NFC Core Wallet Requirements
Version 2.0
15 August 2013

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

Disclaimer

Antitrust Notice

Table of Contents

1. Introduction

This document is a technical candidate specification that defines a set of requirements for mobile operators' mobile wallets and interoperable formats for the provisioning and management of on-device NFC services. Note, this document focuses on mobile wallets provided by mobile operators (designed to interact with applications on the SIM card), rather than mobile wallets from other players.

The GSMA recognises the need for an interoperable approach and has therefore constructed this document as candidate technical specification.

1.1. Objectives

A mobile wallet is a software application which resides on a mobile handset and emulates the functionality of a physical wallet. A mobile wallet can be used to enable the handset to access interoperable NFC services, such as making a payment at point of sale. Although different mobile operators may deploy different mobile wallet applications, they need to agree on core functionality and interfaces to provide an "operator-agnostic" environment to simplify the deployment of applications by service providers, such as retailers, transport companies and banks.

This document proposes formats to achieve interoperability across mobile operators' different mobile wallet platforms. It aims to provide the points of interoperability that will enable mobile wallets from multiple operators to support the same applications. It also defines how a third-party service provider should provide its service on a "mobile wallet."

This document focuses on mobile wallets provided by mobile operators, rather than other players. Other, non-SIM based solutions are neither excluded nor in any way affected by these requirements.

1.2. Intended audience

The intended audience for this document is:

- Service providers who need to know what to expect from a mobile wallet, so they can develop and tune their applications and NFC services accordingly and ensure they interact in a consistent way across different mobile operators' wallet implementations.
- Implementers of a core wallet[1] who need guidance on the basic requirements that should be satisfied.
- Implementers of a provisioning backend system for a core wallet who need guidance on the basic requirements that should be satisfied to support a mobile wallet.

1.3. Scope and structure

The document defines a framework that a service provider can use to provide the same NFC application (interface and applets) to all mobile network operators' wallets without changes to the provisioned package.

---

[1] Core wallet (CW) refers to a subset of features, protocols, interactions models and interfaces mobile operators' wallets should support in order to provide a consistent and interoperable offering

The document:

- Defines the core wallet,
- Outlines a reference architecture,
- Sets out requirements for a core wallet and the requirements for information supplied by service providers seeking to use the functionality of the wallet to offer NFC services.

The following is out of scope of this document:

- A complete definition of the mobile wallet
- The trusted service manager (TSM) interface between mobile operators' and service providers' backend systems.

1.4. Definition of Terms

Term	Description
AFI	Application family identifier
Android	The Android mobile operating system developed by Google
API	Application Programming Interface
Applet	Java program for execution on the UICC (same as cardlet)
Cardlet	Java program for execution on the UICC (same as applet)
CLF	Contact Less Frontend
CRS	Contactless Registry Service
CW	Core Wallet
DAP	Data Authentication Pattern
ETSI	European Telecommunications Standards Institute
GP	Global Platform
GSMA	GSM Association
GUI	Graphical User Interface
IRI	International Resource Identifier
ISO	International Organization for Standardization
J2ME	Java 2 Micro Edition
MMI	Man to Machine Interface
MNO	Mobile Network Operator
MNO TSM	Mobile Network Operator Trusted Service Manager

MNO_Backend	Server(s) and network within a MNO organization used to handle CW and UICC management. It communicates with CW, UICC and SP_Backend; It also includes MNO TSM.
NA	Not Apply
Native SP_MMI	SP_MMI coded as a native mobile application for a specific mobile operating system platform
NFC	Near Field Communications
NFC_Service	An NFC_Service consists of one SP_Applet and zero or more SP_MMIs
OS	Operating System
OTA	Over The Air
POS	Point of Sales Terminal
RFID	Radio Frequency Identification
RIM	Research In Motion
SDK	Software Developer Kit
SMS	Short Message Service
SE	Secure Element
SIM	Subscriber Identity Module
SP	Service Provider
SP TSM	Service Provider TSM
SP_Backend	Server(s) and network within SP organization used to handle NFC service(s). It communicates with SP_Applet and SP_Application as well as with MNO TSM; It may also include a SP TSM.
SP_Applet	SP Applets (an application/applet intended to run in Java Card VM providing secure services, such as payment, transaction processing, secure keystore, etc.)
SP_CP	SP Core Package is a file archive that includes NFC_service(s) assets – icons, descriptions, metadata, application and applets packages, applet installation parameters, etc.); it is signed with a SP valid certificate
SP_MMI	SP application that provides a dedicated user interface on a mobile device
SP UI app	This is another term for the SP_MMI
SSD	Supplementary Security Domain
TSM	Trusted Service Manager
UI	User Interface
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
XML	Extensible Markup Language

1.5. Terminology

As per IETF Requirements terminology, reference [RFC2119], the following terms have the following meaning.

Terms	Description
SHALL	Denotes a mandatory requirement
SHOULD	Denotes a recommendation
MAY	Denotes an optional requirement

1.6. References

Terms	Description
[NFC_UICC]	NFC UICC Requirement Specification, Version 2.0, GSMA
[NFC_HANDS]	NFC Handset APIs & Requirements, Version 2.0, GSMA
[GP_AMENDC]	GlobalPlatform Card Specification Version 2.2, Amendment C: Contactless Services
[RFC3987]	Internationalized Resource Identifiers (IRIs) RFC3987 - M. Duerst, M. Suignard. http://www.ietf.org/rfc/rfc3987
[W3C_PC]	Widget Packaging and XML Configuration, http://www.w3.org/TR/widgets/
[RFC1032]	Domain Administrators Guide, IETF RFC1032 http://www.ietf.org/rfc/rfc1032
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels, IETF RFC2119, http://www.ietf.org/rfc/rfc2119.txt
[ISO14443-3]	Identification cards -- Contactless integrated circuit(s) cards -- proximity cards -- Part 3: Initialization and anti-collision
[GP_MSG]	GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services v1.0
[GP_CARD]	GlobalPlatform Card Specification v2.2.1
[JCARD]	JAVA CARD CLASSIC PLATFORM SPECIFICATION 3.0.4, http://www.oracle.com/technetwork/java/javame/javacard/download/specs-jsp-136430.html
[J2ME]	JAVA FOR MOBILE DEVICES, http://www.oracle.com/technetwork/java/javame/javamobile/overview/getstarted/index.html
[ANDROID]	Android, http://www.android.com/
[RFC2396]	Uniform Resource Identifiers (URI): Generic Syntax, IETF RFC2396, http://www.ietf.org/rfc/rfc2396.txt
[REG_EXP]	POSIX-Extended regular expression
[AAUI]	EMVCo AAUI - EMVCo Contactless Mobile Payment – Application Activation User Interface – Overview, Usage Guidelines, and PPSE Requirements, v1.0, December 2010
[E.212]	E.212 Amend. 3: The international identification plan for public networks and subscriptions, ITU

1.7. List of tables and figures

2. The Mobile Wallet

2.1. Core wallet

The mobile wallet is a software application which resides on a mobile handset and emulates the functionality of a physical wallet. Designed to enhance the user experience, a mobile wallet enables mobile operators, banks, retailers and other service providers to provide targeted and convenient access to value-added services enabled by the NFC chip and the UICC in the device. The wallet, for example, can typically list all the NFC-related services loaded onto the mobile device or SIM (the UICC) and display their current status. The wallet may also allow users to manage the NFC settings of their mobile device**.**

The term "core wallet" (CW) refers to a subset of features, protocols, interactions models and interfaces different mobile operators' mobile wallets should support. The core wallet is designed to provide a consistent and interoperable offering to service providers for NFC-based services and to host applications produced by the service providers. In this technical document, these applications are referred to as SP_MMIs, Service Provider Man-Machine Interfaces. In accompanying documents, the same applications may also be referred to as UI apps (User Interface applications) because they provide a dedicated user interface. An SP_MMI can be installed directly from the core wallet or it can be downloaded from an applications store. How the service provider's applet is installed on the UICC is outside the scope of this document.

This document covers the first version of the core wallet. Subsequent versions of the core wallet may also support additional services/APIs (features) that can interact with service provider applications. These features will be agreed and standardized in the future.

Service providers can consider two approaches to application development:

2.2. Native SP_MMI for the mobile platform:

The service provider uses the application run time framework natively supported by the mobile phone operating system. Depending on the targeted handset operating system, the service provider uses the target Software Developer Kit (SDK) and the appropriate programming language. The resulting application will be managed by the operating system and will run as a standalone application. In this case, the CW will launch and interact with the MMI. Depending on its implementation, this MMI application may be installed on the mobile phone via a mobile operator or service provider download site and/or an application store.

Some approaches and tools may simplify the development of a native application. For example, a code generator could produce a native SP_MMI from information (text, images, and configuration data) contained in a template.

2.3. Extended Wallet MMI:

Some mobile operators (and other actors) may provide optional functionality in their core wallets to manage a set of standard applications. They may also provide the infrastructure and interfaces to enable the core wallet to manage NFC services for service providers not willing to afford the development and testing of native applications on multiple phones and operating systems. For example, instead of producing native code, the service provider would complete a pre-defined template with data and parameters (xml, text, icon etc.) that characterize its application. The service provider template data is then pushed on to an end-user's mobile phone, where a template interpreter, within the core wallet, configures itself based on the service provider's data. In addition to the CW specifications outlined below, this approach requires the standardization of additional features and formats. This will be the subject of future work, in concordance with market requirements.

In the case of both approaches, the standardisation work required to achieve full interoperability has not yet been completed.

Note the GSMA anticipates that these approaches are not exhaustive.

2.4. Compliance Declaration

The following systems can claim compliance against this document:

System	System Description	Requirements
CW	A mobile application that implements a CW	All requirements marked with CW
SP_CP	A file provided by a service provider (SP) to a mobile operator	All requirements marked as SP_CP

3. Reference Architecture

This chapter depicts a reference architecture and interface. The expected interfaces of a CW are also listed and discussed.
Figure 1 describes the most basic scenario where the service provider's NFC_Service only consists of an applet provisioned into the UICC without any dedicated SP_MMI. It provides basic functionality at NFC acceptance points (e.g. a point of sale terminal with a NFC reader). The end user can see a graphical representation of the installed applet in the CW user interface, but does not have a dedicated MMI to interact with. Instead, the service is provided by the core wallet's UI which interacts with the service provider's applet on the SIM card via the mobile operator's contactless registry service (CRS), also on the SIM card.
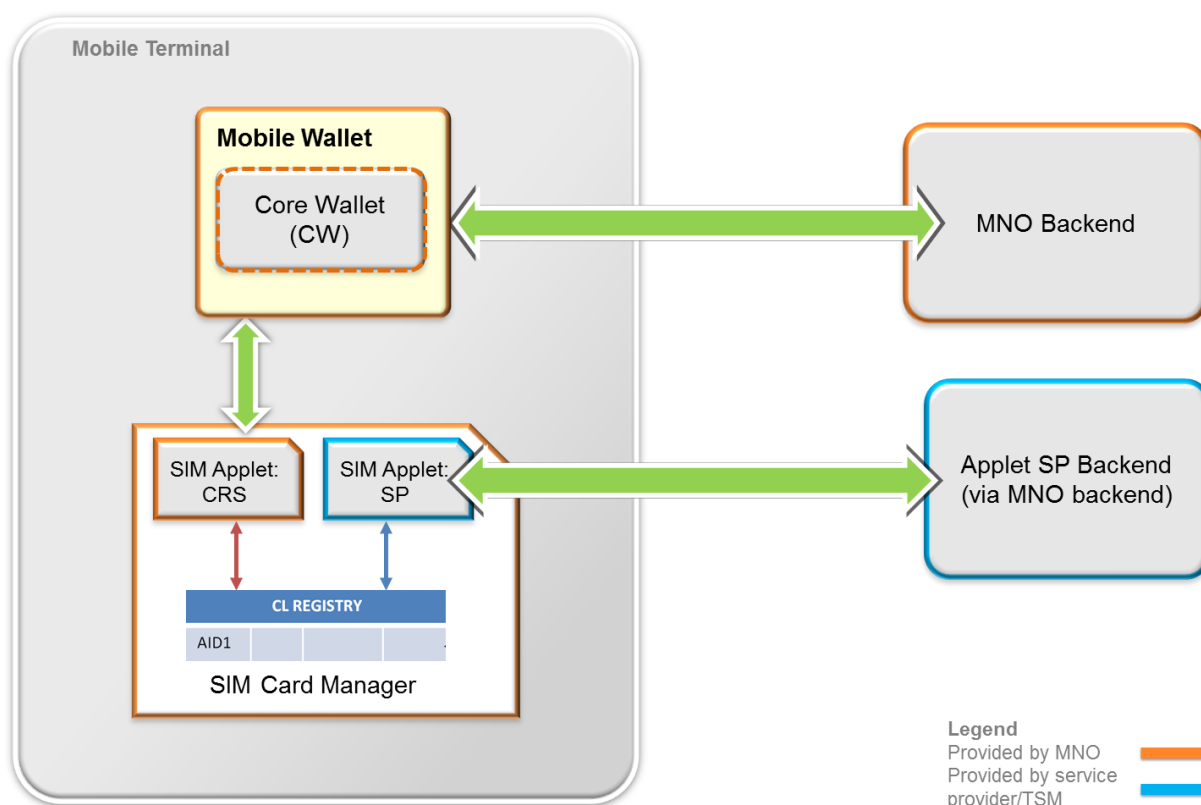
Figure 1: Core Wallet Architecture with Applets Only

Figure 2 shows a Native SP_MMI, i.e. an application that runs natively on the handset's operating system. This Native SP_MMI can provide a user interface for the functions of the SP Applet installed on the UICC, as well as access to the backend services of the service provider located in the network (e.g. ticket provisioning for public transport services).

In addition to displaying information in the form of icons and text about the installed NFC_Service, the CW is also able to invoke the Native SP_MMI. The Native SP_MMI may take over the screen of the user's handset while the CW terminates or runs in the background. The service provider needs to develop native apps for all the targeted handset platforms (e.g. APK files for Android, JAR/JAD files for J2ME devices, COD for RIM, etc.).
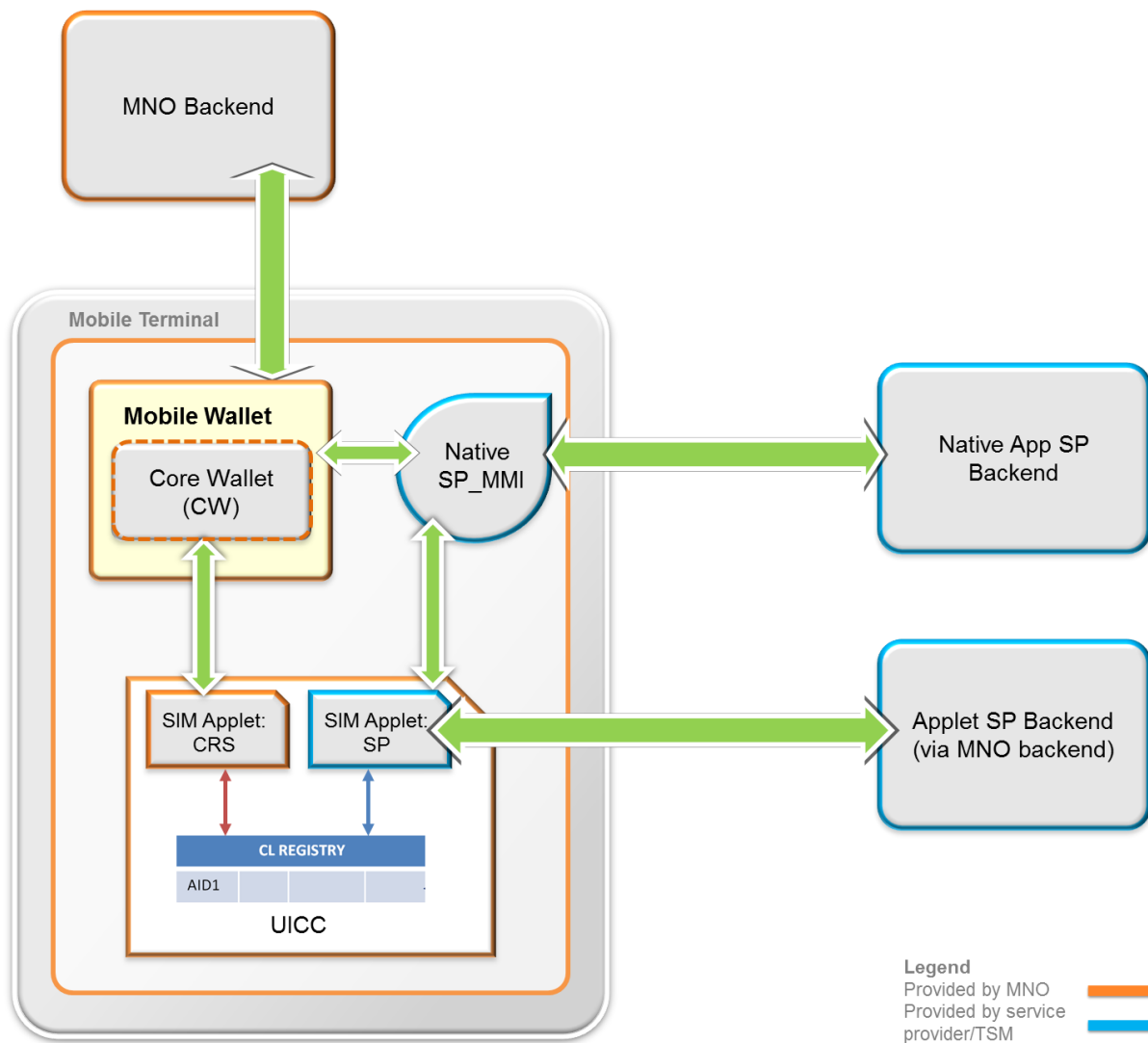
Figure 2: Core Wallet Architecture with Native SP_MMI

Figure 3 highlights the scope of the specification covered in this paper:

- Core Wallet (CW) as a basic set of functionalities to be supported by all mobile operators' mobile wallets.
- SP Core Package (SP_CP) is the package a service provider should provide to a mobile operator to provision its NFC_Service(s) on a CW. Each mobile network operator backend will process the package in order to enable the CW to discover, install and deploy the SP MMI and SP_Applet; within a SP_CP, a service provider can insert assets to publish an NFC_Service. This NFC_Service can be installed on the user handset and the UICC card via the installation of zero or more MMI(s) and one or more SP_Applet(s).
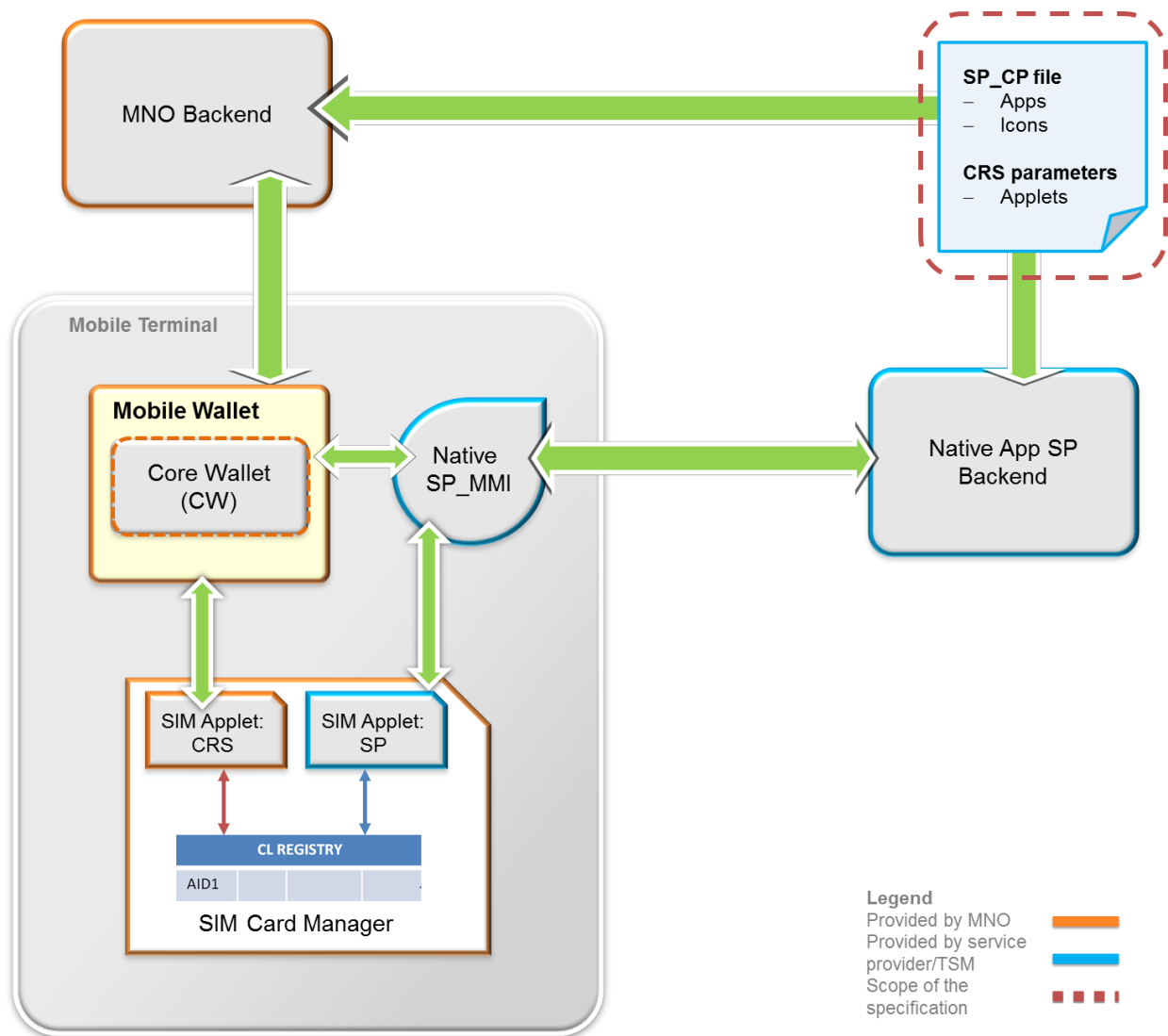
Figure 3: Core Wallet architecture and the scope of the specification covered in this paper

3.1. Interface List

In this chapter, the identified interfaces within the reference architecture are listed with the related reference document.

Interface Name	Explanation and Reference Documents
CW-MNO_Backend	Network Interface between the CW and MNO_Backend: This interface is defined by each mobile operator specifically. In this document, only the basic functionality provided by this interface is defined.

CW-SIM	Interface between CW and SIM card: This interface is defined by each mobile operator specifically. In this document, only the basic functionality provided by this interface is defined. The CW communicates with the SIM in order to activate, deactivate or list installed SP_Applets; The interface leverages on [GP_AMENDC] mechanisms, but the implementation of CRS application is left to each mobile operator's mobile wallet implementation. In addition, [NFC_HANDS] defines the SIM APIs and Access Control Mechanisms.
CW-MMIs	Interface between MMIs and CW: This is the interface between the SP_MMI and the CW. The functionality may be operating system dependent. In this document only *mwallet:* schema is defined in section 6.11 allowing basic interaction between CW and SP_MMI. The GSMA currently anticipates that further security mechanisms will be specified in the next release of the CW.
Provisioning Formats between MNO Backend-SP Backend	Interface between the service provider and mobile operator backends used by the service provider to provide MMIs, metadata and (if needed) applets: In this document, a SP_CP file format is defined as an interoperability mechanism to enable a service provider to provision an application on different mobile operator CW backends. Note this is only a file format. APIs, protocols and procedures to provide this file are out of scope of this document. The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO

4. Core Wallet Requirements

This chapter lists the requirements for the CW.

4.1. SP Service Discovery and Installation

ID	Requirement CW
1	The CW MAY allow users to discover services that can be installed and used. For example, an available services catalogue MAY be used.

4.2. SP Service Life Cycle

ID	Requirement CW
2	The CW SHOULD be able to trigger the installation and update of SP NFC_services or provide options for NFC_service installation and update via the SP
3	The CW SHOULD allow the user to trigger the uninstallation of SP NFC_services or provide options for NFC_service uninstallation via the SP
4	The CW SHALL be able to trigger the launch of SP_MMIs
5	The CW SHOULD be able to launch an URL in case of external URLs (e.g. no SP_MMI is needed and only opening a web page is requested by SP)

6	The CW MAY intercept and process the "*mwallet:*" schema as defined in 6.11 [2]

4.3. Applets Activation and Conflicts

ID	Requirement CW
7	The CW SHALL display the active SP_Applet(s) to the user
8	The CW SHOULD allow the user to trigger the activation of a SP_Applet
9	The CW SHOULD allow the user to trigger the deactivation of a SP_Applet
10	The CW SHOULD guide the user to choose the preferred SP_Applets. In a case where the user chooses to activate a SP_Applet that cannot coexist with (an)other already active SP_Applet(s), the CW SHOULD present proper prompting to set the preferred applet(s) to be made active and to resolve the conflict.

4.4. Applets and MMIs synchronization

ID	Requirement CW
11	CW SHOULD give (eventually after user consent) the possibility to trigger the reinstallation of all SP_MMIs that are not installed and whose related SP_Applets are installed

5. Core Package Requirements

This chapter provides the requirements for SP_ CP.

The SP Core Package (SP_CP) is the package a service provider should supply to a mobile operator to publish its service on the CW. The SP_CP package will be processed by the mobile operator backend in order to enable the CW to discover, install and deploy the SP MMI and SP_Applet. The SP_CP file SP_CP is based on [W3C_PC] and it is a zip file with a configuration file and a defined folder structure to store SP_MMI(s) (also includes variants to cover proper handset portfolio), SP_Applet[3].

ID	Requirement SP_CP
12	An SP_CP provided by an SP to MNO(s) SHALL use the format defined in 6.1

---

[2] As explained in 6.11, in modern OS, schema can be used to do action on a certain application. It is used to launch CW (for instance from a SP_MMI) or get details; for example, J2ME Content Handler API or Android filters are method to use schema as a mean - independent from OS - to call action on CW

[3] For the avoidance of doubt, SP_CP is NOT intended to be consumed directly by a CW, but it is intended to be consumed by the mobile operator backend. The operator backend will use the SP_CP resources to properly instruct the CW and the UICC through a TSM(s) to deploy SP_MMI and (in some case) SP_Applet on the user mobile terminal and SIM when needed.

[4] Common methods to satisfy this requirement are, for example, J2ME Content Handler API or Android filters.

13	A native SP_MMI contained in the SP_CP SHALL register itself to enable it be invoked by the URL of its id as defined in 6.2[4]

The GSMA currently anticipates that further developer guidelines will be given for SP_MMI and SP_Applet contained within SP_CP.

6. SP Core Package

6.1. SP Core Package Format

The table below lists the requirements for SP_CP.

ID	Requirement SP_CP
14	SP_CP SHALL be a package as defined in [W3C_PC]; additional elements and attributes are defined within GSMA namespace.
15	SP_CP configuration document SHALL at least include the elements as defined in 0
16	In order to reference SP_MMIs, SP_CP configuration document SHALL include one or more gsma:mmi element pointing to SP_MMI(s) as defined in 0
17	In order to reference SP applets, SP_CP configuration document SHALL include one or more gsma: applet element pointing to SP_Applet(s) to be instantiated as defined in 0.
18	In order to reference SP applet packages, SP_CP configuration document SHALL include one or more gsma:applet-package element pointing to SP_Applet(s) packages to be deployed as defined in 0.
19	In order to reference SSD, SP_CP configuration document SHALL include one or more gsma:ssd element pointing to SSD(s) in which deployed applet has to be instantiated as defined in 0.
20	SP_CP SHALL include at least one signature.xml whose certificate leads to a well-known CA
21	SP_CP MAY define features other than those defined in 6.10
22	SP_CP MAY also include additional preference elements

6.2. SP_CP Identifier

Each SP_CP has to be identified by a unique identifier.

ID	Requirements SP_CP
23	The SP_CP service SHALL be identified by an URL as defined in the ID widget attribute of [W3C_PC]
24	The SP_CP ID widget attribute URL domain SHALL be a subdomain of a domain owned by the SP (e.g. Registrant Organization as defined in [RFC1032] SHALL be the SP)

6.3. Version

The SP_CP are identified by a version number.

ID	Requirements SP_CP
25	The SP_CP SHALL be versioned using rec-version-tag grammar as described in [W3C_PC]: rec-version-tag = 1*DIGIT „." 1*DIGIT [„." 1*DIGIT] *[1*ALPHA / SP / 1*DIGIT]
26	The SP_CP MAY have a version name associated using rec-version-tag grammar as described in [W3C_PC]: rec-version-tag = 1*DIGIT „." 1*DIGIT [„." 1*DIGIT] *[1*ALPHA / SP / 1*DIGIT]

6.4. Localization

ID	Requirement SP_CP
27	The SP_CP MAY include at root a *Container for localized content* as defined in [W3C_PC]. [5]
28	Within folder-based package structure, SP_CP SHALL include files with filenames in the form name-extension (ABNF): package_name[6] = 1*ALPHA package_extension=1*ALPHA name-extension = package_name "." package_extension

6.5. SP_CP configuration document elements and attributes

In this chapter, all parameters that can be declarable by the SP within SP_CP manifest are listed.

In following tables:
- Group: is the group parameter belong to; following groups are defined
  - Service Provider information
  - NFC Service information
  - SSD information
  - Applet information
  - MMI information
- Name: indicates the name of the element or attribute
- Occurrence: in case of element indicates how many time the element can occur
- Format: indicates the format as defined in 6.6
- Localizable: indicates if the element is localizable via xml-lang as defined in [W3C_PC]
- MNO Specific: indicates if the element can be defined and specified for a certain MNO via gsma:mno attribute. This mean is used as temporary way to address some

---

[5] For the avoidance of doubt, installation packages can also be localized using locales folder-based localization.

interoperability differences that may happen during first phase of cross MNO services deployment. It is currently anticipated that GSMA will try to reduce and minimize the areas in which usage of this mean is needed.

- Namespace: indicates the namespace of the element or attribute. In particular, in order to declare parameters, elements defined within [W3C_PC] are used; in addition as per [W3C_PC], the configuration document format is extended with the XML elements and attributes within namespace: http://gsma.org/ns/nfc. In table they are referred as:

  - o xmlns: http://www.w3.org/ns/widgets
  - o gsma: http://gsma.org/ns/nfc
- xPaths: indicates the XPath(s) of the element or attribute used to retrieve the information querying the CP_SP manifest

1.	Group: N/A	Role
It describes the role of icon or content; Supported values are defined in 6.1.		
Name: role Occurrence: N/A Format: String Context: Attribute of icon and content Namespace: gsma Localizable: N/A MNO Specific: false xPaths: @gsma:role		

2.	Group: N/A	Target
It describes the target platform of a content. Supported values are defined in 6.2 and 6.3.		
Name: target Occurrence: N/A Format: String Context: Attribute of gsma:content Namespace: gsma Localizable: N/A MNO Specific: false xPaths: @gsma:target		

3.	Group: N/A	MNO
It specifies the MNO the element content refers to. The behaiour of the processor is the same as per xml:lang element as defined in [W3C-XML]. Only element with MNO specific = true can use this attribute. It should be noticed that this attribute is used only as Integerim solution to solve interoperability differences between MNOs, but in future it should be removed and avoided.		
The value of the attribute is defined in ABNF as:		
MNO-Tag = mnotag mnotag = (mcc ["-" mnc])		

mcc = 3DIGITS; mobile country code as defined in [E.212]

mnc = 3DIGITS; mobile network code

Name: mno
Occurrence: N/A
Format: String
Context: Attribute of gsma:service-id and gsma:dap and gsma:exclusion-id
Namespace: gsma
Localizable: N/A
MNO Specific: false
xPaths: @gsma:mno

4.	Group: N/A	Identifier

It is an identifier of the ssd, applet and package within the SP_CP manifest. It is used to refer to this ssd, applet and package whitin this file.;each element has to be progressivelly numbered using this attribute.

Name: id
Occurrence: One
Format: id
Context: Attribute of gsma:ssd, gsma:Applet and gsma:applet-package
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:ssd[@id]

gsma:applet[@id]

gsma:applet-package[@id]

5.	Group: SP Info	SP TSM Name

It defines the name of TSM SP of the service provider. It shall be a univocal name chosen by SP. It may be a URI derived by a Domain onwed by the SP

Name: tsm-name
Occurrence: One
Format: String
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:tsm-name

6.	Group: SP Info	SP Contacts Email

It defines the name of the Service Provider; it shall be the complete commercial name of the legat entity that has the business relation with the MNO

Name: author
Occurrence: One
Format: Email
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: author

7.	Group: SP Info	Content
It defines several URI within SP with a certain roles as defined in 6.10		
Name: content Occurrence: OneOrMore Format: URI Context: Child of widget Namespace: xmlns Localizable: true MNO Specific: false xPaths: content		

8.	Group: SP Info	SP Service Main Contacts
It defines the email and phone numbers of primary contact whitin SP; Supported schema are "tel" [RFC 3966], "mailto" [RFC 6068], "sms" [RFC 5724]		
Name: NA Occurrence: OneOrMore Format: URI Context: Child of widget Namespace: xmlns Localizable: true MNO Specific: false xPaths: content[@gsma:role= main-contact]		

9.	Group: SP Info	TSM SP web service
It defines the host domain name of end point of TSM SP as defined in [GP_MSG]		
Name: NA Occurrence: One Format: String Context: Child of widget Namespace: xmlns Localizable: true MNO Specific: false xPaths: content[@gsma:role= TSM]		

10.	Group: SP Info	TSM SP heartbeat
It defines the host domain name of TSM SP heartbeat . An example of implementation of this host can be found in [AFSCM].		
Name: NA Occurrence: One Format: String Context: Child of widget Namespace: xmlns Localizable: true MNO Specific: false xPaths: content[@gsma:role= TSM-heartbeat]		

11.	Group: SP Info	SP Service Customer Support

It defines the phone number , email of support number of the SP.[1]; supported schema is "tel" [RFC 3966]

Name: NA
Occurrence: ZeroOrMore
Format: URI
Context: Child of widget
Namespace: xmlns
Localizable: true
MNO Specific: false
xPaths: content[@gsma:role= support]

[1] The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO.

12.	Group: SP Info	SP Service Customer Support information

It defines the customer support information by SP. The format is human readable text.

Name: support-information
Occurrence: ZeroOrMore
Format: String
Context: Child of widget
Namespace: xmlns
Localizable: true
MNO Specific: false
xPaths: gsma:support-information

13.	Group: NFC Service info	Icons and Graphics

It defines the icon used as image by CW to display the NFC Service as defined in 6.8 and 6.9

Name: icon
Occurrence: OneOrMore
Format: URI
Context: Child of widget
Namespace: xmlns
Localizable: true
MNO Specific: false
xPaths: icon[@gsma:role=launch|inactive|id-1|screenshot|video|promotional]

14.	Group: NFC Service info	Service Common Name

It defines the name (Display Name as defined in [GP_MSG]) of the NFC services that is displayed in CW

Name: name
Occurrence: One
Format: String
Context: Child of widget
Namespace: xmlns
Localizable: true
MNO Specific: false
xPaths: name

15.	Group: NFC Service info	Service Technical Name

It defines the NFC Service name (Name as defined in [GP_MSG] of the NFC services

Name: gp-name
Occurrence: One
Format: String
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:gp-name

16.	Group: NFC Service info	Service Common Description

It defines the a human-readable description of the services that is dysplayed in CW

Name: description
Occurrence: One
Format: String
Context: Child of widget
Namespace: xmlns
Localizable: true
MNO Specific: false
xPaths: description

17.	Group: NFC Service info	Last Changes

It defines a human-readable description of the last changes which have been made since the previous versions

Name: last-changes
Occurrence: One
Format: String
Context: Child of widget
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:last-changes

18.	Group: NFC Service info	Service ID

It defines the Service ID as defined in [GP_MSG]. It is currently anticipated that GSMA may handle a common database for assignment of Service ID

Name: service-id
Occurrence: One
Format: Integer
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: true
xPaths: gsma:service-id

19.	Group: NFC Service info	Service and Core Package version

It defines the version of the SP_CP as defined in 6.3

Name: version
Occurrence: One
Format: version
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: version

20.	Group: NFC Service info	License

It defines the License and Terms and Conditions for the NFC Service to be shown in the CW to the user [1]

Name: license
Occurrence: ZeroOrOne
Format: String or URL
Context: Child of widget
Namespace: gsma
Localizable: true
MNO Specific: true
xPaths: license

[1] The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO.

21.	Group: NFC Service info	MNO authorized to Delete

It defines if MNO is authorized to delete the service from UICC after user request [1]

Name: NA
Occurrence: ZeroOrOne
Format: Boolean
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: preference[@name="MNO-delete"; @value="yes|no"]

[1] The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO.

22.	Group: NFC Service info	MNO authorized to GP lock

It defines if MNO is authorized to lock the service from UICC after user request [1]

Name: NA
Occurrence: ZeroOrOne
Format: Boolean
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false

xPaths: preference[@name="MNO-lock"; @value="yes|no"]

[1] The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO.

23.	Group: NFC Service info	MNO authorized to Display in MNO discovery service

It defines if the NFC Service is visible within MNO discovery service catalog in CW [1]

Name: NA
Occurrence: ZeroOrOne
Format: Boolean
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: preference[@name="MNO-visibility"; @value="yes|no"]

[1] The values provided in this field are technical information that may be used by the MNO provisioning system, but does not represent nor replace any contractual agreement which could exist between the SP and the MNO.

24.	Group: NFC Service info	SP Service subscribe web URL

It defines the mobile web page URL to redirect the user to in order to subscribe the service; it is reaccommended that the target web site is optimized for mobile, tablets and Desktop (using usual device recognition or adaptative techniques); different roles are defined in 6.10 [2]

Name: NA
Occurrence: ZeroOrOne
Format: URL
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: content[@gsma:role= install]

[2] Depending on MNO architecture, there is several possibilities to trig the installation of a SP service from the MNO Wallet. This field only apply in case the installation of the service is triggered directly from the Wallet (direct URL from Wallet to SP Back end).

25.	Group: NFC Service info	SP Service lock web URL

It defines the mobile web page URL to redirect the user to in order to lock the service; it is reaccommended that the target web site is optimized for mobile, tablets and Desktop (using usual device recognition or adaptative techniques); different roles are defined in 6.10 [2]

Name: NA
Occurrence: ZeroOrOne
Format: URL
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: content[@gsma:role= lock]

[2] Depending on MNO architecture, there is several possibilities to trig the installation of a SP service from the MNO Wallet. This field only apply in case the installation of the service is triggered directly from the Wallet (direct URL from Wallet to SP Back end).

26.	Group: NFC Service info	SP Service unlock web URL

It defines the mobile web page URL to redirect the user to in order to unlock the service; it is reaccommended that the target web site is optimized for mobile, tablets and Desktop (using usual device recognition or adaptative techniques); different roles are defined in 6.10 [2]

Name: NA
Occurrence: ZeroOrOne
Format: URL
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: content[@gsma:role= unlock]

[2] Depending on MNO architecture, there is several possibilities to trig the installation of a SP service from the MNO Wallet. This field only apply in case the installation of the service is triggered directly from the Wallet (direct URL from Wallet to SP Back end).

27.	Group: NFC Service info	SP Service delete web URL

It defines the mobile web page URL to redirect the user to in order to delete the service; it is reaccommended that the target web site is optimized for mobile, tablets and Desktop (using usual device recognition or adaptative techniques); different roles are defined in 6.10 [2]

Name: NA
Occurrence: ZeroOrOne
Format: URL
Context: Child of widget
Namespace: xmlns
Localizable: false
MNO Specific: false
xPaths: content[@gsma:role= delete]

[2] Depending on MNO architecture, there is several possibilities to trig the installation of a SP service from the MNO Wallet. This field only apply in case the installation of the service is triggered directly from the Wallet (direct URL from Wallet to SP Back end).

28.	Group: NFC Service info	Installation exclusion

It defined the list of Service ID that cannot be subscribed and installed with parent NFC Service. For avoidance of doubts, this parameters impact only on presentations of services within CW and does not impact on the activation on SIM within [AmendC]

Name: exclusion-id
Occurrence: ZeroOrMore
Format: Integer
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:exclusion-id

29.	Group: NFC Service Keywords	Keywords Type of Service

It defines a comma separated list of keywords to identity the type of services.As keyword the AFI (as defined in [ISO14443-3]) value as hexadecimal string SHOULD be used; alternative string values may be used in case AFI values does not apply

Name: keywords
Occurrence: ZeroOrMore
Format: String
Context: Child of widget
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:afi-keywords

30.	Group: ssd Info	ssd

It defines necessary information related to the ssd creations hosting the SP service cardlet(s)

Name: ssd
Occurrence: ZeroOrMore
Format: N/A
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:ssd

31.	Group: ssd Info	ssd hierarchy

It defines gsma:ssd[@id] of parent ssd; in case of ISD this attribute is not defined.

Name: hierarchy
Occurrence: ZeroOrMore
Format: id
Context: Attribute of gsma:ssd
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:ssd[@hierarchy]

32.	Group: Applet info	Applet

It defines necessary information related to the Applets to be instantiated

Name: applet
Occurrence: ZeroOrMore
Format: N/A
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet

33.	Group: Applet Info	Applet Package
	It defines necessary information related to the Applets Package to be installed.	

Name: applet-package
Occurrence: ZeroOrMore
Format: N/A
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package

34.	Group: Applet, SSD info	Applet/Package/SSD Name
	It defines a human-readable label used by technical team to easily identify and understand role of the applet/package/ssd.	

Name: label
Occurrence: OneOrMore
Format: String
Context: Child of gsma:applet, gsma:applet-package and gsma:ssd
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:applet\gsma:label

gsma:applet-package\gsma:label

gsma:ssd\gsma:label

35.	Group: Applet, SSD info	Applet/Package/SSD Description
	It defines a human-readable description used by technical team to easily identify and understand role of the applet/package/ssd.	

Name: description
Occurrence: ZeroOrMore
Format: String
Context: Child of gsma:applet, gsma:applet-package and gsma:ssd
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:applet\gsma:description

gsma:applet-package\gsma:description

gsma:ssd\gsma:description

36.	Group: Applet info	InstanceOf

It defines the ID of the package the applet is instance of. In the manifest a applet element should be defined with instanceOf undefined and id attribute

Name: instance-of
Occurrence: One
Format: id
Context: Attribute of gsma:Applet
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet[@instance-of]

37.	Group: Applet, SSD info	AID

It defines the package AID or the applet package and applet instance AID. It defines ssd AID that the Service Provider would like to be used. Notice that as it may interfer with existing already set ssd AID, MNO can decide or not to use this information. Also notice that the real set values are retrieved from the reponse to createOrAllocatessd request from SP TSM to MNO TSM as defined in [GP_MSG].

Name: aid
Occurrence: One
Format: AID
Context: Attribute of gsma:ssd, gsma:applet and gsma:applet-package
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:ssd[@aid]

gsma:applet[@aid]

gsma:applet-package[@aid]

38.	Group: Applet info	Package version

It defines package version

Name: version
Occurrence: One
Format: version
Context: Attribute of gsma:applet-package
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package[@version]

39.	Group: Applet info	Parent ssd AID

It defines the parent SD for the instance or the package refering to gsma:ssd[@id]. This field indicates where package should be deployed or instance will be extradite/instanciate. If not defined applet will be oaded in

Issuer SD
Name: ssd-parent-id Occurrence: ZeroOrOne Format: id Context: Attribute of gsma:applet and gsma:applet-package Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet[@ssd-parent-id] gsma:applet-package[@ssd-parent-id]

40.	Group: Applet info	Executable Module Aid
It defines the class/module AID to be instanciate		
Name: executable-module-aid Occurrence: One Format: AID Context: Attribute of gsma:applet Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet[@executable-module-aid]		

41.	Group: Applet info	Instance TAR
It defines TAR value that allows SP TSM to directly target its applet instance as defined in [GP_MSG]. By convention, this value should be forth, third and second to last byte of the long AID		
Name: tar Occurrence: ZeroOrOne Format: String Context: Attribute of gsma:applet and gsma:ssd Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet[@tar] gsma:ssd[@tar]		

42.	Group: Applet info	Volatile Memory
It defines the Volatile data space limit in bytes that an application would require to run properly. It should be noticed that this information is provided in this field for information only, and shall not override information that may be present in install parameters."		
Name: volatile Occurrence: ZeroOrOne Format: Integer Context: Attribute of gsma:applet Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet[@volatile]		

43.	Group: Applet info	Non Volatile Memory

It defines the Non Volatile data space limit in bytes that an application would require at installation time. It should be noticed that this information is provided in this field for information only, and shall not override information that may be present in install parameters.

Name: nonvolatile
Occurrence: ZeroOrOne
Format: Integer
Context: Attribute of gsma:applet
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet[@nonvolatile]

44.	Group: Applet info	**DAP signing**

It refers to DAP signature as defined in [GP_CARD] sent back by the Service Provider (DAP) or a security officer in charge of the Validation Authority after the verification/validation of the Service Provider Applet against security and applet development guidelines (mandated DAP). This tag is not relevant in DM as it is part of the Load command. This is a mandatory tag in SM in case

1) The Service Provider SSD has the DAP privilege OR

2) A SSD with Mandated DAP privilege is present on the card

Name: dap
Occurrence: ZeroOrMore
Format: NA
Context: child of gsma:applet-package
Namespace: gsma
Localizable: false
MNO Specific: true
xPaths: gsma:applet-package\gsma:dap

45.	Group: Applet info	**DAP Card Profile Id**

It referes to MNO card profile id as defined in [GP_MSG]

Name: card-profile-id
Occurrence: One
Format: Integer
Context: Attribute of gsma:dap
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet/gsma:dap[@card-profile-id]

46.	Group: Applet and ssd info	**Instantiate Application Command**

It specifies the identifier of the parameters profile to be used in Simple mode, or to be checked against in DM mode.

If not present, default privileges and install parameters SHALL be used by the function provider.

Name: instantiate-application-command
Occurrence: ZeroOrMore
Format: N/A
Context: child of gsma:ssd and child of gsma:applet
Namespace: gsma
Localizable: false
MNO Specific: false

xPaths: gsma:ssd\gsma:instantiate-application-command

gsma:applet\gsma:instantiate-application-command

47.	Group: Applet info	Load Elf Command

It specifies the identifier of the parameters profile to be used in Simple mode, or to be checked against in DM mode.

If not present, default parameters values SHALL be used by the function provider.

Name: load-elf-command
Occurrence: ZeroOrMore
Format: N/A
Context: child of gsma:applet-package
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package\gsma:load-elf-command

48.	Group: Applet info	Make Selectable Application Command

It specifies the identifier of the parameters profile to be used in Simple mode, or to be checked against in DM mode.

If not present, default parameters values SHALL be used by the function provider.

Name: make-selectable-application -command
Occurrence: ZeroOrMore
Format: N/A
Context: child of gsma:applet
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet\gsma:make-selectable-application-command

49.	Group: Applet info	Application Registry Update Command

It specifies the identifier of the parameters profile to be used in Simple mode, or to be checked against in DM mode.

If not present, default parameters values SHALL be used by the function provider.

Name: application-registry-update-command
Occurrence: ZeroOrMore
Format: N/A
Context: child of gsma:applet (with id and ef)
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet\gsma:application-registry-update-command

50.	Group: Applet, ssd Info	GP Parameters Profile Id

It defines theprofile id of the parameter as defined by [GP_MSG];

Name: gp-parameters-profile-id
Occurrence: one
Format: id
Context: Attribute of gsma:load-elf-command,

gsma:instantiate-application-command,

gsma:make-selectable-application-command,

gsma:application-registry-update-command
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package\gsma:load-elf-command[@gp-parameters-profile-id]

gsma:ssd\gsma:instantiate-application-command[@gp-parameters-profile-id]

gsma:applet\gsma:instantiate-application-command[@gp-parameters-profile-id]

gsma:applet\gsma:make-selectable-appl

51.	Group: Applet, ssd Info	GP Parameters Profile id Default

It defines default profile to be used in case parameters are not provided in service request, as defined by [GP_MSG]

Name: gp-parameters-profile-id-default
Occurrence: One
Format: Boolean
Context: Attribute of gsma:load-elf-command,

gsma:instantiate-application-command,

gsma:make-selectable-application-command,

gsma:application-registry-update-command
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package\gsma:load-elf-command[@gp-parameters-profile-id-default]

gsma:ssd\gsma:instantiate-application-command[@gp-parameters-profile-id-default]

gsma:applet\gsma:instantiate-application-command[@gp-parameters-profile-id-default]

gsma:applet\g

52.	Group: Applet, ssd Info	EF tag parameters

It defines the content of the EF tag as defined in [GP_CARD]; only content value of the EF tag SHALL be provided (without the EF tag included)

Name: ef
Occurrence: one
Format: String
Context: Attribute of gsma:load-elf-command,

 gsma:instantiate-application-command,

gsma:make-selectable-application-command,

gsma:application-registry-update-command
Namespace: gsma
Localizable:
MNO Specific: false
xPaths: gsma:applet-package\gsma:load-elf-command[@ef]

gsma:applet\gsma:instantiate-application-command[@ef]

gsma:ssd\gsma:instantiate-application-command[@ef]

gsma:applet\gsma:make-selectable-application-command[@ef]

gsma:applet\gsma:applet\gsma:application-regi

53.	Group: Applet, ssd Info	Privileges parameters

It defines the application privileges as defined in [GP_CARD]

Name: privileges
Occurrence: one
Format: String
Context: Attribute of gsma:instantiate-application-command,

gsma:make-selectable-application-command
Namespace: gsma
Localizable:
MNO Specific: false
xPaths: gsma:applet\gsma:instantiate-application-command[@privileges]

gsma:ssd\gsma:instantiate-application-command[@privileges]

gsma:applet\gsma:make-selectable-application-command[@privileges]

54.	Group: Applet, ssd Info	Application Specific Parameters

It defines the application specific installation parameters as defined in [GP_CARD]; only content value of the C9 tag SHALL be provided (without the c9 tag included)

Name: c9
Occurrence: one
Format: String
Context: Attribute of gsma:instantiate-application-command
Namespace: gsma
Localizable:
MNO Specific: false
xPaths: gsma:applet\gsma:instantiate-application-command[@c9]

gsma:ssd\gsma:instantiate-application-command[@c9]

55.	Group: Applet, ssd Info	System Specific Parameters

It defines the UICC system specific parameters as defined in [GP_CARD] and [AAUI]; only content value of the

EA tag SHALL be provided (without the EA tag included)
Name: ea Occurrence: one Format: String Context: Attribute of gsma:instantiate-application-command Namespace: gsma Localizable: MNO Specific: false xPaths: gsma:applet\gsma:instantiate-application-command[@ea] gsma:ssd\gsma:instantiate-application-command[@ea]

56.	Group: Applet info	Load file data block hash
It defines Load File Data Block Signature as defined in [GP_CARD]		
Name: load-file-data-block-hash Occurrence: One Format: String Context: Attribute of gsma:applet-package Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet-package[@load-file-data-block-hash]		

57.	Group: Applet info	Type
It defines the type of applets as defined in GP [GP_MSG]. Supported values are "head", "member" or "standalone" application; "it should be noticed that this information is provided in this field for information only, and shall not override information that may be present in install parameters		
Name: type Occurrence: ZeroOrOne Format: String Context: Attribute of gsma:Applet Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet[@type]		

58.	Group: Applet info	Applet File
It defines installation file containing the applet		
Name: content Occurrence: One Format: URI Context: Child of gsma:applet-package Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:applet-package\gsma:content		

59.	Group: Applet info	Applet File Path
It defines the path to the install file containing the applet (e.g. cap file)		

Name: src
Occurrence: One
Format: URI
Context: Attribute of gsma:applet-package\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package\gsma:content[@src]

60.	Group: Applet info	Mimetype

It defines the mimetype of the file; Supported values are listed in 6.6. At today only CAP file are accepted as defines in [CAP]

Name: type
Occurrence: One
Format: String
Context: Attribute of gsma:Applet\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:applet-package\gsma:content[@type]

61.	Group: MMI Info	MMI

It defines necessary information related to the MMI to be installed

Name: mmi
Occurrence: OneOrMore
Format: N/A
Context: Child of widget
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi

62.	Group: MMI Info	File

It defines the MMI file to be installed

Name: content
Occurrence: OneOrMore
Format: String
Context: Child of gsma:mmi
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:mmi\gsma:content

63.	Group: MMI Info	Description

It defines a human readable description for the MMI

Name: description
Occurrence: ZeroOrMore
Format: String
Context: Child of gsma:mmi
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:mmi\gsma:description

64.	Group: MMI Info	Name

It defines a human readable label for the MMI

Name: label
Occurrence: OneOrMore
Format: String
Context: Child of gsma:mmi
Namespace: gsma
Localizable: true
MNO Specific: false
xPaths: gsma:mmi\gsma:label

65.	Group: MMI Info	version

It defines the version of the MMI

Name: version
Occurrence: One
Format: version
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@version]

66.	Group: MMI Info	Download URL

It defines the path or URL (to a web site or marketplace) to install the MMI. Supported schema for URL schema "http:", "https:" and specific platform dependent schema (e.g. "market:" for Android as defined in [ANDROID])

Name: src
Occurrence: OneOrMore
Format: URI
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@src]

67.	Group: MMI Info	Mimetype

It defines the mimetype of the file; it depends on the target OS as defined in 6.5.

Name: type
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@type]

68.	Group: MMI Info	Target

It defines a subtag attribute that indicates the target OS or UICC platform for that content as defined in 17;

Name: target
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@gsma:target]

69.	Group: MMI Info	Package Name

It defines the package name of the Android application

Name: package-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@package-name]

70.	Group: MMI Info	Application Activity Class Name

It defines the full path class name of the Android application (used to launch the MMI)

Name: class-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@class-name]

71.	Group: MMI Info	Application Midlet Name

It defines the application midlet name for J2ME applet

Name: midlet-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@midlet-name]

72.	Group: MMI Info	Application Midlet Vendor Name

It defines the application midlet vendor name for J2ME applet

Name: vendor-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@vendor-name]

73.	Group: MMI Info	Application Content Handler To Invoke

It defines the application content handler to invoke for J2ME applet

Name: content-handler
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@content-handler]

74.	Group: MMI Info	Application Module Name

It defines the application module name for RIM application

Name: module-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@module-name]

75.	Group: MMI Info	Application Vendor Name

It defines the application vendor name for RIM application

Name: vendor-name
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@vendor-name]

76.	Group: MMI Info	Application GUID (productID)

It defines the application GUID (productID) for Windows 8

Name: ms-guid
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@ms-guid]

77.	Group: MMI Info	Compatibility UA

It defines a regular expressions as defined in [REG-EXP] to check the handset user agent against to declare compatibility of the MMI

Name: compatibility
Occurrence: One
Format: String
Context: Attribute of gsma:mmi\gsma:content
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi\gsma:content[@compatibility]

78.	Group: MMI Info	Device Application identifier

It defines the device application identifier as defined in [GP_MSG]

Name: device-application-identifier
Occurrence: ZeroOrOne
Format: String
Context: Attribute of gsma:mmi
Namespace: gsma
Localizable: false
MNO Specific: false
xPaths: gsma:mmi[@device-application-identifier]

79.	Group: MMI Info	Sha1
It defines a String attribute as hexadecimal String representing SHA1 of the certificate used to sign the SP-MMI		
Name: sha1 Occurrence: OneOrMore Format: SHA1 Context: Child of gsma:mmi Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:mmi\gsma:sha1		

80.	Group: MMI Info	Bind Applet Id
It defines ID of applet and ssd that need to be binded with this MMI. it refers to gsma:Applet[@id]; in some cases it may refer to gsma:ssd[@id] when allowed.		
Name: bind-applet Occurrence: ZeroOrMore Format: id Context: Child of gsma:mmi Namespace: gsma Localizable: false MNO Specific: false xPaths: gsma:mmi\gsma:bind-applet		

6.6. Formats

Formats	Description
AID	AID format as defined in [GP_MSG] A string attribute as hexadecimal string representing the long AID of the package. The length has be 10 up to 32: e.g. A001020304050607
Version	A version attribute using rec-version-tag grammar as described in [W3C_PC]
Id	An integer used to refer to an element within SP_CP manifest
String	A string
URI	A URI as defined in [RFC2396]
SHA1	A hex string of 12 character representing a SHA1 of a certificate as defined in [NFC_HANDS]
Mdap	An integer referencing the cardProfile (as defined in [GP_CARD]).

6.7. OS Platforms Subtag and Related Mimetype

OS Platforms Subtag	Mimetype	file extension
android	application/vnd.android.package-archive	Apk
android-<api_level>	application/vnd.android.package-archive	Apk

j2me	text/vnd.sun.j2me.app-descriptor application/java-archive	Jar
rim	text/vnd.sun.j2me.app-descriptor application/vnd.rim.cod	Cod

The GSMA anticipates this list will be extended in future in line with the evolution and support of mobile operating systems and platforms.

6.8. UICC Platforms Subtag and Related Mimetype

UICC Platforms Subtag	Mimetype	File Extension
all	application/java-archive	cap

The GSMA anticipates that this list will be enlarged in future in line with the evolution and support of UICC and platforms.

6.9. Role Attribute

In this chapter Role Attribute is define

6.9.1. Icons Role[7]

gsma:role	Dimensions	Description
launch	512 x 512 px	High resolution icon to be used to produce icons to launch the application
inactive	512 x 512 px	High resolution icon to be used to produce icons when corresponding applet is inactive
screenshot	320 x 480 px, 480 x 800 px, 1280 x 800, 1280 x 720	Screenshot of application
id-1	812 x 512 px	High resolution image targeting ISO/IEC 7810 ID-1 format

It should be noted that these icons may be drastically resized when shown on a CW user interface (e.g. 80x80 px) so they should be designed accordingly.

6.9.2. Other Media Role

gsma:role	Dimensions	Description
launch-small	64x64 px	Customized small icons that MAY be used by CW instead of resized high resolution icons
Inactive-small	64x64 px	
Video	Not defined	Promotional video
Promotional	Not defined	Promotional images

6.9.3. Url Role

gsma:role	Description
Install	URL to be open when a user requests activation of a certain NFC_service
Lock	URL to be open when a user requests lock of a certain NFC_service
Unlock	URL to be open when a user requests unlock for a certain NFC_service
Delete	URL to be open when a user requests deletion for a certain NFC_service
Maincontact	URI to the email and/or phone numbers of primary contact within SP
TSMURL	DNS Name end point of TSM SP as defined in [GP_MSG]
TSMheartbeat	DNS name heartbeat of TSM SP as defined in [GP_MSG]

It should be noted that site pointed by URL should be designed for mobile and portable devices..

6.10. Features definitions for future wallet extensions

As defined in [W3C_PC] feature element can be used to extend CW capabilities; example follows.

Features
<feature name=http://gsma.org/nfc/af/<ef name>" required=true|false>   <param name="<af_param1>" value="<value1>"/>   <param name="<af_param2>" value="<value2>"/> </feature> where: <af_paramX> are possible additional feature params

6.11. mWallet: Schema

A new URL schema is defined. The "*mwallet:*" URL scheme is used for requesting actions to the CW. As example, *mwallet:* schema can be used in following use case:

- Open CW from a native SP_MMI and/or native application
- Launch an SP_MMI from a native application
- Request installation (if not already installed) of an SP_MMI from a native application
- Share a certain SP_MMI by means of sending a URL *mwallet:* link through SMS or email between users (also with two different mobile operator subscriptions) - if the receiver doesn't have a wallet, the received link will have no effect or raise an error
- Open detail page of SP_MMI and related NFC_Services to show details and management page within the CW

Schema	Description
mwallet:	The URLs are of form: mwallet: <action>?param1 = value1&param2 = value2& … where *action* is the action to be performed The <param_> <value_> couples refer to parameters analogous to those used in http: https: URI

Action	Params	Description
Open	None	Used to open the CW: mwallet:open
Launch	id=<sp_mmi id>	Used to launch (or invite to download/install) a SP_MMI; in case of launch action, the id usually refers to a SP_MMI already locally installed; it should be noted, however, that if the SP_MMI is not already locally installed and the application handling the scheme is capable, <sp_mmi> may be used also to download the SP_MMI (and related SP_Applet) and then install and launch it. < sp_mmi id> is SP_MMI id.
Details	id=<sp_mmi id>	Open detail page of SP_MMI identified < sp_mmi id> is SP_MMI id.

It should be noted that, on some systems, schema handling can be subject to user choice and more than one program can be registered on that schema leading to a phishing attach. Proper security mechanisms for mutual authentication must be put in place.

6.11.1.   Examples (INFORMATIVE)

Some mwallet schema examples:

mwallet:launch?id= http%3a%2f%2faservice.aspprovider.com

mwallet:details?id=http%3a%2f%2faservice.aspprovider.com

mwallet:open

Annex A   SP_CP Examples (INFORMATIVE)

A.1   Examples of simple SP_CP structure and configuration file

In this chapter, an example of SP_CP package is shown where:

- The native SP_MMI resides in an external market (e.g. Android market)

```xml
<?xml version="1.0" encoding="UTF-8"?>
<widget xmlns="http://www.w3.org/ns/widgets"

xmlns:gsma="http://mcommerce.gsma.com/gsma/gsmaWidget"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://mcommerce.gsma.com/gsma/gsmaWidget
http://mcommerce.gsma.com/gsma/cp/xsd"

    id="id0"
    version="version0">


    <name>
        seek-for-android
    </name>

      <name xml:lang="es">
          seek-for-android
      </name>

    <author>
        http://groups.google.com/group/seek-for-android
    </author>
    <description>
        Secure Element Evaluation Kit for the Android platform - the
\"SmartCard API\"
    </description>

    <description xml:lang="es">
        Kit de Evaluación de Elemento Seguro para la plataforma Android.
    </description>

    <preference name="MNO-delete"       value= "no"/>
    <preference name="MNO-visibility"    value= "yes"/>
    <preference name="MNO-lock"          value= "yes"/>

    <license href="http://www.apache.org/licenses/LICENSE-2.0"> </license>

    <gsma:tsm-name>
        tsm1
    </gsma:tsm-name>


    <gsma:content role="main-contact"
      src="http://groups.google.com/group/seek-for-android"/>


    <gsma:icon role="launch" src="icons/icon-highres.png"/>
    <gsma:icon role="screenshot" src="icons/icon-screenshot.png"/>
```

```xml
    <gsma:icon role="screenshot" src="icons/icon-id.png"/>
    <gsma:icon role="id-1" src="icons/badge-image.png" />

    <gsma:gp-name>
        Foo-GP-NFC-Service
    </gsma:gp-name>


    <gsma:support-information>
        Open Hours: Mo-Fr 8:00-17:00, Sa 9:00-12:00
    </gsma:support-information>
    <gsma:support-information lang="es">
        Horario de atención al público: Lunes a viernes 8:00-17:00,
Sábados 9:00-12:00
    </gsma:support-information>


    <gsma:last-changes>
        v2.4.0
        -    GlobalPlatform ARA support
        -    ACA removed
        -    ICS (Android-4.0.3) reference
        -    compatible with SCAPI-2.3.2
        -    Issues.5/6/7/11/13/16/20/21/22/23/26 resolved
    </gsma:last-changes>
    <gsma:last-changes lang="es">
        v2.4.0
        -    Soporta ARA de GlobalPlatform
        -    ACA eliminado
        -    Plataforma de referencia ICS (Android-4.0.3)
        -    Compatible con SCAPI-2.3.2
        -    Resueltas incidencias 5/6/7/11/13/16/20/21/22/23/26
    </gsma:last-changes>

    <gsma:service-id mno="214-07">
        11
    </gsma:service-id>

    <gsma:exclusion-id mno="214-05">
        22
    </gsma:exclusion-id>

    <gsma:version>
        2.4.0
    </gsma:version>



    <gsma:ssd
        id="1"
        hierarchy=""
        aid="A001020304050607"
        privileges="2">

        <gsma:label>
            Oath ssd
        </gsma:label>

        <gsma:description>
```

```xml
            seek-for-android ssd
        </gsma:description>

        <gsma:instantiate-application-command
            gp-parameter-profile-id="1"
            gp-parameter-profile-id-default="1"
            privileges="0f0f0A"
            ef="5a448df"
            c9="6a048de"
            ea="5a4f4dc"/>
    </gsma:ssd>

    <gsma:applet
        id="1"
        version="1"
        aid="A221020305060609"
        ssd-parent-id="1"
        data-block-signature="90af46d675c013fce4555ccf567880eaab345c4"
        executable-module-aid="A001020309250607"
        type="member"
        install-size="10000"
        stk-tar="800002"
        instance-of="1" >

        <gsma:label>
            Oath
        </gsma:label>
        <gsma:label lang="es">
            Oath
        </gsma:label>
        <gsma:description>
            seek-for-android applet
        </gsma:description>
        <gsma:description lang="es">
            Applet de seek-for-android
        </gsma:description>

        <gsma:mdap card-profil-id="1"/>

        <gsma:instantiate-application-command
            gp-parameter-profile-id="1"
            gp-parameter-profile-id-default="1"
            privileges="0f0f0A"
            ef="5a448df"
            c9="6a048de"
            ea="5a4f4dc"/>

        <gsma:make-selectable-application-command
            gp-parameter-profile-id="1"
            gp-parameter-profile-id-default="1"
            privileges="0f0f0A"
            ef="E7" />
        <gsma:application-registry-update-command
            gp-parameter-profile-id="2"
            gp-parameter-profile-id-default="1"
            ef="E8"/>

    </gsma:applet>
```

```xml
<gsma:applet-package
    id="1"
    version="4"
    aid="A221020304090607"
    load-file-data-block-
hash="a0aaf9209098f46d675c013fc04555ccf567880eaab345c0666">
    <gsma:label lang="es">
        Oath
    </gsma:label>
    <gsma:description>
        seek-for-android package
    </gsma:description>

    <gsma:load-elf-command
        gp-parameter-profile-id="1"
        gp-parameter-profile-id-default="1"
        ef="5a448df"/>

    <gsma:content src="/oath.cap" type="application/java-archive"/>

</gsma:applet-package>

<gsma:mmi>
    <gsma:sha1>
        92f3d8bd1aaf9866191d5b2d4a7c0b4108dab8ec
    </gsma:sha1>
    <gsma:description>
        This sample application can be used to create OTPs for the 2-
step verification of your Google account
    </gsma:description>
    <gsma:description lang="es">
        Aplicación de ejemplo que puede usarse para crear OTPs para la
verificación en 2 pasos de su cuenta Google
    </gsma:description>

    <gsma:content
        version="0.2"

src="http://play.google.com/store/apps/details?id=com.gieseckedevrient.and
roid.googlemscauthenticator"
        type="application/vnd.android.package-archive"
        compatibility=".*Android \d{1,3}\.\d{1,3}\.\d{1,3}.*"
        package-
name="com.gieseckedevrient.android.googlemscauthenticator"
        class-
name="com.gieseckedevrient.android.googlemscauthenticator.MainActivity"
        target = "android" />

    <gsma:bind-applet>
        1
    </gsma:bind-applet>
</gsma:mmi>


</widget>
```
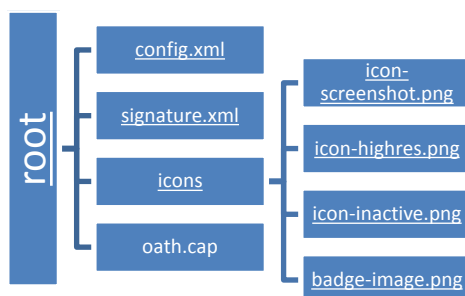
Figure 4: Example of SP_CP structure

A.2   Examples of SP_CP structure and configuration file for DM

In this chapter, an example of SP_CP package is shown where:

- The native SP_MMI resides in an external market (e.g. Android market)
- The service provider would like to use a trusted service manager in Delegate Mode so it is not going to provide an SP_Applet

```xml
<?xml version="1.0" encoding="UTF-8"?>
<widget xmlns="http://www.w3.org/ns/widgets"

xmlns:gsma="http://mcommerce.gsma.com/gsma/gsmaWidget"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://mcommerce.gsma.com/gsma/gsmaWidget
http://mcommerce.gsma.com/gsma/cp/xsd"

   id="id0"
   version="version0">

  <name>
        seek for android
    </name>
    <name lang="fr">
        seek pour android
    </name>

    <author>
         SP name
    </author>

  <description>
     First version
</description>
<description lang="fr">
     Première version
</description>

  <preference name="MNO-delete"        value= "no"/>
  <preference name="MNO-visibility"    value= "yes"/>
  <preference name="MNO-lock"            value= "yes"/>
```

```xml
    <gsma:tsm-name>
        tsm marker name for SP owner of this example
    </gsma:tsm-name>

      <gsma:content role="main-contact"    src="tel:+331234567890"/>


      <gsma:icon role="launch"            src="icons/icon-highres.png"/>
    <gsma:icon role="screenshot"     src="icons/icon-screenshot.png"/>
    <gsma:icon role="screenshot"     src="icons/icon-id.png"/>
    <gsma:icon role="id-1"                src="icons/badge-image.png" />
    <gsma:icon role="video"          src="http://foo-bar-
sp.org/exampleSP/avideo"/>

    <gsma:gp-name>
        SeekFA_GP_NFC_Service
    </gsma:gp-name>


    <gsma:last-changes>
        1.0.0: First version
        2.0.0: updated according to gsma definition
    </gsma:last-changes>
    <gsma:last-changes  lang="fr">
        1.0.0 : Première version
        2.0.0 : Mise à jour suivant les règles GSMA de définition de
service
    </gsma:last-changes>

    <gsma:service-id>
        12345
    </gsma:service-id>

    <gsma:exclusion-id>
        12346
    </gsma:exclusion-id>

  <gsma:version>
     2.0.0
  </gsma:version>

    <gsma:afi-keywords>20
    </gsma:afi-keywords>
    <!--
        SSD sections. 2 SSDs, father id=1 and son id=2 with multiple
possibilities of their install command as define in GP messaging by gsma.
    -->
    <gsma:ssd
        id="1"
        aid="d2760001180003ff4910008900000100" >
        <gsma:label>
        father ssd
    </gsma:label>

    <gsma:description>
        seek-for-android father SSD SCP80
    </gsma:description>

        <gsma:instantiate-application-command gp-parameter-profile-
```

```xml
                id="1" ef="" privileges="" c9="" ea="" gp-parameter-profile-id-
        default="true"/>
            </gsma:ssd>

            <gsma:ssd
                    id="2"
                    hierarchy="1"
                    aid="d2760001180003ff4910008900000101"
                    tar="000001" >
                    <gsma:label>
                    son ssd
              </gsma:label>

                <gsma:description>
                    seek-for-android son SSD SCP02 under father SSD SCP80
                </gsma:description>
                    <gsma:instantiate-application-command gp-parameter-profile-
        id="2" ef="" privileges="" c9="" ea="" gp-parameter-profile-id-
        default="true"/>
            </gsma:ssd>


            <!--
                    Applet instance section
            -->
            <gsma:applet
                    id="4"
                    instance-of="3"
                    ssd-parent-id="2"
                    executable-module-aid="A221020304050607"
                    aid="d2760001180003ff4910008980000201"
                    tar="800002"
                    type="head" >

                <gsma:label>
                    Oath instance 1
                </gsma:label>
                <gsma:label lang="fr">
                    Oath instance 1
                </gsma:label>
                <gsma:description>
                    seek-for-android applet instance 1
                </gsma:description>
                <gsma:description lang="fr">
                    Instance 1 de l'applet de seek-for-android
                </gsma:description>
                    <gsma:instantiate-application-command gp-parameters-profile-
        id="1" ef="" privileges="" c9="" ea="" gp-parameters-profile-id-
        default="true" />
                    <gsma:make-selectable-application-command gp-parameter-
        profile-id="1" ef="" privileges="" gp-parameter-profile-id-
        default="true"/>
                    <gsma:application-registry-update-command gp-parameter-
        profile-id="1" ef="" gp-parameter-profile-id-default="true"/>
            </gsma:applet>

            <gsma:applet
                    id="5"
                    instance-of="3"
```

```xml
                    ssd-parent-id="2"
                    executable-module-aid="A221020304050608"
                    aid="d2760001180003ff4910008980000202"
                    type="member" >
                 <gsma:label>
                     Oath instance 2
                 </gsma:label>
                 <gsma:label lang="fr">
                     Oath instance 2
                 </gsma:label>
                 <gsma:description>
                     seek-for-android applet instance 2
                 </gsma:description>
                 <gsma:description lang="fr">
                     Instance 2 de l'applet de seek-for-android
                 </gsma:description>
                 <gsma:instantiate-application-command gp-parameters-profile-
id="1" ef="" privileges="" c9="" ea="" gp-parameters-profile-id-
default="true"/>
                 <gsma:make-selectable-application-command gp-parameter-
profile-id="1" ef="" privileges="" gp-parameter-profile-id-
default="true"/>
                 <gsma:application-registry-update-command gp-parameter-
profile-id="1" ef="" gp-parameter-profile-id-default="true"/>

        </gsma:applet>


    <!--
            PACKAGE SECTION
        -->

    <gsma:applet-package
        id="3"
        aid="d2760001180003ff4910008900000200"
        version="1.0.0"
        ssd-parent-id="2"
        load-file-data-block-hash="01234358AFC55402398EFDDDBC1CA1"
        >

        <gsma:label>
            Oath package
        </gsma:label>
        <gsma:label lang="fr">
            Oath package
        </gsma:label>
        <gsma:description>
            seek-for-android applet package
        </gsma:description>
        <gsma:description lang="fr">
            Applet package de seek-for-android
        </gsma:description>

        <gsma:load-elf-command gp-parameter-profile-id="3" ef="" gp-
parameter-profile-id-default="true"/>

        <gsma:content src="" type="application/java-archive"/>
```

```xml
        <gsma:dap card-profile-id="162" gsma-mno="XXX-YY">
            0123345677565423484848539
        </gsma:dap>

        <gsma:mdap card-profile-id="168" gsma-mno="XXX-YY">
            01233456775654234848539346034239132832888757638204
        </gsma:mdap>


    </gsma:applet-package>

    <!--
        MMI section
    -->
    <gsma:mmi device-application-identifier="1">
        <gsma:sha1>92f3d8bd1aaf9866191d5b2d4a7c0b4108dab8ec
        </gsma:sha1>
        <gsma:label>
                    OTPAuthenticator
        </gsma:label>
        <gsma:label lang="fr">
                    OTPAuthenticator
        </gsma:label>

        <gsma:description>
                    This sample application can be used to create OTPs
for the 2-step verification of your OTP account
        </gsma:description>
        <gsma:description lang="fr">
                    une simple application ....
        </gsma:description>

        <gsma:content
            version="1.0.0"

    src="market://details?id=com.gieseckedevrient.android.googlemscauthe
nticator"
                type="application/vnd.android.package-archive"
                target="android"
                compatibility=".*Android 4.0.\d{1,3}.*"

                package-
name="com.gieseckedevrient.android.googlemscauthenticator"
                class-
name="com.gieseckedevrient.android.googlemscauthenticator.MainActivity"/>


        <gsma:bind-applet>
            2
        </gsma:bind-applet>
        <gsma:bind-applet>
            4
        </gsma:bind-applet>
        <gsma:bind-applet>
            5
        </gsma:bind-applet>
    </gsma:mmi>

    <gsma:mmi device-application-identifier="1">
```

```xml
            <gsma:sha1>92f3d8bd1aaf9866191d5b2d4a7c0b4108dab8ec
            </gsma:sha1>
            <gsma:label>
                        OTPAuthenticator
            </gsma:label>
            <gsma:label lang="fr">
                        OTPAuthenticator
            </gsma:label>

            <gsma:description>
                        This sample application can be used to create OTPs
for the 2-step verification of your account
            </gsma:description>
            <gsma:description lang="fr">
                        une simple application ....
            </gsma:description>

            <gsma:content
                version="1.0.0"

    src="market://details?id=com.gieseckedevrient.android.googlemscauthe
nticator"
                type="application/vnd.android.package-archive"
                target="android"
                compatibility=".*Android 4.1.\d{1,3}.*"
                package-
name="com.gieseckedevrient.android.googlemscauthenticator"
                class-
name="com.gieseckedevrient.android.googlemscauthenticator.MainActivity"/>


            <gsma:bind-applet>
                2
            </gsma:bind-applet>
            <gsma:bind-applet>
                4
            </gsma:bind-applet>
            <gsma:bind-applet>
                5
            </gsma:bind-applet>
    </gsma:mmi>

    <gsma:mmi device-application-identifier="1">
            <gsma:sha1>92f3d8bd1aaf9866191d5b2d4a7c0b4108dab8ec
            </gsma:sha1>
            <gsma:label>
                        OTPAuthenticator
            </gsma:label>
            <gsma:label lang="fr">
                        OTPAuthenticator
            </gsma:label>

            <gsma:description>
                        This sample application can be used to create OTPs
for the 2-step verification of your account
            </gsma:description>
            <gsma:description lang="fr">
                        une simple application ....
            </gsma:description>
```

```xml
        <gsma:content
                version="1.0.0"

    src="market://details?id=com.gieseckedevrient.android.googlemscauthe
nticator"
                type="application/vnd.android.package-archive"
                target="android"
                compatibility=".*Android 4.2.\d{1,3}.*"
                package-
name="com.gieseckedevrient.android.googlemscauthenticator"
                class-
name="com.gieseckedevrient.android.googlemscauthenticator.MainActivity"/>


        <gsma:bind-applet>
                2
        </gsma:bind-applet>
        <gsma:bind-applet>
                4
        </gsma:bind-applet>
        <gsma:bind-applet>
                5
        </gsma:bind-applet>
    </gsma:mmi>



</widget>
```
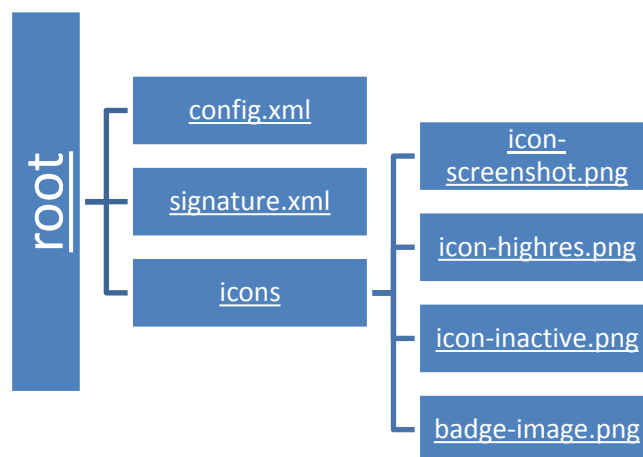

Figure 5: Example of SP_CP structure for application residing in an external market without applet

Annex B   Authors

This document defines the mobile wallet requirements necessary to deliver NFC Secure Services, and has been jointly developed by France Télécom, Telefónica, Telecom Italia, Deutsche Telekom and Vodafone. This specification will be shared with other operators, device manufacturers, and with service providers and third party developers.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	03 October 2012	Technical (Industry) Proposal submitted to DAG and PSMC for 7 day Committee Email approval	NFC, PSMC	Fabio Ricciato, Telecom Italia
2.0	15 August 2013	Technical Candidate Specification submitted to DAG and PSMC for approval	NFC, PSMC	GSMA NFC Fast Track Project, Fabio Ricciato Telecom Italia

Other Information

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.