Network Settings Exchange
Version 4.0
20 April 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. 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 permitted under the security classification without the prior written approval of the Association.

Copyright Notice (Test)

Disclaimer

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.

Antitrust Notice

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

Table of Contents

1 Introduction

1.1 Overview

This document specifies the requirements for a database enabling the efficient transfer of settings from mobile network operators (including mobile virtual network operators) to device manufacturers in order to allow for the appropriate customization of devices.

1.2 Scope

This document specifies the operation of the database, including:

- the mechanism(s) by which mobile network operators and MVNOs (Mobile virtual network operator) can upload settings to the database
- the mechanisms by which device manufacturers can extract information from the database.

The settings themselves, and the use of the settings are out of the scope of this document. For a definition of the settings and their usage, please see GSMA PRD TS.32 Technical Adaptation of Devices through Late Customisation [1]

1.3 Definitions

Term	Description
Group of settings	A set of network identifiers (see section **Error! Reference source not found.**) and a set of settings (see **Error! Reference source not found.**)
Network identifiers	The set of identifiers used to identify a particular set of settings (see **Error! Reference source not found.**). This may include one or more of MCC, MNC, EF_GID1 file, etc.
Settings Providing Organization	An entity which provides settings corresponding to their network to the database

1.4 Abbreviations

Term	Description
API	Application Programming Interface
APN	Access Point Name
DCS	Device Configuration Server
EF_GID1	Elementary File - Group Identifier level 1
GPRS	General Packet Radio Service
IMSI	International Mobile Subscriber Identity
JSON	JavaScript Object Notation
LTE	Long-Term Evolution
MCC	Mobile Country Code
MNC	Mobile Network Code

Term	Description
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MVNO	Mobile virtual network operator
NSX	Network Settings Exchange
OEM	Original Equipment Manufacturer
PLMN	Public Land Mobile Network
PLMN ID	PLMN identity – this comprises one MCC and one MNC (see 3GPP TS 24.008)
PRD	Permanent Reference Document
SMSC	Short Message Service Centre
SPN	Service Provider Name
SPO	Settings Providing Organization
XML	eXtensible Markup Language

1.5 References

Ref	Doc Number	Title
[1]	GSMA PRD TS.32	Technical Adaptation of Devices through Late Customisation
[2]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[3]	3GPP TS 23.003	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
[4]	GSMA PRD N2020.05	Device Configuration Server Mechanisms
[5]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words

1.6 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 (RFC2119) [2] (RFC8174) [5] when, and only when, they appear in all capitals, as shown here.

2 Architecture

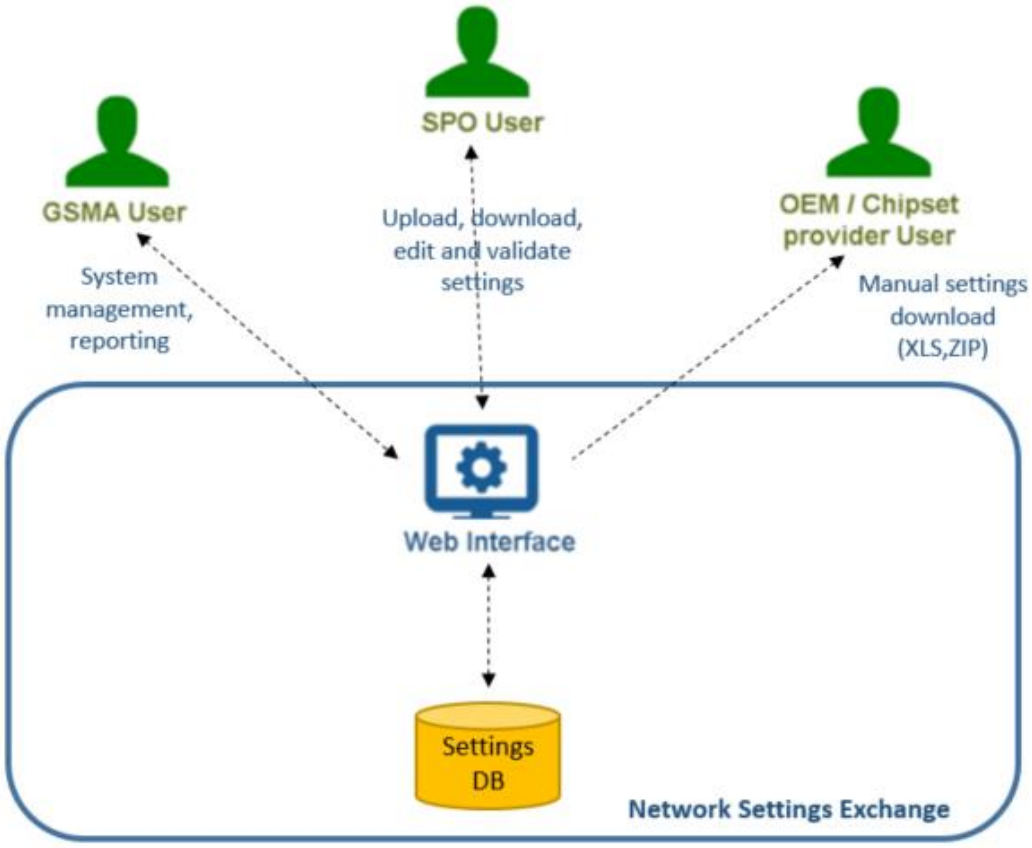

Figure 1 - Overall process

Error! Reference source not found. shows the overall process defined in this document. The uploading of settings from SPO (Settings Providing Organization) to the database is defined in section **Error! Reference source not found.**; the definition of a group of settings is defined in section **Error! Reference source not found.**; the validation process is described in section **Error! Reference source not found.**; the download of settings from the database to an SDU (Network Settings Exchange User) is described in section **Error! Reference source not found.**. The configuration of the devices is the OEMs / chipset providers responsibility and is out of scope of this document.

3 Settings Definition

3.1 General

A group of settings consists of the complete set of:

- settings as defined in GSMA PRD TS.32 **Error! Reference source not found.** is applicable to all operators,
- optional MNO Supplementary Settings, which shall be clearly distinguished from other settings as defined in GSMA PRD TS.32 [1],
- a set of network identifiers to indicate the applicability of the group of settings.

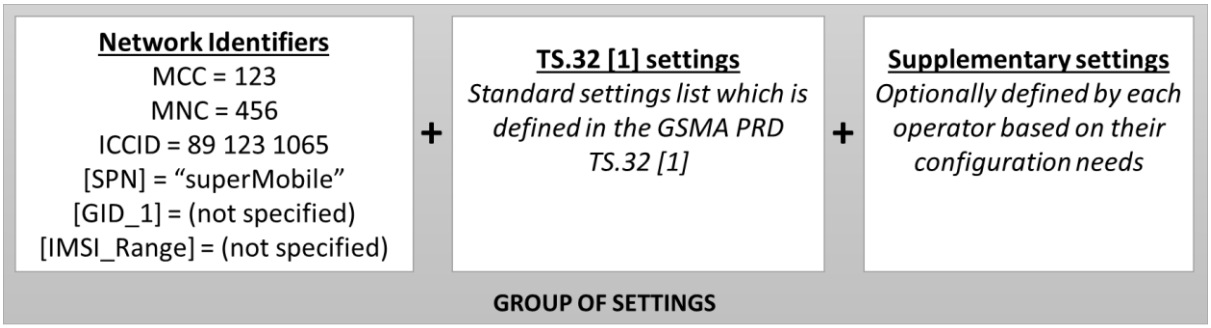

Figure 2 - Example group of settings

GSMA PRD TS.32 [1] is updated periodically. Therefore there shall be a web interface for GSMA users to update the settings list in the database dynamically. The update shall be done by uploading an XML schema that has the parameter descriptions and the default values. The schema shall be used for validating the settings when SPO users upload their settings. The web interface shall reject the settings which do not comply with the XML schema.

GSMA PRD TS.32 [1] settings should be handled as a set with a version number rather than updating the settings individually on a single set. Any change to the existing GSMA PRD TS.32 [1] shall require a new TS.32 version setting on the database.

Only the last version of the GSMA PRD TS.32 [1] settings shall be available for operators who wish to submit their settings. When the GSMA PRD TS.32 [1] settings are updated:

- Operators submitting new settings shall see the final GSMA PRD TS.32 [1] settings version to enter their data
- The existing operator settings shall remain with the previously used GSMA PRD TS.32 [1] settings version. When the operator wants to update the settings then the new GSMA PRD TS.32 [1] settings version shall be used..

3.2 Settings Types

The possible values of each setting are defined in GSMA PRD TS.32 **Error! Reference source not found.**.

Settings may be of one of the following types:

1. Boolean ("Activate / Deactivate"): if "Activate", a device which supports the indicated feature is to activate the feature; if "Deactivate", a device is to deactivate this feature.
2. Integer: the value a device should use in carrying out a specified procedure; this may be an upper or lower limit (e.g. maximum LTE category)
3. String: a string of characters used in carrying out a specified procedure (e.g. APN). A string may contain one or more spaces.
4. Sequence: A sequence of settings of one of the above types (e.g. permitted GPRS classes)

3.3 Network identifiers

A group of settings shall include a set of network identifiers to indicate their applicability. The PLMN (Public Land Mobile Network) identity (MCC (Mobile Country Code) and MNC

Mobile Network Code)) shall be specified. These values shall be recorded in the SPO registration process and shall be filled into dropdown lists on the web interface while uploading the settings. Please see section 4.1 for further details about the SPO registration.

One or more identifiers (other than the PLMN ID) may be left blank, in which case the group of settings applies regardless of the value of that identifier.

The algorithm used to match network identifiers to the fields on a device's USIM is specified in section **Error! Reference source not found.**.

The database should generate a warning to an SPO after an upload which results in potentially ambiguous network identifiers being used, e.g. where two (or more) groups of settings are uploaded for the same PLMN ID, where different network identifier fields are used.

The network identifiers may additionally include a human-readable text field to indicate the intended usage of the corresponding settings e.g. "superMobile, MyPLMN-UK MVNO". This field is provided for convenience only and shall not be relied upon to distinguish or identify groups of settings.

3.4 Default values

Some settings may be associated with a default value in GSMA PRD TS.32 **Error! Reference source not found.**. These values to be registered to the database while GSMA users define the GSMA PRD TS.32 [1] settings list on the web form.

For string type settings (see **Error! Reference source not found.**), the database shall be able to distinguish from empty fields (i.e. a string of zero length) and an omission, indicating the desired use of a default value.

The database shall have the capability for the default values to be updated within the process to update TS.32 [1] settings set, in response to changes to GSMA PRD TS.32 **Error! Reference source not found.**.

3.5 Access rights associated with settings

By default, all settings are accessible to any OEM and chipset provider user and restricted to other SPO users. An SPO may restrict access to their settings (e.g. by means of a check box on the web interface) to their preferred OEMs and chipset providers.

Furthermore, an SPO may indicate that a group of settings may be accessed only by one or more specified OEMs and chipset providers. If a group of settings are restricted in this way, the SPO should provide a group of settings with the same network identifiers which are not restricted to one or more specified entities.

These restrictions may be modified at any time by the SPO (see section **Error! Reference source not found.**).

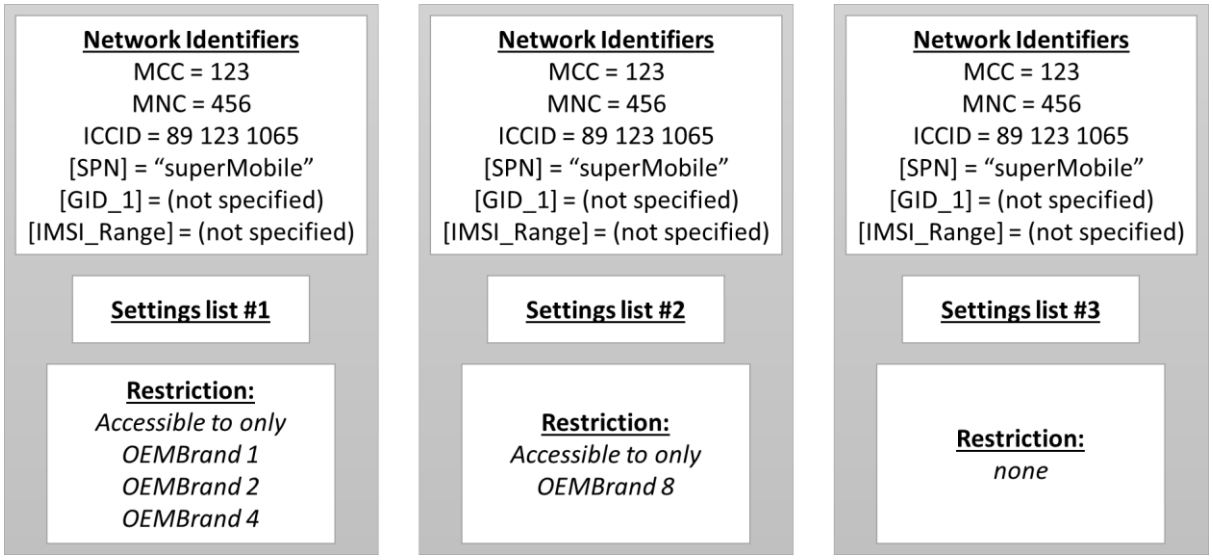

Figure 3 - Restricted settings

Error! Reference source not found. shows a number of settings provided by an SPO for the same set of subscribers (i.e. using the same PLMN ID and SPN) but with different access restrictions. The group on the left and the group in the middle will be made available only to the OEMs / chipset providers indicated. OEMs and chipset providers not indicated in these groups will receive the unrestricted group of settings on the right hand side column (Settings list #3).

Whenever an unrestricted group of settings corresponding to a set of network identifiers is changed, the database should notify the SPO if there also exists a restricted group of settings corresponding to the same network identifiers.

NOTE: This is to avoid the risk that an SPO modifies its public settings but fails to update a corresponding set of restricted settings.

3.6 Settings Validation

Incorrect settings of certain parameters may render a device almost unusable on a mobile network. It is therefore important that certain settings values are carefully enabled on the NSX as downloadable and accessible by the OEMs and chipset providers.

GSMA Working Group TSG (Terminal Steering Group) therefore recommends that a mobile device-based validation application be provided to carry out the following steps:

- using the login credentials of the SPO, obtain the current settings for that SPO from the database
- implement these in the mobile device
- confirm correct behaviour of the device based on the settings e.g. transmit an SMS, access the internet, send an MMS (Multimedia Messaging Service) message.
- in response to confirming this behaviour, send a notification to the database.

The settings that are to be validated shall include at least the internet APN (and credentials), SMSC (Short Message Service Centre) and MMS settings.

NOTE: Settings to be validated should be the ones which are typically accessible to the device's end-user, and therefore could be manually changed by the user or accessible via an API without requiring special permissions on the device.

4 Upload of settings to database

4.1 SPO Registration and access permissions

Only SPO users are permitted to upload settings to the database.

- Full Members of the GSMA shall be granted SPO status.
- MVNOs shall be granted SPO status after signing a GSMA Non-Member Participation Agreement (NMPA). The Network Settings Exchange NMPA will only be applicable to this activity. MNOs may upload their MVNO partners settings if requested by their MVNO, and in this case they would not need to sign an NMPA.

NOTE: Only MNOs can be GSMA full members.

NOTE: MVNOs and some MNOs are not GSMA full members.

SPO registration steps shall follow the given order:

- SPO user candidate shall fill the registration form on the web site by
    - selecting the country of operation from a dropdown list
    - selecting the organization name from a dropdown list (only applicable for MNOs, not for MVNOs)
    - entering the MCC/MNC identifiers list that will be managed by the SPO user
    - filling user contact details.
- The form submission triggers a notification email to the GSMA NSX operation team email address.
- GSMA NSX operation team authorizes the user, the organization, membership and the MCC/MNC identifiers list and then approves the registration request. An auto generated password will be sent to the SPO user email address. The random passwords shall be at least 8 characters including numeric and both upper-case and lower-case alphanumeric characters.
- The first registered SPO user shall be the master user for that SPO and shall be able to authorize the other user registration requests from that SPO without the need of the GSMA NSX operation team's registration approval.

SPO users shall change their login passwords by a web interface on the web portal. The new password shall also be 8 characters including numeric and both upper-case and lower-case alphanumeric characters. The system shall be able to send a password reset link to the user's email address if the user forgets their password.

The database shall store, for all SPOs, the MCC/MNC identifiers for which the SPO is permitted to upload settings. The database shall detect and block any cases where multiple MNOs upload settings for the same MCC/MNC setting.

The database should prevent an SPO from uploading settings for networks (MCC / MNC) that it does not control.

4.2 Upload mechanism

The database shall provide a web-based interface for the uploading of the group of settings.

The database shall validate the data according to the requirements within this document and within GSMA PRD TS.32 **Error! Reference source not found.**. The database should validate APN (Access Point Name) settings against the requirements in 3GPP TS 23.003 [3].

The database shall validate the uploaded settings against the defined schema and provide the results to the SPO.

5 Download of settings from database

5.1 OEM and chipset provider registration and access permissions

Addition to the SPO users downloading their own settings for consistency checks, only registered and authorised OEMs and chipset providers shall be permitted to request access to the database to download settings. Registration of an OEM / chipset provider shall be approved by the GSMA and the authorisation to download the settings shall be given by the SPO of the settings.

OEMs and chipset providers which are not GSMA Associate Members shall sign a GSMA Non-Member Participation Agreement (NMPA) within the registration process. The Device Setting Database NMPA will only be applicable to this activity.

OEM and chipset provider registration steps shall follow in the given order:

- The user shall complete the registration form on the website by entering their company and contact details.
- The user downloads, signs and uploads the NMPA if it is a non-member company
- The form submission triggers a notification email to the GSMA NSX operation team email address.
- The GSMA NSX operation team authorizes the user, the organization, membership and then approves the registration request.
- The first registered OEM / shipset provider user shall be the master user for that organization and shall be able to authorize the other user registration requests from that organization without the need of GSMA NSX operation team’s registration approval.

The OEM / chipset provider users shall change their login passwords by a web interface on the web portal. The new password shall also be at least 8 characters including numeric and both upper-case and lower-case alphanumeric characters. The system shall be able to send a password reset link to the user’s email address if case the user forgets their password.

If an OEM / chipset provider has a DCS as described in [4] N2020.05 PRD - Device Configuration Server Mechanisms, then it shall be connected to the database server and authenticated with OEM ID and Credentials (or certificate) in order to guarantee the security

of the communication channel. A DCS may represent multiple OEMs in which case it will have multiple corresponding OEM IDs and credentials.

The database shall restrict the download of settings where the SPO has indicated (see section **Error! Reference source not found.**) based on OEM ID (or certificate). Restricted settings shall be indicated as such, and shall be treated as confidential by the OEM / chipset provider, to the extent as technically feasible.

Where a setting is normally accessible (i.e., would be accessible in the case where settings are applied which are not restricted) via a user interface or programming API by a device, the device should prevent it from being accessed.

5.2 Download mechanism

The database shall allow the download, via an HTTPS web interface and a programming API:

- The web interface shall list all settings which are made available by the SPO and given permission for download to the relevant OEM/Chipset provider. The settings shall be listed with the operator names and network identifiers and the interface shall allow OEM / chipset provider users to do searching with these criteria. SPO users shall also have access to this interface, however only their own settings should be displayed for downloading. The eligible users should then be able to download the network settings in a CSV format as single files per network.
- The API shall allow OEMs / chipset providers to able to download available settings in JSON and XML format. The API shall have a method to download all settings with a single request and a method to request all settings of an operator by providing its MCC and MNC identifiers. The API authentication shall require the user credentials of the OEMs / chipset provider user.

5.3 Use of settings and network identifiers

The implementation of a group of settings within a device shall be carried out in accordance with GSMA PRD TS.32 **Error! Reference source not found.**. The method by which a device is configured with a group of settings is out of the scope of this document.

Identifying the group of settings applicable to a device, is performed by using the network identifiers associated with the groups of settings and the corresponding fields on the USIM.

Where multiple groups of settings are provided for a given PLMN ID but where other identifiers differ or are absent, the following matching algorithm shall be applied.

A group of settings shall apply to any device using a (U)SIM where:

a) if one or more identifiers in addition to the PLMN ID (MCC, MNC) are provided for the group of settings, all provided identifiers match those of the (U)SIM;
b) else, if no identifiers other than the PLMN ID (MCC, MNC) are provided for the group of settings, these match those of the (U)SIM.

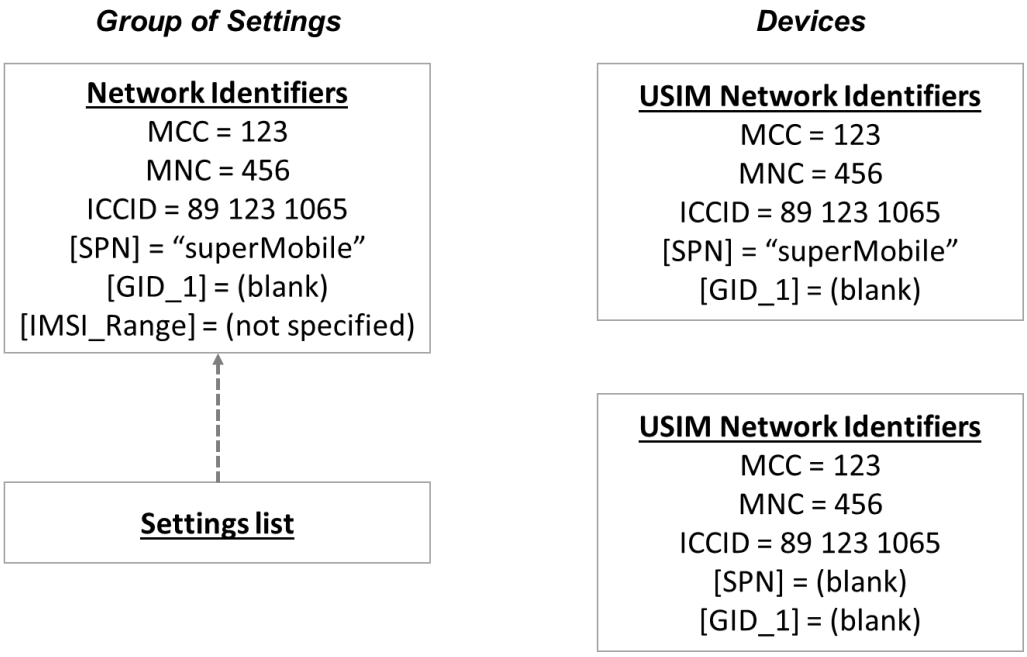

Figure 4 – Only the top device on the right would use the settings on the left

It is possible that multiple groups of settings will match according to a) above. In this case, the selection of which settings to apply is implementation-specific.

NOTE: The use of identifiers used on the SIM profile for Remote SIM Provisioning is for further study.

6 Database management and operation

6.1 General

Industry best practice for the management of an internet-accessible database shall be followed in particular in respect of (but not limited to):

- data backup,
- data consistency,
- security including confidentiality and authentication and authorization.

6.2 Management tools

The database shall enable an SPO to:

- download an existing group of settings it has uploaded
- Update an existing group of settings or alter and save them as a new group of settings
- delete a group of settings
- modify the access permissions associated with a group of settings

6.3 Notifications

The database shall generate notifications (e.g. by email) as follows:

5. An SPO shall be notified whenever a group of settings is uploaded by another SPO with MCC / MNC matching one or more groups of settings previously uploaded by the member. This ensures that MNOs have full visibility of updates made by their MVNO partners
6. All SPO's will be notified when a new OEM / chipset provider is added to the database so that they have the option to allow or deny access to their settings. If the SPO is using the default option to share

The database shall permit OEM / chipset providers to subscribe for notifications of:

- New SPOs
- The upload of new groups of settings
- Modification of permissions associated with a group of settings such that the group of settings is now (but was not previously) accessible to the OEM / chipset provider or is no longer accessible (but was previously) to the OEM / chipset provider .

These subscriptions may limit the rate at which notifications are sent to immediately (i.e. no limit), or once per day / week / month. Notifications shall identify the relevant group of settings and the nature of the modification.

Subscriptions may limit the MNO/MVNOs for which notifications are received.

6.4 Settings download report for SPO users

The SPO users should able to query the download logs of their own settings. The settings download report shall include the following columns:

- OEM / chipset provider name
- Downloaded settings id and version
- Download date and time

6.5 GSMA user rights and reporting

Addition to the all functions that SPO and OEM / chipset provider users have, the following reporting and management facilities are also to be available for GSMA users:

- Approval of the company and user registration requests
- Add, remove and edit organization names in the MNO registration dropdown list
- Edit network identifiers of the registered operators
- Deactivate / activate
    - SPOs, OEMs / chipset providers. Users of the deactivated can no longer login to the web interface or the API and settings are not visible in the system.
    - SPO, OEM / chipset provider users. Deactivated users can no longer login to the web interface or the API.
- Total numbers report including
    - Number of SPOs registered (active / passive)
    - Number of SPO users (active / passive)
    - Number of OEMs / chipset providers registered (active / passive)

  - Number of OEM / chipset provider users (active / passive)
  - Number of settings available (per TS.32 version)

- User transaction log
  - Select organization, user and the report displays all activities on the system like login, add settings, download settings, API calls, etc.

Annex A Settings XML Template

Use the following XML template when an SDU downloads the values from NSX and an SPO uploads the values to NSX:

xml schema_v3.xml

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	16 June 2016	New PRD	TSG/PSMC	David Hole / BlackBerry
2.0	24 March 2017	Changes detailed in CR1002 implemented	TSG at TSG#27	David Hole / BlackBerry
3.0	Sept 2017	Changes detailed in CR1003 implemented	TSG at TSG#29	Erdem Ersoz / GSMA
4.0	April 2020	Changes detailed in CR1004 implemented	TSG - email	Tyler Smith / GSMA

B.2 Other Information

Type	Description
Document Owner	GSMA
Editor / Company	Paul Gosden

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.