



Smart Card Group - Smart SIM Project – Use Cases
Version 1.0
1st October 2009

This is a non-binding permanent reference document of the GSM Association.

Security Classification: This document contains GSM A Non Confidential Information

Access to and distribution of this document is restricted to the persons listed under the heading Security Classification Category. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those listed under Security Classification Category without the prior written approval of the Association. The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Security Classification – NON- CONFIDENTIAL GSM A Material

Copyright Notice

Copyright © 2008 GSM Association

Antitrust Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.



Table of Contents

1. methodology	3
2. General assumptions.....	3
3. Use cases	4
3.1 Overview	4
3.2 Use case detail	6
3.2.1 <i>Use case one: simple customer migration between devices.....</i>	<i>6</i>
3.2.2 <i>Use case two: deliver applications and services to customer in device agnostic way.....</i>	<i>26</i>
3.2.3 <i>Use case three: provide security for sensitive data.....</i>	<i>38</i>
4. Use Case PRIORITIZATION	48
5. use case input Documents.....	54
6. Appendix 1: Generic Standards (All Cards).....	54
7. DOCUMENT MANAGEMENT	55

1. METHODOLOGY

During the early stages of the project, participants were asked to share use cases. This document seeks to summarise those use cases, and identify benefits for the customer, MNO and device supplier.

This document forms part of Phase 1 of the GSMA Smart SIM Project

- Phase 1
 - Business opportunity review :
 - General and specific use cases
 - Functional requirement

2. GENERAL ASSUMPTIONS

During discussions at Meeting 2, 14th & 15th January 2009, a number of general assumptions were discussed and agreed.

1. Whilst we use the term “SIM” in this project and associated documentation, technically the cards under discussion are always UICCs. “SIM” is used out of habit, and because it is easier to say.
2. We must ensure secure and consistent interoperability exists between devices and the SIM
 - a. The card works consistently in legacy devices, as a legacy UICC.
 - b. Although some features on the card will only be supported if the device supports them (For example:- SCWS (Smart Card Web Server)), the basic card functionality remains always supported
 - c. Features such as SCWS are supported in a consistent and standardised way on those devices which do support it.
3. SIMs must remain device agnostic – that is they cannot have either device or application specific SIMs.
4. Solutions must deliver overall cost savings: either in terms of time to market of devices, or reduced development costs (preferably both).
5. A technical solution which increases time to market or overall costs is not of commercial interest.

Additionally, Meeting 2 noted that,

1. This project does not seek to state the size of memory required: memory requirements will vary depending on the number of features deployed by the MNO, and the amount of free memory left for the customer to use.
2. Protocol requirements will vary depending on use cases (but ISO and USB-IC are both standardised).
3. It is noted that some applications will be easier to implement than others
 - Example:- technically easier to implement: IM, MMS, Certificate Management, Address Book (but hard to change customer or device vendor usage)
 - Example:- technically more difficult to implement: Smart card web server, user data backup/secure storage

This project supports the following GSMA strategic objectives:

- SO#1 Stimulation of new products and services
- SO#2 Ensuring mobile services are interoperable
- SO#3 Supporting the evolution of GSM family of technologies

3. USE CASES

3.1 Overview

These use cases have been identified from the Input Documents, refer to Section [5.0](#). They have been reviewed, and classified into 3 different areas.

1. simple customer migration between devices
 - a. ensure device settings are automatically managed and configured
 - b. store customer generated content on card, and management of content
 - i. synchronise address book data base between device and SIM (see also 2.a for support of multimedia address book application)
 - ii. customer created photos, videos and so on
 - iii. customer generated messages (SMS, MMS, emails)
 - iv. customer content from and to example laptop, moved to SIM card – personal secure USB stick
 - c. customer (bill payer) preferences
 - i. for volume settings, wallpaper, favourites (bookmarks)
 - ii. list of the customer-purchased applications which were on the previous device (which then need to be downloaded or upgraded)
 - iii. ensure corporate customers can securely manage the UI (for example OMA DM and device management, use of Enterprise Management Authority)
 - d. store customer purchased content
 - i. ringtones, music and so on (note: associated DRM certificates handled in Part [3c](#))
 - e. distribute and store MNO content on card
 - i. content (note: associated (DRM or media) certificates handled in Part [3c](#))
(but independently from the scheme)
2. deliver applications and services to customer in device agnostic way
 - a. multimedia address book application (see also part [1.b.i](#) for syncing of the data base, and SIM applications/services based on address book data base)
 - b. take a vanilla device, and enable MNO customisation of device (excluding applications, and device settings as covered separately) in device agnostic manner
 - c. take a vanilla device, and enable MNO customisation to occur via the insertion of the SIM by installing the applications onto the device (application distribution), in device agnostic manner
 - i. MNO applications
 1. Instant Messaging
 2. Helpdesk
 3. Email with pictographs

4. Widgets
 5. Mobile auction service (with presence status for item sale information)
 6. MNO applications store
 7. Language Pack
 - ii. 3rd party applications
- d. take a vanilla device, and enable MNO customisation to occur via the insertion of the SIM by enabling access to these applications which remain on the card, in device agnostic manner
- i. MNO applications
 1. Instant Messaging
 2. Helpdesk
 3. Email with pictographs
 4. Widgets
 5. Mobile auction service (with presence status for item sale information)
 6. MNO applications store
 7. Language Pack
 8. Services Discovery Portal
 9. Mobile advertising, banners, promotion push
 - ii. 3rd party applications
3. provide security for sensitive data
- a. protect personal data stored on card
 - b. provide secure authentication mechanism for online and offline (contactless) transactions
 - c. DRM or media certificates associated with content use cases identified above
 - d. authentication to multiple (all) network types, thanks to credentials stored on the card
 - e. securely store passwords and login details
 - i. example, email access credentials, automatically accessed by device email client on device set-up
 - ii. company VPN credentials
 - f. Certificate Management
 - i. MNO certificate for Device applications

3.2 Use case detail

This section will now take each use case in turn and provide,

- description of use case (or as appropriate, problem statement)
- proposed Smart SIM solution
- benefits (consumer, device supplier, MNO)
- alternative mechanisms for implementation
- issues

3.2.1 Use case one: simple customer migration between devices

Within these use cases, all ideas enabling the customer’s smooth migration from one device to another are included. Such use cases will enable a customer to change devices more frequently – for example, at the weekend – as well as the less frequent device upgrade (approximately annually).

<i>3.2.1.1 Use Case 1a: Ensure device settings are automatically managed and configured</i>	
Description	<p>Currently, if a customer receives a generic device, or a device which was customised for a different MNO (either at point of manufacture, or after sale), then the customer is likely to experience problems with device settings.</p> <p>Typically these problems will relate to GPRS, MMS and internet settings.</p> <p>This solution will ensure that when the UICC is inserted, a network event is triggered. The customer sees a simple statement on their screen saying “Device change detected, would you like us to correct and optimise your device settings?” If the customer hits yes, the device settings are updated. (Customer is given the choice, because it is their device.) There is no need to turn the phone off/on again for the settings to become active.</p>
Benefits - consumer	<p>Device always works: no need to manually enter configurations.</p> <p>Can easily and confidently change device, not a barrier to device change.</p> <p>Can utilise new applications which require a data connection (for example, Facebook).</p> <p>Simple and straightforward process.</p>
Benefits - device supplier	<p>No need to customise the device settings for each MNO.</p> <p>Less to do, less to test.</p> <p>Because the process of device configuration is simple and straightforward for the customer, it encourages the customer to own multiple devices, or change more frequently, it lowers the threshold to own a new device.</p>

<i>3.2.1.1 Use Case 1a: Ensure device settings are automatically managed and configured</i>	
Benefits - MNO	<p>Customers with the correct device settings will generate more revenue, as they are able to use MMS, internet and so on (service continuity). Customers with the correct device settings will generate revenue from their use of new data-using applications (like Facebook and others).</p> <p>Customers are less likely to call or ask retail stores for assistance: such support can be complex and time consuming.</p> <p>Customers, who are confident that their device will work correctly, are more likely to remain with that MNO (churn benefits).</p> <p>As the volume of SIM-only connections and second hand device market increases, this issue of incorrect device settings is increasing.</p> <p>Aids time to markets of generic and customised devices purchased by the MNO.</p> <p>Transferring data between devices is so complex that it also often triggers the customer to investigate changing MNO at the same time – when all the data is on the SIM, this decision need not arise.</p> <p>Because support for Smart SIM has improved overall support for SIM cards, it makes the decision to invest further in SIM technology easier to make.</p> <p>The solution is fully standardised and commercially available today.</p>
Proposed solution 1	<p>Comprises two components,</p> <p>OMA DM Bootstrapping File on card containing sufficient data for card to connect to the home network’s device management platform for the first time, even if the device contains no settings data at all.</p> <p>IMEI tracking STK application The application interacts with the device management platform on the network. This platform has a history of the devices used by this customer, and also contains the correct device settings for every device.</p>

<i>3.2.1.1 Use Case 1a: Ensure device settings are automatically managed and configured</i>	
	Note: these features are fully standardised today.
Proposed solution 2	Can store MMS and GPRS settings on the SIM. (These are generic, device agnostic.) Note: these features are fully standardised today.
Issues	The solutions identified above require device support.
Existing applicable device standards ¹	Mandatory, OMA DM 1.2 (Bootstrapping, Provisioning) For the solution to work a mechanism to detect IMEI change is needed.

¹ Note: standards related to the support and implementation of “normal” non-SCWS cards, are listed in Section 7 Appendix 1: Generic Standards (All Cards)

<i>3.2.1.1 Use Case 1a: Ensure device settings are automatically managed and configured</i>	
	network based solution or, STK IMEI tracking application + device management platform in the network.
Existing applicable card standards	Generic Bootstrapping Architecture 3GPP TS 33.220 v9.0.0 3GPP TS 33.223 v8.40 3GPP TR 33.919 v8.00 3GPP TR 33.920 v7.5.0
"Missing" standards features	None

<i>3.2.1.2 Use Case 1b: Store customer generated content on card</i>	
Description	<p>Currently when a customer changes device, if they simply move their SIM from one device to another, then they lose all of the content they have generated on their device (address book, photos, videos, messages), or their own content they have moved from their laptop to their device (like a personal USB stick).</p> <p>The customer may choose to use device supplier software to move data from one device to another, however, this generally only works if moving between devices from the same device supplier (for example Nokia to Nokia). Moving content between different device suppliers is far more difficult and frustrating.</p> <p>The customer may choose to use device supplier software to move data from one device to another, however, this generally only works if moving between devices from the same device supplier (for example Nokia to Nokia). Moving content between different device suppliers is far more difficult and frustrating.</p> <p>This solution will ensure that when the customer changes devices, all of the content they have generated is accessible transparently, with no further actions required. In detail, The customer can synchronise address books between device and SIM. This will allow the customer to always have a local copy on the SIM. On insertion of the SIM into a new device, the address book data is synchronised, so that all device applications can access the address book content. (The data on the device remains the active copy.) Additionally, the data on the card is accessible via the SIM</p>

3.2.1.2 Use Case 1b: Store customer generated content on card

interface (so that the customer can check it is the same, and is in synchronisation with the device content).
MNOs that have a SIM address book backup solution, with a web interface, enable their customers to edit the data on the web. The data is then synchronised back to the SIM, which in turn triggers a synchronisation with the data on the device.
MNOs that have a device address book backup solution, with a web interface, enable their customers to edit the data on the web. The data is then synchronised back to the device, which in turn triggers a synchronisation with the data on the SIM.

The solution would support various customer options: automatically, on request, and never.
The customer has the option to synchronise the data with the device: for example, if the card is temporarily inserted into a friend's phone, then the customer needs to be able to prevent a synchronisation from occurring.

Store customer created photos, videos and so forth on their SIM
Take a photo for the first time -> where do you want to save your images? Options of SIM, Device, Removable Media
Ability to change default location at any time
Using the devices "file explorer" capability
the customer can easily move, copy, paste, and delete files between the different storage areas
the customer can easily check the amount of available memory on the card
The device does not create new directories automatically: if there are existing photos / images / pictures directory on the SIM, then this is used for storing the relevant data, rather than the device automatically creating a new "my images" directory. If appropriate, the customer is also given this choice.
Folder and tree structure should be consistent across devices.
This is also an issue on language changes.

Store customer generated / received messages on their SIM (SMS, MMS, email)
With options to store securely (see [Use Case 3](#))
Email: storage of messages would only be enabled between the same application (out of scope: access to Blackberry emails on non-Blackberry devices).

Store customer content moved from, for example their laptop and stored on their SIM (a personal secure USB stick).
Connectivity between the device and laptop to be managed by the device and not the SIM.

<i>3.2.1.2 Use Case 1b: Store customer generated content on card</i>	
	Also allow for the SIM to be physically transferred between a mobile device and a laptop.
Benefits - consumer	<p>The data I have created is always there when I change device.</p> <p>Its simple and straightforward – I don't have to install software on my laptop, or convert data from one format to another.</p>
Benefits - device supplier	<p>A customer is more likely to use multiple devices (a different one at the weekend from the one in the week) because it's much easier for them to change the device settings so the sale of devices will increase.</p> <p>Because the process of moving data between devices is simple and straightforward for the customer, it encourages the customer to own multiple devices, or change more frequently, it lowers the threshold to own a new device.</p>
Benefits - MNO	<p>Reduction in customer care calls (customer no longer asking how to transfer data between devices).</p> <p>Customers, who are confident that their data is seamlessly available on a new device, are more likely to remain with that MNO (churn benefits).</p> <p>Customers who store all their data on the SIM are less likely to change MNO (because effort is required to copy data between devices).</p> <p>Transferring data between devices is so complex that it also often triggers the customer to investigate changing MNO at the same time – when the data is all on the SIM, this decision need not arise.</p> <p>Because support for Smart SIM has improved overall support for SIM cards, it makes the decision to invest further in SIM technology easier to justify.</p>
Proposed Smart SIM solution	<p>Comprises a number of components,</p> <p>The customer can synchronise address book between device and SIM</p> <p>Utilises two existing specifications, 3GPP defined 2 standards on Contact Manager (advanced Phone Book), 1 - TS 31.220 rel-8 defining interface between Card/device. This is based on OMA DS and allow to synchronize the</p>

3.2.1.2 Use Case 1b: Store customer generated content on card

	<p>« user's personal data » between the device and the card. Phonebook is part of such data. 2- TS 31.221 rel-8 defined a Java API to manage such data synchronized in the card.</p> <p>The address book content accessible on the card is limited by the cards specification. Additional records and file content not supported by the card address book implementation can be accessed via SCWS, and presented to the customer. Could investigate standardised implementation of full multi-media address book (underway in TS 31.221 R9) Data on the card is synchronised thanks to SyncML with the data on the device. This process can either be automatic (on content change), or manually triggered by the customer. It inter-works with the existing Device and or Card address book backup solutions – they are effectively independent.</p> <p>Store customer created photos, videos on their SIM Requires support for high density cards, and probably high speed protocol (depending on file size, and total memory). Requires access from device file management software (Example:- file explorer)</p> <p>Store customer generated / received messages on their SIM SMS can already be stored on SIM MMS can already be stored on SIM requires. Further storage may be needed, depending on how much MMS storage wants to be offered, and this may therefore require use of high density high speed protocol cards (USB-IC) Email: email application on device enables customer to chose location of mail messages (device, removable memory card or SIM), enabling offline storage. Data stored on the SIM could then be encrypted, see use case 3 below.</p> <p>Store customer content moved from example their laptop and stored on their SIM (a personal secure USB stick) Ability to connect device to laptop (USB cable, Bluetooth, IR, NFC – does not matter, independent of connection mechanism), and using device as a card reader, the high density memory on the card is accessible over high speed protocol USB-IC. The memory on the card appears as an extra drive (mass storage) within Windows File Explorer (or equivalent) on the laptop. The memory on the card can also be accessed via SCWS, via the laptop browser.</p>
Alternative implementations	Customer data stored on removable memory card.

<i>3.2.1.2 Use Case 1b: Store customer generated content on card</i>	
	<p>Very cheap, MNO independent. Variation in form factor exists, however de-facto proprietary solution is micro-SD.</p> <p>Customer data transferred via device supplier software on laptop. Very difficult to transfer data between devices from different suppliers.</p> <p>Customer data transferred via MNO network based solutions. Expensive solutions to deploy. Systems to stop the auto-creation of new folders, “my pictures”, “photos” – the auto-generated folders</p> <p>Album feature only looks in device default location, doesn’t search all locations.</p> <p>If a photograph is taken, give the customer a choice of where the data is stored, and future ability to change the default.</p>
Risks & Issues	<p>A solution will be required to copy all the data from one SIM to another to support the SIM upgrade.</p> <p>Systems to stop the auto-creation of new folders, “my pictures”, “photos” – the auto-generated folders</p> <p>“Album” device application generally only looks in device default location for photographs, doesn’t search all locations.</p>
Existing applicable device standards	<p>Synchronise address book between device and SIM:-</p> <ul style="list-style-type: none"> - OMA SCWS v1.1 : enable access to content on SIM - SyncML (part of OMA DS) : adapted for Contact Manager => referred 3GPP specs : synchronise data on the card with the data on the device. <p>Store customer created photos, videos on their SIM, and store customer generated / received messages on their SIM:-</p> <ul style="list-style-type: none"> - USB-IC ETSI TS 102 600, including EEM (TCP-IP if using SCWS) + ICCD + mass storage <p>Store customer content moved from, fro example their laptop and stored on their SIM:-</p> <ul style="list-style-type: none"> - USB-IC ETSI TS 102 600, including EEM (TCP-IP if using SCWS) + ICCD + mass storage

<i>3.2.1.2 Use Case 1b: Store customer generated content on card</i>	
	<ul style="list-style-type: none"> - ETSI R9 Multimedia File System : For large amount of content distribution and management. - OMA SCWS : enable access to content on SIM: both ETSI contact book & synchronised contacts book
Existing applicable card standards	<p>Synchronise address book between device and SIM:-</p> <p>3GPP TS 31 220 v8.0.0 Characteristics of the Contact Manager for 3GPP UICC Applications</p> <p>: Define interface between card and device. This is based on OMA DS and allows the synchronization of the customers personal data between the device and the card. Phonebook is part of such data:-</p> <ul style="list-style-type: none"> - 3GPP TS 31 221 v8.0.1 Contact Manager Application Programming Interface (API); Contact Manager API for Java Card Define a Java API to manage such data synchronized in the card. - OMA SCWS v1.1 : Enable access to content on SIM - SyncML (part of OMA DS) : Adapted for Contact Manager ==> referred 3GPP specs : Synchronise data on the card with the data on the device. <p>Store customer created photos, videos on their SIM, and store customer generated / received messages on their SIM</p> <ul style="list-style-type: none"> - USB-IC ETSI TS 102 600, : Mass storage if control by the device or EEM (TCP-IP) using SCWS if controlled by the SIM : For large amount of content distribution and management. - ETSI R9 Multimedia File System - ETSI file system for SMS, ETSI Large file + Pro Active session for MMS <p>Store customer content moved from, for example, their laptop and stored on their SIM</p> <ul style="list-style-type: none"> - USB-IC ETSI TS 102 600, : mass storage & TCP-IP for SCWS - ETSI R9 Multimedia File System : For large amount of content distribution and management. - OMA SCWS : Enable access to content on SIM: both ETSI contact book & synchronised contacts book

3.2.1.2 Use Case 1b: Store customer generated content on card

<p>"Missing" standards features</p>	<p>Systems to stop the auto-creation of new folders, "my pictures", "photos" – the auto-generated folders. Instead, need consistent structure and consistent access to folders located on the SIM.</p> <p>ETSI R9 Multimedia File System will address multi media management over EEM IC-USB interface – it may not specifically cover mass storage class usage.</p>
-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<i>3.2.1.3 Use Case 1b: Store customer preferences</i>	
Description	<p>Current Experience</p> <p>Currently when the customer changes devices they lose all data associated with their favourites (bookmarks), ringtones associated with specific settings, language, time zone, volume settings, wallpaper settings, short dials, and any other changes from the default settings they have made. (Note this use case excludes the content associated with example ringtones.)</p> <p>Separately, on the customers original device, if provided by the employer (a corporate customer for example), then the employer may have configured the device – for example they may have disabled or removed some applications, deliberately prevented MMS from being used, have specified a customised user interface and applications.</p> <p>When the customer changes device, no data associated with the applications they have paid for, is available or transferred to the new device.</p> <p>When the customer changes device, currently all of their old settings and personalised features remain on the device. Smart SIM will allow the customer to take all the preferred contents with them</p> <p>This solution will ensure that the customers personalised device customisations will be transferred to the new device. On inserting the SIM into the new device, the customer will be given the option to import the settings on the SIM into the new device.</p> <p>The solution will provide relevant security features to ensure a corporate customer can restrict changes to the settings they have made (and update them remotely).</p> <p>The solution will inter-work with application distribution platforms, to offer to download applications which were on the old device and which are available for the new device.</p> <p>The solution will ensure that when the SIM is removed from the old device the settings on that device return to the default.</p>
Proposed Smart SIM solution	<p>Proposed solution could refer to the work that is under development in OMA DM SC Group</p> <p>This OMA Group has recently finalised the <i>OMA DM Smart Card Requirements</i> specification (OMA-RD-DM_SC-V1_0-</p>

<i>3.2.1.3 Use Case 1b: Store customer preferences</i>	
	<p>20070904-C) where they are enhancing the role of the Smart Card started in the OMA DM v1.2 specifications and defining use cases and requirements in order to store Management Object into the Smart Card and to restore them back from the card to the new device. Technical specification work is going on and plans to use smart card web server features. This specification work should be completed within August 2009.</p>
Benefits - consumer	<p>No personal settings data left on old device.</p> <p>Convenient: no need to waste time configuring new device to behave like the old device – can start using it immediately. Behaviour is as similar as possible to old device, familiar to use, so less of a barrier to change devices. Allows customer to focus on new features of the device.</p>
Benefits - device supplier	<p>Removes two barriers to customer buying a new device, What do I do with my old device to make sure no-one can see my personal data on old device It is difficult setting up a new device.</p>
Benefits - MNO	<p>Reduction in customer care calls (customer no longer asking how to configure devices).</p> <p>Customers, who are confident that their data is seamlessly available on a new device, are more likely to remain with that MNO (churn benefits).</p> <p>Customers who store all their data on the SIM are less likely to change MNO (because effort is required to copy data between devices).</p> <p>Transferring data between devices is so complex that it also often triggers the customer to investigate changing MNO at the same time – when the data is all on the SIM, this decision need not arise.</p>
Alternative implementations	<p>Deleting all data on device can be achieved by customer selecting “restore to factory settings” option or equivalent on device.</p> <p>Some device vendors provide software which enables customer preferences and settings to be transferred between devices (usually same series from same manufacturer).</p>
Risks	<p>Taking time to set up the device forces the customer to investigate the device.</p>
Existing applicable	<p>Mandatory:</p>

<i>3.2.1.3 Use Case 1b: Store customer preferences</i>	
standards	<p>USB-IC specification: USB Implementers Forum specifications & ETSI 102 600 mass storage class: if data are controlled and accessed directly in mass storage by the device</p> <p>OMA Smartcard Web Server specification version 1.1</p> <p>ICCD (APDU): ETSI TS 31.101 to ensure telecom feature backward compatibility as no ISO/USB-IC concurrency</p>
"Missing" standards features	<p>A standard needs to be defined for a structure on the card to store customer preferences. The device would need to know where to look for this data and then import it into device, (and export before changing device).</p> <p>Device manufacturers would need to be convinced to implement this.</p>

<i>3.2.1.4 Use Case 1d: Store customer purchased content</i>	
Description	<p>Currently a customer buying for example ringtones or music from content providers is strictly tied to the device they used to make the purchase. In fact, with the OMA DRM scheme, when the customer wants to change the player (for example, the device), the purchased rights have to be downloaded onto the new device and the certificates have to be recalculated with the new terminal ID. This scheme works as long as a network connection is available and/or the terminal belongs to the same user domain and from the customer perspective it is a too complex a procedure.</p> <p>The SmartSIM solution will ensure that the customer can purchase content, and know that they will be able to use it as long as the SIM is plugged into a device. When the customer wants to change to a new or different device, they just need to plug the SIM in the new device moving rights and content completely.</p> <p>The customer could use the SIM card as a backup of the contents and certificates purchased. These are usually stored in the device. A customer could play the DRM-protected content stored in his SIM without transferring the content and rights to the rendering device, in the case where he does not own the device, or the device has not enough free space.</p> <p>In summary, either buying content without SRM buying content with DRM And being able to play it on the mobile device of your choice.</p>
Benefits - consumer	High level of portability from one device to another. Devices could belong to different users and could be of a different type (Example:- mobile phone and a PC)
Benefits - device supplier	The customer won't be tied to a specific device to play the contents, so the customer could easily change their old device with a new one
Benefits - MNO	The solution is completely controlled by the MNO that can offer a more flexible service to customers (purchased contents may be played in different devices, some promotional contents could be pre-stored inside the SIM.
Proposed Smart SIM solution	<p>Proposed solutions should refer to OMA SRM specifications and also to the ETSI SCP work ongoing in liaison with OMA.</p> <p>OMA has standardised "SRM", a Secure Removable Media used to store and distribute DRM Contents and Rights Objects in a secure manner. Examples of SRM Devices may</p>

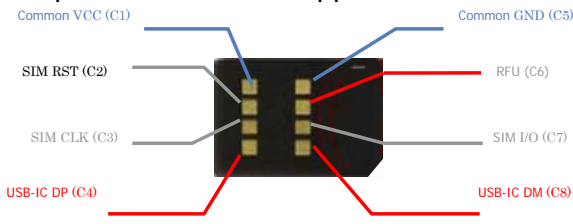
<i>3.2.1.4 Use Case 1d: Store customer purchased content</i>	
	<p>be SMC and SIM/Smart Card. In particular, for SIM and Smart Card, ETSI SCP is working in order to clarify in which way the SIM or Smart Card may be used as an OMA Secure Removable Media</p> <p>References: - OMA Secure Removable Media Requirements - ETSI TS 102 412 V8.3.0 Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8) [4.21 paragraph – Digital Right Management]</p>
Alternative implementations	OMA SRM may be implemented also in Secure SD or memory card but with a lack of control from the MNO's perspective in comparison with a SRM on SIM solution
Issues	<p>Large size files, could require that the proposed Smart SIM solution is implemented as large memory SIM cards requiring high speed interface devices. MNO will pay for the memory that needs to be well targeted with the services needs.</p>
Existing applicable standards	<p>If DRM is required, then the following standards apply:- - OMA Secure Removable Media Requirements - ETSI TS 102 412 V8.3.0 Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8) [4.21 paragraph – Digital Right Management]</p> <p>And whether DRM is required or not, USB-IC OMA SCWS</p>
"Missing" standards features	To be checked, ETSI R9 Multimedia File System – may not cover mass storage, to be checked

3.2.1.5 Use Case 1e: Distribute and store MNO content on card

<p>Description</p>	<p>Currently if an MNO needs to distribute content, for example, ring tone video, music (teaser or full track) service usage information device usage information ... to be able to, interest customers and encourage more use of content:- Promote multimedia content To extend their brand footprint thanks to its services promotion To support a segmentation offer strategy thanks to targeted specific contents, To use or propose a new support for Mobile advertising thanks to video, banners, coupons and open it to partners/3rd parties There is no unique, simple, secure and controlled way to do it.</p> <p>This solution will ensure that , in pre-issuance the MNO will be able to personal the SmartSIM with its own content it will be possible to define different area & security attribute depending of the distributed content. Such as read only by the customer and not erasable, hidden form customer</p> <p>free the device multimedia players (example music & video player, flash player) or any other device applications to access the content stored in the Smart SIM it will be possible the update the content remotely in case of: content obsolescence new content to be pushed to adapt the content format to new device (portability)</p> <p>This solution will ensure an easy and way to access and display MNO distributed content to generate purchase and usage.</p>
<p>Benefits - consumer</p>	<p>Not easy to find interests for the end-user</p> <p>Easy portability of my MNO contents regardless of my device. Transparent/Auto adaptation of my MNO contents</p> <p>Easier and unified way to access and display my MNO distributed multimedia contents (using SCWS)</p>
<p>Benefits - device supplier</p>	<p>No need to customize/personalize the device for each MNO. Simplifying their process, tests, stock management.</p>

<i>3.2.1.5 Use Case 1e: Distribute and store MNO content on card</i>	
	<p>Because the process of moving data between devices is simple and straightforward for the customer, it encourages the customer to own multiple devices, or change more frequently, it lowers the threshold to own a new device.</p>
Benefits - MNO	<p>Reduce complexity by using only one token, the Smart SIM, to add new services avoiding addition of a new token/device. (device or external memory stick) Simplify content distribution by using the well-known SIM personalization process.</p> <p>Be able to combine both aspects of content distribution and content usage (display, update) managed by the same entity Smart SIM</p> <p>Bring a secure and controllable token belonging to the MNO contrary to device or external memory stick.</p> <p>Allow MNO to define the required security attribute to be applied to the content. Ensure the pre-loaded content not to be reused in case of SIM churn. Content is linked to the Smart SIM.</p> <p>MNOs can pre-load targeted content like ring tones, full track music or games in order to improve loyalty & relationships (segmentation approach) with their customers, and to encourage the use and purchasing of multimedia content which can then generate new revenues.</p> <p>Use the SmartSIM to distribute for the customer explanation on MNO services and encouraging their usage. (helpdesk resources)</p> <p>Open this new support to 3rd parties to distribute mobile advertising (promotion video, banners) and generate new revenues.</p>
Proposed Smart SIM solution	<p>Content can be pre-loaded in the Smart SIM thanks to its large memory capacity and access by the device Media Player or other applications (device or Smart SIM applications).</p> <p>To bring performances for large amount of content management, High Speed Protocol is mandatory (USB-IC) between the device and the Smart SIM.</p> <p>Depending of the content type and device Media Player/application, the content can be retrieve using either USB-IC mass storage directly from the Smart SIM</p>

<i>3.2.1.5 Use Case 1e: Distribute and store MNO content on card</i>	
	<p>or using SmartCardWebServer interface (BIP server mode over ISO or TCP-IP over USB-IC depending of required performances and data size) to retrieve and display the content (helpdesk resources, content store resources, MNO generic contents display).</p> <p>IMEI tracking application can be used when changing device to inform the remote platform of :- the new supported device features to adapt the current pre-loaded content to push new content now supported by the device.</p> <p>Possible Right Objects linked to the Multimedia content can be either Stored in the Smart SIM bringing a transparent portability. The device media player retrieving both content from the Smart SIM Or stored in the device Media Player. The device Media player retrieving the content from the Smart SIM from the remote server.</p>
Alternative implementations	<p>Use of removable memory card/stick Bigger available memory Low cost solution</p> <p>Add a new token to be bought by the MNO (if pure MNO content pushed) new personalisation process to be put in place with new supplier no insurance that the removable memory will be inserted in the device No remote management</p> <p>Device customization More complex to manage already personalized device stock & obsolescence.</p>
Risks & Issues	<p>Make the device to access the SIM either in USB-IC Mass Storage (Media Player) or through SCWS (ISO/BIP server mode or USB-EEM) for media content display & access, rich helpdesk display, rich content store display.</p> <p>Make the device Media Player to access the SmartSIM for Right Objects management.</p> <p>Small possible issue on Multimedia CODEC which are standard</p> <p>In case of rights linked to the content,</p>

3.2.1.5 Use Case 1e: Distribute and store MNO content on card	
	<p>Secure the link between the device player and the SIM to exchange Rights Objects. Fragmentation of DRM / certificates solutions</p>
Existing applicable device standards	<p>Mandatory:</p> <p>For large amount of MNO pre-loaded photos, videos on their SIM: USB-IC mass storage class: if data are controlled and accessed directly in mass storage by the device or EEM class (TCP-IP) using SCWS if data are controlled and accessed by the SIM this mean also to make the multimedia applications of the device to interface with SCWS</p> <p>SIM 8 pins connector to support USB-IC:</p>  <p>Optional: In case of rights linked to the content, it will be mandatory to use OMA DRM or SRM.</p>
Existing applicable card standards	<p>Mandatory:</p> <p>For large amount of MNO pre-loaded photos, videos on their SIM: USB-IC specification: USB Implementers Forum specifications & ETSI 102 600 mass storage class: if data is controlled and accessed directly in mass storage by the device</p> <p>or EEM class (TCP-IP): using SCWS if data are controlled and accessed by the SIM ETSI TS 102 483 OMA Smartcard Web Server specification version 1.1</p> <p>ICCD (APDU): ETSI TS 31.101 to ensure telecom feature backward compatibility as no</p>

<i>3.2.1.5 Use Case 1e: Distribute and store MNO content on card</i>	
	<p>ISO/USB-IC concurrency In case of mass storage: the card shall support at least a FAT16 file system memory part</p> <p>Optional: In case of rights linked to the content, the it will be mandatory to use OMA DRM or SRM.</p>
"Missing" standards features	<p>As per use case 4.2.1, i.e.</p> <p>Systems to stop the auto-creation of new folders, "my pictures", "photos" – the auto-generated folders. Instead, need consistent structure and consistent access to folders located on the SIM.</p> <p>ETSI R9 Multimedia File System still under specification at ETSI + may not cover mass storage for the time being ➔ new inputs/requirements to be done at ETSI</p> <p>Power management in TS 102 600 does not cover the case of large memory SIM cards embedding external memory.</p> <p>Until a standard is available to cover this, we would propose to use a vendor's proprietary solution so that this UC can be included in the trials.</p>

3.2.2 Use case two: deliver applications and services to customer in device agnostic way

For use case 2 only device agnostic applications and services are to be considered. This therefore excludes all of the traditional distributed run times – JME, Symbian, .net and so on. Agnostic environments include Smart Card Web Server (SCWS)

Need ability to support different categories and security models to allow manufacturers, third parties, customers and MNOs to install applications. Pre-installed applications may require OTA unlocking.

3.2.2.1 Use Case 2a: Multimedia address book

Description	<p>Currently the customer has different possibilities to store the phonebook entries – on the phone itself or on the SIM. In most of the cases the subscriber does not know the storage location of his contact data.</p> <p>In the case of a device change it is very often the phonebook data on the device is difficult to transfer.</p> <p>The multimedia phonebook also can present different data for each contact such as SMS/MMS traffic, call history, instant messaging and pictures/videos.</p> <p>The phonebook can use the Smart Card Web Server on the SIM as the service environment for the storage and usability of the multimedia phonebook. This environment also can be enriched with the integration of Macromedia flash technology. The SCWS uses standardised interfaces such as BIP (Bearer independent protocol) or USB IC (InterChip) to the device</p> <p>This solution will ensure that customers have their individual data stored on the secure SmartSIM, which will be available on any device in the similar design.</p> <p>Currently, when a subscriber wants to transfer the address book data from an one device to another one it is important to know where the data are stored. The address book data on the SIM are easy to transfer, as this data will be available immediately after inserting the SIM into another device. In the case of a new SIM card, there are simple to use offline tools to perform the copying from one SIM to another. Also available are online backup and restore solutions from different MNOs.</p> <p>In case the address book data is stored on the device it is necessary to use software installed on the computer of the customer to synchronise the data. Based on the experience and feedback from customers this solution causes some problems, when changing the device brand which requires a new software tool or different/special software such as MS outlook / Lotus Notes are used. Some customers don't like</p>
-------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<i>3.2.2.1 Use Case 2a: Multimedia address book</i>	
	<p>the installation of software on their PC only for synchronising contacts.</p> <p>This solution will ensure that address book data will be easier to transfer and therefore reduce the obstacle for subscriber to buy a new device. It furthermore makes the interaction of the different address books on the device and on the SIM possible and an automatic synchronisation of both will increase the ease of use.</p> <p>Two distinct capabilities: Multimedia address book stored on SIM and primary (Active) user address book. Interfaces to all phone services Complete backup for phone based address book. Active data would remain in the device; An application on the SmartSIM takes care that all address book data on the phone are automatically copied to the phonebook on the SIM. Therefore the SmartSIM is an ideal tool for secure backup and portability of address book data. The SmartSIM with the cryptographic capabilities also allows to en-/decryption of these data. Therefore the address book data are protected</p>
Benefits - consumer	Change of devices is becoming easier
Benefits - device supplier	<ul style="list-style-type: none"> - Use of security mechanisms a SmartSIM can offer - Customer reduce the product-change-cycle as it is easier to transfer address book data in case of changing devices
Benefits - MNO	<ul style="list-style-type: none"> -The service can be activated and managed over the air (OTA) - A network MNO can actively offer SIM phonebook backup services to their subscriber. As the SmartSIM would hold all phonebook data the service only has to interact with the SmartSIM which is based on established communication channels of a network MNO
Proposed Smart SIM solution	<p>Today's USIM cards offer a 3G phonebook, which offers multiple data per contact similar to the address book of the device. This standardised SIM 3G phonebook can be used for the storage of entries. There are some data per contact (example:- picture, ringtone), which will require a different way of storage. One option is to store the data in a separate database on the SIM card.</p> <p>The Smart Card Web Server has the capability to act as the general interface for entering, modifying and showing the contact data. The SCWS would also combine the data stored in the 3G phonebook with the "special" data stored in the SIM database.</p> <p>For the synchronisation of device address book and SmartSIM phonebook there would be an application triggered</p>

<i>3.2.2.1 Use Case 2a: Multimedia address book</i>	
	manually or automatically.
Alternative implementations	Online synchronisation solutions based on SyncML for device data
Issues	<ul style="list-style-type: none"> - The automatic synchronisation of new phonebook entries is based on a triggering event which could be used by the SmartSIM - In case the SmartSIM would like to store special phonebook data such as contact picture in a standardised format (3G phonebook) there has to be an extension of the specification.
Existing applicable standards	<p>Note: use case 4.2.1.2 desires the solution to store and sync the CONTENT of the address book. This use case is about the structure of the address book.</p> <p>Assume: data on card is used only to migrate between devices (import/export), and stored as part of the card address book file structure.</p> <ul style="list-style-type: none"> - 3GPP TS 31 220 v8.0.0 Characteristics of the Contact Manager for 3GPP UICC Applications : define interface between Card and device. This is based on OMA DS and allows for the synchronization of the user's personal data between the device and the card. Phonebook is part of such data - 3GPP TS 31 221 v8.0.1 Contact Manager Application Programming Interface (API); Contact Manager API for Java Card defines a Java API to manage such data synchronized in the card. - OMA SCWS v1.1 : enable access to content on SIM <p>No new standards required to support encryption of the data on the card.</p>
"Missing" standards features	<ul style="list-style-type: none"> - In case the SmartSIM would like to store special phonebook data such as contact picture in a standardised format (3G phonebook) there has to be an extension of the specification.

<i>3.2.2.2 Use Case 2b: Vanilla device: MNO customisation of device (excluding applications, and device settings as covered separately)</i>	
Description	<p>Most MNOs deliver what is known as ‘variant’ devices to their customers when the purchase mobile telephony service. These devices are effectively customised in many ways so that are not only ‘working out of the box’, but have many elements of MNO branding incorporated, including, but not limited to, wallpapers, screensavers, menu icons, pre-installed service URLs, important service numbers.</p> <p>In addition to this, customers may choose to purchase/acquire devices that are ‘SIM-free’. These devices are generally from the device manufacturer and do not contain any MNO-specific branding.</p> <p>The problems start when the customer changes the SIM in a device; an activity becoming more prevalent in today’s environment where MNOs are providing SIM-only deals to the customer – here the customer keeps their device, but can change MNO. In the case of these devices it is quite possible for a device from one MNO to contain another MNOs SIM card, but still be branded as the original MNO and contain the MNO-specific features and services.</p> <p>This situation causes problems including each MNOs service dial numbers not working with the new MNO, for example – the customer may ask themselves ‘am I now being charged by both MNOs?’</p> <p>Additionally for ‘SIM-free’ devices there is no opportunity for the MNO to add branding/services into the device, to add value to the customer.</p> <p>SmartSIM rectifies this by allowing MNO customisation to occur via the insertion of the SIM, in device agnostic manner.</p> <p>This solution will ensure that the customer’s device is always customised to the particular MNO of the SIM that is inserted so that all services operate correctly and the customer feels that they are indeed using a service provided by that particular MNO, and not any other, or no MNO at all.</p>
Benefits - consumer	<p>The customer will obtain the correct MNO environment and experience on their device together with all the working MNO services when they insert their SIM into a new or different device.</p> <p>Particularly when changing MNOs, the customer will visually see that the change from the old MNO to the new MNO is complete.</p>
Benefits - device supplier	<p>If devices can easily be ‘customised’ to a particular MNO</p>

<i>3.2.2.2 Use Case 2b: Vanilla device: MNO customisation of device (excluding applications, and device settings as covered separately)</i>	
	such they are then usable then this encourages the whole process of the second-hand device market, which in turn leads to new device sales.
Benefits - MNO	The MNO is able to ensure their branding and specific services are automatically available on whatever device the customer chooses to use.
Proposed Smart SIM solution	OMA DM with part of the DM tree residing on the SIM HSP and large-scale memory SIM SCWS
Alternative implementations	Configuration application stored on the SIM then uploaded and executed on the device – or SCWS web page to do a similar effect
Risks & Issues	Keep in line with any necessary regulatory requirements
Existing applicable device standards	The mandatory specifications which are required to be implemented on the device to support this use case are: OMA DM 1.2 (which includes SCWS and bootstrapping) Note: this is preferred to OMA DM 1.1 It is recommended that the device also support, OMA DM_SC 1.0 OMA LFC 1.0 4) USB-IC ETSI TS 102 600, including EEM (TCP-IP if using SCWS) + ICCD + mass storage 5) ETSI R9 Multimedia File System
Existing applicable card standards	The mandatory specifications which are required to be implemented on the device to support this use case are, 1) OMA DM 1.2 2) OMA DM_SC 1.0 3) OMA LFC 1.0 4) USB-IC 5) ETSI R9 Multimedia File System
“Missing” standards features	None, provided OMA DM is able to manage all of the device settings that an MNO would customise in any variant device

3.2.2.3 Use Case 2c: Vanilla device: deployment of applications (both MNO & 3 rd party) by installation of applications onto the device	
Description	<p>SmartSIM is ideally suited to deploy applications to the device. Deployment of applications through the SIM provides a method for users to install applications for configuring the vanilla device.</p> <p>Also this use case is not just limited to vanilla device. The SmartSIM feature can apply to normal device as a way for MNO to deploy their application or 3rd party application without the device supplier's involvement.</p> <p>Normally, when MNO wants to pre-embed applications in a device, cooperation with the device supplier is needed. It leads to delay of development of the device and increased cost and time.</p> <p>This solution will ensure that when the SIM is inserted, a exchange of profile ,which represents what kind of applications the device/the UICC has, is triggered, The customer sees a simple statement on their screen saying "Applications are detected" and the screen shows the list to customer letting them select which applications they would install. Once the customer finishes selecting applications, the device starts to be updated.</p>
Benefits - consumer	<p>Can configure vanilla device in their preferred way.</p> <p>Can install MNO / third party application without accessing the network.</p>
Benefits - device supplier	<p>No need to meet the variety of device requirements from MNOs. Let the MNO deal with their application through the SIM.</p> <p>Can deploy vanilla devices more.</p>
Benefits - MNO	<p>Can configure the device in MNO's preferred way.</p> <p>Can offer pre-embedded services regardless of device technology and OS</p>
Proposed Smart SIM solution	<p>Need to develop fully standardized way.</p> <p>Either via mass storage, - USB-IC - auto-install when insert card into device – only possible for open OS devices</p> <p>Or, can install via SCWS (open and closed OS devices), - if want an interface and more security need SCWS - could either install from SIM to device, or connect to online web page and download OTA from web to device</p>
Alternative implementations	

3.2.2.3 Use Case 2c: Vanilla device: deployment of applications (both MNO & 3 rd party) by installation of applications onto the device	
Issues	Note: because almost every device application is specific and different for every device, (and sometimes even different for a different ROM version of the same device), we need to know the device IMEI. So if the application is pre-loaded on the card, then effectively that card is specific to one device variant only. To ensure the application can be downloaded to any device, it will be necessary to know the IMEI and OTA download the correct version of the application for that device, via web session.
Existing applicable standards	Open OS devices, - USB IC Open or closed OS devices, - SCWS And, an IMEI tracking solution.
"Missing" standards features	

3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3 rd party) by running the applications from the SIM (nothing installed onto the device)	
Description	<p>Smart SIM is ideally suited to deploy applications to mobile device. Running the applications from the SIM provides customer with consistent access to services irrespective of device changes.</p> <p>This use case applies to vanilla devices for configuring it with applications of MNO or 3rd party's and also apply to a normal device for using applications which have benefit through running from the SIM.</p> <p>Normally customers lose services when they change the device. Customers need to download, install and configure the application in the device for using the services again but it becomes a big burden for customers.</p> <p>This solution will ensure that when the customers change devices, applications they have been using are accessible transparently, with no further actions required. When the SIM is inserted, an exchange of profile, which represents what kind of applications the device/ the SIM have, is triggered. Service link for the application from the SIM is added in the device application menu.</p>

3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3rd party) by running the applications from the SIM (nothing installed onto the device)

For the vanilla device, application configuration is covered by inserting the SIM. For the normal device, some applications which can give benefit to customer, MNO and device supplier through running from the SIM are covered by inserting the SIM. In detail.

a) MNO specific application

Can be any application followed by MNO's policy.

For example,

1. Instant Messaging
2. Helpdesk
3. Email with pictographs
4. Widgets
5. Mobile auction service (with presence status for item sale information)
6. MNO applications store

b) Language Package.

The customer can change the device language setting with their preferred language even though the device does not support it. This will allow the customer to always have their preferred language in the SIM, so that when they change device it is with them.

c) Personalization Information.

Currently when an MNO gathers data from customer, there are obstacles such as a regulation and customer's concern with the possibility of infringement of personal information, and which make it difficult for MNO to make their service more personalized.

If the personalization information is located in the SIM, the user side not in the MNO side, there will be fewer infringement issues and then MNO can more easily process improvement in service personalization. Also the information is all there when customer change the device.

- When customer uses browser to access web, the browser can send the URL data to an agent application (for example, SCWS) located in the SIM. (There are many ways to gather data for making personalization information) Personalization information can be extracted from the gathered data and stored in the SIM. And other applications in the device can use the extracted information in the SIM via the SIM interface.

<i>3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3rd party) by running the applications from the SIM (nothing installed onto the device)</i>	
	<p>d) Application update. Even if applications are pre-embedded in the SIM, there need to be a way to update it and to download new application. Customer can download MNO's or 3rd party's application in the SIM. Also application update is processed automatically.</p>
Benefits – consumer	<p>No need to download and install the application again when they change the device.</p> <p>Can easily and confidently change device, not a barrier to device change.</p> <p>For MNO specific application Ex) MNO application store - Mobile purchases require one less step since the billing function can be integrated on the SIM in applications by the mobile network MNO</p> <p>For the language package - Can use the preferred language in any device</p> <p>For the personalisation service case - Can get more personalised service. - Doesn't need to concern infringement of personal information.</p> <p>For Application update - Can configure the application on the SIM in their preferred way.</p>
Benefits - device supplier	<p>No need to meet the variety of device requirements from MNOs. Let the MNO deal with their application through the SIM. This lowers R&D cost and time to market for device supplier. Can deploy vanilla more devices.</p> <p>More and better applications are possible, thereby encouraging higher end device sales.</p> <p>The device supplier can be free to offer devices with different operating systems</p>
Benefits - MNO	<p>Can configure the device in MNO's preferred way.</p> <p>Can offer pre-embedded services regardless of device technology and OS</p> <p>Will not lose customers when they change the device.</p> <p>For MNO specific application Ex) MNO application store</p>

<i>3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3rd party) by running the applications from the SIM (nothing installed onto the device)</i>	
	<p>- Device purchases require one less step since the billing function can be integrated on the SIM in applications by the MNO</p> <p>For the personalisation service case</p> <ul style="list-style-type: none"> - can supply service customisation with each customer, which will give more service satisfaction to the customer and give service differentiation to MNOs. - Well organised personalisation information gives more chance to develop new service. - Will get less challenge about infringement of personal information. <p>For the application update case</p> <ul style="list-style-type: none"> - can manage the application on the SIM easily. - can deploy new application to user easily. <p>Less phone customisation effort, cost and time-to-market</p> <p>Defragmentation of platforms via a standard SIM can potentially enable more applications and services to offer to customers and with less effort</p>
Proposed Smart SIM solution	<ul style="list-style-type: none"> - Mobile browser, combined with ECMAScript <p>The mobile browser, combined with ECMAScript (the standardized form of JavaScript) including XMLHTML Request capability provides a device-independent means of supporting rich, user-friendly applications regardless of phone type or operating system. The mobile browser is a well proven platform for quick and easy development by millions of developers.</p> <ul style="list-style-type: none"> - OMA SCWS <p>Static or dynamic content can be served from the SIM, acting as a SCWS to the device browser, as described in the OMA SCWS spec. To further leverage resources on the device, such as PIM data (calendar, contacts,), GPS, camera, battery status, . in a standardized way available this committee may wish to explore OMTP's BONDI initiative (http://bondi.omtp.org/BWiki/BONDI%20Primer.aspx). To standardize mobile network resources, such as MNO-based billing, network availability, SMS or other messaging, this committee may wish to explore the GSMA OneAPI initiative (http://gsma.securespsite.com/access/default.aspx)</p>
Alternative implementations	<p>JavaME on the device could provide an alternative UI platform to the mobile browser, but in practice, this is plagued</p>

<i>3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3rd party) by running the applications from the SIM (nothing installed onto the device)</i>	
	<p>with technical inconsistencies as well as inconsistent market support. So this is not as device agnostic as one might wish.</p> <p>Others to be determined</p>
Issues	<p>While new browsers and lots of innovation are on the immediate horizon, the mobile browser market is not as mature as the desktop browser market. In the near term, certain browser features or rendering implementations may not be consistently available across browsers and devices, which may initially require more efforts from developers.</p> <p>Browsers are designed to reformat relative HTML content to different screen sizes, and a least common denominator approach to HTML and application functions can serve basic requirements. For mid-range to high-end applications, the SIM as an application server can provide a better user experience by consciously adjusting content and UI input variables depending device screen size, CSS support variances, keyboard types, languages, and other factors. While this is not the only approach available, W3C has developed a Device Description Repository and API (http://www.w3.org/2005/MWI/DDWG/) which may be interesting to explore further.</p>
Existing applicable device based standards	<p>There are 3 mandatory requirements to support this use case,</p> <p>ETSI TS 102 600 (Release 7): UICC-Terminal interface IC-USB characteristics, including electrical contacts, power requirements, UICC standby / resume. Key dependencies of TS 102 600 are referenced within the publication, example Ethernet Emulation Mode, and IC-USB electrical requirements under the USB forum.</p> <p>ETSI TS 102 483 (Release 8 – currently finalised, but not yet frozen) : Data forwarding service to route TCP/IP traffic from SIM to/from internet a.k.a. "Card Application Interface". This allows the UICC to be able to act as a TCP/IP or UDP/IP server or client for a client or server located on the terminal or out on the network.</p> <p>OMA SCWS v1.1</p> <p>Recommendation: it would be helpful to support, OMTB BOND: Set of standard APIs to enable web browser based applications to access device resources (GPS, screen profile, calendar/contact/PIM data), SIM resources. GSMA OneAPI initiative: Provides standard API to access MNO-based billing, network availability, SMS or other messaging.</p>

<p><i>3.2.2.4 Use Case 2d: Vanilla device: deployment of applications (both MNO & 3rd party) by running the applications from the SIM (nothing installed onto the device)</i></p>	
	<p>And in the future, ETSI TS 102 412 (Release 9): Smart Card Platform Requirements Stage 1 discusses several aspects such as registering SCWS applications on SIM, launching SCWS apps on SIM, contactless services and Digital Rights Management.</p> <p>And specifically on the Card, it is mandatory to support the relevant standards above, and in addition, GlobalPlatform v2.2, + Amendments A&B (Gil to confirm - + do we also need the Networked Framework Amendment?)</p>
<p>“Missing” device based standards features</p>	<p>These capabilities or standards are either currently missing or not clearly found as an interoperable standard,</p> <p>It is recommended that these items are supported, There is no standard that specifies a set of web browser capabilities for HD-SIMs, or classes of Smart SIMs, for instance :</p> <ul style="list-style-type: none"> - HTML 4.01, XHTML 1.0 (basic and mobile profile) - CSS 2.1 - JavaScript 1.5 (standard ECMA-262) - XMLHttpRequest(AJAX) - DOM (Document Object Model) Level 2 <p>For SCWS enabled applications, it is not clear if there is a standard mechanism for triggering the device when SIM is inserted to recognize new applications in a device application menu. (May be in one of OMA SCWS docs...)</p> <p>Unclear what are standards for changing the device preferred language setting and storing language libraries on the SIM.</p>

3.2.3 Use case three: provide security for sensitive data

Use of SIM for these applications may enhance user experience through a combinational effect. Additionally, whilst one of these features may singularly not require enhanced SIM capabilities, the combination of all may require an enhanced SIM.

<i>3.2.3.1 Use Case 3a: Protect personal data stored on card</i>	
Description	<p>There could be several levels of protection of data stored on the SIM card. Simplest is PIN code protection where personal data is only protected by a PIN code. However, PIN entry is a manual operation and regarded as a hassle for users. A PIN code could also be compromised.</p> <p>PIN entry can be utilized in two ways when accessing data; PIN entry for a session or PIN entry for each access.</p> <p>In the first case, the PIN is entered the first time data is accessed, and the data remains accessible for a given amount of time or operations. This PIN entry scheme can lead to compromising of data if the device used by someone else than the owner after PIN entry.</p> <p>In the latter case, PIN entry is required every time data is accessed. This is more secure than the first case, but leads to repeated PIN entries. This might be frustrating for the user.</p> <p>By introducing authentication vectors in addition, or instead of PIN entry, data access can be based on mechanisms such as location, presence, or document owner-controlled access. Additional authentication vectors can both increase protection of data and ease the access to the data when appropriate.</p> <p>Currently <describe current experience when changing device></p> <p>This solution will ensure that <describe the customer experience of using Smart SIM solution></p>
Benefits - consumer	<p>High protection of data Provide easy access to user's data Give data owner increased access control to his/her data</p>
Benefits - device supplier	<p>Easier to promote top range models to enterprise customers given that the enterprise sees the opportunities of having company information distributed and stored at their employees SIM cards and devices</p>
Benefits - MNO	<p>Improved customer satisfaction and customer acceptance for high capacity cards (as data protection may improve customer satisfaction and willingness to pay more for a high capacity card).</p>

<i>3.2.3.1 Use Case 3a: Protect personal data stored on card</i>	
	<p>Revenue from providing extra protection measures (that provide extra protection to private content and at the same time are user friendly). Churn benefits</p>
Proposed Smart SIM solution	<p>The first proposed solution is network assisted location, where locations can be white or black-listed for data access. If the user is within a blacklisted location, he/she will be required to enter a PIN or even be denied access to data. In the opposite case, the user can access the data freely. A typical example would be confidential documents that should be freely available within a company's office premises, but protected by the employers PIN code outside the office.</p> <p>A second vector could be presence information, example if the document is accessed during business hours, a user is in a meeting or on holiday, or the user is active or inactive. This vector can also be combined with PIN-entry, where PIN is entered when the user's presence is not the preferred presence.</p> <p>A third vector could be document/data owner controlled instant-access. In this case the document/data owner can remotely give/deny access to users' data real time. In this case, PIN entry can only be combined as an extra layer of security when access is granted by the owner.</p> <p>How data is accessed is up to the type of data and the user's preferences to access data. Data could also be accessed remotely example through the PC. However, the access control remains in the SIM.</p>
Alternative implementations	Private data stored on memory card and to provide a locking mechanism controlled by the SIM card. SanDisk has proposed such a solution which is named Virtual MegaSIM card and Trusted Flash memory card.
Issues/Risks	<p>Willingness to pay for high capacity SIM cards Device manufacturer's willingness to implement additional functionality if needed.</p>
Existing applicable standards	
"Missing" standards features	

3.2.3.2 Use Case 3b: Provide secure authentication mechanism for offline & online transactions	
Description	<p>The SIM is a secure entity, whereas mechanisms in the device deployed over the years are more vulnerable to attack. Additionally the SIM is personal to the customer, and so are transactions such as payment and signing. For these two reasons having the capability on the SIM and not the device is the preferred route.</p> <p>Consider the case where the customer wishes to sign a document or conduct some kind of payment – both use cases generally require some kind of User Interface (UI) to manage the process and if on the mobile this would typically be an application.</p> <p>When the customer changes device however, if that application is not present on the new device (and even if present is not configured for that particular customer) those authentication services will no longer operate.</p> <p>SmartSIM resolves this problem by ensuring both the authentication capability (mechanism) and UI reside on the SIM. That way everything moves when the customer’s SIM is placed in the new device and the services will still operate.</p>
Benefits - consumer	The consumer is still able to utilise authentication services no matter which device they change to.
Benefits - device supplier	The device supplier benefits from the fact that that customers can and will regularly change devices, meaning new devices can and will be purchased by customers.
Benefits - MNO	Those MNO services will work on any device.
Proposed Smart SIM solution	SCWS linked with security services in the SIM, which could include digital signatures and NFC.
Alternative implementations	
Issues	
Existing applicable standards	
“Missing” standards features	

<i>3.2.3.3 Use Case 3c: DRM & Media certificates</i>	
Description	<p>This use case focuses on broadcast material and protecting broadcasters' rights. DRM for audio and applications a low priority.</p> <p>The end user downloads and stores content to his mobile device that is offered by content providers. In general, content providers will wish to protect their content from being consumed by non-paying users, while at the same time making it readily and easily available to paying customers.</p> <p>By storing rights objects on the user's UICC, the user is able to carry rights objects from device to device without having to reacquire rights that were previously purchased. The encrypted content itself is easily ported between devices or shared between multiple devices (indeed, ready accessibility of the encrypted content is key to the DRM business model), but rights objects are not so easily transferred. By keeping rights objects on the UICC, they are tied to the paying subscriber and can be transferred to another device when the UICC is inserted into the second device.</p> <p>This gives subscribers the option to render protected content on any device that accepts their UICC and therefore enhances the user experience. As an example, a user may acquire a video clip while browsing with their device, but later may wish to watch the clip on their PC, which has a larger screen. If the PC can accept the user's UICC, either via a dongle or PCMCIA card, the user can potentially watch the clip on the larger screen.</p> <p>The Mobile Device Provider pre-installs and pre-configures the DRM agent for storing / retrieving Rights Objects on / from the UICC.</p>
Benefits - consumer	<p>Agent always works: no need to manually enter configurations.</p> <p>Can easily and confidently move content to a different device, not a barrier to device change.</p> <p>Simple and straightforward process.</p>
Benefits - device supplier	<p>Customer more likely to use multiple devices (weekdays / weekends) because it's much easier for them to change devices -> sell more devices.</p> <p>Because the process of moving agents between devices is simple and straightforward for the customer, it encourages the customer to use more devices, or change more frequently</p>
Benefits - MNO	<p>Customer is more likely to obtain DRM protected content from an MNO, as the content can be transferred between devices</p> <p>MNO does not specifically need to focus on delivery of</p>

3.2.3.3 Use Case 3c: DRM & Media certificates	
	content for mobile devices as the user can transfer the content.
Proposed Smart SIM solution	DRM separate delivery of Content and Rights Objects (as for example in OMA DRM 2.x)
Alternative implementations	-
Issues	Incompatibilities between different in DRM agents might impair the actual implementation
Existing applicable standards	
"Missing" standards features	

3.2.3.4 Use Case 3d: Authentication to multiple (all but mainly non-mobile) network types	
Description	<p>User authentication to access to fixed or wireless networks using UICC capabilities can be applied from end-users up to organizations or specific corporate users, the mandatory prerequisite will be to have a valid subscription and support any authentication method based on smart cards.</p> <p>UICC can be: The key element for providing nomadic access (not only authenticating different networks – 2G, 3G, LTE, ..., ADSL, WLAN, WiMAX, and so on - but also authenticating different services on top of them example VoIP, IP-TV) The key element for providing portability of services among different devices (TV on mobile and TV on IP-TV)</p> <p>Once secure network access has been guaranteed, the UICC could supply access to services and applications located in the network, example mobile TV. These applications and services may have different security requirements, thus requiring different validation types.</p>
Benefits - consumer	<p>Current UICC can be used to provide secure access to multiple network types and provides a simple, consistent and straightforward authentication process. UICC solution also brings both portability and remote management.</p>
Benefits - device supplier	
Benefits - MNO	<p>Provides converged access to different network types as well as access to different fixed/mobile network services. MNO can off-load heavy network traffic onto another network type (Wi-Fi) to reduce network loading.</p>
Proposed Smart SIM solution	Smart SIM need to provide support for networks and services authentications.

<i>3.2.3.4 Use Case 3d: Authentication to multiple (all but mainly non-mobile) network types</i>	
	<p>Smart SIM shall be able to support Single Sign-on experience for mobile users when consuming services/applications hosted by the MNO or external 3rd parties.</p> <p>The Smart SIM will contain credential to:</p> <ul style="list-style-type: none"> authenticate the end-user on the network authenticate the end-user on services available on each network
Alternative implementations	<p>Authentication to network: Credential embedded in the device: see CDMA, device already supported Wifi access without UICC security</p> <p>Authentication to services: Identity management such as OpenID, LibertyAlliance, InfoCard can run without UICC even if it can be one possibility to store credentials.</p>
Issues	Anticipate in pre-issuance all required authentication applications (NAA) and credentials.
Existing applicable device standards	The mandatory specifications which are required to be implemented on the device to support this use case are: see applicable card standard
Existing applicable card standards	<p>The mandatory specifications which are required to be implemented on the card to support this use case are,</p> <p>Network Access Application: 2G: SIM (3GPP TS 11.11): 3G: USIM (3GPP TS 31.111) LTE: USIM (3GPP TS 31.111 R8) CDMA: C-SIM (3GPP2 C.S0065-0_v2) IMS: ISIM (3GPP 31.103) WLAN (Wifi): EAP-AKA or EAP-SIM (ETSI TS 102 310) WiMax: WiMAX forum specification : WiMAX-SIM application on UICC</p> <p>Applicative level: For any services : GBA (3GPP 33.220 and 3GPP 33.223), Global Platform v2.2 (GP Card Specification V2.2) mTV: BCAST(OMA Service and Content Protection for Mobile Broadcast Services : OMA-TS-BCAST_SvcCntProtection-V1_0-20090212-A) MBMS (3GPP 33.246) Note : key generation and distribution for both services are relying on GBA</p>

3.2.3.4 Use Case 3d: Authentication to multiple (all but mainly non-mobile) network types	
"Missing" standards features	<p>mNFC: interoperability for authentication between application in the UICC and application in the reader (such as Mifare): IP-TV is currently discussed in TSPAN: BCAST and MBMS are the potential alternatives Identity management : OpenID, LibertyAlliance, InfoCard do not specify any authentication solution but UICC involvement is possible</p>

3.2.3.5 Use Case 3ei: Securely store passwords and login details	
Description	<p>In today's world customers have to manage more and more secret information in order to access their services (including banking and other web-based services).</p> <p>Writing down these credentials (usernames and passwords) on paper would certainly allow the customer to remember them, but of course this presents a bigger problem if that paper is lost or stolen.</p> <p>The mobile device is an ideal place to store such data, and there are many applications available on the open market to do this, but the problem comes when the user wishes to change device. The old device will have all the security credentials (which will be PIN or password protected so no-one else can access), but the new device will not, unless the customer is provided with some kind of transfer mechanism, and generally these are tedious and require specialist skills.</p> <p>SmartSIM is able to solve this problem if all the security credentials are stored on the SIM, together with the UI that allows those credentials to be displayed (again under PIN or password protection). In addition the SIM, being highly secure, means that those credentials are safe.</p>
Benefits - consumer	The consumer is provided with a useful service that will operate regardless of which device the SIM is placed into.
Benefits - device supplier	The fact that customers can change devices without loss of services means new device sales will occur.
Benefits - MNO	The MNO is able to provide a securely-managed password service to the customer.
Proposed Smart SIM solution	<p>A solution which stores the usernames and passwords for specific URLs, securely on the SIM.</p> <p>The usernames and passwords are either auto-populated or suggested by the application as you access the associated URLs.</p> <p>The customer may add or delete further credentials, and</p>

<i>3.2.3.5 Use Case 3ei: Securely store passwords and login details</i>	
	securely export or backup the entire file (in case of UICC replacement or upgrade).
Alternative implementations	SIM Toolkit (but cannot interact with open browser sessions and auto-populate fields). Open ID. Liberty Alliance solution. InfoCard
Risks & Issues	
Existing applicable device standards	Mandatory, SCWS GBA-ME
Existing applicable card standards	Mandatory, SCWS GBA-U
"Missing" standards features	Optional: browser supporting plug-in to detect username password fields, and automatically populate fields

3.2.3.6 Use Case 3e ii: Company VPN credentials	
Description	<p>The UICC can be used to allow the user to access different networks (3GSM/HSPA/Wi-Fi) and establish a trusted connection (VPN). For access to corporate IT networks, a strong authentication mechanism is used. Usually this is either a onetime password (OTP) or digital signature based authentication mechanism using a physical token. 3In case of OTP, the user has to type the displayed code into his PC.</p> <p>The adoption of the UICC in such a scheme can both authenticate the user accessing the network and provide cryptographic keys for encryption of data.</p> <p>This business application consists of two sub use cases: The UICC is used as an authentication token accessed through the notebook's 3GSM Module The mobile station is used as an authentication token by using connectivity options between notebook and mobile device (for example Bluetooth, cable)</p> <p>The solution can be implemented following two scenarios: Fully outsourcing of key parameters management to access the Corporate IT infrastructure to the MNO/TSM: mainly suitable for SME Sharing of memory space on the UICC to host key parameters for IT infrastructure access: mainly suitable to Large Enterprise Customers.</p>
Benefits - consumer	Current UICC can be used to provide secure access to multiple network types and provides a consistent and straightforward authentication process.
Benefits - device supplier	
Benefits - MNO	
Proposed Smart SIM solution	<p>Key management : Two methods are available for providing the cryptographic keys: GBA and PKI applet in UICC (i.e. WIM, PKCS#15)</p> <p>Authentication method: The authentication process can rely on existing Identity Management mechanisms.</p>
Alternative implementations	
Issues	
Existing applicable standards	Key management : GBA (3GPP 33.220 and 3GPP 33.223)
"Missing" standards features	Identity management : OpenID, LibertyAlliance, InfoCard do not specify any authentication solution but UICC involvement is possible

3.2.3.7 Use Case 3f: Store Application Certificates	
Description	<p>Storage and management of security certificates for applications, especially J2ME. To correlate with security domains. Provide ability for third party certificates.</p> <p>Currently <describe current experience when changing device></p> <p>This solution will ensure that <describe the customer experience of using Smart SIM solution></p>
Benefits - consumer	
Benefits - device supplier	
Benefits - MNO	
Proposed Smart SIM solution	PKCS#15 and GlobalPlatform Secure Domain – fully standardised. Implementation discussion ongoing at GSMA SCaG.
Alternative implementations	
Issues	
Existing applicable standards	
“Missing” standards features	

4. USE CASE PRIORITIZATION

Scoring

Market Impact: scored in terms of future market impact and commercial viability, high (3) / medium (2) / low (1)

Availability of standard: easy (3- existing standard) / medium (2- standard in the pipeline) / hard (1- no standard currently planned)

Technical Ease of Deployment: easy (3) / medium (2) / hard (1)

Notes

Please feel free to add comments as well as your score.

If you do not feel comfortable in scoring a column or feature, then either please leave it blank, or ask a colleague with the relevant expertise to score it.

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
2. Deliver applications and services to customer in device agnostic way	Section 4.2.2.4 2d. Deployment of applications by running the applications from the SIM	- OMA SCWS : enable applications to be run on SIM - USB-IC EEM (TCP-IP) for performances - Global Platform	3.0	2.8	2.4	2.6	1
2. Deliver applications and services to customer in device agnostic way	Section 4.2.2.2 2b. MNO customization of device	==> see basic custom 1.a - OMA LFC ==> availability of the spec? Usage of the SIM? : allow Customization of a device Look and Feel.	3.0	1.6	1.4	1.5	2

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
1. Simple customer migration between devices.	Section 4.2.1.1 1a. Ensure device settings are automatically managed and configured	<ul style="list-style-type: none"> - OMA CP Smart Card Profile - OMA DM (Bootstrapping, Provisioning) to be preferred versus OMA CP <ul style="list-style-type: none"> : define a process of provisioning the DM client to a state where it is able to initiate a management session to the DM server. - IMEI tracking application interacts with device management platform in the network. 	2.8	3.0	2.5	2.8	3
3. Provide security for sensitive data	Section 4.2.3.5 3e. Securely store passwords and login details	<ul style="list-style-type: none"> - OMA SCWS <ul style="list-style-type: none"> : enable applications to be run on SIM 	2.6	2.4	2.4	2.4	4
1. Simple customer migration between devices.	Section 4.2.1.2 1b. Store customer generated content on card	<p><i>The customer can synchronise address book between device and SIM</i></p> <ul style="list-style-type: none"> - 3GPP TS 31.220 rel-8 <ul style="list-style-type: none"> : define interface between Card and device. This is based on OMA DS and allows the synchronization of the user's personal data between the device and the card. Phonebook is part of such data - 3GPP TS 31.221 rel-8 <ul style="list-style-type: none"> Define a Java API to manage such data synchronized in the card. - OMA SCWS <ul style="list-style-type: none"> : enable access to content on SIM - SyncML <ul style="list-style-type: none"> : adapted for Contact Manager ==> refer 3GPP specs : synchronise data on the card with the data on the device. 	2.4	2.6	2.1	2.3	5

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
		<p><i>Store customer created photos, videos on their SIM</i></p> <ul style="list-style-type: none"> - USB-IC <ul style="list-style-type: none"> : mass storage if control by the device or EEM (TCP-IP) using SCWS if controlled by the SIM : for large amount of content distribution and management. - ETSI R9 Multimedia File System <p><i>Store customer generated / received messages on their SIM</i></p> <ul style="list-style-type: none"> - ETSI file system for SMS, ETSI Large file + PmoActive session for MMS <p><i>Store customer content moved from example their laptop and stored on their SIM</i></p> <ul style="list-style-type: none"> - USB-IC <ul style="list-style-type: none"> : mass storage & TCP-IP for SCWS - ETSI R9 Multimedia File System <ul style="list-style-type: none"> : for large amount of content distribution and management. - OMA SCWS <ul style="list-style-type: none"> : enable access to content on SIM: both ETSI contact book & synchronised contacts book 					

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
1. Simple customer migration between devices.	1e. Distribute and store MNO content on card	<ul style="list-style-type: none"> - USB-IC : for large amount of content distribution and management. - OMA SCWS : for content distribution and management. - IMEI tracking application : Interacts with the remote platform in the network. - OMA DRM / SRM : define a way of storing and distributing DRM contents and Rights Objects in a secure manner 	2.4	2.7	1.4	2.1	6
1. Simple customer migration between devices.	1c. Store customer preferences	<ul style="list-style-type: none"> - OMA LFC ==> not using the SIM? : allow Customization of a device Look and Feel, which composes of <ul style="list-style-type: none"> - Background, wallpaper and screensaver - Ring tones, audio cues or sounds - Start-up / Shutdown experience - Animations and splash screens - Status indicators - Fonts - Notification and error messages - Keyboard: soft keys and navigation keys, and shortcuts - Menus: menu items and arrangement - Homepage and bookmarks 	2.4	1.1	1.4	1.3	7
2. Deliver applications and services to customer in	2a. Multimedia address book. (this use case is not about the synchronization the data on device with the data on SIM)	<ul style="list-style-type: none"> - OMA SCWS : enable applications to be run on SIM * Address book data synchronization is covered in 4.2.1.2 use case. 	2.3	2.6	2.1	2.3	8

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
device agnostic way							
3. Provide security for sensitive data	3b. Provide secure authentication mechanism for offline & online transitions	<ul style="list-style-type: none"> - OMA SCWS : enable applications to be run on SIM - OATH – One Time Password - ETSI Secure Channel - 3GPP GBA - Liberty Alliance Framework 	2.3	2.4	1.6	2.0	9
3. Provide security for sensitive data	3f. Company VPN credentials		2.3	1.7	1.6	1.6	10
3. Provide security for sensitive data	3d. Authentication to multiple network types.	<ul style="list-style-type: none"> - EAP-SIM - EAP-AKA 	2.2	3.0	2.6	2.8	11
2. Deliver applications and services to customer in device agnostic way	2c. Deployment of applications by installation of applications onto the device	<ul style="list-style-type: none"> - OMA DM : define software upgrades to provide for new software to be loaded on the device - USB-IC : mass storage with the application store in the SIM and deployed on the device ==> for large amount of content distribution and management. - SCWS: over ISO or USB-IC EEM (TCP-IP) : to display interface allowing to retrieve applications 	2.2	1.7	2.0	1.8	12

Use Case Summary	Use Case Detail	Related Standard / Solution	Market Impact	Availability of Standard	Technical Ease of Deployment	Average Ease of Implementation	Use Case Priority
		from distant server					
1. Simple customer migration between devices.	1d. Store customer purchased content	- OMA SRM define a way of storing and distributing DRM contents and Rights Objects in a secure manner - USB-IC : for large amount of content - ETSI R9 Multimedia File system	2.1	2.3	1.1	1.7	13
3. Provide security for sensitive data	3g. Store application certificates	==> linked to the Device Application Distribution use case 2.c J2ME - MIDP2: use the card for application installation authorization	2.0	2.3	2.6	2.5	14
3. Provide security for sensitive data	3c. DRM & Media certificates	- OMA DRM / SRM : DRM separate delivery of content and rights objects	1.8	2.5	1.4	1.9	15
3. Provide security for sensitive data	3a. Protect personal data stored on card	- PIN code protection : PIN entry for session or PIN entry for each access. - Authentication vectors : Data access can be based on mechanisms (location, presence, document owner-controlled access) - ETSI R9 Multimedia File system	1.7	2.6	2.7	2.6	16

5. USE CASE INPUT DOCUMENTS

SoftBank Mobile - GSMA Smart SIM Meeting 1, 3rd December 2008 - "USIM_Initiative 20081202_SBM_kono.ppt"

SK Telecom – Cartes Conference 2008 – "2008_C06_hong.pdf"

GSMA Smart SIM Meeting 1, 3rd December 2008 – "smart_sim_pre_kickoff_ic_279817.ppt"
- captures use cases from Orange, Gemalto, SKT, SoftBank Mobile, TIM, Telefonica and Vodafone.

GSMA Smart SIM Meeting 2, 14th and 15th January 2009 – capture use cases from Orange, Gemalto, SKT, SoftBank Mobile, TIM and Telefonica.

6. APPENDIX 1: GENERIC STANDARDS (ALL CARDS)

All UICCs need to support, as default,

3GPP TS 11 11 v8.13.0 Specification of the Subscriber Identity Module- Mobile Equipment (SIM-ME) Interface

3GPP TS 31 102 v8.5.0 Characteristics of Universal Subscriber Identity Module (USIM) Application

3GPP TS 11 14 v8.18.0 Specification of the SIM Application Toolkit for the Subscriber Identity Module- Mobile Equipment (SIM-ME) Interface

3GPP TS 31 111 v8.5.1 Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)

3GPP TS 31 220 v8.0.0 Characteristics of the Contact Manager for 3GPP UICC Applications

3GPP TS 31 221 v8.0.1 Contact Manager Application Programming Interface (API); Contact Manager API for Java Card

7. DOCUMENT MANAGEMENT

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0		New PRD (SCaG SC.06)	SCaG#52 EMC#	Gwen Edwards, FT Orange

Other Information

Type	Description
Document Owner	SCaG
Editor / Company	Gwen Edwards, FT Orange