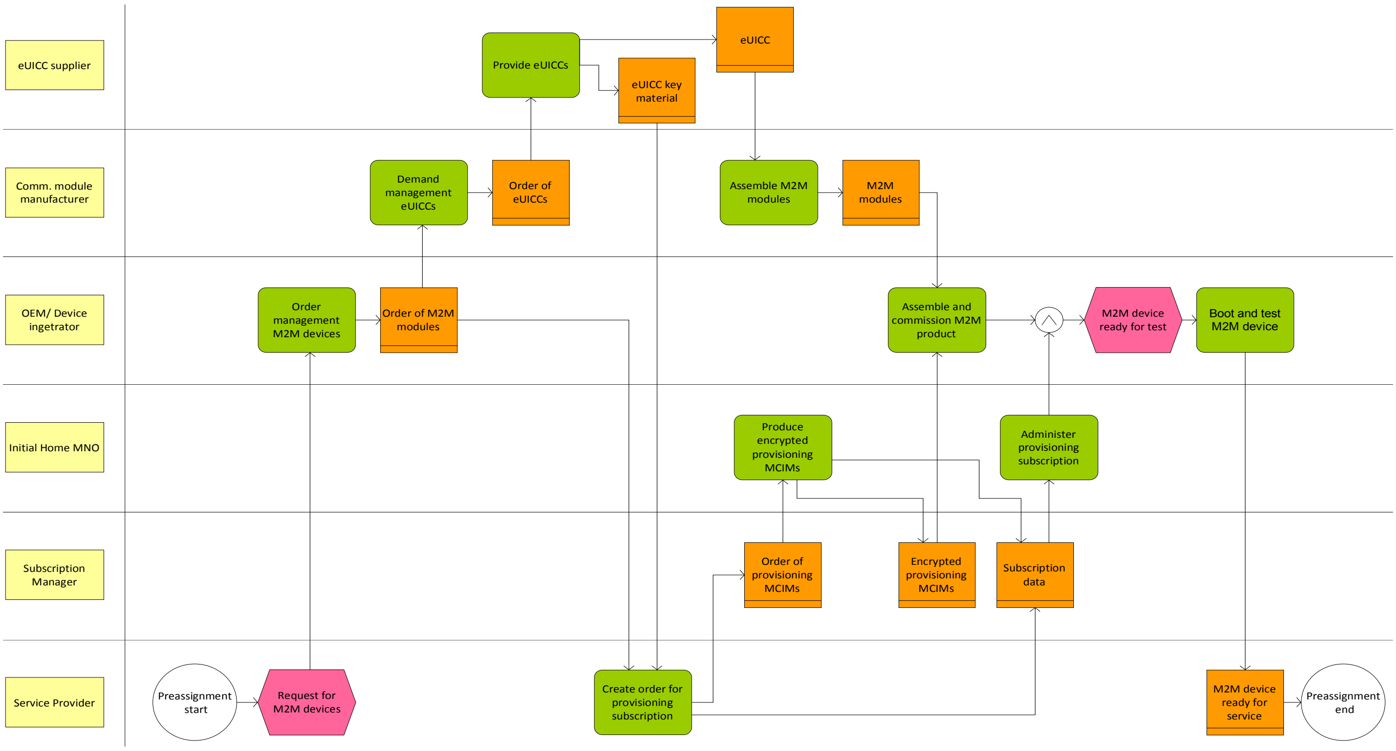

Figure 4. Preassignment phase

Either the Service Provider or a Retailer will trigger this process step and order a subscription together with the creation of a related (encrypted) MCIM from an MNO (MNO 2 in the diagram). With the creation of the related subscription data in the Business Support System (BSS) and in HLR of the MNO and with the activation of the related MCIM in the device the particular M2M service is ready for wireless operation (figure 5).

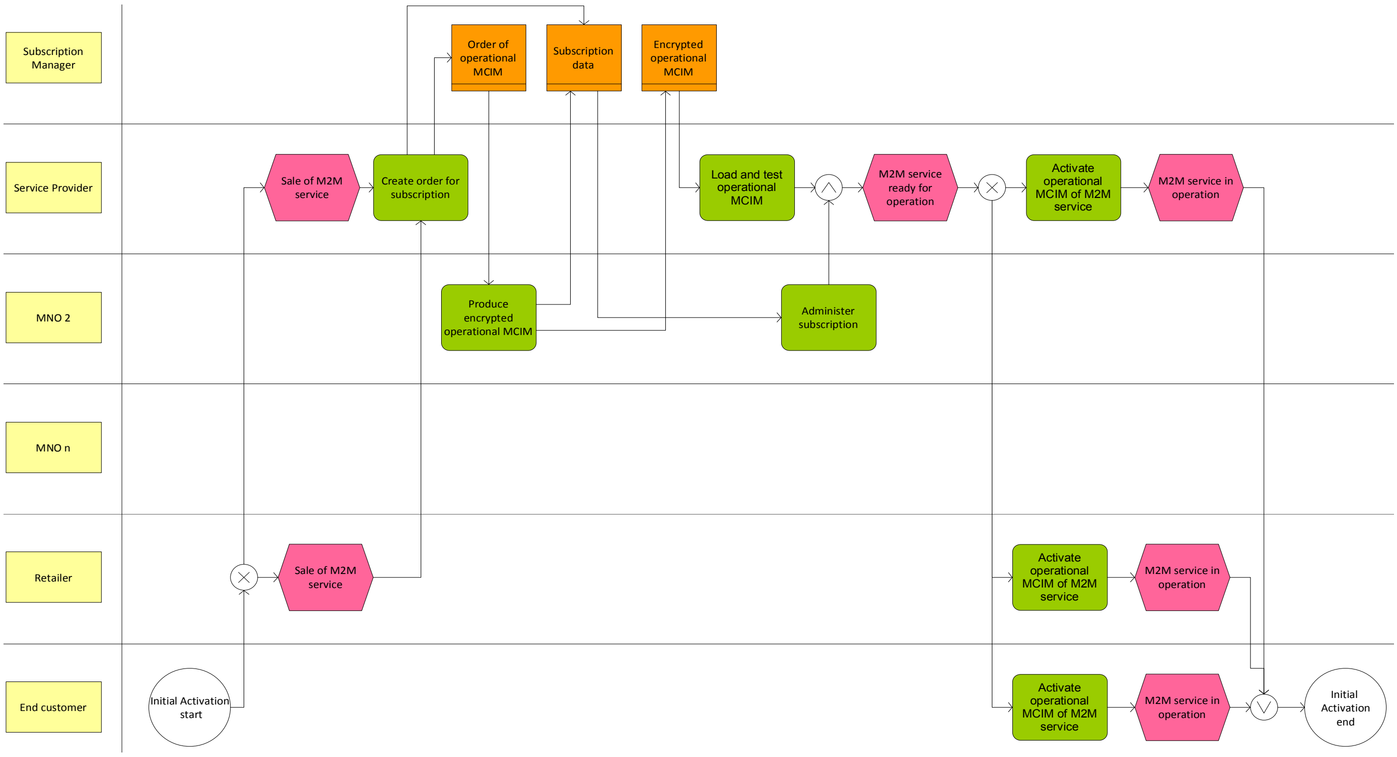
Subscription Manager
Service Provider
MNO 2
MNO n
Retailer
End customer
Order of operational MCIM
Subscription data
Encrypted operational MCIM
Sale of M2M service
Create order for subscription
Load and test operational MCIM
M2M service ready for operation
Activate operational MCIM of M2M service
M2M service in operation
Produce encrypted operational MCIM
Administer subscription
Sale of M2M service
Activate operational MCIM of M2M service
M2M service in operation
Initial Activation start
Activate operational MCIM of M2M service
M2M service in operation
Initial Activation end

Figure 5. Initial Activation phase

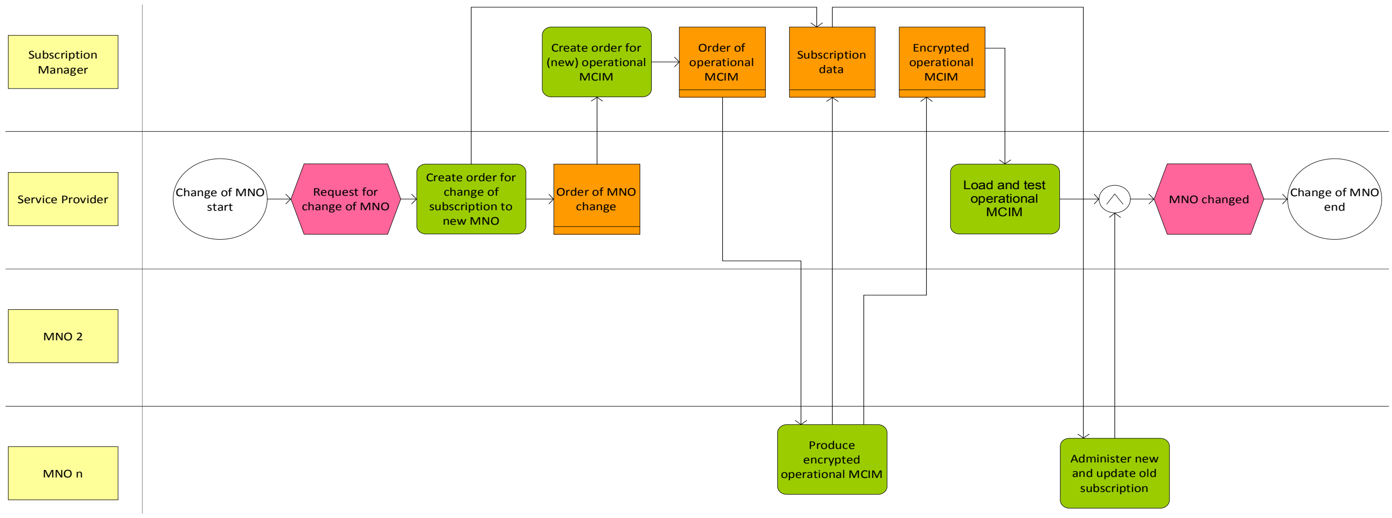
Subscription Manager
Service Provider
MNO 2
MNO n
Create order for (new) operational MCIM
Order of operational MCIM
Subscription data
Encrypted operational MCIM
Change of MNO start
Request for change of MNO
Create order for change of subscription to new MNO
Order of MNO change
Load and test operational MCIM
MNO changed
Change of MNO end
Produce encrypted operational MCIM
Administer new and update old subscription

Figure 6. Operation Lifecycle phase

It depends very much on the specific service provided in a particular vertical industry to what extent a change of subscriptions is necessary. This addresses the frequency of the subscription change and the average response time to a request for a swap of the subscription.

The Change of Operator is one of the use cases during the normal lifecycle operation and is one of the most important cases. The scenario is depicted in the diagram below (figure 6)

The M2M Service Provider has a central role for all steps in the workflow. He is the one to trigger the process and has a certain responsibility. E.g. in the case of change of operator it is the M2M Service Provider who initiates the ordering of new subscriptions and the associated encrypted MCIMs from the new operator. Once the encrypted MCIM is downloaded to the device a switch-over to the new subscription can take place..

As in the Preassignment and in the Initial Activation the new operator has to administer the subscription in the respective databases and systems. Once this is completed and the new downloaded MCIM is activated the new subscription is operational.

Finally it's necessary that the previous operator will get the information about the subscription change that he can deactivate the old subscription and release the related resources.

IV. Conclusion

Solutions for delayed and remote subscription change were outlined. The handover of credentials approach appears as a fast stop gap solution, however requires an extended circle of trust. The Embedded UICC proposal with a subscription manager as new role has some drawbacks mainly around the flexibility with regard to the change of the operator. A revised variant puts the device owner in a more responsible role addressing the flexibility needs of M2M service providers paired with remarkable less administrative effort for the network operators.

The visualization of the provisioning process points it out that additional stakeholders in new roles are joining the value chain, which makes it more sophisticated to get to the required higher degree of automation and standardization of that business process.

References

[1] OECD (2012), "Machine-to-Machine Communications: Connecting Billions of Devices", OECD Digital Economy Papers, No. 192, OECD Publishing. http://dx.doi.org/10.1787/5k9gsh2gp043-en

[2] Michael Chui, Markus Löffler, and Roger Roberts, "The Ineternet of Things", McKinsey Quarterly 2010 Number 2

[3] Harbor Research, "The Emergence Of Smart Business", Harbor Research Inc, 2010

[4] Harald Bender et al, "Business Transformation of the Provisioning Process for Machine-to-Machine", 15th Conference on Intelligence in Next Generation Networks, 2011

[5] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, "Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment", Release 9, 3GPP TR 33.812 V9.2.0, www.3gpp.org, 2010.

[6] GSM Association (GSMA), "Embedded SIM Task Force Requirements and Use Cases", Version 1.0, February 2011.

[7] GSM Association (GSMA), "Embedded SIM Remote Provisioning System", available at http://www.gsma.com/e-sim/, accessed March 2012.

[8] AT&T, Deutsche Telekom, France Telecom, Gemalto, Giesecke & Devrient et al, "Recommendations to ETSI SCP REQ on Embedded UICC work item", SCPREQ(11)0147r5, ETSI SCP REQ group, September 2011.

[9] ARIS: Architecture of Integrated Information Systems; available at http://www.softwareag.com/corporate/products/aris_platform/default.asp