Mobile Codes

Candidate Version 1.0 – 30 November 2010

Open Mobile Alliance

OMA-TS-MC-V1_0-20101130-C

Contents

Figures

Tables

1. Scope

Mobile Codes EnablerThis document provides the Technical Specification of the Mobile Codes Enabler to fulfill the requirements outlined in the Mobile Codes Requirements document [MC-RD] for Mobile Codes V1.0 and in compliance to the architecture described in Mobile Codes Architecture document [MC-AD]. The Technical Specification provides the definition of data elements of the Mobile Codes Enabler and the description of the procedures/behaviour for the features supported by the Mobile Codes Enabler.

2. References

2.1 Normative References

[DATAMATRIX] "Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification", ISO/IEC 16022:2006, URL: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44230

[ISO3166-1] "Codes for the representation of names of countries and their subdivisions – Part 1: Country codes", ISO 3166-1:2006, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719

[ISO8601] "Data elements and interchange formats -- Information interchange -- Representation of dates and times", ISO 8601:2004, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874

[MC-AD] "Mobile Codes Architecture", Version 1.0, Open Mobile Alliance™, OMA-AD-MC-V1_0, URL:http://www.openmobilealliance.org/

[MC-RD] "Mobile Codes Requirements", Version 1.0, Open Mobile Alliance™, OMA-RD-MC-V1_0, URL:http://www.openmobilealliance.org/

[QR] "Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification", ISO/IEC 18004:2006, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43655

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2616] "Hypertext Transfer Protocol -- HTTP/1.1", R. Fielding et. al, June 1999, URL:http://www.ietf.org/rfc/rfc2616.txt

[RFC2822] "Internet Message Format", P. Resnick, April 2001, URL: http://www.ietf.org/rfc/rfc2822.txt

[RFC3966] "The tel URI for Telephone Numbers", H. Schulzrinne, December 2004, URL: http://www.ietf.org/rfc/rfc3966.txt

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[VCARD2.1] "vCard The Electronic Business Card Version 2.1", A versit Consortium Specification, September 18, 1996, URL: http://www.imc.org/pdi/vcard-21.doc

2.2 Informative References

[EAN/UPC] "Information technology — Automatic identification and data capture techniques — EAN/UPC bar code symbology specification", ISO/IEC 15420:2009, URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46143

[ISO/IEC 15415] Information technology -- Automatic identification and data capture techniques -- Bar code print quality test specification -- Two-dimensional symbols, URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=27658

[ISO/IEC 8859-1] Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1, URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=28245

[ISO 8995-1] Lighting of work places -- Part 1: Indoor, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=28857

[JIS X 0201] 7-bit and 8-bit coded character sets for information interchange, URL: http://www.webstore.jsa.or.jp/webstore/Com/FlowControl.jsp?bunsyoId=JIS+X+0201%3A1997&dantaiCd=JIS&status=1&pageNo=3&lang=en

[JIS X 0208] 7-bit and 8-bit double byte coded KANJI sets for information interchange, URL: http://www.webstore.jsa.or.jp/webstore/Com/FlowControl.jsp?lang=en&bunsyoId=JIS+X+0208%3A1997&dantaiCd=JIS&status=1&pageNo=0

[JIS X 0510] Two dimensional symbol – QR Code – Basic specification, URL: http://www.webstore.jsa.or.jp/webstore/Com/FlowControl.jsp?lang=en&bunsyoId=JIS+X+0510%3A2004&dantaiCd=JIS&status=1&pageNo=0

[NTTDOCOMOGUIDE] "Rough Measures and criteria for creating QR codes compatible with all terminals", NTT DoCoMo, URL: http://www.nttdocomo.co.jp/english/service/imode/make/content/barcode/about/#p02

[NTTDOCOMOFUNC] "Outline of Functions", NTT DoCoMo, URL: http://www.nttdocomo.co.jp/english/service/imode/make/content/barcode/function/

[OMADICT] "Dictionary for OMA Specifications", Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, URL:http://www.openmobilealliance.org/

[OMAURI] "URI Schemes for the Mobile Applications Environment", Version 1.0, Open Mobile Alliance™, OMA-TS-URI_Schemes-V1_0-20080626-A, URL:http://www.openmobilealliance.org/

[REST] "Architectural Styles and the Design of Network-based Software Architectures", Roy Fielding, 2000, URL: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

[RFC2104] "HMAC: Keyed-Hashing for Message Authentication", H. Krawxzyk et. al, February 1997, URL:http://www.ietf.org/rfc/rfc2104.txt

[RFC4868] "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", S. Kelly et. al, May 2007, URL:http://www.ietf.org/rfc/rfc4868.txt

[URI] "RFC 3986. Uniform Resource Identifier (URI): Generic Syntax", IETF, URL: http://www.ietf.org/rfc/rfc3986.txt

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Code Clearing House function	The process of Indirect Code routing based on the Indirect Code Identifier, through which: a) the Resolving CMP is determined, and b) the Indirect Code Identifier is forwarded to the Resolving CMP.
Code Management Platform	The Code Management Platform provides a resolution service pertaining to Indirect Codes; it is normally capable of performing both the Code Clearing House (CCH) function and Code Resolution (CR) and may also interact with other Code Management Platforms, as required. In certain deployment scenarios, the CCH function and the CR function may be implemented in two separate Code Management platforms. (See Split-CMP-Parent and Split-CMP-Child).
Code Marker	A marker consisting of an octet %x03, a text string “OMA” and %x20 that is placed in the beginning of Data String to explicitly specify the Mobile Code as an Indirect Code.
Code Resolution (or Code Resolution function)	The process of mapping a Direct Code or an Indirect Code into either content to be consumed directly by the device, or the address of content (or a service) to be accessed by the device. Typically, Code Resolution for Indirect Codes requires access to network service..
Code Transfer	The ability for a Mobile Code Publisher to change the Resolving CMP for a single or multiple Indirect Code Identifiers.
Data String	Data that represent a Direct Code or an Indirect Code. A Data String is encoded by a Symbology to yield a Mobile Code.
Direct Code	A Mobile Code that contains either (a) content for direct consumption for the device, or (b) the address of the service to be accessed (typically a URI [URI]).
Direct MC Format	A generic common data format to specify data formats for Direct Codes for the OMA MC enabler. It is defined by ABNF notations in 7.1.2.1.
Home CMP	The CMP to which a particular MCC is configured to send all Code Resolution requests. Where applicable in a Split-CMP deployment scenario, the Home CMP may be a Split-CMP-Parent.
Indirect Code	A Mobile Code that contains an Indirect Code Identifier.
Indirect Code Identifier	An identifier in the Indirect Code that has to be resolved in order to access the intended content or service. See also Code Resolution.
Mailbox	A Mailbox is a conceptual entity which receives mail (as defined by Section 3.4 of [RFC2822] with further clarifications that are specified in this specification.). Normally, a Mailbox is comprised of two parts: (1) an optional display name that indicates the name of the recipient that could be displayed to the user of a mail application, and (2) an addr-spec address enclosed in angle brackets ("<" and ">"). There is also an alternate simple form of a Mailbox where the addr-spec address appears alone, without the recipient's name or the angle brackets.
Mobile Code	A 1D or 2D barcode as read by camera-equipped devices
Mobile Code Client	The MC Enabler software entity that resides in the device, and contains the functionality to acquire, decode, and extract the encoded information for further processing as required. This is often referred to as a Mobile Code Reader and these terms can be used synonymously.
Mobile Code Data Format	The syntactical description of the information contained within a Mobile Code.
Mobile Code Publisher	This is a brand (business, organisation or individual) who distributes certain content or services (e.g. an advertising campaign) to a mass audience by using Mobile Code scanning as a channel.
Mobile Code Registry	A local registry responsible for sub-allocation of Mobile Code Routing Prefixes within the ranges of

	Routing Prefixes obtained from OMNA. The Mobile Code Registry (MCR) also supports a data look-up facility accessible by authorised principals (e.g. CMPs or Split-CMP-Parents) for Routing Prefixes in its database.
Mobile Code Service Policy	A set of Policy Conditions [OMADICT] that convey any service level constraints that are placed on Code Resolution. Mobile Code Service Policy is typically defined by the Mobile Code Publisher and is applicable to one or more Indirect Code Identifiers.
Multi-lateral Arrangement	An arrangement amongst specific CMPs (including Split-CMP-Parents, where applicable) that are not associated with any Mobile Code Registry, in which the parties agreed to support each other in a multi-lateral way in order to manage sub-allocation of MC Routing Prefixes as well as discovery and updates thereof; details of such MLAs are not specified in the MC Enabler TS.
Quiet Zone	A Quiet Zone is a region which shall be free of all other markings, surrounding the symbol on all four sides. For QR Code symbols and for dark on light Data Matrix symbols its nominal reflectance value shall be equal to that of the light modules. For reflectance reversed (light on dark) Data Matrix symbols its nominal reflectance value shall be equal to that of the dark modules.
Recognizable Format	A data format that is included in a Direct Code and is recognised by the MCC, to enable causing certain actions, such as displaying the recognition results to the user along with the messages if any, offering options for the user to select, and/or invoking an application.
Registry-ID Recipient	An entity that is qualified to apply for and receive an OMNA Registry-ID assignment. This entity can be an MCR or another qualified entity (e.g. a designated entity within an MLA).
Remote CMP	The CMP that receives a Code Resolution request when the Home CMP (or Split-CMP-Parent, where applicable) is unable to resolve a particular Indirect Code Identifier.
Resolution Identifier	That part of the Indirect Code Identifier that is used to index the content or service.
Resolving CMP	The CMP (or Split-CMP-Child, where applicable) that is able to resolve a particular Indirect Code Identifier.
Routing Prefix	That part of the Indirect Code Identifier that contains a value that is uniquely assigned to the CMP (Split-CMP-Child, as applicable) and is used for routing.
Split-CMP-Child	A CMP in the Split-CMP deployment scenario, where only the Code Resolution function is implemented. In addition, subject to business relationship, a Split-CMP-Child may be associated with one and only one Split-CMP-Parent.
Split-CMP-Parent	A CMP in the Split-CMP deployment scenario, where only the Code Clearing House function is implemented. In addition, subject to business relationship, a Split-CMP-Parent may be associated with multiple Split-CMP-Children.
Symbology	The algorithm by which data is encoded as visual elements (typically arrangements of lines or squares), and the resultant “look and feel” for the user.
Telephone-Number-String	A Telephone-Number-String is a string of characters to represent a telephone number to human. It consists of phone digits, “+”, ”*”, and “#”. It may contain visual separators that are commonly used in various places in the world. It is defined in Section 7.2.2.1.

3.3 Abbreviations

1D	1-Dimensional
2D	2-Dimensional
ABNF	Augmented BNF for Syntax Specifications
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CCH	Code Clearing House
CMP	Code Management Platform
DM	Device Management
CR	Code Resolution
CR	Carriage Return

CRI	Calculated Resolution Identifier
DMF	Direct MC Format
DNS	Domain Name System
EAN	European Article Number, see EAN/UPC
EAN/UPC	Barcode symbology family including EAN-8, EAN-13, UPC-A, and UPC-E [EAN/UPC]
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
ERI	Encrypted Resolution Identifier
ERIH	Encrypted Resolution Identifier Hash
ERX	Encrypted Resolution Identifier Part Index
HMAC	Hash-based Message Authentication Code
ID	Identifier
IOP	Interoperability
HTTP	Hypertext Transfer Protocol
ICI	Indirect Code Identifier
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JIS	Japanese Industrial Standards
LF	Line Feed
MC	Mobile Code
MCC	Mobile Code Client
MCCSDCD	Minimum Conformance Characters Set for Direct Code Display
MCR	Mobile Code Registry
MLA	Multi-lateral Arrangement
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
QR	Quick Response, a type of barcode symbology [QR]
REST	Representational State Transfer
RI	Resolution Identifier
RP	Resolution Prefix
RSA	Rivest, Shamir and Adleman
SMS	Short Message Service
TS	Technical Specification
UPC	Universal Product Code, see EAN/UPC
URI	Uniform Resource Identifier [URI]
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
XML	Extensible Markup Language

4. Introduction (Informative)

Mobile codes – 2D and 1D barcodes – have emerged as a promising enabler of the mobile Internet in some markets. Camera-equipped devices now have good enough optics, image resolution and processing capacity to read mobile codes on printed materials and electronic displays. These symbols encode information such as URLs, phone numbers, and in-line content such as business cards.

There is, however, still a lack of interoperability between different markets and players. The majority of consumers are unlikely to adopt the technology before it comes pre-installed on their devices. Similarly, marketing, publishing and other industries that are otherwise motivated to provide mobile codes will not adopt them without adequate potential for consumer take-up. That in turn would entail deployment on a large variety of devices, and interoperability between different service providers.

Example			
Symbology	QR [QR]	Data Matrix [DATAMATRIX]	EAN-13 [EAN/UPC]
Data	http://www.openmobilealliance.org	http://www.openmobilealliance.org	5901234123457

4.1 Version 1.0

The Mobile Codes Enabler contains support for a full ecosystem for both Direct and Indirect Codes.

Technology, interface behavior and procedures for interoperability (some of which are optional) are specified for:

- Symbology(s)
- Mobile Code Data Format
- Direct encoding of content or address of content or service
- Encoding of Indirect Code Identifiers
- Resolution of Indirect Code Identifiers
- Security
- Tracking and Reporting of Mobile Code usage
- Transfer of Indirect Code Identifiers

4.2 Version 2.0

Future versions of the Mobile Codes Enabler may add enhancements as required.

5. Symbologies

5.1 Mandated 2D Standard Symbologies

A 2D Symbology or two-dimensional bar code frequently appears square in shape and contains data which is read both horizontally and vertically by the scanner. It is a two-dimensional way of representing information. The mandated 2D standardised bar code symbologies have the capacity to encode both direct and indirect code formats.

The MCC SHALL support both QR Code [QR] and Data Matrix [DATAMATRIX].

These two standard bar code symbologies provide a good basis for global interoperability and represent the majority of the mobile code symbologies used in the world today. Both the QR Code and Data Matrix are ISO standards.

5.1.1 QR Code Support

The MCC SHALL support QR Code as defined in ISO/IEC 18004:2006 [QR], with the following clarifications in order to ensure interoperability.

5.1.1.1 Model

The MCC SHALL support QR Code Model 2.

5.1.1.2 Versions

The MCC SHALL support Versions 1 to 10.

The MCC MAY support Versions 11 or higher.

5.1.1.3 Error Correction Levels

QR Code 2005, which is the basis of the specification [QR] that is normatively referenced in this specification, employs Reed-Solomon error control coding to detect and correct errors. For QR Code there are four user-selectable levels of error correction, i.e., L, M, Q and H, offering the capability of recovery from the following amounts of damage, i.e., 7%, 15%, 25% and 30%, respectively.

The MCC SHALL support Error Correction Levels, L, M, Q and H, for all the mandatory Versions (i.e., Versions 1 to 10).

5.1.1.4 Modes

The MCC SHALL support the following Modes:

- Numeric mode,
- Alphanumeric mode,
- Byte mode, and
- Kanji mode.

The MCC SHALL support any combination of the above modes.

5.1.1.5 Character Set for Direct Code Display

In Byte mode, data is encoded at 8 bits per character. As defined in ISO/IEC 18004:2006 [QR], the default character set for Byte mode is ISO/IEC 8859-1 [ISO/IEC 8859-1]. ISO/IEC 8859-1 is one of the families of various 8-bit single-byte coded graphic character sets that are standardised in the world, e.g., ISO/IEC 8859-2 to 8859-16, or JIS X 0201 [JIS X 0201] (for Japan). The lower 7 bit code spaces of these families share almost the same characters as those of ASCII Code, while higher bits define characters for different languages respectively.

For Direct Code that is intended to be displayed, the data that is encoded in Byte mode is displayed to the users using one of the character sets that are supported by the device if appropriate character set is available. It is not possible for OMA to specify all the character sets for all the languages that may be used in the world. Therefore, the following printable ASCII characters are defined as the Minimum Conformance Characters Set for Direct Code Display, MCCSDCD, for the default Byte mode when it is used for Direct Code.

MCCSDCD = %x20-7E / %x0D / %x0A ; all ASCII printable characters, CR and LF.

Whenever conformance to this specification is tested or elaborated for displaying the data of Direct Code from Byte mode, e.g., IOP testing, MCCSDCD SHALL be used. Note that there are a few well-known exceptions even in this range. For example, the display glyphs of 0x5C (back slash) and 0x7F (tilde) in JIS X 0201 are different from those of ASCII.

Any character set may be used in Byte mode, depending on the country or market. When an alternative character set is specified, however, the parties intending to read the QR Code symbols require to be notified of the applicable character set in the application specification or by bilateral agreement. Appendix C summarises some best practices in the industry for the character sets that are used for Direct Code.

5.1.1.6 Quiet Zone

- The MCC SHALL be able to read a QR Code symbol with a Quiet Zone that is equal to or larger than 4X wide on all four sides, where the X dimension is the width of a module.
- The MCC SHOULD be able to read a QR Code symbol with a Quiet Zone that is equal to 3X wide on all four sides.

The ISO standard [QR] mandates the minimum 4X Quiet Zone to be read. This specification mandates the same 4X Quiet Zone. In order to ensure readability of actual printed QR Code symbols, however, the 3X recommendation is added in order for the MCC to have an extra margin to cope with such problems as misalignment, etc. that may arise in physical printing.

This specification does not specify the actual X dimension since it has impact on the design of the scanning technology such as cameras, lenses and optics that are used in devices, which is out of the scope of this specification. However, Appendix E provides informative recommendations for the module width X dimension in order to increase compatibility between the printed QR code symbols and the devices that implements the OMA MCC. Appendix E also provides informative recommendations that are essential in order to make code reading successful.

5.1.1.7 Structured Append mode

Structured Append mode that is supported by QR Code is used to split the encoding of the data from a message over a number of QR Code symbols. All of the symbols require to be read and the data message can be reconstructed in the correct sequence.

The MCC SHALL support Structured Append mode to enable up to 16 QR Code symbols to be concatenated.

As the Structured Append mode requires the user to capture a multiple number of QR Code symbols, the MCC needs to implement a mechanism to enable the user to capture the complete set of symbols. An example of capturing a multiple number of QR Code symbols in the Structured Append mode is described in Appendix F.

The MCC SHALL support a mechanism that allows the user to exit from the process of capturing multiple QR Code symbols wherever and whenever the user may be in the process of capturing these symbols if the user wishes to do so.

5.1.1.8 QR Code terminology

The following list shows terminologies that are used for QR Code:

Alphanumeric mode	One of the modes that is supported by QR Code. It encodes data from a set of 45 characters, i.e. 10 numeric digits (0 - 9) (byte values %x30 to %x39), 26 alphabetic characters (A - Z) (byte values %x41 to %x5A), and 9 symbols (SP, $, %, *, +, -, ., /, :) (byte values %x20, %x24, %x25, %x2A, %x2B, 2D to %2F, %x3A respectively). Normally, two input characters are represented by 11 bits.
Byte mode	One of the modes that is supported by QR Code. In this mode, data is encoded at 8 bits per character. Corresponds to the term "Base 256" within the context of Data Matrix.
Kanji mode	One of the modes that is supported by QR Code. The Kanji mode efficiently encodes Kanji characters in accordance with the Shift JIS system based on JIS X 0208.
Mode	Method of representing a defined character set as a bit string that is used to encode the character string into a QR Code symbol. Corresponds to the term "Encodation Scheme" within the context of Data Matrix.
Model	QR Code family contains four different technologies, i.e., QR Code Model 1, QR Code Model 2, QR Code 2005, and the Micro QR Code format. QR Code Model 2 symbols are fully compatible with QR Code 2005 reading systems.
Numeric mode	One of the modes that is supported by QR Code. It encodes data from the decimal digit set (0 – 9) (byte values %x30 to %x39). Normally, 3 data characters are represented by 10 bits.
Version	Size of the QR Code symbol represented in terms of its position in the sequence of permissible sizes. QR Code 2005 defines 40 Versions (1 to 40) among others. For QR Code symbols, the sizes are from 21 × 21 modules (Version 1) to 177 × 177 (Version 40) modules.

5.1.2 Data Matrix Support

The MCC SHALL support Data Matrix as defined in ISO/IEC 16022:2000 [DATAMATRIX], with the clarifications below to ensure interoperability.

5.1.2.1 Type of Data Matrix

The MCC SHALL support Data Matrix type ECC 200.

5.1.2.2 Data Matrix symbol sizes

Data Matrix ECC 200 supports square symbols of several sizes ranging from 10x10 modules up to 144x144 modules as well as non-square rectangular shaped symbols of six different sizes.

The MCC SHALL support Data Matrix symbol sizes up to 52x52 modules, including the 6 rectangular symbols. Specifically these are the ECC 200 symbols of sizes 10x10, 12x12, 14x14, 16x16, 18x18, 20x20, 22x22, 24x24, 26x26, 32x32, 36x36, 40x40, 44x44, 48x48, 52x52, 8x18, 8x32, 12x26, 12x36, 16x36, 16x48.

The MCC MAY support Data Matrix ECC 200 symbol sizes of 64x64 or larger.

5.1.2.3 Encodation Schemes

The MCC SHALL support the following Encodation Schemes:

- ASCII
- C 40
- Text
- X12
- EDIFACT
- Base 256.

The MCC SHALL support any combination of the above encodation schemes.

5.1.2.4 Quiet Zone

- The MCC SHALL be able to read a Data Matrix symbol with a Quiet Zone that is equal to or larger than 1X wide on all four sides, where the X dimension is the width of a module.

The ISO standard [DATAMATRIX] mandates the minimum 1X Quiet Zone to be read. This specification mandates the same 1X Quiet Zone.

This specification does not specify the actual X dimension since it has impact on the design of the scanning technology such as cameras, lenses and optics that are used in devices, which is out of the scope of this specification. However, Appendix E provides informative recommendations for the module width X dimension in order to increase compatibility between the printed Data Matrix symbols and the devices that implements the OMA MCC. Appendix E also provides informative recommendations that are essential in order to make code reading successful.

5.1.2.5 Structured Append Mode

Structured Append mode that is supported by Data Matrix is used to split the encoding of the data from a message over a number of Data Matrix symbols. All of the symbols require to be read and the data message can be reconstructed in the correct sequence.

The MCC SHALL support Structured Append to enable up to 16 Data Matrix symbols to be concatenated.

As the Structured Append mode requires the user to capture a multiple number of Data Matrix symbols, the MCC needs to implement a mechanism to enable the user to capture the complete set of symbols. An example of capturing a multiple number of Data Matrix symbols in the Structured Append mode is described in Appendix F.

The MCC SHALL support a mechanism that allows the user to exit from the process of capturing multiple Data Matrix symbols, wherever and whenever the user may be in the process of capturing these symbols if the user wishes to do so.

5.1.2.6 Data Matrix terminology

The following list shows terminologies that are used for Data Matrix:

ASCII encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. In this scheme, double digit numerics are encoded at 4 bits per character digit, ASCII values 0-127 are encoded at 8 bits per character, and extended ASCII values 128-255 are encoded at 16 bits per character.
Base 256 encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. In this scheme, data is encoded at 8 bits per character. Corresponds to the term “Byte mode” within the context of QR code.
C 40 encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. It encodes data from a set of 37 characters in a Basic Set, i.e. 10 numeric digits (0 - 9) (byte values 48 to 57), the SPACE symbol (byte value 32) and 26 uppercase alphabetic characters (A - Z) (byte values 65 to 90), and it encodes the remaining data values from the range (0-127) in a Shifted Set. Three characters belonging to the Basic Set are represented by 16 bits.
EDIFACT encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. It encodes 63 ASCII values (byte values 32 to 94). Four characters are represented by 24 bits.
Encodation Scheme	Method of representing a defined character set as a bit string that is used to encode the character string into a Data Matrix symbol. Corresponds to the term “Mode” within the context of QR Code.
Text encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. It encodes data from a set of 37 characters in a Basic Set, i.e. 10 numeric digits (0 - 9) (byte values 48 to 57), the SPACE symbol (byte value 32) and 26 lowercase alphabetic characters (a - z) (byte values 97 to 122), and it encodes the remaining data values from the range (0-127) in a Shifted Set. Three characters belonging to the Basic Set are represented by 16 bits.
X12 encodation	One of the encodation schemes that is supported by Data Matrix ECC 200. It encodes data from the standard ANSI X12 electronic data interchange characters, i.e. 10 numeric digits (0 - 9) (byte values 48 to 57), the SPACE symbol (byte value 32), the three standard ANSI X12 terminator and separator characters (having byte values 13, 42, 62) and 26 uppercase alphabetic characters (A - Z) (byte values 65 to 90). Three characters are represented by 16 bits.

5.1.3 Character Set for Direct Code Display

(1) QR Code

In Byte mode, data is encoded at 8 bits per character. As defined in ISO/IEC 18004:2006 [QR], the default character set for Byte mode is ISO/IEC 8859-1 [ISO/IEC 8859-1]. This default character set may be overridden by the MCC configuration (e.g., see Appendix C for details).

(2) Data Matrix

As defined in ISO/IEC 16022:2000 [DATAMATRIX], the default character interpretation for character values 0 to 127 shall conform to ANSI X3.4. The default character interpretation for character values 128 to 255 shall conform to ISO/IEC 8859-1: Latin Alphabet No. 1. [ISO/IEC 8859-1]. This default character set may be overridden by the MCC configuration.

ISO/IEC 8859-1 is one of the families of various 8-bit single-byte coded graphic character sets that are standardised in the world, e.g., ISO/IEC 8859-2 to 8859-16, or JIS X 0201 (for Japan). The lower 7 bit code spaces of these families share almost the same characters as those of ASCII Code, while higher bits define characters for different languages respectively.

For Direct Code that is intended to be displayed, the data is displayed to the users using one of the character sets that are supported by the device if appropriate character set is available. It is not possible for OMA to specify all the character sets for all the languages that may be used in the world. Therefore, the following printable ASCII characters are defined as the Minimum Conformance Characters Set for Direct Code Display, MCCSDCD, for the default Byte mode when it is used for Direct Code.

MCCSDCD = %x20-7E / %x0D / %x0A ; all ASCII printable characters, CR and LF.

Whenever conformance to this specification is tested or elaborated for displaying the data of Direct Code, e.g., IOP testing, MCCSDCD SHALL be used. Note that there are a few well-known exceptions even in this range. For example, the display glyphs of 0x5C (back slash) and 0x7F (tilde) in JIS X 0201 are different from those of ASCII.

Any character set may be used, depending on the country or market. When an alternative character set is specified, however, the parties intending to read the QR Code or the Data Matrix symbols require to be notified of the applicable character set in the application specification or by bilateral agreement. Appendix-A summarises some of the best practices of the industry for the character sets that are used for Direct Code.

6. Mobile Code Differentiation

Both Direct Code and Indirect Code are addressed in this specification; thus there is a need to explicitly mark the Mobile Code so that the Mobile Code Client can handle each type accordingly.

6.1 OMA Mobile Code Header Format

OMA Mobile Code Enabler supports both Direct and Indirect Codes. The MCC decodes the Symbology of a Mobile Code to extract a Data String. A Data String contains data and/or data formats of either a Direct Code or an Indirect Code, of which details are specified in Section 7 and 8, respectively.

In order to differentiate between a Direct Code and an Indirect Code, a Code-Marker is placed at the beginning of a Data String for an Indirect Code to explicitly specify the Mobile Code as an Indirect Code. Lack of a Code-Marker at the beginning of a Data String specifies the Mobile Code as a Direct Code. A Code-Marker is defined in the ABNF notation as follows:

Code-Marker = %x03 "OMA" %x20 ; ABNF strings are case-insensitive.

The length of a Code Marker is fixed. A Code-Marker consists of two parts; i) an octet %x03 for the MCC to use as a part of the key to distinguish an Indirect Code from a Direct Code, and ii) a human readable string, "OMA". The string is for those who attempt to read OMA Indirect Codes using mobile code clients that do not support the OMA MC Enabler, e.g., conventional direct code devices. The string combined with %x03 is used as the key to distinguish an Indirect Code from any other data. Note that the string is case-insensitive.

- The MCC SHALL recognise a Mobile Code as an Indirect Code if the Data String starts with the Code-Marker.
- The MCC SHALL recognise a Mobile Code as a Direct Code if the Data String does not start with the Code-Marker.

7. Direct Mobile Code Resolution

7.1 Plain Text in Direct Code and the Structure

A plain text refers to any string of characters that consists entirely of printable characters (i.e., human-readable characters) and, optionally, a very few specific types of control characters (e.g., characters indicating carriage returns and line feeds).

A Data String for a Direct Code contains human readable plain text messages and data formats that are specified by this specification and are recognised by the MCC. Such a data format is defined as a Recognizable Format.

A Data String for a Direct Code may contain any number of plain text messages and Recognizable Formats that are discussed in Section 7.1.1. The plain text messages and Recognizable Formats may appear in a Data String of a Direct Code in any order or in any number of occurrences within the physical limitation of the mobile code. The MCC recognises the Recognizable Formats, leading to enable causing certain actions, while the MCC only presents the plain text messages to the user as they are written.

A Data String for a Direct Code may contain unprintable-control-characters.

The MCC SHALL display the plain text messages and the actionable images of Recognizable Formats, which are specified in each Recognizable Format section, in the order they are embedded in the Data String.

The MCC SHALL replace an unprintable-control-character by an appropriate printable character, e.g., a white space %x20, if it appears anywhere outside of the Recognizable Formats. How to handle the unprintable-control-characters is specified in each Recognizable Format.

unprintable-control-character = %x00-09 / %x0B-0C / %x0E-1F / %x7F

How to handle displaying characters of such character sets that are not supported by the device is subject to the implementation.

7.1.1 Recognizable Formats

The Recognizable Formats include: i) existing standard formats and standard schemes such as http: [OMAURI] that are referenced and specified further in this specification, and ii) the data formats that are specified for the Direct Code within this specification. To specify the latter, a generic common format, the Direct MC Format (DMF) that is defined in the next section, is used. Table 1 lists all the Recognizable Formats. The details of the Recognizable Formats are specified in the subsequent sections in this specification.

7.1.2 Direct MC Format (DMF)

This specification uses a generic common format, Direct MC Format (DMF), to specify Recognizable Formats, where standard formats or schemes are not available or suitable for the use of Direct Codes. Direct Codes typically have capacity limits for the amount of information to be embedded, due to performances of optics and cameras of various mobile devices, and/or limitations from printing requirements relative to the physical appearances. The DMF is an efficient, flexible and generic common format suitable for defining Recognizable Formats for the Direct Code.

7.1.2.1 DMF Definition

The generic format of the DMF is defined by using the ABNF (augmented Backus-Naur form) described in RFC 4234 [RFC4234]. The DMF enables defining various data formats with printable characters as well as with binary data.

The DMF is identified by Identifier followed by ":", and is a collection of Properties. The DMF terminates with a ";" at the end of the format. The DMF allows for specifying a Recognizable Format without a single Property.

Each Property contains a Property-Name and, one or more Property-Values. Properties are delimited by a “;”. When there are multiple Property-Values, each of those values SHALL be delimited by a ",'.

Property-Values SHALL be escaped according to the rule defined in 7.1.2.2.

When binary data is encoded, the type of the content, e.g., jpeg, gif, and the length of the binary data must be included in the Recognizable Format. The “Length”, must be equal to the actual length of the binary data.

The generic DMF in the ABNF notation is defined as follows:

DMF-DATA = Identifier ":" *Property / Binary-Data-Object ";"

Identifier = 1*(ALPHA / DIGIT / “-“)

Property = Property-Name ":" Property-Value *("," Property-Value) ";"

Property-Name = 1* (ALPHA / DIGIT / “-“)

Property-Value = *(printable-ASCII-character/ ISO8Bit/ ShiftJISChar / UTF8-char))

Printable-ASCII-character = %x20-2B / %x2D-39 / %3C-%x5B / %x5D-7E / CRLF

ISO8Bit = %x80-FF

ShiftJISChar = (%x81-9F / %xE0-FC) (%x40-7E / %x80-FC) ; Shift JIS char

UTF8-char = UTF8-2 / UTF8-3 / UTF8-4 ; UTF8-1 is deleted

UTF8-2 = %xC2-DF UTF8-tail

UTF8-3 = %xE0 %xA0-BF UTF8-tail / %xE1-EC 2(UTF8-tail) / %xED %x80-9F UTF8-tail / %xEE-EF 2(UTF8-tail)

UTF8-4 = %xF0 %x90-BF 2(UTF8-tail) / %xF1-F3 3(UTF8-tail) / %xF4 %x80-8F 2(UTF8-tail)

UTF8-tail = %x80-BF

Binary-Data-Object = "TYPE:" CONTENT-TYPE ";" "LNG:" Length ";" "BODY:" Binary-Data ";"

Length = 1*DIGIT

Binary-Data = 1*OCTET

CONTENT-TYPE = ALPHA *(Printable-ASCII-character)

ALPHA = %x41-5A / %x61-7A ; A-Z / a-z

DIGIT = "0"/ "1"/ "2"/ "3"/ "4"/ "5"/ "6"/ "7"/ "8"/ "9"

OCTET = %x00-FF

CRLF = %x0D %x0A

ISO8Bit covers the extended range of characters from ASCII character set, such as JIS X 0201 (for Japan), ISO/IEC-8859-1 to ISO/IEC8859-16 character sets.

The character set used for Property-Value is not specified in this specification except for the ASCII printable characters as defined by MCCSDCD in Section 5.1.3. When characters in a Direct Code are displayed, a default character set of the device is used. Such a character set may be determined by the service provider, the current location of the device, user's setting, etc.

If an appropriate display cannot be achieved by the default character set as judged by the user, it is an implementation specific matter how to resolve the issue. For example, some implementation may allow the user to select alternative character sets by menu selections.

7.1.2.2 Escaping DMF Property-Values

Certain characters using as a parameter of Property, i.e. ",", ";", ":", and "\", SHALL be denoted by using the escape sequence with a backslash "\". For example, http://www.openmobilealliance.org/ must be denoted as http\://www.openmobilealliance.org/.

7.1.3 List of Recognizable Formats

Table 1 lists all the Recognizable Formats that are specified in this specification. The MCC recognises the Recognizable Formats, leading to enable causing certain actions. The details of the syntax and semantics of each Recognizable Format are specified in the corresponding sections that are indicated in Table 1.

	Recognizable Format	Description	Section
1	http: , https:	Web access	7.2.1
2	Telephone-Number-String , tel:	Telephone Number String Recognition and Tel URI Scheme	7.2.2
3	Mailbox	Mail Address Recognition	7.2.3
4	MECARD:	Business Card Recognition	7.2.4
5	MEBKM:	Bookmark Recognition	7.2.5
6	MATMSG:	Email Linkage Data Format Recognition	7.2.6
7	MELOC:	Location Information	7.2.7

Table 1: List of Recognizable Formats

7.2 Recognisable Formats

7.2.1 Web Access

7.2.1.1 HTTP: and HTTPS: URI Schemes

The MCC SHALL recognise http: and https: URI schemes as the Recognizable Formats, with the following clarifications.

The MCC SHALL support the following sections of OMA-URI [OMAURI]:

- Section 5.0,
- Section 5.1, and
- Section 5.2.

The MCC SHALL recognise http: and https: as a Recognizable Format wherever such a format is present in the Direct Code; such a format may exist alone, in the middle of a plain text message, with other Recognizable Format, or inside of other Recognizable Format. When http: or https: URI Scheme appears in other Recognizable Formats that are specifically listed in Table 10, the MCC SHALL conduct recognition based on the rules that are specified in Section 7.3.

7.2.1.2 Behaviour

After recognizing the Recognizable Format;

- The MCC SHALL display the recognised URIs with other data such as plain text messages and/or other Recognizable Formats;
- The MCC SHALL make such a URI selectable by the user for invocation;
- If multiple URIs are recognised, the MCC SHALL provide means for the user to choose one from them;
- In order to ensure user authorization, the MCC SHALL display the URIs in texts so that the user is able to see the URIs before invoking a browser;
- If a URI is selected and clicked by the user, the MCC SHALL invoke a browser with the URI to be passed to;
- The MCC SHOULD make the URIs available for other applications such as registering them into a bookmark in the device if the user wishes; and
- Once the invoked application is terminated the control SHOULD be returned to the MCC if such control is possible in the device.

7.2.2 Telephone Number String Recognition and Tel URI Scheme

This section defines the Telephone-Number-String recognition. The syntax of the Telephone-Number-String is defined below using the ABNF [RFC4234]. A Telephone-Number-String consists of phone digits, “+”, ”*”, and “#”. It may include visual separators that are commonly used in various places in the world. Also this section defines the optional support of Tel URI scheme [RFC3966].

7.2.2.1 Telephone Number String Recognition

1. The MCC SHALL recognise a Telephone-Number-String as a Recognizable Format.

A Telephone-Number-String may contain visual separators. Visual separators merely aid readability by human and are not used for a URI to place a call or send a message. Visual separators must be removed when a Telephone-Number-String is used as a URI.

2. The MCC SHALL recognise a Telephone-Number-String as a Recognizable Format wherever such a format is present in the Direct Code; such a format may exist alone, in the middle of a plain text message, with other Recognizable Format, or inside of other Recognizable Format. When a Telephone-Number-String appears in other Recognizable Formats that are specifically listed in Table 10, the MCC SHALL conduct recognition based on the rules that are specified in Section 7.3.

Definition of Telephone-Number-String using the ABNF notation:

Telephone-Number-String = String-1 / String-2 / String-3

String-1 = (“+“ / DIGIT) 9*25Phonedigit [Visual-Separator]

String-2 = (“*“ / “#“) 4*25Phonedigit [Visual-Separator]

String-3 = TEL (“+” / DIGIT2) 2*25Phonedigit [Visual-Separator]

Phonedigit = [Visual-Separator] DIGIT2

DIGIT = “0“/ “1“/ “2“/ “3“/ “4“/ “5“/ “6“/ “7“/ “8“/ “9“

DIGIT2 = DIGIT / “*“ / “#“

Visual-Separator = 1*4VS

VS = “(“ / “)“ / “.“ / “-“ / “/“ / SP

SP = %x20

TEL = “tel:“ ; ABNF strings are case-insensitive.

Implementation may have additional detection methods to enhance recognition results.

7.2.2.2 Tel URI scheme Recognition

The MCC MAY recognise the “tel:” scheme [RFC3966] as a Recognizable Format. The "tel" URI describes resources identified by telephone numbers.

7.2.2.3 Behaviour

After recognizing the Recognizable Format that represents a telephone number either by the specifications 7.2.2.1 or 7.2.2.2;

- The MCC SHALL display the recognised format with any other data such as plain text messages and/or other Recognizable Formats;
- The MCC SHALL make the format that represents a telephone number selectable by the user for initiating a voice call, sending an SMS / MMS message or other types of communications. Such communications may include initiating a push-to-talk call, a video phone call, etc, which are available on the device;
- If multiple Recognizable Formats that represent telephone numbers are recognised, the MCC SHALL provide means for the user to choose one from them;
- The MCC SHOULD make the telephone number obtained from the Recognizable Format that represents a telephone number available for other applications such as saving it into a contact book in the device if the user wishes.

7.2.3 Mail Address Recognition

7.2.3.1 Mailbox

1. The MCC SHALL recognise a Mailbox as the Recognizable Format.

2. The Mailbox SHALL follow the definition in [RFC2822].
The following exceptions to [RFC2822] apply in order for successful recognition of a Mailbox.

- Any white spaces or comments (i.e., CFWS (comments and/or folding white space) as defined in [RFC2822]) SHALL NOT be used in a Mailbox.
- In the case of name-addr, display-name SHALL follow the same syntax as that of local-part.

3. The MCC SHALL recognise a Mailbox as a Recognizable Format wherever such a Mailbox is present in the Direct Code; such a Mailbox may exist alone, in the middle of a plain text message, with other Recognizable Format, or inside of other Recognizable Format. When a Mailbox appears in other Recognizable Formats that are specifically listed in Table 10, the MCC SHALL conduct recognition based on the rules that are specified in Section 7.3.

7.2.3.2 Behaviour

After recognizing the Mailbox;

- The MCC SHALL display the Mailbox with any other data such as plain text messages and/or other Recognizable Formats;
- The MCC SHALL make the Mailbox selectable by the user for invoking an email client application, with the Mailbox being inserted as the destination in the email application.
- If multiple Mailboxes are recognised, the MCC SHALL provide means for the user to choose one from them;
- The MCC SHOULD make the Mailbox available for other applications such as saving it into a contact book in the device if the user wishes.

7.2.4 Business Card Recognition

7.2.4.1 MECARD Format

The MECARD format recognises data that are essential for business cards.

- The definition of MECARD syntax SHALL be based on the DMF Definition in Section 7.1.2, with the following specifications and clarifications that SHALL supersede the generic definition in Section 7.1.2.
- The MCC SHALL recognise MECARD: as a Recognizable Format.
- The MCC SHALL NOT recognise MECARD: as a Recognised Format when MECARD: is found embedded within another Recognizable Format.

An example of MECARD format is shown below (CR/LF added for human readability):

MECARD:

N:Bill Jones;

TEL:+18586230741;

TEL:+18586230742;

EMAIL:foo@openmobilealliance.org;

EMAIL:hoo@openmobilealliance.org;

URL: http\://www.openmobilealliance.org;

;

The table below defines the Properties of the MECARD, the number of Property-Values, and the semantic descriptions. The MCC conformance criteria are described in the specific property descriptions (below).

Property	Number of Property-Value	Semantic Description
N	1	The name of the person associated with the MECARD
SOUND	1	A sound annotation for the name of the person associated with the MECARD
TEL	1	A telephone number associated with the MECARD
EMAIL	1	An electronic mail address associated with the MECARD

BDAY	1	The date of birth associated with the MECARD
ADR	1	The physical delivery address associated with the MECARD
NOTE	1	Supplemental information or a comment associated with the MECARD
URL	1	A URL associated with the MECARD
NICKNAME	1	A nick name of the person associated with the MECARD

Table 2: Properties of the MECARD

- The MCC SHALL ignore any Property that is found in the MECARD but is not included in this table. It is recommended to display such ignored data as it may help the user to understand what are written in the symbol.
- All the Properties have one Property-Value, respectively. The following characters; comma, ",", semicolon, ";", colon, ":", and back slash, "\", SHALL be escaped as defined in Section 7.1.2.1 using a back slash, "%x5C", if such a character needs to be included in the Property-Value. If such characters that need to be escaped are found without being escaped in the Property, they SHALL be ignored.

7.2.4.2 N Property

- The MCC SHALL support the N Property.
- The string of characters in the Property-Value of the N Property SHALL be recognised as the name of the person associated with the MECARD.
- If more than one N Property is found, the MCC SHALL recognise as many N Properties as it can process. The N Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.

7.2.4.3 SOUND Property

- The MCC SHOULD support the SOUND Property.
- The string of characters in the Property-Value of the SOUND Property SHALL be recognised as the sound annotation for the name of the person associated with the MECARD.
- If more than one SOUND Property is found, the MCC SHALL recognise as many SOUND Properties as it can process. The SOUND Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.

7.2.4.4 TEL Property

- The MCC SHALL support the TEL Property.
- The string of characters in the Property-Value SHALL comply with the definition of Telephone-Number-String, as defined in Section 7.2.2.
- The string of characters in the Property-Value of the TEL Property SHALL be recognised as the telephone number associated with the MECARD.
- If more than one TEL Property is found, the MCC SHALL recognise as many TEL Properties as it can process. The TEL Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.
- In addition to recognizing MECARD as a structure, the MCC SHALL recognise the Property-Value in the TEL Property by itself, if it complies with the above definition, as the telephone number associated with the MECARD and provide the functions that are defined in Section 7.2.2. The MCC SHALL provide a means to the user to be able to choose which one, i.e., the MECARD or the telephone number, is to be invoked. If multiple TEL Properties are

found, the MCC SHALL provide these functions for all the telephone numbers that the MCC is capable of supporting.

7.2.4.5 EMAIL Property

- The MCC SHALL support the EMAIL Property.
- The string of characters in the Property-Value SHALL comply with the definition of the Mailbox, as defined in Section 7.2.3.
- The string of characters in the Property-Value of the EMAIL Property SHALL be recognised as the electronic mail address associated with the MECARD.
- If more than one EMAIL Property is found, the MCC SHALL recognise as many EMAIL Properties as it can process. The EMAIL Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.
- In addition to recognizing MECARD as a structure, the MCC SHALL recognise the Property-Value in the EMAIL Property by itself, if it complies with the above definition, as the electronic mail address associated with the MECARD and provide the functions that are defined in Section 7.2.3. The MCC SHALL provide a means to the user to be able to choose which one, i.e., the MECARD or the electronic mail address, is to be invoked. If multiple EMAIL Properties are found, the MCC SHALL provide these functions for all the electronic mail addresses that the MCC is capable of supporting.

7.2.4.6 BDAY Property

- The MCC SHALL support the BDAY Property.
- The string of characters in the Property-Value of the BDAY Property SHALL be recognised as the date of birth associated with the MECARD.
- If more than one BDAY Property is found, the MCC SHALL recognise as many BDAY Properties as it can process. The BDAY Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.
- The string of characters in the BDAY Property-Value SHALL be a string of 8 characters consisting of ASCII characters, "%x30-39". The first 4 characters from the head SHALL represent the year, the next 2 characters SHALL represent the month, and the last 2 characters SHALL represent the day of the birth, respectively. If there are more than 8 characters found, the excessive characters SHALL be set to be NULL.

7.2.4.7 ADR Property

- The MCC SHALL support the ADR Property.
- The string of characters in the Property-Value of the ADR Property SHALL be recognised as the physical delivery address associated with the MECARD.
- If more than one ADR Property is found, the MCC SHALL recognise as many ADR Properties as it can process. The ADR Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.

7.2.4.8 NOTE Property

- The MCC SHALL support the NOTE Property.
- The string of characters in the Property-Value of the NOTE Property SHALL be recognised as the supplemental information or a comment associated with the MECARD.

- If more than one NOTE Property is found, the MCC SHALL recognise the NOTE Properties as many as it can process. The NOTE Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.

7.2.4.9 URL Property

- The MCC SHALL support the URL Property.
- The string of characters in the Property-Value SHALL comply with the definition of the http: and https:, as defined in Section 7.2.1.
- The string of characters in the Property-Value of the URL Property SHALL be recognised as the http: and https: URI schemes associated with the MECARD.
- If more than one URL Property is found, the MCC SHALL recognise as many URL Properties as it can process. The URL Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.
- In addition to recognizing MECARD as a structure, the MCC SHALL recognise the Property-Value in the URL Property by itself, if it complies to the above definition, as the http: and https: URI schemes associated with the MECARD and provide the functions that are defined in Section 7.2.1. The MCC SHALL provide a means to the user to be able to choose which one, i.e., the MECARD or the URI scheme, is to be invoked. If multiple URL Properties are found, the MCC SHALL provide these functions for all the URI schemes that the MCC is capable of supporting.
- It should be noted that, as defined by Section 7.1.2, DMF Definition, certain characters in the URI scheme SHALL be denoted by using the escape sequence with a backslash "\".

7.2.4.10 NICKNAME Property

- The MCC SHALL support the NICKNAME Property.
- The string of characters in the Property-Value of the NICKNAME Property SHALL be recognised as the nick name of the person associated with the MECARD.
- If more than one NICKNAME Property is found, the MCC SHALL recognise as many NICKNAME Properties as it can process. The NICKNAME Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.

7.2.4.11 Behaviour

If MECARD is chosen by the user, an appropriate application SHALL be invoked to store the data contained in the MECARD to a phone book on the device.

Some Property-Values in the MECARD are also Recognizable Formats, in addition to be elements of the MECARD structure. They are the Property-Values of TEL, EMAIL, and URL Properties, as defined in Sections 7.2.2, 7.2.3, and 7.2.1, respectively. If such Property-Values exist and are found to be satisfying the respective definitions, the MCC SHALL recognise these values as Recognizable Formats in addition to recognizing the MECARD itself, and SHALL offer the functions that are specified in the respective sections of this specification, in addition to that for the MECARD. The MCC SHALL provide the user with a means of selecting which application is to be invoked, e.g., by displaying the values with actionable strings allowing the user to select and invoke the desired application.

The following table summarises the elements of MECARD that are recognised as actionable strings and displayed as text.

Property	Actionable String	Description
MECARD	Yes	"MECARD" may be displayed using any string that may be

		familiar to users in the desired language. If this is selected, the data in the MECARD is to be stored in the phone book by appropriate application(s).
N	No	The name of the person associated with the MECARD is displayed.
SOUND	No	A sound annotation for the name of the person associated with the MECARD is displayed.
TEL	Yes	A telephone number associated with the MECARD is displayed. If the actionable link is selected instead of MECARD, it invokes applications, e.g., initiating a phone call. Details are specified in Section 7.2.2.
EMAIL	Yes	An electronic mail address associated with the MECARD is displayed. If the actionable link is selected instead of MECARD, the user is presented application(s) that may be invoked, e.g., invoking an email client with this email address being set as the destination address. Details are specified in Section 7.2.3.
BDAY	No	The date of birth associated with the MECARD is displayed.
ADR	No	The physical delivery address associated with the MECARD is displayed.
NOTE	No	Supplemental information or a comment associated with the MECARD is displayed.
URL	Yes	A URL associated with the MECARD is displayed. If the actionable link is selected instead of MECARD, the user is presented application(s) that may be invoked, e.g., a web browser to access the page designated by the URL. Details are specified in Section 7.2.1.
NICKNAME	No	A nick name of the person associated with the MECARD is displayed.

Table 3: MECARD Elements

7.2.5 Bookmark Recognition

7.2.5.1 MEBKM format

The MEBKM format recognises data that are essential for a bookmark.

- The definition of MEBKM syntax SHALL be based on the DMF Definition in Section 7.1.2, with the following specifications and clarifications that SHALL supersede the generic definition in Section 7.1.2.
- The MCC SHALL recognise MEBKM: as a Recognizable Format.
- The MCC SHALL NOT recognise MEBKM: as a Recognised Format when MEBKM: is found embedded within another Recognizable Format.

An example of MEBKM format is shown below (CR/LF added for human readability):

MEBKM:

TITLE:OMA Home Page;

URL: http\://www.openmobilealliance.org;

;

The table below defines the Properties of the MEBKM, the number of Property-Values, and the semantic descriptions. The MCC conformance criteria are described in the specific property descriptions (below).

Property	Number of Property-Value	Semantic Description
TITLE	1	A title associated with the MEBKM, e.g., the name of the location pointed by the URL
URL	1	A URL associated with the MEBKM

Table 4: Properties of the MEBKM

- The MCC SHALL ignore any Property that is found in the MEBKM but is not included in this table. It is recommended to display such ignored data as it may help the user to understand what are written in the symbol.
- All the Properties have one Property-Value, respectively. The following characters; comma, ",", semicolon, ";", colon, ":", and back slash, "\", SHALL be escaped as defined in Section 7.1.2.1 using a back slash, "%x5C", if such a character needs to be included in the Property-Value. If such characters that need to be escaped are found without being escaped in the Property, they SHALL be ignored.

7.2.5.2 TITLE Property

- The MCC SHALL support the TITLE Property.
- The string of characters in the Property-Value of the TITLE Property SHALL be recognised as the title associated with the MEBKM.

7.2.5.3 URL Property

- The MCC SHALL support the URL Property.
- The string of characters in the Property-Value SHALL comply with the definition of the http: and https:, as defined in Section 7.2.1.
- The string of characters in the Property-Value of the URL Property SHALL be recognised as the http: and https: URI schemes associated with the MEBKM.
- In addition to recognizing MEBKM as a structure, the MCC SHALL recognise the Property-Value in the URL Property by itself, if it complies to the above definition, as the http: and https: URI schemes associated with the MEBKM, and SHALL provide the functions that are defined in Section 7.2.1. The MCC SHALL provide a means to the user to be able to choose which one, i.e., the MEBKM or the URI scheme, is to be invoked.
- It should be noted that, as defined by Section 7.1.2, DMF Definition, certain characters in the URI scheme SHALL be denoted by using the escape sequence with a backslash "\".

7.2.5.4 Behaviour

If MEBKM is chosen by the user, an appropriate application SHALL be invoked to store the data contained in the MEBKM to a bookmark registry on the device.

The URL Property-Value in the MEBKM is also a Recognizable Format, in addition to be an element of the MEBKM structure. It is defined in Sections 7.1.2.2. The MCC SHALL recognise the Property-Value of URL Property as a Recognizable Format in addition to recognizing the MEBKM itself, and SHALL offer the functions that are specified in Section 7.1.2.2, in addition to that for the MEBKM. The MCC SHALL provide the user with a means of selecting which application is to be invoked, e.g., by displaying the values with actionable strings allowing the user to select and invoke the desired application.

The following table summarises the elements of MEBKM that are recognised as actionable strings and displayed as text.

Property	Actionable String	Description
MEBKM	Yes	"MEBKM" may be displayed using any string, e.g., "Add to bookmark", that may be familiar to users in the desired language. If this is selected, the data in the MEBKM is to be stored in the bookmark registry by appropriate application(s).
TITLE	No	The title associated with the MEBKM is displayed.
URL	Yes	A URL associated with the MEBKM is displayed. If the actionable link is selected instead of MEBKM, the user is presented application(s) that may be invoked, e.g., a web browser to access the page designated by the URL. Details are specified in Section 7.2.1.

Table 5: MEBKM Actionable Strings

7.2.6 Email Linkage Data Format Recognition

7.2.6.1 MATMSG format

The MATMSG format is used to link email data contained in the format to applications such as email clients.

- The definition of MATMSG syntax SHALL be based on the DMF Definition in Section 7.1.2, with the following specifications and clarifications that SHALL supersede the generic definition in Section 7.1.2.
- The MCC SHALL recognise MATMSG: as a Recognizable Format.
- The MCC SHALL NOT recognise MATMSG: as a Recognised Format when MATMSG: is found embedded within another Recognizable Format.

An example of the MATMSG format is shown below (CR/LF added for human readability):

MATMSG:

TO:foo@openmobilealliance.org;

SUB:Hello;

BODY:This is the message body.;

;

The TO Property must be present in the MATMSG data. If TO Property is not found, it is an erroneous mobile code. The number of TO Properties is 1 or more. The number of the SUB Property may be zero or one. The number of the BODY Property may be zero or one.

The table below defines the Properties of the MATMSG format, the number of Property-Values, and the semantic descriptions. The MCC conformance criteria are described in the specific property descriptions (below).

Property	Number of Property-Value	Semantic Description
TO	1	An electronic mail address associated with the MATMSG, whose Property-Value will be inserted in the destination address field if an application, e.g., an email client, is invoked.
SUB	1	A subject of the message associated with the MATMSG, of which Property-Value will be inserted in the subject field if an application, e.g., an email client, is invoked.
BODY	1	A body of the message associated with the MATMSG, of which Property-Value will be inserted in the body field if an application, e.g., an email client, is invoked.

Table 6: Properties of the MATMSG

- The MCC SHALL ignore any Property that is found in the MATMSG format but is not included in this table. It is recommended to display such ignored data as it may help the user to understand what are written in the symbol.
- All the Properties have one Property-Value, respectively. The following characters; comma, ",", semicolon, ";", colon, ":", and back slash, "\", SHALL be escaped as defined in Section 7.1.2.1 using a back slash, "%x5c", if such a character needs to be included in the Property-Value. If such characters that need to be escaped are found without being escaped in the Property, they SHALL be ignored.

7.2.6.2 TO Property

- The MCC SHALL support the TO Property.
- The string of characters in each TO Property-Value SHALL comply with the definition of the Mailbox, as defined in Section 7.2.3.
- The MCC SHALL recognise each Property-Value of the TO Property as a Mailbox associated with the MATMSG.
- If more than one TO Property is found, the MCC SHALL recognise as many TO Properties as it can process as a group. Any TO Properties over and above the maximum number that can be processed as a group SHALL be ignored.
- The MATMSG SHALL be displayed as an actionable string of characters that is familiar to users in the desired language, e.g., "Create email". Additionally, the MCC SHALL display each individual TO Property-Value as an actionable string of characters, to the extent that the MCC can process. Note that, depending on the MCC implementation, the number of TO Property-Values that the MCC can process individually as actionable strings may be different than the number of TO Properties that can be processed as a group in the MATMSG.
- For the MATMSG, the MCC SHALL insert the group of recognised TO Property-Values into the destination address fields of an application, e.g., an email client that is selected and invoked. Additionally, for individual TO Property-Values, the MCC behavior is defined in Section 7.2.3.2.

7.2.6.3 SUB Property

- The MCC SHALL support the SUB Property.

- The string of characters in the Property-Value of the SUB Property SHALL be recognised as the subject of the message associated with the MATMSG.
- If present, the Property-Value of the SUB Property SHALL be inserted in the subject field of the application, e.g., an email client, that is selected and invoked.

7.2.6.4 BODY Property

- The MCC SHALL support the BODY Property.
- The string of characters in the Property-Value of the BODY Property SHALL be recognised as the body of the message associated with the MATMSG.
- If present, the Property-Value of the BODY Property SHALL be inserted in the body field of the application, e.g., an email client, that is selected and invoked.

7.2.6.5 Behaviour

- The MCC SHALL provide the user with a means of selecting any one of the actionable strings, i.e., the MATMSG or an individually displayed TO Property-Value.
- If one of the actionable strings is selected by the user, an appropriate application, e.g., an email client, SHALL be invoked and the data in the format that is selected by the user SHALL be inserted in the respective fields of the email in the application.

The following table summarises the elements of MATMSG that are recognised as actionable strings and displayed as text.

Property	Actionable String	Description
MATMSG	Yes	"MATMSG" may be displayed by using any string that is familiar to users in the desired language, e.g., "Create email". If this actionable string is selected by the user, an appropriate application, e.g., an email client, is invoked and the data in the MATMSG is inserted in the respective field of the email in the selected application.
TO	Yes	The Property-Value, i.e., an electronic mail address associated with the MATMSG, is displayed as an actionable string if it complies with the definition. In case where multiple TO Properties are found, each of the Property-Values are displayed as an actionable string if it complies with the definition. If the actionable string representing the Property-Value or one of the Property-Values (as appropriate) is selected by the user, an appropriate application, e.g., an email client, is invoked and the data in the Property-Value is inserted in the destination header of the email in the selected application.
SUB	No	The subject of the message associated with the MATMSG is displayed. No part of the Property-Value is recognised as a Recognizable Format.
BODY	No	The body of the message associated with the MATMSG is displayed. No part of the Property-Value is recognised as a Recognizable Format.

Table 7: MATMSG Actionable Strings

7.2.7 Location Information

7.2.7.1 MELOC Format

1. The MCC SHALL recognise MELOC: as the Recognizable Format.

2. The MCC SHALL NOT recognise MELOC: as the Recognised Format when the MELOC: is found in other Recognizable Format.

MELOC contains geolocation (GEO) information which is borrowed from [VCARD2.1]

Example (CR/LF added for human readability):

MELOC:

ADR: 1234 Broadway Av., Richardson Tx, 75081 USA;

BLD: I;

FLR: 14;

ROOM: 29;

GEO:37.386013-122.082932;

ALT: 36.5

;

The table below defines the Properties of the MELOC format, the number of Property-Value and the composer conformance criteria. The MCC conformance criteria are described in the specific property description.

Property	Number of Property-Value	Semantic Description	
ADR	1	The physical address of the location indicated by the Property GEO.	
BLD	1	The building code of the location indicated by the Property GEO.	
FLR	1	The floor number of the location indicated by the Property GEO.	
ROOM	1	The room number of the location indicated by the Property GEO.	
GEO	1	The location information as specified by [VCARD2.1]	
ALT	1	The altitude information complementing the GEO information. The altitude information is expressed in WGS84 reference system.	

Table 8: MELOC Format

For the Properties ADR, BLD, FLR, ROOM, GEO and ALT the Property-Value of each Property is a single string of characters that may contain any number of commas “,” and/or semicolons “;”. For a comma in the string, an escape sequence is not used. For a semicolon in the string, an escape sequence SHALL be used so that “;” is denoted as “\;”.

ADR Property

At a minimum, an input of 100 bytes data SHALL be supported for the Property-Value.

BLD Property

At a minimum, an input of 1 bytes data SHALL be supported for the Property-Value.

FLR Property

At a minimum, an input of 4 bytes data SHALL be supported for the Property-Value.

ROOM Property

At a minimum, an input of 4 bytes data SHALL be supported for the Property-Value.

GEO Property

At a minimum, an input of 17 bytes data SHALL be supported for the Property-Value.

ALT Property

At a minimum, an input of 4 bytes data SHALL be supported for the Property-Value.

7.2.7.2 Behavior

After recognizing the MELOC:

1. The MCC SHALL display the MELOC with other data such as plain text messages and/or other Recognizable Formats;
2. If multiple Recognizable Formats are recognised, the MCC SHALL provide means for the user to choose one from them.
3. The MCC SHALL make such a format selectable by the user for initiating the appropriate application e. g. map, indoor routing, workforce tracking etc.

7.3 Recognition of overlapping Recognizable Formats

There are cases where the whole or a portion of a Recognizable Format overlaps with other Recognizable Formats. For overlapping Recognizable Formats, a rule is needed to determine how such overlapping formats are recognised consistently among the various implementations of this specification, so as to ensure consistency between the expectation of the publisher of the mobile code and the recognition results to be presented to the user. In order to ensure consistency, a priority must be

defined in order for the MCC to be able to select those that are most suitable. The following examples show such overlapping formats and suitable prioritised recognition.

	Examples	Description	Suitable Priority
1	http://www.omaorg.org/test@omaorg.org	An email address is embedded in an http: schema	http://www.omaorg.org/test@omaorg.org Prioritise the http: schema
2	09012345678@omaorg.org	A telephone number is embedded in an email address	09012345678@omaorg.org Prioritise the email address.
3	tel:09012345678@omaorg.org	Tel: appears in front of an email address in which a telephone number is embedded.	tel:09012345678@omaorg.org Prioritise the telephone number.
4	012 345 678 987@omaorg.org	A telephone number containing SPs as visual separator overlaps with an email address	0012 345 678 987@omaorg.org (i) Prioritise the email address, and (ii) Recognised the telephone number as a separate Recognizable Format

Table 9: Examples of a Recognizable Format Appearing in Other Recognizable Format

The following specifies the rules for recognizing the following Recognizable Formats that are listed in Table 10when they are overlapping:

Recognizable Format	Note
http: and https:	
tel:	(String-3)
telephone number	(String-1 and String-2)
mail address	

Table 10: Recognizable Formats that Need to be Resolved When Overlapping

In case where overlapping Recognizable Formats are found:

- When a telephone number and an email address are overlapping each other, and the telephone number contains one or more SPs, %x20, as a visual separator, then;
  - The MCC SHALL select the email address as the first priority Recognizable Format, and
  - The MCC SHALL recognise a partial string that does not overlap with the string representing the email address as a separate telephone number if the partial string satisfies the definition of a telephone number as defined in 7.2.3.1.
- The MCC SHALL select the email address as the first priority Recognizable Format if the email address starts with a telephone number.
- Otherwise, among the Recognizable Formats that overlap each other, the MCC SHALL select the Recognizable Format whose first character starts closest to the beginning of the Data String as the first priority Recognizable Format.
- The MCC SHALL display the actionable image of the first priority Recognizable Format. How to handle other Recognizable Formats that overlap with the selected first priority Recognizable Format is subject to each implementation.

8. Indirect Code Handling

8.1 Data Format

This section describes the data format used for Indirect Code.

The Indirect Code data format is shown below.

Field	Code-Marker	Version-Number	ICI	ICI-DT-Separator	Display-Text (DT)
Length	5 octets	1 octet	Variable length (4 or more octets)	0 or 1 octet	Variable length (0 or more octets)
Description	See Section 6.1	The most significant 4 bits identify the major version; the least significant 4 bits identify the minor version.	Contains the Indirect Code Identifier.	%x04	Contains the text to be displayed on the mobile device.

Table 11: Indirect Code Data Format

Total length of the Indirect Code Data String is constrained by the symbology and symbol size.

The five fields of the Indirect Code data format SHALL follow Table 11.

The ICI SHALL start at immediately after the Version-Number field and end just before the ICI-DT-Separator field.

The ICI-DT-Separator SHALL only be present if and only if there is Display-Text to follow.

Additional fields may be added in a future version after the last field of the latest version (e.g., “Display-Text” field is the last field of v1.0). When new fields are added, a new major version number should be used and SHALL be one higher than the latest major version number.

The five fields are described in the sections below.

8.1.1 Code-Marker

The Code-Marker is described in Section 6.1 and SHALL be used to indicate that the Mobile Code is an Indirect Code. Note: The Code-Marker is excerpted to this section for readability.

A Code-Marker is defined in the ABNF notation as follows:

Code-Marker = %x03 "OMA" %x20 ; ABNF strings are case-insensitive.

8.1.2 Version-Number

The Version-Number SHALL indicate the version number of this specification. The most significant 4 bits SHALL indicate the major version number. The least significant 4 bits SHALL indicate the minor version number. For this specification, this field SHALL contain the value "%x10".

8.1.3 ICI

The Indirect Code Identifier (ICI) SHALL comprise of the following format:

Field	Routing-Prefix			Resolution-Identifier
	Length-Indicator	Registry-ID	Remaining-Part-of-Routing-Prefix	
Length	1 hex digit	3 hex digits	Variable length (1 to 16 octets)	Variable length (1 or more octets)
Description	Indicates the length of the "Remaining Part of Routing Prefix" field in octets.	Contains the Registry ID.	Contains the remaining part of the Routing Prefix after excluding the first 2 octets.	Contains the Resolution Identifier.

Table 12: Indirect Code Identifier (ICI) Format

The ICI SHALL consist of two major fields: the Routing-Prefix and the Resolution-Identifier. The length of the ICI field SHALL NOT be more than 36 octets.

The two fields are described in the following sections.

8.1.3.1 Routing-Prefix

The Routing-Prefix contains the Length-Indicator field, Registry-ID field and Remaining-Part-of-Routing-Prefix field. The three fields are described below.

8.1.3.1.1 Length-Indicator

The Length-Indicator SHALL be 4-bit long and contains a 1-hex digit value that indicates the length of the Remaining-Part-of-Routing-Prefix field. If the value of the Length-Indicator is N, where N is any value from 0 to 15, the length of the Remaining-Part-of-Routing-Prefix field is N+1.

8.1.3.1.2 Registry-ID

The Registry-ID SHALL be assigned by OMNA. A Registry-ID comprises of a fixed length of 3-hex digits and with the following specific details:

- The value "%x000" SHALL be reserved.

– The value "%x001" SHALL be used by OMNA to assign Routing-Prefix directly to entities that are not a Registry-ID Recipient.

– The range of values from %x002 to %xFFF SHALL be assigned by OMNA to a Registry-ID Recipient.

8.1.3.1.3 Remaining-Part-of-Routing-Prefix

The Remaining-Part-of-Routing-Prefix SHALL be assigned by OMNA or a Registry-ID Recipient to a Resolving CMP. The length of the Remaining-Part-of-Routing-Prefix SHALL be equal to the value in the Length-Indicator field + 1. Each octet in the Remaining-Part-of-Routing-Prefix SHALL contain any value from %x00 to %xFF, except %x04 (i.e., value used as the ICI-DT-Separator).

8.1.3.2 Resolution-Identifier

The Resolution-Identifier SHALL be assigned by the Resolving CMP for purposes of resolving each ICI. Each octet in the Resolution-Identifier SHALL contain any value from %x00 to %xFF, except %x04 (value used as the ICI-DT-Separator).

8.1.4 ICI-DT-Separator

The ICI-DT-Separator, when present, SHALL be equal to %x04 to indicate the presence of Display-Text that follows immediately after the ICI.

8.1.5 Display-Text

Display-Text MAY be present after the ICI and, when present, is preceded immediately by the ICI-DT-Separator. The Display-Text, when present, SHALL contain the text string to be displayed on the mobile device while the MCC resolves the ICI and SHALL contain only the following ASCII characters:

%x20-7E, %x0A (LF) and %x0D (CR).

8.2 Code Resolution Procedures

An ICI needs to be mapped into either content to be consumed directly by the device, or the address of content (or a service) to be consumed by the device. This section describes the procedures for the functional entities that are involved in the ICI resolution.

8.2.1 Overview of Code Resolution Procedures

When the MCC detects that a scanned Mobile Code is an Indirect Code, it retrieves the ICI from the Indirect Code and sends the Code Resolution request to the Home CMP. If user personal data or location information is available and stored locally on the MCC, the MCC includes the location information and user personal data such as age, gender, household income and postal code in the Code Resolution request if the user has opted in to allow the inclusion of the information in the Code Resolution request.

In the case of the Home CMP that hosts the specified ICI, it resolves the ICI and returns the response to the MCC. In the case of the home Split-CMP-Parent where its Split-CMP-Child hosts the specified ICI, it sends the Code Resolution request to the

Resolving Split-CMP-Child, receives the response from the Resolving Split-CMP-Child and returns the response to the MCC.

Otherwise, the Home CMP sends the Code Resolution request to the Remote/Resolving CMP (or the Split-CMP-Parent where applicable) based on the locally available routing information or by querying the MCR for the routing information. If no routing information is available for the specified ICI, the Home CMP returns an error to the MCC.

The Remote/Resolving CMP (or the Split-CMP-Parent where applicable) performs procedures similar to those performed by the Home CMP as described above. The major differences are that the Remote/Resolving CMP (or the Split-CMP-Parent where applicable):

- Returns the MC-3-RESOLVE_ICI_RESPONSE to the requestor CMP (or the Split-CMP-Parent where applicable) instead of returning the MC-1-RESOLVE_ICI_RESPONSE to the MCC.
- Does not perform procedures that the Home CMP does that manipulate the parameters (e.g., related to tracking) to be returned in the response to the MCC.

Normally when the Remote CMP (or the Split-CMP-Parent where applicable) is involved, the Code Resolution request will eventually reach the Resolving CMP that resolves the ICI and the response is returned to the MCC in the backward sequence via the CMPs (or the Split-CMP-Parent where applicable) that were involved in routing the Code Resolution request. Any failure in routing the Code Resolution request before reaching the Resolving CMP or in resolving the ICI at the Resolving CMP would cause an error to be returned to the MCC in the backward sequence through the CMPs (or the Split-CMP-Parent where applicable) that were involved in routing the Code Resolution request.

8.2.2 Specific Code Resolution Procedures

8.2.2.1 Procedures at MCC

When the MCC detects an Indirect Code in the scanned Mobile Code based on the presence of the “Code-Marker”, it will perform the following actions:

- If the “Display-Text” (as specified in Section 8.1.5) is present, the MCC SHALL display that text.
- The MCC sends the MC-1-RESOLVE_ICI_REQUEST message to the Home CMP as specified in Section 10.3.1.1:
    - The MCC SHALL parse the Indirect Code as specified in Section 8.1 to extract the ICI value as the “ici” parameter and the Version-Number as the “enablerver” parameter.
    - The request SHALL contain the following mandatory parameters as specified in Table 15: “ici”, “appid”, “enablerver”, “clientid”, “optout”.
    - The request MAY contain the following of the optional parameters as specified in Table 15: “btype”, “networkidhome”, “networkidroam”.
    - If the “optout” parameter is FALSE and the data is available on the MCC, then the request MAY contain the following optional parameters as specified in Table 15: “cc”, “post”, “age”, “income”, “gender”, “locationinfo”. Otherwise, the MCC SHALL not send any of these mentioned parameters.
- If the MC-ERROR message is received, the MCC SHALL display an appropriate text to the user based on following parameters as specified in Table 13: “status”, “description”.
- If the MC-1-RESOLVE_ICI_RESPONSE message is received, the MCC SHALL:
    - invoke the appropriate action based on the “codecontentset” parameter as specified in Tables 16, 17, 18. Additionally:
        - If the “contentdescription” (as specified in Table 16) is present, the MCC SHALL display the data to the user.
    - invoke the appropriate action based on the “tracking-indicator” (as specified in Table 16) being set to “True” and the MCC supports optional tracking as specified in Section 8.4. Additionally:

- If the "tracking-address" parameter (as specified in Tables 16) is present, the MCC SHALL invoke tracking for the specified ICI using the received parameter.
- Otherwise, it SHALL invoke tracking for the specified ICI using the pre-provisioned tracking address on the MCC.

8.2.2.2 Procedures at Home CMP (or Split-CMP-Parent Where Applicable)

When the Home CMP receives an MC-1-RESOLVE_ICI_REQUEST message from an MCC, it performs the following sequential steps:

1. If an error is detected while processing the received request, see Sections 10.2.1 and 10.2.2 for the error handling procedures.
2. Otherwise, if the "ici" is managed by the Home CMP:
    a. If the "ici" is hosted on it, it SHALL follow the procedures specified in Section 8.2.2.5.2.
    b. Otherwise, in the case of a Split-CMP-Parent where the "ici" is hosted on a Split-CMP-Child served by it, it SHALL follow the procedures specified in Section 8.2.2.5.3.
3. Otherwise, if the Home CMP has the routing information for the specified "ici", it SHALL follow the procedures specified in Section 8.2.2.5.3.
4. Otherwise, if the Home CMP is configured to query an MCR, it SHALL follow the procedures specified in Section 8.2.2.5.4.
5. Otherwise, the Home CMP SHALL set the 'status" to "MC_CANNOT_RESOLVE_ICI" and send the MC-ERROR message as specified in Section 10.2.2 to the MCC.

8.2.2.3 Procedures at the Remote CMP (or Split-CMP-Parent or Child, as applicable)

When the Remote CMP receives an MC-3-RESOLVE_ICI_REQUEST message from another CMP, it will perform the following sequential steps:

1. If an error is detected while processing the received request, see Sections 10.2.1 and 10.2.2 for the error handling procedures.
2. Otherwise, if the "ici" is managed by the Remote CMP:
    a. If the "ici" is hosted on it, it SHALL follow the procedures specified in Section 8.2.2.5.2.
    b. Otherwise, in the case of a Split-CMP-Parent where the "ici" is hosted on a Split-CMP-Child served by it, it SHALL follow the procedures specified in Section 8.2.2.5.3.

Steps 3 and 4 are only required if the Remote CMP is not the Resolving CMP and business policies allow it to further route the MC-3-RESOLVE_ICI_REQUEST message.

3. Otherwise, if the Remote CMP has the routing information for the specified "ici", it SHALL follow the procedures specified in Section 8.2.2.5.3.
4. Otherwise, if the Remote CMP is configured to query an MCR, it SHALL follow the procedures specified in Section 8.2.2.5.4.
5. Otherwise, the Remote CMP SHALL set the 'status" to "MC_CANNOT_RESOLVE_ICI" and send the MC-ERROR message as specified in Section 10.2.2 to the requestor CMP.

8.2.2.4 Procedures at MCR

When the MCR receives an MC-2-ROUTE_ICI_REQUEST message from a CMP, it performs the following sequential steps:

1. If an error is detected while processing the received request, see Sections 10.2.1 and 10.2.2 for the error handling procedures.
2. Otherwise, the MCR SHALL retrieve the network address associated with the ICI in the "ici" and generate the MC-2-ROUTE_ICI_RESPONSE as specified in Table 20 in Section 10.4.1.2.
3. The MCR SHALL send the MC-2-ROUTE_ICI_RESPONSE message to the CMP.

8.2.2.5 Common CMP Procedures for Code Resolution

The following sub-sections describe procedural steps referenced in Sections 8.2.2.2 and 8.2.2.3.

8.2.2.5.1 Setting the Parameters for ICI Tracking

This section describes the procedures followed by a CMP to set the "trackingindicator" and the "trackingaddress" parameters in its response (either the MC-1-RESOLVE_ICI_RESPONSE message to the MCC or the MC-3-RESOLVE_ICI_RESPONSE message to another CMP):

- If the CMP is the Home CMP and does not support tracking of ICIs as specified in Section 8.4, it SHALL set the "trackingindicator" to 0. This is independent of whether it receives a "trackingaddress" as part of an MC-3-RESOLVE_ICI_RESPONSE message. The "trackingaddress" SHALL NOT be present in the MC-1-RESOLVE_ICI_RESPONSE message.
- Otherwise, if the CMP is the Home CMP and supports tracking as specified in Section 8.4 and the specified ICI is to be tracked, the Home CMP SHALL set the "trackingindicator" to 1.
    - If the "trackingaddress" is present in an MC-3-RESOLVE_ICI_RESPONSE message and in accordance with the Home CMP business policies, it SHALL include the "trackingaddress" received in the MC-3-RESOLVE_ICI_RESPONSE message. If the Home CMP is interested in receiving tracking information, it SHALL prepend its designated tracking server address to the received "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message. Otherwise, the Home CMP SHALL set the "trackingaddress" parameter to the received "trackingaddress" value, subject to local policy.
    - If the "trackingaddress" is not present in an MC-3-RESOLVE_ICI_RESPONSE message, it SHALL set the "trackingaddress" to the appropriate address if there is no pre-provisioned tracking address on the MCC or it does not wish to use the pre-provisioned tracking address on the MCC for tracking the specified ICI.
- Otherwise, if the CMP is not the Home CMP and supports tracking of ICIs as specified in Section 8.4 and the specified ICI is to be tracked, the CMP SHALL prepend its designated tracking server address to the received "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message. If there is no "trackingaddress" present in the MC-3-RESOLVE_ICI_RESPONSE message, the Remote CMP SHALL set the "trackingaddress" to its designated tracking server address when it wants to track the ICI.
- A non-Home Resolving CMP that is interested in receiving tracking information SHALL set the "trackingaddress" to its designated tracking server address.

8.2.2.5.2 The Resolving CMP

This section describes the procedures followed by the Resolving CMP for a specific "ici":

- Based on the MC Service Policy conditions, if any, as specified in Section 8.2.3, the Resolving CMP SHALL follow the error handling procedures in Sections 10.2.2 if any of the applicable MC Service Policy conditions is not satisfied.
- Otherwise, the Resolving CMP SHALL follow the procedures specified in Section 8.2.2.5.1 to set the parameters for ICI tracking.
- The Resolving CMP SHALL generate the MC-1-RESOLVE_ICI_RESPONSE message as specified in Table 16 if it is the Home CMP, and send the message to the MCC; otherwise, it SHALL generate the MC-3-RESOLVE_ICI_RESPONSE as specified in Table 22 and send the message to the requestor CMP.

8.2.2.5.3 Sending the MC-3-RESOLVE_ICI_REQUEST and Processing the Response

This section describes the procedures followed by a CMP to send the MC-3-RESOLVE_ICI_REQUEST message to a Remote CMP based on the incoming Code Resolution request message and process the response from the Remote CMP.

- The CMP generates the MC-3-RESOLVE_ICI_REQUEST message as specified in Section 10.5.1.1:
  - The request MAY contain the following optional parameters as specified in Table 21: “apikeyid”, “signature”, “addr”.
  - The request SHALL contain all parameters present in the incoming Code Resolution request message that are relevant to the Code Resolution.
  - If the incoming Code Resolution message is an MC-1-RESOLVE_ICI_REQUEST message (e.g., the CMP is the Home CMP) and if the value of the “optout” is “FALSE”, the request MAY contain additional user personal data and location information if they are available in the Home CMP.
- The CMP sends the MC-3-RESOLVE_ICI_REQUEST message to the Remote CMP and waits for the response.
  - If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.2 for the error handling procedures.
  - Otherwise, the CMP SHALL follow the procedures specified in Section 8.2.2.5.1 to set the parameters for ICI tracking.
  - The CMP SHALL generate the MC-1-RESOLVE_ICI_RESPONSE message as specified in Table 16 if it is the Home CMP, and send the message to the MCC; otherwise, it SHALL generate the MC-3-RESOLVE_ICI_RESPONSE as specified in Table 22 and send the message to the requestor CMP.

.

8.2.2.5.4 Sending the MC-2-ROUTE_ICI_REQUEST and Processing the Response

This section describes the procedures followed by a CMP to send the MC-2-ROUTE_ICI_REQUEST message to an MCR and process the response from that MCR.

- The CMP sends the MC-2-ROUTE_ICI_REQUEST message as specified in Section 10.4.1.1 to the MCR and waits for the response.
  - If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.2 for the error handling procedures.
  - Otherwise, the CMP SHALL use the returned “addr” (as specified in Table 20) to identify the Remote CMP to receive the Code Resolution request and follow the procedures in Section 8.2.2.5.3.

8.2.3 MC Service Policy Management

Mobile Code (MC) Service Policy provides a set of policy conditions that convey any service level constraints that are placed on Mobile Code Resolution. For each Indirect Code, the Resolving CMP specifies the action associated with the ICI to convey either content, or an URI to access service or content, in coordination with the Mobile Code Publisher. To meet the

business requirements of the Mobile Code Publisher, the Resolving CMP MAY specify optional MC Service Policy conditions that must be satisfied prior to resolution of the ICI.

8.2.3.1 MC Service Policy Specification

MC Service Policy conditions are optionally supported for each ICI, or a range of ICIs; if supported, the following procedures apply:

1. Code Resolution request validity period of the ICI, if specified, SHALL comprise of a "START DATE –TIME" and an "END DATE-TIME" in according with ISO 8601 [ISO8601] format, as follows:

   ICI START DATE-TIME is: YYYY-MM-DDThh:mm:ss

   ICI END DATE-TIME is: YYYY-MM-DDThh:mm:ss

   Note: "T" is a separator; it appears literally in the string, to indicate the beginning of the time element.

2. Code Resolution request geographic area origin of the ICI, if specified, SHALL comprise of either one, or both, of the following geographic location identification information:

   a) MNO network identifier (either 'home', 'roamed to', or both), if available, of the mobile device subscriber.

   b) LOC Data, if available, of the mobile subscriber device at the time the Indirect Code is scanned.

   Due to variations of the syntax used to represent the above geographic location identification information by the MCC, mobile device and network, the Resolving CMP is expected to recognise a wider range of syntaxes used in the location information included in the MC-1-RESOLVE_ICI_REQUEST message or MC-3-RESOLVE_ICI_REQUEST message (as applicable) when comparing with the syntax used for the location information policy conditions specified and stored for an ICI or range of ICIs. Such details are implementation specific and not specified further in the MC TS.

8.2.3.2 MC Service Policy Enforcement

When MC Service Policy has been specified for an ICI, Code Resolution SHALL only be completed by the Resolving CMP if all applicable MC Service Policy conditions are satisfied.

The following MC Service Policy enforcement action is taken for each ICI, or a range of ICIs, by the Resolving CMP:

1. If Code Resolution request validity period policy condition has been specified for the ICI, or a range of ICIs, the Resolving CMP verifies the arrival time of the MC-1-RESOLVE_ICI_REQUEST message or MC-3-RESOLVE_ICI_REQUEST message (as applicable).
   a. If the arrival time as above falls within the range of the validity period policy conditions as specified in Section 8.2.3.1 (1) stored for the ICI, or range of ICIs, then Code Resolution SHALL be completed and the information retrieved.
   b. If the arrival time as above falls outside of the range the validity period policy conditions as specified in Section 8.2.3.1 (1) stored for the ICI, or range of ICIs, then Code Resolution SHALL NOT be completed and an appropriate MC-ERROR message as specified in Table 13 SHALL be returned.
2. If Code Resolution request geographic area origin policy condition has been specified for the ICI, or a range of ICIs, the Resolving CMP verifies the geographic location identification information included in the MC-1-RESOLVE_ICI_REQUEST message or MC-3-RESOLVE_ICI_REQUEST message (as applicable), if available.
   a. If the geographic location identification information received as above falls within the range of geographic area origin policy conditions as specified in Section 8.2.3.1 (2) stored for the ICI, or range of ICIs, then Code Resolution SHALL be completed and the information retrieved.
   b. If the geographic location identification information received as above falls outside of the range of geographic area origin policy conditions as specified in Section 8.2.3.1 (2) stored for the ICI, or range of ICIs, then Code Resolution SHALL NOT be completed and an appropriate MC-ERROR message as specified in Table 13 SHALL be returned.

c. If no geographic location identification information as above is received, this constitutes an indeterminate condition. Under such a case, it is subject to local policy agreement between the Resolving CMP and the Code Publisher whether Code Resolution is to be completed, or not.

8.3 Code Transfer Procedures

Code Transfer allows an MCP to change from one Resolving CMP to another for the ICI or ICI blocks assigned to it.

Code Transfer is only applicable to Indirect Code because it involves changing the Resolving CMP for the ICI or ICI block allocated to an MCP. The reasons for an MCP to transfer its ICI or ICI block may be because the new Resolving CMP offers better quality of service, cheaper price and/or more features in resolving the ICI or ICI block.

Support of Code Transfer is optional so each community of interest decides if to support Code Transfer within the community of interest or not. Code Transfer can be supported by involving an MCR or without an MCR (e.g., by multi-lateral agreement) so each community of interest chooses if to involve an MCR in managing Code Transfer if it decides to support Code Transfer.

This section describes how Code Transfer is accomplished by involving an MCR in managing the Code Transfer by using the REST APIs described in Sections 10.7.1, 10.7.2, 10.8.1 and 10.8.2. Using multi-lateral agreement or non-REST APIs to support Code Transfer or supporting inter-MCR Code Transfer is outside the scope of this document. For example, an email can be used to inform the old Resolving CMP about the successful completion of the Code Transfer instead of using the REST APIs.

NOTE: The procedures in this section assume that the involved CMPs (or the Split-CMP-Parents) are in business.

8.3.1 Overview of Code Transfer Procedures

An MCP who wants to change to a new Resolving CMP first gets an approval token from the current (old) Resolving CMP. The old Resolving CMP reports the to-be-transferred out ICI or ICI block and the associated token to the MCR. The MCP then approaches the new Resolving CMP about Code Transfer and provides its assigned ICI or ICI block, the token and how the ICIs are to be resolved. The new Resolving CMP then submits a Code Transfer request to the MCR. For a new or an old Resolving Split-CMP-Child, its Split-CMP-Parent is in the path to handle the messages exchanged between the Resolving Split-CMP-Child and MCR.

When the MCR receives the Code Transfer indication from the old Resolving CMP (or Split-CMP-Parent where applicable) for an ICI or ICI block, it stores the token and other information (e.g., timestamp) associated with the to-be-transferred ICI or ICI block. When the MCR receives the Code Transfer request from the new Resolving CMP (or Split-CMP-Parent where applicable), it compares the token received in the request against the stored token. If the tokens match, the Code Transfer is successful and the MCR updates the database so that the network address of the new Resolving CMP (or Split-CMP-Parent where applicable) becomes effective for the transferred ICI or ICI block. The MCR responds to the request to confirm the Code Transfer with the new Resolving CMP (or Split-CMP-Parent where applicable), and notifies the old Resolving CMP (or Split-CMP-Parent where applicable) about the successful completion of the Code Transfer. The Code Transfer fails if the tokens do not match, or if the old Resolving CMP (or Split-CMP-Parent) has not provided the token for the to-be-transferred ICI or ICI block to the MCR when the MCR receives the Code Transfer request from the new Resolving CMP (or Split-CMP-Parent).

When both the old Resolving Split-CMP-Child and new Resolving Split-CMP-Child are served by the same Split-CMP-Parent, the Split-CMP-Parent may not need to report the Code Transfer to the MCR if the policies within its community of interest allow that. The Split-CMP-Parent is responsible for notifying the old Resolving Split-CMP-Child about the successful completion of the Code Transfer.

8.3.2 Specific Code Transfer Procedures

8.3.2.1 Procedures at Old Resolving CMP

8.3.2.1.1 Code Transfer request procedures

After assigning and storing a token to an MCP that requested to transfer its assigned ICI or ICI block or when redoing the procedures due to a prior failure to complete the Code Transfer request procedures, the old Resolving CMP performs the following procedures:

1. In the case of the old Resolving CMP, it generates the MC-5-CODE_TRANSFER_REQUEST message as specified in section 10.7.1.1, sends the message to the MCR and waits for the response. In the case of the old Resolving Split-CMP-Child, it generates the MC-6-CODE_TRANSFER_ REQUEST message as specified in section 10.8.1.1, sends the message to the Split-CMP-Parent and waits for the response.
    a. If an error is detected in the received response including the receipt of the MC-ERROR message, see section 10.2.3 for the error handling procedures.
    b. Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message in the case of the old Resolving CMP or MC-6-CODE_TRANSFER_RESPONSE message in the case of the old Resolving Split-CMP-Child. The old Resolving CMP SHALL mark "confirmation pending" for the to-be-transferred out ICI or ICI block.

8.3.2.1.2 Code Transfer confirmation procedures

When receiving the MC-5-TRANSFER_CONFIRMATION_REQUEST message from the MCR in the case of the old Resolving CMP or the MC-6-TRANSFER_CONFIRMATION_REQUEST message from the old Split-CMP-Parent in the case of the old Resolving Split-CMP-Child, the old Resolving CMP performs the following procedures:

1. If an error is detected while processing the received request, see section 10.2.1 and 10.2.3 for the error handling procedures.
2. Otherwise, the old Resolving CMP SHALL mark "transfer out confirmed" for the transferred-out ICI or ICI block or remove information related to the transferred-out ICI or ICI block.
3. In the case of the old Resolving CMP, it SHALL generate the MC-5-TRANSFER_CONFIRMATION_RESPONSE message as specified in section 10.7.2.2 and send the message to the MCR. In the case of the old Resolving Split-CMP-Child, it SHALL generate the MC-6- TRANSFER_CONFIRMATION_RESPONSE message as specified in section 10.8.2.2 and send the message to the old Split-CMP-Parent.

8.3.2.2 Procedures at Old Split-CMP-Parent

8.3.2.2.1 Code Transfer request procedures

When receiving the MC-6-CODE_TRANSFER_REQUEST message from the old Resolving Split-CMP-Child, the old Split-CMP-Parent performs the following procedures:

1. If an error is detected while processing the received request, see sections 10.2.1 and 10.2.3 for the error handling procedures.
3. Otherwise, the old Split-CMP-Parent SHALL store the token or replace the stored token with the value in the "token" received from the request for the ICI or ICI block indicated in the received "ici" or "icibk".
4. The old Split-CMP-Parent SHALL generate the MC-5-CODE_TRANSFER_REQUEST message as specified in section 10.7.1.1, send the message to the MCR and wait for the response.

a. If an error is detected in the received response including the receipt of the MC-ERROR message, see section 10.2.3 for the error handling procedures.

b. Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message. The old Split-CMP-Parent performs the following steps:

i. SHALL mark "pending confirmation" for the to-be-transferred-out ICI or ICI block.

ii. Generate the MC-6-CODE_TRANSFER_RESPONSE message as specified in section 10.8.1.2 and send the message to the old Resolving Split-CMP-Child.

8.3.2.2.2 Code Transfer confirmation procedures when receiving the MC-5-TRANSFER_CONFIRMATION_ REQUEST message from the MCR

When receiving the MC-5-TRANSFER_CONFIRMATION_REQUEST message from the MCR, the old Split-CMP-Parent performs the following procedures:

1. If an error is detected while processing the received request, see sections 10.2.1 and 10.2.3 for the error handling procedures.
2. Otherwise, the old Split-CMP-Parent performs the following steps:
    a. SHALL mark "transfer out confirmed, pending notification" for the transferred-out ICI or ICI block.
    b. Execute the Code Transfer confirmation procedures in Section 8.3.2.2.3 to notify the old Resolving Split-CMP-Child about the successful completion of the Code Transfer of an ICI or ICI block.

8.3.2.2.3 Code Transfer confirmation procedures initiated by the old Resolving Split-CMP-Parent

When invoked upon the successful completion of the Code Transfer of an ICI or ICI block or redoing the procedures due to a prior failure to complete the Code Transfer confirmation procedures, the old Split-CMP-Parent performs the following procedures:

1. The old Split-CMP-Parent generates the MC-6-TRANSFER_CONFIRMATION_REQUEST message as specified in Section 10.8.2.1, sends the message to the old Resolving Split-CMP-Child and waits for the response.
    a. If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.3 for the error handling procedures.
    b. Otherwise, process the received MC-6-TRANSFER_CONFIRMATION_RESPONSE message. The old Split-CMP-Parent SHALL mark "transferred out" for the transferred-out ICI or ICI block, or remove information related to the transferred-out ICI or ICI block.

Note: This process is not necessary if any other non-web service means (e.g. email notification) is used.

8.3.2.3 Procedures at MCR

8.3.2.3.1 Code Transfer request procedures

When receiving the MC-5-CODE_TRANSFER_REQUEST message from the old or new Resolving CMP (or Split-CMP-Parent where applicable), the MCR performs the following procedures:

1. If an error is detected while processing the received request, see Sections 10.2.1 and 10.2.3 for the error handling procedures.
2. Otherwise, check if the request contains the "addr'.
    a. If "addr" is not present indicating that the request comes from the old Resolving CMP:

i. If the requestor CMP (or Split-CMP-Parent where applicable) is not the old Resolving CMP (or Split-CMP-Parent where applicable), the MCR SHALL set the "status" to "MC_UNAUTHORISED" and send the MC-ERROR message to the requestor CMP as specified in Section 10.2.3.

ii. Otherwise, the MCR performs the following steps:

1) SHALL store the token or replace the stored token for the to-be-transferred ICI or ICI block indicated by the "ici" or "icibk".

2) Generate the MC-5-CODE_TRANSFER_RESPONSE message as specified in Section 10.7.1.2 and send the message to the requestor CMP.

b. If "addr" is present indicating that the request comes from the new Resolving CMP (or the Split-CMP-Parent where applicable):

i. If there is not a stored token associated with the ICI or ICI block indicated in the "ici" or "icibk", or the received token does not match the stored token, the MCR SHALL set the "status" to "MC_CT_TOKEN_MISMATCH" and send the MC-ERROR message to the requestor CMP as specified in Section 10.2.3.

ii. Otherwise, the MCR performs the following procedures:

a. The MCR SHALL update the network address associated with the ICI or ICI block indicated in the "ici" or "icibk" with that in the received "addr".

b. The MCR SHALL remove the stored token for the transferred ICI or ICI block.

c. The MCR SHALL generate the MC-5-CODE_TRANSFER_RESPONSE message as specified in Section 10.7.1.2 and send the message to the requestor CMP.

d. If the old Split-CMP-Parent and new Split-CMP-Parent involved in the Code Transfer are the same, the MCR SHALL mark "transfer completed" or "normal" or remove any flag for the transferred ICI or ICI block.

e. Otherwise, the MCR SHALL mark "transferred, pending notification" for the transferred ICI or ICI block.

f. The MCR SHALL execute the Code Transfer confirmation procedures described in Section 8.3.2.3.2.

Note: This step is not necessary if any other non-web service means (e.g. email notification) is used.

8.3.2.3.2 Code Transfer confirmation procedures

When invoked upon the successful completion of the Code Transfer of an ICI or ICI block or redoing the procedures due to a prior failure to complete the Code Transfer confirmation procedures, the MCR performs the following procedures:

1. The MCR generates the MC-5-TRANSFER_CONFIRMATION_REQUEST message as specified in Section 10.7.2.1, sends the message to the old Resolving CMP (or Split-CMP-Parent where applicable) and waits for the response.

a. If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.3 for the error handling procedures.

b. Otherwise, process the received MC-5-TRANSFER_CONFIRMATION_RESPONSE message. The MCR SHALL mark "transferred and confirmed" or "normal" or remove any flag for the transferred ICI or ICI block.

8.3.2.4 Procedures at New Resolving CMP

8.3.2.4.1 Code Transfer request procedures

When requested by an MCP to transfer-in an ICI or ICI block, the new Resolving CMP performs the following procedures:

1. In the case of the new Resolving CMP, it generates the MC-5-CODE_TRANSFER_REQUEST message as specified in Section 10.7.1.1, sends the message to the MCR and waits for the response. In the case of the new Resolving Split-CMP-Child, it generates the MC-6-CODE_TRANSFER_ REQUEST message as specified in Section 10.8.1.1, sends the message to the Split-CMP-Parent and waits for the response.
    a. If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.3 for the error handling procedures.
    b. Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message in the case of the new Resolving CMP or MC-6-CODE_TRANSFER_RESPONSE message in the case of the new Resolving Split-CMP-Child. The new Resolving CMP SHALL update the database with the transferred-in ICI or ICI block and information on the MCP and how to resolve the ICI or ICI block.

8.3.2.5 Procedures at New Split-CMP-Parent

8.3.2.5.1 Code Transfer request procedures

When receiving the MC-6-CODE_TRANSFER_REQUEST message from the new Resolving Split-CMP-Child, the new Split-CMP-Parent performs the following procedures:

1. If an error is detected while processing the received request, see Sections 10.2.1 and 10.2.3 for the error handling procedures.
2. Otherwise, if the new Split-CMP-Parent is also the old Split-CMP-Parent for the to-be-transferred ICI or ICI block:
    a. If this Split-CMP-Parent did not receive the token from the old Resolving Split-CMP-Child, or the received token does not match with the stored token, the new Split-CMP-Parent SHALL set the "status" to "MC_CT_TOKEN_MISMATCH" and send the MC-ERROR message to the new Resolving Split-CMP-Child as specified in Section 10.2.3.
    b. If the value in the "token" received from the request matches with the stored token:
        i. The new Split-CMP-Parent SHALL update the database for the transferred in ICI or ICI block with the identification of the new Resolving Split-CMP-Child.
        ii. The new Split-CMP-Parent SHALL generate the MC-6-CODE_TRANSFER_RESPONSE message as specified in Section 10.8.1.2 and send the message to the new Resolving Split-CMP-Child .
        iii. The new Split-CMP-Parent SHALL mark "transferred, pending notification" for the transferred ICI or ICI block.
        iv. The new Split-CMP-Parent invokes the Code Transfer confirmation procedures in Section 8.3.2.2.3 to inform the old Resolving Split-CMP-Child about the successful completion of the Code Transfer in a separate session.

            Note: In this case, since the new Split-CMP-Parent is also the old Split-CMP-Parent, it invokes the procedures in Section 8.3.2.2.3 as the old Split-CMP-Parent.

        v. If the new Split-CMP-Parent needs not inform the MCR about the intra-Split-CMP-Parent Code Transfer, it SHALL remove the stored token for the transferred ICI or ICI block.
        vi. If the new Split-CMP-Parent needs to inform the MCR about the intra-Split-CMP-Parent Code Transfer:
            1) The new Split-CMP-Parent SHALL store the value in the "token" received from the request for the ICI or ICI block indicated in the "ici" or "icibk".

2) The new Split-CMP-Parent SHALL mark "pending report to MCR" for the transferred ICI or ICI block.

3) The new Split-CMP-Parent generates the MC-5-CODE_TRANSFER_REQUEST message as specified in Section 10.7.1.1, sends the message to the MCR and waits for the response.

   a. If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.3 for the error handling procedures

   b. Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message. The new Split-CMP-Parent SHALL remove the "pending report to MCR" flag and remove the stored token for the transferred ICI or ICI block.

3. Otherwise, the new Split-CMP-Parent SHALL store the value in the "token" and the ICI or ICI block indicated in the "ici" or "icibk" in the received request.

4. The new Split-CMP-Parent generates the MC-5-CODE_TRANSFER_REQUEST message as specified in Section 10.7.1.1, send the message to the MCR and wait for the response.

   a. If an error is detected in the received response including the receipt of the MC-ERROR message, see Section 10.2.3 for the error handling procedures

   b. Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message. The new Split-CMP-Parent performs the following steps:

      i. SHALL update the database with the transferred-in ICI or ICI block and the identification of the new Resolving Split-CMP-Child.

      ii. Generate the MC-6-CODE_TRANSFER_RESPONSE message as specified in Section 10.8.1.2 and send the message to the new Resolving Split-CMP-Child.

8.4 Tracking and Reporting Procedures

This section describes the procedures for tracking and reporting chargeable events related to Indirect Code usage.

8.4.1 Overview of Tracking and Reporting Procedures

This section describes the procedures required to track and report chargeable events. Support of tracking and reporting chargeable events is optional. Further details on message formats can be found in Sections 10.6.1.1, 10.6.1.2, 10.8.3.1 and 10.8.3.2.

During Code Resolution, CMPs involved in the resolution path that are interested in receiving tracking and reporting information can add their designated tracking addresses(es) to the resolution response. More specifically, if the Home CMP can resolve the ICI, it sets the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message to its designated tracking address(es) and sets the "trackingindicator" to "true". Otherwise, if the Home CMP cannot resolve the ICI, the Resolving CMP may set the "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message to be its designated tracking address(es). Any other Remote CMPs in the resolution path can then prepend their designated tracking addresses to the received "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message to create the subsequent MC-3-RESOLVE_ICI_RESPONSE message in the resolution path. Finally, the Home CMP can prepend its designated tracking address to the "trackingaddress" parameter received in the MC-3-RESOLVE_ICI_RESPONSE message and set the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message to the new "trackingaddress" and set the "trackingindicator" to "true".

An MCC which supports tracking and reporting uses the "trackingaddress" parameter(s) received in the MC-1-RESOLVE-ICI_RESPONSE message to send an MC-4-TRACKING_REPORT message to the tracking server(s) as indicated by the "trackingaddress" parameter(s). If no "trackingaddress" parameter(s) are available in the MC-1-RESOLVE_ICI_RESPONSE message but the "trackingindicator" is set to "true", the MCC sends an MC-4-TRACKING_REPORT message to the tracking address pre-provisioned by the Home CMP.

After receiving the tracking information in the MC-4-TRACKING_REPORT message, the tracking server as designated by the Home CMP will send an MC-6-TRACKING_REPORT message to the subsequent CMP's designated tracking server as identified by the "trackingaddress" parameter, subject to policy control and business agreements. After receiving an MC-6-TRACKING_REPORT message, each Remote CMP's designated tracking server sends an MC-6-TRACKING_REPORT message to the subsequent CMPs' designated tracking address(es) as identified by the "trackingaddress" parameter, subject to policy control and business agreements.

8.4.2 Specific Tracking and Reporting Procedures

Actions specified in sub-sections 8.4.2.1 to 8.4.2.5 are applicable only when tracking and reporting is implemented.

8.4.2.1 Procedures at MCC

In order to track chargeable events, the MCC SHALL send the MC-4-TRACKING_REPORT message to the Home CMP over the MC-4 interface. This message is used to report usage of the resolved content, applications making use of the resolved content, and device information (e.g. location).

The MC-4-TRACKING_REPORT message SHALL contain at least the Indirect Code Identifier and an identifier of the MCC. The detailed parameters of the MC-4-TRACKING_REPORT message are described in Section 10.6.1.1. Aside from data collected at the MCC, the MCC may also insert tracking and reporting data as reported by/retrieved from other applications on the device (e.g. user called a phone number retrieved from a Mobile Code that was stored in the device address book). Such actions may be reported by various ways, including by having the MCC implementation register application listeners. The means by which to gather user action data from applications are considered out of scope of this specification.

If a "trackingaddress" is present in the MC-1-RESOLVE_ICI_RESPONSE message sent from the Home CMP to the MCC, the MCC SHALL send the MC-4-TRACKING_REPORT message to the indicated "trackingaddress" associated with this ICI.

If a "trackingaddress" is not present but the *trackingindicator* is set to "true" in the MC-1-RESOLVE_ICI_RESPONSE message sent from the Home CMP to the MCC, the MCC SHALL send the MC-4-TRACKING_REPORT message to the default pre-provisioned Tracking Address by the Home CMP (see Section 9.1.1).

8.4.2.2 Procedures at Home CMP

This section describes the steps performed at the Home CMP in relation to tracking and reporting.

If the Home CMP supports tracking and reporting it SHALL set the "trackingindicator" to "true" in the MC-1-RESOLVE_ICI_RESPONSE. Otherwise, the "trackingindicator" SHALL be set to "false".

If the Home CMP is the Resolving CMP and is interested in receiving tracking information from the MCC for the specified ICI and does not want to use the pre-provisioned tracking address or no tracking address was pre-provisioned on the MCC, the Home CMP SHALL include the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message and set it to its designated tracking address(es).

Each "trackingaddress" fragment SHALL have the following format,

http://[HOME_CMP_TRACKING_ADDRESS]

where, [HOME_CMP_TRACKING_ADDRESS] represents the tracking address identifying the tracking server as designated by the Home CMP.

When the Home CMP receives an MC-3-RESOLVE_ICI_RESPONSE and is interested in receiving tracking information, it prepends its designated tracking address(es) to the received "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message. If the Home CMP is not interested in receiving tracking information, it uses the "trackingaddress" received in the MC-3-RESOLVE_ICI_RESPONSE message to set the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message.

If the "trackingaddress" parameter is not received in the MC-3-RESOLVE_ICI_RESPONSE message but the Home CMP is interested in receiving tracking information for the specified ICI, the Home CMP sets the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message to its designated tracking address(es).

8.4.2.3 Procedures at Home CMP involving Tracking Address(es)

Upon reception of the MC-4-TRACKING_REPORT message, the tracking server as designated by the Home CMP SHALL be able to remove and/or anonymise some data elements in the tracking report prior to distributing the information to subsequent entities, subject to service provider policies.

If multiple CMPs were involved in Code Resolution and are interested in receiving tracking information, the tracking server as designated by the Home CMP SHALL send the MC-6-TRACKING_REPORT message to the "trackingaddress" received in the MC-3- RESOLVE_ICI_RESPONSE identifying the subsequent entities in the reporting path. Sending of the MC-6-TRACKING_REPORT message by the tracking server as designated by the Home CMP to the next entity as identified by the next tracking address fragment in the "trackingaddress" is subject to Home CMP policy control and business agreements. The tracking server as designated by the Home CMP MAY remove this tracking address fragment if the Home CMP does not have business agreements with this entity.

8.4.2.4 Procedures at Remote CMP

When there are multiple CMPs involved in Code Resolution, the "trackingaddress" in the MC-3-RESOLVE_ICI_RESPONSE SHALL represent a combination of the tracking address fragments provided by the subsequent CMPs involved in content acquisition by way of Code Resolution which are interested in tracking chargeable events.

Each "trackingaddress" fragment SHALL have the following format,

http://[REMOTE_CMPx_TRACKING_ADDRESS]

where, [REMOTE_CMPx_TRACKING_ADDRESS] represents the tracking address identifying the tracking server at CMPx.

Under certain circumstances (e.g. as mandated by community restrictions) the [REMOTE_CMPx_TRACKING_ADDRESS] MAY be a commonly designated entity, such as, a neutral 3rd party entity in a given community.

An example of this format illustrating three CMPs involved in Code Resolution and in tracking of chargeable events is shown below:

http://www.cmp1.com/tracking?t2=http://www.cmp2.com/metrics/2009?t3=http://www.cmp3.net/report

Legend: Home CMP Tracking Address URL: http://www.cmp1.com/tracking
Next CMP Tracking Address URL: http://www.cmp2.com/metrics/2009
Resolving CMP Tracking Address URL: http://www.cmp3.net/report

Under certain circumstances, some or all [REMOTE_CMPx_TRACKING_ADDRESS_URL] fragments MAY point to a commonly designed neutral 3rd party.

If the Remote CMP is interested in receiving tracking information for the specified ICI and is not the Resolving CMP, the Remote CMP (or Split-CMP-Parent where applicable) SHALL prepend its designated tracking address(es) to the "trackingaddress" parameter of the received MC-3-RESOLVE_ICI_RESPONSE message and use this value to set the "trackingaddress" of the outgoing MC-3-RESOLVE_ICI_RESPONSE message. If the Remote CMP is not interested in receiving tracking information for the specified ICI and is not the Resolving CMP, it SHALL set the "trackingaddress" parameter of the outgoing MC-3-RESOLVE_ICI_RESPONSE message to the "trackingaddress" value that was received in the MC-3-RESOLVE_ICI_RESPONSE message.

If the Remote CMP is interested in receiving tracking information for the specified ICI and is also the Resolving CMP, the Remote CMP (or Split-CMP-Child where applicable) SHALL set the "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE to its designated tracking address(es).

8.4.2.5 Procedures at Remote CMP involving Tracking Address(es)

Upon reception of the MC-6-TRACKING_REPORT message, the tracking server as designated by the Remote CMP (or Split-CMP-Parent) SHALL be able to remove and/or anonymise some data elements in the tracking report prior to distributing the information to subsequent entities, subject to service provider policies.

The tracking server as designated by the Remote CMP (or Split-CMPs-Parent) SHALL use URL redirection to send the MC-6-TRACKING_REPORT message to the next entity in the reporting path. Sending of the MC-6-TRACKING_REPORT message by the tracking server as designated by the Remote CMP to the next entity as identified by the next tracking address fragment in the "trackingaddress" is subject to business agreements. The tracking server as designated by the Remote CMP MAY remove this tracking address fragment if the Remote CMP does not have business agreements with this entity.

9. System Overview

9.1 MCC Installing, Provisioning and Updating

MCC installation, provisioning and updating (including re-installation) processes are expected to follow existing procedures implemented for application installation, provisioning and updating by service providers or device manufacturer (in case the MCC is preloaded in the mobile device).

Examples of device application installation, provisioning and updating methods for the MCC include the following (not an exhaustive list):

1. Implementation specific OTA method.
2. OMA Device Management Enabler methods.
3. Local data connection (e.g. via a flash card, Bluetooth, data cable or docking station).
4. Other Web services supported by the provider of the MCC.

All of the methods and procedures for device application installation, provisioning and updating as mentioned above are not unique to the MCC application and are implementation specific; hence, no further details for such are specified in the MC Enabler TS.

9.1.1 MCC Configuration Parameters

Upon completion, or as part, of the MCC installation, provisioning or updating, the MCC SHALL be configured on the mobile device in order to use the MC Enabler. The specific method used to configure the MCC is out-of-scope (see Section 9.1 above).

If the MCC supports resolution of Indirect Codes, the following minimum parameters SHALL be configured in the MCC:

- Network Address (i.e. HTTP [RFC2616] URL) of the Home CMP.

If the MCC supports resolution of Indirect Codes, the following charging-related parameters MAY be configured in the MCC:

- Tracking Address of the tracking server at the Home CMP.

9.2 Handling of User Personal Data

The MCC SHALL support the ability for the user to enter and store user personal data on an ‘Opt-in’ basis. User personal data can be entered and stored either in the MCC or the Home CMP. The following user personal data SHOULD be supported at minimum:

a) Age
c) Gender
d) Postal Code/Zip Code
e) Household Income

9.2.1 MCC based solution

If user personal data or location information is available and stored locally on the MCC, it SHALL be possible for the MCC to insert available user personal data information and location information in the MC-1-RESOLVE_ICI_REQUEST message and MC-4-TRACKING_REPORT message.

If user personal data or location information has been entered and stored in the MCC, the user SHALL be able to 'Opt-in' or 'Opt-out' for each (or all) MC-1-RESOLVE_ICI_REQUEST message and MC-4-TRACKING_REPORT message.

9.2.2 Home CMP based solution

If user personal data or location information is available and stored locally on the Home CMP, it SHALL be possible for the Home CMP to insert available user personal data and/or location information in the MC-3-RESOLVE_ICI_REQUEST message and MC-6-TRACKING_REPORT message.

If user personal data or location information has been entered and stored in the Home CMP, the user SHALL be able to 'Opt-in' or 'Opt-out' for each (or all) MC-3-RESOLVE_ICI_REQUEST message and MC-6-TRACKING_REPORT message.

9.3 Security

This on MC Security includes Authentication solutions, as applicable.

The security requirements of the Mobile Codes Enabler are addressed by three separate sets of procedures:

- Between the MCC and its Home CMP, the network element the MCC communicates with.
- Between any two MC Enabler network elements (i.e., between two CMPs, or between a CMP and the MCR when applicable).
- On the Resolving CMP.

Disclaimer: The MC Enabler is intended to facilitate user access to web information via the barcode. The MC application layer makes no claims about fool-proof security of higher layer transactions (e.g. financial or other mission-critical transactions). It is advisable that higher layer transactions, such as, e-commerce applications, implement additional security safeguards as appropriate.

9.3.1 Security between the MCC and its Home CMP

This section describes an optional solution that MAY be used to authenticate the MCC to the Home CMP; if supported, the following procedures SHALL apply:

1. Secure protocol (HTTPS) between the MCC and Home CMP is used.

   Note: Use of the 'clientid' to convey a unique identifier of the MCC installation instance to the Home CMP. The exact mechanism for generating 'clientid' and processing of same is out-of-scope of this specification. For example, UUID version 5 using SHA-1 hash, or 'Sub_ID' assigned by the MNO may be used as the "clientid".

2. Use 'clientid' in conjunction with another MNO based attribute pertaining to the mobile user (e.g. MSISDN, or an alias) to create an association for authenticating the MCC as follows:

   - In case of Wi-Fi or other non-MNO network connection is used during the first-time use of the MCC, the MCC is requested to retry this scan by using an MNO network.

9.3.2 Security between two MC Enabler network elements

To meet the security requirements as applicable to communications between any two MC Enabler network elements (i.e., MC-2, MC-3, MC-5 and MC-6 interfaces) will adhere to the following:

1. Secure, dedicated & managed physical or logical transport connections (i.e. ranging from Layer 1 TDM to Layer 2/3 VPNs) between the requestor and responder network elements (i.e. CMPs or MCR) MAY be used.

2. When insecure or shared transport connections are used (e.g. public Internet connection) between the requestor and responder network elements, the following security measures apply:
    a. All communications between requestor and responder network elements SHALL use HTTPS.
    b. As part of the initial registration process, an "apikeyid" and an "apikey" SHALL be generated and provided by the responder network element (e.g. CMP, or MCR where applicable) to the requestor network element (e.g. CMP). The "apikey" is typically a shared secret key between two network elements for faster symmetric cryptography.
    c. The requestor network element SHALL calculates the digital signature as follows:
        i. SHALL concatenate the "tid", "ici" values – making it unique for each request/response, thus safe from spoofing.
        ii. SHALL use the concatenated value to generate a HMAC hash using the "apikey" provided by the responder network element.
    d. The requestor network element SHALL include the "apikeyid" and the above signature as part of every request to the responder network element.
    e. The responder network element uses the "apikeyid" to retrieve the security information associated with the requestor network element (i.e., the stored "apikey") and SHALL validate the signature before proceeding to execute the request.
    f. If authentication in step (e) fails, the responder network element SHALL not execute the request and SHALL return an appropriate error status.

9.3.3 Security on the Resolving CMP

To ensure that the ICI in the Indirect Code is not altered and is verifiable, the Resolving CMP may add a signature to an ICI for integrity check or encrypt portion of the ICI while allowing the Resolving CMP to retrieve the original ICI, when needed, and verify the ICI integrity. This type of ICIs that contain security information is called "Secure ICI" in this document. When the Resolving CMP receives the Code Resolution request that contains a Secure ICI, it retrieves the original ICI, when needed, verifies the ICI integrity and only resolve the original ICI when all checks are successful.

Since only the Resolving CMP is involved in choosing the scheme to be used for an ICI and to create, process and verify the Secure ICI, the MCC and other non-Resolving CMPs are not impacted by the scheme chosen by any Resolving CMP that decides to use Secure ICI.

Because a Secure ICI appears in the Indirect Code and a complete ICI (e.g., a transferred ICI) or portion of an ICI (e.g., non-transferred ICI where Routing Prefix can be used for routing) is used by the involved CMP(s) to route the Code Resolution request to the Resolving CMP, some guidelines are recommended below for the CMPs that plan to support Secure ICIs.

1. A secure ICI SHALL have the same Routing-Prefix field as that of the original ICI (e.g., none of the octets in the Routing-Prefix can be changed and the Routing Prefix must be sent in clear).
2. The routing of a Secure ICI SHALL NOT be changed if any portion of the Resolution-Identifier field of the original ICI is changed. This particular recommendation only applies to transferred ICIs because non-transferred ICI can be routed on the Routing Prefix of the ICI. A Secure ICI for an ICI in a transferred ICI block would need to keep the block level information unchanged so that this Secure ICI can be routed to its Resolving CMP. For an individual ICI (e.g., not in any ICI block) that has been transferred, none of the octets in the RI can be changed, and only a signature can be appended after the ICI for integrity check.
3. The maximum length of any Secure ICI SHALL NOT exceed 36 octets, the maximum length of the ICI field.
4. Any octet after the Routing-Prefix part of any Secure ICI SHALL NOT contain the value "%x04", the ICI-DT-Separator.
5. When a Secure ICI scheme is used, it SHOULD be used for all the non-transferred ICIs under a particular Routing Prefix or for all the transferred ICIs under the same ICI block. This would allow the Resolving CMP to quickly identify if the ICI in the received Code Resolution request is a Secure ICI and which Secure ICI scheme is used for that ICI.

Two examples are described in Appendix J to show how Secure ICIs can be created, processed and verified by its Resolving CMP using the same Secure ICI scheme for two ICIs with different Routing Prefix lengths.

10. Interface Definitions

10.1 General Interface Considerations

This section specifies the interfaces exposed by the various components of the MC Enabler as applicable to Indirect Codes:

- All MC Enabler interfaces (i.e. MC-1 thru MC-6) follow the procedures below:
  - Each MC interface SHALL expose a REST API [REST] web service.
  - REST API is invoked using either an HTTP POST or an HTTP GET connection request:
    - HTTP POST SHALL be used for MC-4-TRACKING _REPORT and MC-6- TRACKING_ REPORT messages
    - The URL used SHALL always point to one of the MC Enabler network components: the CMP (or Split-CMP-Parent or Split-CMP-Child where applicable) or the MCR.
    - All string parameters containing special characters or spaces SHALL be UTF-8 URL encoded. Please refer to http://www.w3schools.com/TAGS/ref_urlencode.asp for more information.
    - The USER_AGENT text string in the HTTP header SHALL be transmitted unchanged in the requests.
  - There are cases of Code Resolution routing (e.g. chained HTTP sessions) whereby worst-case scenarios might time out at the MCC application level (see Appendix G). Under such conditions, timers at the HTTP layer, MC application layer, or both affecting the MCC or CMP(s) will need to be considered. For example, Code Resolution response time-out conditions should be set to a value long enough to accommodate lower layer system propagation issues (e.g. data rate over radio interfaces, mobility management and international roaming). Management of timers for this purpose is considered out-of-scope from this specification.
  - Each REST API response follows the procedures below:
    - It SHALL be in the form of a XML 1.0 document delivered using the HTTP protocol.
    - The encoding of all these XML documents SHALL be “UTF-8”.
    - The root element of all these XML documents SHALL be “envelope”.
    - Unless otherwise specified, the HTTP header information SHALL contain the 200 OK HTTP status code for all requests that were completed even if the request was not successfully executed, e.g., the ICI was not resolved by the CMP.
      - The HTTP 204 NO CONTENT status code SHALL be used in response to the MC-4-TRACKING_REPORT and MC-6-TRACKING_REPORT messages that were successfully received
      - All other HTTP status codes are expected to be handled by underlying web server platform and are outside the scope of this specification.
  - Each MC web service SHALL have a distinct URL for the request based on the type of web service.
    - The MC Enabler components (i.e. MCC, CMP and MCR) SHALL support the parsing of XML 1.0 documents.

10.2 Error Handling

This section describes error handling procedures for the MC Enabler. Error handling procedures common to Code Resolution, Code Transfer and tracking reporting are described in Section 10.2.1. The procedures specific to Code Resolution are described in Section 10.2.2. The procedures specific to Code Transfer are described in Section 10.2.3.

In case of an unsuccessful execution of the requested MC web service, the response SHALL contain an "mc-error" element as specified in Table 13.

A complete list of MC error status codes and descriptions along with the mapping of the error status codes to specific MC web services is available in Table 14.

Parameter	Requirement	Occurrences	Type	Description
tid	Optional	0..1	String	The "tid" allows the responding entity and the requesting entity to reconcile the transactions at a later date, if needed. It is optional on the MC-1 and MC-4 interface responses but SHALL be present for all other interfaces.
status	Mandatory	1	String	The "status" specifies the type of failure in a brief but descriptive textual form. The value of the MC status code is structured as follows: MC_<text> - where <text> is a brief descriptive text string, e.g., MC_MISSING_PARAMS, MC_INVALID_ICI, etc.
description	Optional	0..1	String	The "description" provides a more detailed description of the failure, providing a finer granularity of the error "status".

Table 13: MC Error Response

Status			Applies to							Description
	MC-1_RESOLVE_ICI	MC-2_ROUTE_ICI	MC-3_RESOLVE_ICI	MC-4_TRACKING_REPORT	MC-5_CODE_TRANSFER	MC-5_TRANSFER_CONFIRMATION	MC-6_TRACKING_REPORT	MC-6_CODE_TRANSFER	MC-6_TRANSFER_CONFIRMATION	
MC_UNAUTHORISED	X	X	X	X	X	X	X	X	X	The request could not be authenticated or some other security violation occurred.
MC_SERVICE_UNAVAILBLE	X	X	X	X	X	X	X	X	X	The requested service is currently unavailable (due to maintenance or other server downtime or for old unsupported requests).
MC_MISSING_PARAMS	X	X	X	X	X	X	X	X	X	The request is missing required parameters.
MC_INVALID_PARAMS					X	X		X	X	The request contains invalid parameters (e.g. both "ici" and "icibk" are present in a request).
MC_INVALID_ICI	X	X	X	X	X	X	X	X	X	The specified ICI (or ICI block) is unknown or invalid and cannot be resolved.
MC_ INACTIVE_ICI	X	X	X		X			X		The specified ICI (or ICI block) is

										inactive (blocked for inappropriate content, part of an expired campaign or transferred out).
MC_FRAUDULENT_ICI	X		X							The specified ICI fails the authentication check and cannot be used.
MC_ CANNOT_RESOLVE_ICI	X		X							The specified ICI cannot be resolved because of a network level failure or because the ICI has been transferred.
MC_TOO_MANY_HOPS			X							The specified ICI cannot be resolved – resolution attempt stopped due to too many hops
MC_ CT_TOKEN_MISMATCH					X			X		The tokens in the Code Transfer requests do not match.
MC_ CT_NOT_SUPPORTED					X			X		Code Transfer is not supported for the specified ICI (or ICI Block).
MC_ CT_ NOT_AVAILABLE					X			X		Code Transfer is not available at this time for the specified ICI (or ICI Block).
MC_ CT_ NOT_REQUESTED						X			X	Code Transfer has not been requested for the specified ICI (or ICI Block).

Table 14: Mapping between Status Codes and MC Interface Messages

10.2.1 Common Error Handling Procedures

This section describes the general error handling procedures that are referred to in Sections 8.2 through 8.4 and how to set the "status" value in an outbound MC-ERROR message by the MC Enabler network components: the CMP (or Split-CMP-Parent or Split-CMP-Child where applicable) or the MCR.

An MC Enabler network component (the responder network component) performs the following when an error is detected while processing a received request but excluding the case when an error is received for a sent request:

1. The responder network component SHALL set the "status" to
    - "MC_UNAUTHORISED" if the requestor (e.g., MCC or an MC Enabler network component) is not authorised to access the responder network component. Examples include:
        - There is no business agreement between the requestor and responder network component.
        - The requestor fails the authentication when the "appid" and "signature" are present in the received request but the "signature" value is invalid.
        - The requestor is required to include the "appid" and "signature" based on the interface agreement but fails to include the two parameters in the received request.
    - "MC_MISSING_PARAMS" if any of the mandatory parameters is missing.
    - "MC_SERVICE_UNAVAILABLE" if there is a problem (e.g., overload or database access problem) to handle the request at any time during the request processing.
    - "MC_INVALID_ICI" if the ICI in the received "ici" is known to be invalid.
    - "MC_INACTIVE_ICI" if the ICI in the received "ici" is known to be inactive currently (e.g., outside the campaign period).
2. The responder network component SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

10.2.2 Code Resolution Specific Error Handling Procedures

This section describes the error handling procedures that are specific to the Code Resolution process and are referred to in Section 8.2 and how to set the "status" value in an outbound MC-ERROR message by the MC Enabler network components: the CMP (or Split-CMP-Parent or Split-CMP-Child where applicable) or the MCR.

The responder network component performs the following when an error is detected while processing a received request but excluding the case when an error is received for a sent request:

1. The responder network component sets the "status" appropriately when one of the errors below is detected.
    - Since several CMPs (or the Split-CMP-Parents when applicable) can be involved in routing the Code Resolution request (see Appendix G) for a specified ICI, a loop could be formed when some involved CMPs (or the Split-CMP-Parents when applicable) have incorrect routing information for the specified ICI. All CMPs (or the Split-CMP-Parents when applicable) are recommended to support some loop-prevention mechanisms to detect looped routing. Applying the loop-prevention mechanisms is considered out-of-scope from this specification.

      If the responder network component supports loop-prevention and detects looped routing, it SHALL set the "status" to "MC_TOO_MANY_HOPS" if the requestor is not an MCC, or to "MC_CANNOT_RESOLVE_ICI" if the requestor is an MCC. The responder network component SHALL NOT forward the newly received Code Resolution request. This action SHALL also be done for the requestor associated with the previously received Code Resolution request.

    - Some CMPs (or Split-CMP-Children when applicable), as the Resolving CMPs, may support the Secure ICI discussed in Section 9.3.3. The procedures to receive and identify a Secure ICI, regenerate the ICI and verify it with the original ICI are out-of-scope from this specification.

      If the responder network component is the Resolving CMP that supports Secure ICI and the "ici" in the received Code Resolution request is a Secure ICI that fails the authentication check, it SHALL set the "status" to "MC_ FRAUDULENT_ICI".

    - The responder network component SHALL set the "status" to "MC_CANNOT_RESOLVE_ICI" if the Code Resolution request cannot be completed for any other reason not specified in Sections 10.2.1 and 10.2.2 (e.g., no routing information) for the ICI in the received "ici".
2. The responder network component SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

The responder network component performs the following when an error is received for a forwarded Code Resolution request:

1. If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following:
    a. Record the tid mis-match related information.
    b. If there is a received request:
        i. SHALL set the "status" to "MC_CANNOT_RESOLVE_ICI".
        ii. SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.
2. If the MC-ERROR message with the correct "tid" is received, the responder network component performs the following:
    a. Record the error related information.
    b. If there is a received request:
        i. SHALL set the "status" to

- the same received error if the "status" in the received MC-ERROR message is "MC_CANNOT_RESOLVE_ICI", "MC_INVALID_ICI", "MC_INACTIVE_ICI" or "MC_FRAUDULENT_ICI".
- the same received error if the "status" in the received MC-ERROR message is "MC_TOO_MANY_HOPS" and if the requestor is not an MCC.
- "MC_CANNOT_RESOLVE_ICI" in all other cases.

ii. SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

10.2.3 Code Transfer Specific Error Handling Procedures

This section describes the error handling procedures that are specific to Code Transfer process and are referred to in Section 8.3 and how to set the "status" value in an outbound MC-ERROR message by the MC Enabler network components: the CMP (or Split-CMP-Parent or Split-CMP-Child where applicable) or the MCR.

An MC Enabler network component (the responder network component) performs the following when an error is detected while processing a received request but excluding the case when an error is received for a sent request:

1. The responder network component SHALL set the "status" to
   - "MC_MISSING_PARAMS" if both the "ici" and "icibk" are absent in the received request.
   - "MC_INVALID_PARAMS" if both the "ici" and "icibk" are present in the received request.
   - "MC_UNAUTHORISED" if the requestor submits a Code Transfer request to transfer out an ICI or ICI block but is not authorized to do so (e.g., not the Resolving CMP for that ICI or ICI block).
   - "MC_INVALID_ICI" if the ICI block in the received "icibk" is known to be invalid.
   - "MC_INACTIVE_ICI" if the ICI block in the received "icibk" is known to be inactive currently (e.g., outside the campaign period).
   - "MC_CT_NOT_SUPPORTED" if the responder network component receives a Code Transfer request but it does not support Code Transfer.
   - "MC_CT_NOT_REQUESTED" if the ICI in the "ici" or ICI block in the "icibk" in the received code confirmation request is known but no Code Transfer has been requested for that ICI or ICI block.
   - "MC_CT_TOKEN_MISMATCH" if there is token mis-match problem. Examples include:
     - The token received in the Code Transfer request from the new Resolving CMP does not match with the token received from the old Resolving CMP.
     - A Code Transfer request is received from the new Resolving CMP but the old Resolving CMP has not provided the token.
   - "MC_CT_NOT_AVAILABLE" if the Code Transfer request cannot be completed for any other reason not specified in Section 10.2.1 and 10.2.3 for the ICI in the received "ici" or ICI block in the received "icibk".
2. The responder network component SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

The responder network component performs the following when an error is received for a sent request:

1. If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following:
   a. Record the tid mis-match related information.
   b. If there is a received request:

i. SHALL set the "status" to "MC_CT_NOT_AVAILABLE".

ii. SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

2. If the MC-ERROR message with the correct "tid" is received, the responder network component SHALL perform the following:
   a. Record the error related information.
   b. If there is a received request:
      i. SHALL set the "status" to
         - the same error if the "status" in the received MC-ERROR message is "MC_CT_NOT_AVAILABLE", "MC_INVALID_ICI", "MC_INACTIVE_ICI", "MC_CT_NOT_SUPPORTED" or "MC_CT_TOKEN_MISMATCH".
         - "MC_CT_NOT_AVAILABLE" in all other cases.
      ii. SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.

10.3 MC-1 Interface

The MC-1 interface is used for the transfer of latency-critical information.

The MC-1 interface SHALL support the following REST APIs:

- MC-1-RESOLVE_ICI web service.

10.3.1 MC-1-RESOLVE_ICI Web Service

10.3.1.1 Resolve ICI Request

The MC-1-RESOLVE_ICI web service request is made as specified below:

- The URL in the request SHALL be the MC-1-RESOLVE_ICI_REQUEST_URL that is currently configured in the MCC.
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.
- The "cc" SHALL be present when the "post" is present.

Parameter	Requirement	Occurrences	Type	Description
ici	Mandatory	1	String	The "ici" contains the value of the ICI to be resolved by the Home CMP
appid	Mandatory	1	String	The "appid" uniquely identifies the MCC software version as assigned by the MCC vendor.
enablerver	Mandatory	1	String	The "enablerver" indicates the OMA MC Enabler version, as defined as part of the Section 8.1 - Data Format.
clientid	Mandatory	1	String	The "clientid" is used for identifying an instance

				of the MCC installation on the specific device. This parameter is generally used by the Home CMP only. 'clientid' may be referred to as 'user id' in some application development environments.
btype	Optional	0..1	String	The "btype" identifies the barcode type (Symbology) of the barcode that was decoded by the MCC. This may be "QR", "DM", "EZ", "1D", etc.
optout	Mandatory	1	Boolean	The "optout" is set to: i) "TRUE" when the user has opted out to include the user personal data and location information in the Code Resolution request; and ii) "FALSE" when the user has opted in to include the user personal data and location information in the Code Resolution request.
cc	Optional	0..1	String	The "cc" identifies the alpha-2 country code [ISO3166-1] that is associated with the "post".
post	Optional	0..1	String	The "post" identifies the postal code or zip code.
age	Optional	0..1	String	The "age" provides the age information. It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range (e.g., 22-55) or a free text phrase (e.g., "young" or "retired") in the language associated with "cc" up to 20 octets long.
income	Optional	0..1	String	The "income" provides the household income information. A numeric value, when provided, is tied to the currency associated with the "cc". It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with "<" or ">" (e.g., <30,000 or >100,000) or a free text phrase (e.g., "middle-class" or "rich") in the language associated with "cc" up to 20 octets long.
gender	Optional	0..1	String	The "gender" provides gender information. It can be "female" or "male".
locationinfo	Optional	0..1	String	Provides the user's LOC Data (e.g. latitude and longitude) at the time the Mobile Code was scanned.
networkidhome	Optional	0..1	String	The home MNO Identifier of the user's device.
networkidroam	Optional	0..1	String	The roamed-to MNO Identifier from where the Mobile Code was scanned.

Table 15: MC-1-RESOLVE_ICI_REQUEST Message

10.3.1.2 MC-1 RESOLVE_ICI_RESPONSE Message Structure

Parameter	Requirement	Occurrences	Type	Description
codecontentset	Mandatory	1	Complex	The resolved content as specified in Section 10.3.1.2.1. This parameter SHALL be present on the successful resolution of the "ici".
contentdescription	Optional	0..1	String	Free text describing the resolved content for user consumption (e.g. for displaying to the user).
trackingindicator	Mandatory	1	Boolean	Indicates whether to track content usage for accounting purposes.
trackingaddress	Conditional	0..n	URI	URL specifying a location to which to send tracking data. Home CMP SHALL have full control over this parameter and is likely to enforce that the tracking server in the Home CMP domain is the first entity to receive this data. Present if "trackingindicator" is true, is allowed by local policy and any one of the following conditions is true : (1) There is no pre-provisioned tracking address on the MCC. (2) Home CMP wants to uitilise a different tracking address from the pre-provisioned tracking address for this particular ICI. (3) "trackingaddress" is present in the MC-3-RESOLVE_ICI_RESPONSE.

Table 16: MC-1-RESOLVE_ICI_RESPONSE Message

10.3.1.2.1 Structure of the "codecontentset" and "codecontent" parameters

In the case of a successful execution of the MC-1-RESOLVE_ICI web service, the response SHALL contain a "codecontentset" parameter as specified in Table 17.

Parameter	Requirement	Occurrences	Type	Description
codecontent	Mandatory	1..n	Complex	The resolved content items as specified below in Table 18. One or more “codecontent” parameters SHALL be present.

Table 17: Structure of the “codecontentset” Parameter

Parameter	Requirement	Occurrences	Type	Description
type	Mandatory	1	String	Specifies an open, documented XML schema type including those defined in the XML namespace "http://www.openmobilealliance.com/oma-mc/1.0". Examples include a URL, contact, telephone number, etc.
title	Optional	0..1	String	The title of the code to be displayed on the MCC.
contentelement	Mandatory	1..n	Complex	One or more XML elements that constitute the “codecontent”.

Table 18: Structure of the “codecontent” Parameter

10.3.1.3 Resolve ICI Failure

The MC-1-RESOLVE_ICI web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The “tid” SHALL NOT be present.
- One of the possible “status” errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_ICI
  - MC_INACTIVE_ICI
  - MC_CANNOT_RESOLVE_ICI
  - MC_FRAUDULENT_ICI

10.4 MC-2 Interface

The MC-2 interface is used for the transfer of latency-critical information.

The MC-2 interface SHALL support the following REST API:

- MC-2-ROUTE_ICI web service.

10.4.1 MC-2-ROUTE_ICI Web Service

10.4.1.1 Route ICI Request

The MC-2-ROUTE_ICI web service request is made as specified below:

- The URL in the request SHALL be the MC-2-ROUTE_ICI_REQUEST_URL that is currently configured in the CMP (or the Split-CMP/Parent where applicable).
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the CMP (or the Split-CMP-Parent where applicable) and MCR to reconcile code routing transactions at a later date, if needed.
ici	Mandatory	1	String	The "ici" contains the value of the ICI to be used by the MCR.
apikeyid	Optional	0..1	String	The "apikeyid" is used by the MCR to retrieve security information associated with the requestor CMP (or Split-CMP-Parent where applicable), i.e., the stored "apikey", and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP (or Split-CMP-Parent, where applicable) as described in Section 9.3.2.

Table 19: MC-2-ROUTE_ICI_REQUEST Message

10.4.1.2 Route ICI Response

The MC-2-ROUTE_ICI web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.
- The "addr" SHALL be present when the MCR has the routing information for the ICI or ICI block.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the CMP (or the Split-CMP-Parent where applicable) and MCR to reconcile code routing transactions at a later date, if needed.
addr	Mandatory	1	String	The "addr" specifies the URL of a Remote or Resolving CMP (or the Split-CMP-Parent where applicable).

Table 20: MC-2-ROUTE_ICI_RESPONSE Message

10.4.1.3 Route ICI Failure

The MC-2-ROUTE_ICI web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.
- One of the possible "status" errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_ICI
  - MC_INACTIVE_ICI

10.5 MC-3 Interface

The MC-3 interface is used for the transfer of latency-critical information.

The MC-3 interface SHALL support the following REST APIs:

- MC-3-RESOLVE_ICI web service.

10.5.1 MC-3-RESOLVE_ICI Web Service

10.5.1.1 Resolve ICI Request

The MC-3-RESOLVE_ICI web service request is made as specified below:

- The URL in the request SHALL be the MC-3-RESOLVE_ICI_REQUEST_URL that is provided by the Remote CMP (or the Split-CMP-Parent where applicable) that is to receive the request and currently configured in the CMP (or the Split-CMP-Parent where applicable).
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request:

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the communicating CMPs to reconcile resolution transactions at a later date, if needed.
ici	Mandatory	1	String	The "ici" contains the value of the ICI to be resolved by the Home CMP
clientid	Mandatory	1	String	The "clientid" is used for identifying an instance of the MCC installation on the specific device. This parameter is generally used by the Home CMP only. 'clientid' may be referred to as 'user id' in some application development environments.
apikeyid	Optional	0..1	String	The "apikeyid" is used by the responder CMP to

				retrieve security information associated with the requestor CMP (i.e., the stored "apikey") and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2.
cc	Optional	0..1	String	The "cc" identifies the alpha-2 country code [ISO3166-1] that is associated with the "post".
post	Optional	0..1	String	The "post" identifies the postal code or zip code.
age	Optional	0..1	String	The "age" provides the age information. It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range (e.g., 22-55) or a free text phrase (e.g., "young" or "retired") in the language associated with "cc" up to 20 octets long.
income	Optional	0..1	String	The "income" provides the household income information. A value, when provided, is tied to the currency associated with the "cc". It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with "<" or ">" (e.g., <30,000 or >100,000) or a free text phrase (e.g., "middle-class" or "rich") in the language associated with "cc" up to 20 octets long.
gender	Optional	0..1	String	The "gender" provides gender setting in the MCC. It can be "female" or "male".
addr	Optional	0..1	String	The "addr" specifies the URL of the Resolving CMP. It may be included in certain cases (e.g., where tandem Split-CMP-Parents and Code Transfer is involved).
locationinfo	Optional	0..1	String	Provides the user's LOC Data (e.g. latitude and longitude) at the time the Mobile Code was scanned.
networkidhome	Optional	0..1	String	The home MNO Identifier of the user's device.
networkidroam	Optional	0..1	String	The roamed-to MNO Identifier from where the Mobile Code was scanned.

Table 21: MC-3-RESOLVE_ICI_REQUEST Message

10.5.1.2 Resolve ICI Response

The MC-3-RESOLVE_ICI web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the CMP (or the Split-CMP-Parent where applicable) and MCR to reconcile code routing transactions at a later date, if needed.
codecontentset	Mandatory	1	Complex	The resolved content as specified in Section 10.3.1.2.1. This parameter SHALL be present on successful resolution of the "ici".
contentdescription	Optional	0..1	String	Free text describing the resolved content for user consumption (e.g. for displaying to the user).
trackingaddress	Optional	0..n	URI	URL specifying a location to which to send tracking data. Home CMP SHALL have full control over this parameter and is likely to enforce that the tracking server in the Home CMP domain is the first entity to receive this data.

Table 22: MC-3-RESOLVE_ICI_RESPONSE Message

10.5.1.3 Resolve ICI Failure

The MC-3-RESOLVE_ICI web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the request.
- One of the possible "status" errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_ICI
  - MC_INACTIVE_ICI
  - MC_CANNOT_RESOLVE_ICI
  - MC_TOO_MANY_HOPS
  - MC_FRAUDULENT_ICI

10.6 MC-4 Interface

The MC-4 interface is used for the transfer of non latency-critical information.

The MC-4 interface SHALL support the following REST APIs:

MC-4_TRACKING_REPORT web service.

10.6.1 MC-4-TRACKING_REPORT Web Service

10.6.1.1 Tracking Report

The MC-4-TRACKING_REPORT web service request is made as specified below:

- The URL in the request SHALL be one of:
  - The MC-4-TRACKING_URL that is currently configured in the MCC
  - The MC-4-TRACKING_URL received from the Home CMP in the MC-1-RESOLVE_ICI_RESPONSE
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.

Parameter	Requirement	Occurrences	Type	Description
ici	Mandatory	1	String	The "ici" contains the value of the ICI which was previously sent to the Home CMP for resolution.
enablerver	Mandatory	1	String	The "enablerver" indicates the OMA MC Enabler version as defined as part of the Section 8.1 – Data Format.
clientid	Mandatory	1	String	The "clientid" is used for identifying an instance of the MCC installation on the specific device. This parameter is generally used by the Home CMP only. "clientid" may be referred to as "user id" in some application development environments.
trackingaddress	Optional	0..1	String	The address of the tracking servers associated with the CMPs (or Split-CMP-Children or Split-CMP-Parents where applicable) involved in the resolution of this "ici".
usagestatistics	Optional	0..n	Complex	Usage information as detailed in Section 10.6.1.1.1. At least one of either the "usagestatistics" or "usagecount" parameter SHALL be present.
optout	Mandatory	1	Boolean	The "optout" is set to: i) "TRUE" when the user has opted out to include the user personal data and location information in the Code Resolution request; and ii) "FALSE" when the user has opted in to include the user personal data and location information in the Code Resolution request.
cc	Optional	0..1	String	The "cc" identifies the alpha-2 country code [ISO3166-1] that is associated with the "post".
post	Optional	0..1	String	The "post" identifies the postal code or zip code.
age	Optional	0..1	String	The "age" provides the age information. It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a

				range (e.g., 22-55) or a free text phrase (e.g., "young" or "retired") in the language associated with "cc" up to 20 octets long.
income	Optional	0..1	String	The "income" provides the household income information. A value, when provided, is tied to the currency associated with the "cc". It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with "<" or ">" (e.g., <30,000 or >100,000) or a free text phrase (e.g., "middle-class" or "rich") in the language associated with "cc" up to 20 octets long.
gender	Optional	0..1	String	The "gender" provides gender setting in the MCC. It can be "female" or "male".
contenttype	Optional	0..1	String	Identifies the type of resolved content associated with this "ici".
usagecount	Optional	0..1	Integer	Provides the number of times the resolved content has been accessed. At least one of either the "usagestatistics" or "usagecount" parameter SHALL be present.
networkidhome	Optional	0..1	String	The home MNO Identifier of the user's device.
networkidroam	Optional	0..1	String	The roamed-to MNO Identifier from where the Mobile Code was scanned.

Table 23: MC-4-TRACKING_REPORT Message

10.6.1.1.1 Structure of the "usagestatistics" parameter

Parameter	Requirement	Occurrences	Type	Description
appname	Optional	0..1	String	The application name of the invoked application.
action	Optional	0..1	String	The action as performed by the invoked application (e.g. store, bookmark, display).
timestamp	Optional	0..1	dateTime	Date and time at which the resolved content was accessed.
locationinfo	Optional	0..1	String	Provides the user's LOC Data (e.g. latitude and longitude) at the time the resolved content was accessed.

Table 24: Structure of the "usagestatistics" Parameter

10.6.1.2 Tracking Report Failure

The MC-4-TRACKING_REPORT web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL NOT be present.
- One of the possible "status" errors below SHALL be included:

- MC_UNAUTHORISED
- MC_SERVICE_UNAVAILABLE
- MC_MISSING_PARAMS
- MC_INVALID_ICI

10.7 MC-5 Interface

The MC-5 interface is used for the transfer of non latency-critical information.

The MC-5 interface SHALL support the following REST APIs:

- MC-5-CODE_TRANSFER web service.
- MC-5-TRANSFER_CONFIRMATION web service.

10.7.1 MC-5-CODE_TRANSFER Web Service

10.7.1.1 Code Transfer Request

This request is used by the old CMP (or the Split-CMP-Parent when applicable) to indicate to the MCR its permission for transferring an ICI or ICI block, or by the new CMP (or the Split-CMP-Parent when applicable) to request the transfer of an ICI or ICI block.

The MC-5-CODE_TRANSFER web service request will be made as specified below:

- The URL in the request SHALL be the MC-5-CODE_TRANSFER_REQUEST_URL that is currently configured in the CMP (or the Split-CMP-Parent when applicable).
- The parameters marked “Mandatory” in the table below SHALL be present in the request while the others MAY be present in the request.
- Either “ici” or “icibk” but not both SHALL be present in the request.
- The “addr” SHALL be present in the request that is sent by the new CMP (or the Split-CMP-Parent when applicable) and SHALL NOT be present in the request that is sent by the old CMP (or the Split-CMP-Parent when applicable).

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The “tid” allows the CMP (or the Split-CMP-Parent when applicable) and MCR to reconcile Code Transfer transactions at a later date, if needed.
ici	Conditional	0..1	String	The “ici” contains the value of the ICI to be transferred.
icibk	Conditional	0..1	String	The “icibk” contains the block of ICIs to be transferred.
token	Mandatory	1	String	The “token” contains a value assigned by the old CMP (or Split-CMP-child when applicable) for the to-be-transferred ICI or ICI block.
apikeyid	Optional	0..1	String	The “apikeyid” is used by the MCR to retrieve security information associated with the

				requestor CMP (or Split-CMP-Parent when applicable), i.e., the stored "apikey", and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP (or Split-CMP-Parent, when applicable) as described in Section 9.3.2.
addr	Optional	0..1	String	The "addr" specifies the URL of the Resolving CMP.

Table 25: MC-5-CODE_TRANSFER_REQUEST Message

10.7.1.2 Code Transfer Response

The MC-5-CODE_TRANSFER web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the CMP (or the Split-CMP-Parent where applicable) and MCR to reconcile Code Transfer transactions at a later date, if needed.

Table 26: MC-5-CODE_TRANSFER_RESPONSE Message

10.7.1.3 Code Transfer Failure

The MC-5-CODE_TRANSFER web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.
- One of the possible "status" errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_PARAMS
  - MC_INVALID_ICI
  - MC_INACTIVE_ICI
  - MC_CT_TOKEN_MISMATCH
  - MC_CT_NOT_SUPPORTED
  - MC_CT_NOT_AVAILABLE

10.7.2 MC-5-TRANSFER_CONFIRMATION Web Service

The MC-5-TRANSFER_CONFIRMATION web service MAY be used by the MCR to inform the old CMP (or the Split-CMP-Parent when applicable) about the successful transfer of an ICI or ICI block. It is not used when the MCR uses other means such as email notification.

10.7.2.1 Transfer Confirmation Request

The MC-5-TRANSFER_CONFIRMATION web service request is made as specified below:

- The URL in the request SHALL be the MC-5-TRANSFER_CONFIRMATION_REQUEST_URL that is currently configured in the MCR.
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.
- Either "ici" or "icibk" but not both SHALL be present in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the MCR (or the Split-CMP-Parent where applicable) and CMP (or the Split-CMP-Parent where applicable) to reconcile transfer confirmation transactions at a later date, if needed.
ici	Conditional	0..1	String	The "ici" contains the value of the ICI to be transferred.
icibk	Conditional	0..1	String	The "icibk" contains the block of ICIs to be transferred.
apikeyid	Optional	0..1	String	The "apikeyid" is used by the MCR to retrieve security information associated with the requestor CMP (or Split-CMP-Parent where applicable), i.e., the stored "apikey", and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP (or Split-CMP-Parent, where applicable) as described in Section 9.3.2.

Table 27: MC-5-TRANSFER_CONFIRMATION_REQUEST Message

10.7.2.2 Transfer Confirmation Response

The MC-5-TRANSFER_CONFIRMATION web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.
- The "tid" SHALL be copied from the "tid" in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the CMP (or the Split-CMP-Parent where applicable) and MCR to reconcile transfer confirmation transactions at a later

				date, if needed.

Table 28: MC-5-TRANSFER_CONFIRMATION_RESPONSE Message

10.7.2.3 Transfer Confirmation Failure

The MC-5-TRANSFER_CONFIRMATION web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.
- One of the possible "status" errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_PARAMS
  - MC_INVALID_ICI
  - MC_CT_NOT_REQUESTED

10.8 MC-6 Interface

The MC-6 interface is used for the transfer of non latency-critical information.

The MC-6 interface SHALL support the following REST APIs:

- MC-6-CODE_TRANSFER web service.
- MC-6-TRANSFER_CONFIRMATION web service.
- MC-6-TRACKING_REPORT web service.

The first two web services above are only used between the Split-CMP-Child and the Split-CMP-Parent.

10.8.1 MC-6-CODE_TRANSFER Web Service

10.8.1.1 Code Transfer Request

The MC-6-CODE_TRANSFER web service request is made as specified below:

- This request is used by the old Split-CMP-Child to indicate to the Split-CMP-Parent its permission for transferring an ICI or ICI block, or by the new Split-CMP-Child to request its Split-CMP-Parent for the transfer of an ICI or ICI block.
- The URL in the request SHALL be the MC-6-CODE_TRANSFER_REQUEST_URL that is currently configured in the Split-CMP-Child.
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.
- Either "ici" or "icibk" but not both SHALL be present in the request.

Parameter	Requirement	Occurrences	Type	Description

tid	Mandatory	1	String	The "tid" allows the old/new Split-CMP-Child and the old/new Split-CMP-Parent to reconcile Code Transfer transactions at a later date, if needed.
ici	Conditional	0..1	String	The "ici" contains the value of the ICI to be transferred.
icibk	Conditional	0..1	String	The "icibk" contains the block of ICIs to be transferred.
apikeyid	Optional	0..1	String	The "apikeyid" is used by the responder CMP to retrieve security information associated with the requestor CMP (i.e., the stored "apikey") and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2.
token	Mandatory	1	String	The "token" contains a value assigned by the old CMP (or Split-CMP-child when applicable) for the to-be-transferred ICI or ICI block.

Table 29: MC-6-CODE_TRANSFER_REQUEST Message

10.8.1.2 Code Transfer Response

The MC-6-CODE_TRANSFER web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the old/new Split-CMP-Parent and the old/new Split-CMP-Child to reconcile Code Transfer transactions at a later date, if needed.

Table 30: MC-6-CODE_TRANSFER_RESPONSE Message

10.8.1.3 Code Transfer Failure

The MC-6-CODE_TRANSFER web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.
- The possible "status" errors are :
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE

- MC_MISSING_PARAMS
- MC_INVALID_PARAMS
- MC_INVALID_ICI
- MC_INACTIVE_ICI
- MC_CT_TOKEN_MISMATCH
- MC_CT_NOT_SUPPORTED
- MC_CT_NOT_AVAILABLE

10.8.2 MC-6-TRANSFER_CONFIRMATION Web Service

The MC-6-TRANSFER_CONFIRMATION web service MAY be used by the old Split-CMP-Parent to inform the old Split-CMP-Child about the successful transfer of an ICI or ICI block. It is not used when the old Split-CMP-Parent uses other means such as email notification.

10.8.2.1 Transfer Confirmation Request

The MC-6-TRANSFER_CONFIRMATION web service request is made as specified below:

- This request is used by the old Split-CMP-Parent to confirm the transfer of an ICI or ICI block with the old Split-CMP-Child.
- The URL in the request SHALL be the MC-6-TRANSFER_CONFIRMATION_REQUEST_URL that is currently configured in the Split-CMP-Parent.
- The parameters marked “Mandatory” in the table below SHALL be present in the request while the others MAY be present in the request.
- Either “ici” or “icibk” but not both SHALL be present in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The “tid” allows the old Split-CMP-Child and the old Split-CMP-Parent to reconcile transfer confirmation transactions at a later date, if needed.
ici	Conditional	0..1	String	The “ici” contains the value of the ICI to be transferred.
icibk	Conditional	0..1	String	The “icibk” contains the block of ICIs to be transferred.
apikeyid	Optional	0..1	String	The “apikeyid” is used by the responder CMP to retrieve security information associated with the requestor CMP (i.e., the stored “apikey”) and SHALL be present when using digital signatures for authentication.
signature	Optional	0..1	String	When using digital signatures for authentication, the “signature” field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2.

Table 31: MC-6-TRANSFER_CONFIRMATION_REQUEST Message

10.8.2.2 Transfer Confirmation Response

The MC-6-TRANSFER_CONFIRMATION web service response is made as specified below.

- The parameters marked "Mandatory" in the table below SHALL be present in the response while the others MAY be present in the response.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.

Parameter	Requirement	Occurrences	Type	Description
tid	Mandatory	1	String	The "tid" allows the old Split-CMP-Child and the old Split-CMP-Parent to reconcile transfer confirmation transactions at a later date, if needed.

Table 32: MC-6-TRANSFER_CONFIRMATION_RESPONSE Message

10.8.2.3 Transfer Confirmation Failure

The MC-6-TRANSFER_CONFIRMATION web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The "tid" SHALL be present and SHALL be copied from the "tid" in the request.
- One of the possible "status" errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_PARAMS
  - MC_INVALID_ICI
  - MC_CT_NOT_REQUESTED

10.8.3 MC-6-TRACKING_REPORT Web Service

10.8.3.1 Tracking Report

The MC-6-TRACKING_REPORT web service request is made as specified below:

- The URL in the request SHALL be the MC-6-TRACKING_URL associated with the recipient CMP as received by the sender CMP in the MC-3_RESOLVE_ICI_RESPONSE
- The parameters marked "Mandatory" in the table below SHALL be present in the request while the others MAY be present in the request.

Parameter	Requirement	Occurrences	Type	Description
ici	Mandatory	1	String	The "ici" contains the value of the ICI which was previously sent to the Home CMP for resolution.
clientid	Mandatory	1	String	The "clientid" is used for identifying an

				instance of the MCC installation on the specific handset. This parameter is generally used by the Home CMP only. "clientid" may be referred to as "user id" in some application development environments.
trackingaddress	Optional	0..1	String	The address of the tracking servers associated with the CMPs involved in the resolution of this "ici".
usagestatistics	Optional	0..n	Complex	Usage information as detailed in Section 10.8.3.1.1. At least one of either the "usagestatistics" or "usagecount" parameter SHALL be present.
cc	Optional	0..1	String	The "cc" identifies the alpha-2 country code [ISO3166-1] that is associated with the "post".
post	Optional	0..1	String	The "post" identifies the postal code or zip code.
age	Optional	0..1	String	The "age" provides the age information. It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range (e.g., 22-55) or a free text phrase (e.g., "young" or "retired") in the language associated with "cc" up to 20 octets long.
income	Optional	0..1	String	The "income" provides the household income information. A value, when provided, is tied to the currency associated with the "cc". It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with "<" or ">" (e.g., <30,000 or >100,000) or a free text phrase (e.g., "middle-class" or "rich") in the language associated with "cc" up to 20 octets long.
gender	Optional	0..1	String	The "gender" provides gender setting in the MCC. It can be "female" or "male".
contenttype	Optional	0..1	String	Identifies the type of resolved content associated with this "ici".
usagecount	Optional	0..1	Integer	Provides the number of times the resolved content has been accessed. At least one of either the "usagestatistics" or "usagecount" parameter SHALL be present.
networkidhome	Optional	0..1	String	The home MNO Identifier of the user's device.
networkidroam	Optional	0..1	String	The roamed-to MNO Identifier from where the Mobile Code was scanned.

Table 33: MC-6-TRACKING_REPORT Message

10.8.3.1.1 Structure of the “usagestatistics” parameter

Parameter	Requirement	Occurrences	Type	Description
appname	Optional	0..1	String	The application name of the invoked application.
action	Optional	0..1	String	The action as performed by the invoked application (e.g. store, bookmark, display).
timestamp	Optional	0..1	dateTime	Date and time at which the resolved content was accessed.
locationinfo	Optional	0..1	String	Provides the user’s LOC Data (e.g. latitude and longitude) at the time the resolved content was accessed.

Table 34: Structure of the "usagestatistics" Parameter

10.8.3.2 Tracking Report Failure

The MC-6-TRACKING_REPORT web service error is made as specified below.

- The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.
- The “tid” SHALL NOT be present.
- One of the possible “status” errors below SHALL be included:
  - MC_UNAUTHORISED
  - MC_SERVICE_UNAVAILABLE
  - MC_MISSING_PARAMS
  - MC_INVALID_ICI

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-MC-V1_0	11 Feb 2009	Cover page	Created skeleton TS
	07 Apr 2009	1 2 3 4	Implemented Agreed Changes: OMA-MC-2009-0050-CR_Adding_Scope,_References,_Definitions_to_TS OMA-MC-2009-0052-CR_Adding_Introduction_and_Versioning_to_TS
	22 Jun 2009	Cover page, 5, 6, 7, 8, 9, 10, Change History	Implemented: OMA-MC-2009-0045-CR__to_TS__Mandated_Standard_Symbologies OMA-MC-2009-0076R01-CR_TS_Structure Removed example text and structure from former Section 5.
	05 Oct 2009	Cover page, 2, 3, 5, 7, 8, 9, 10	Implemented Agreed Changes: OMA-MC-2009-0088R05-CR_Location_Data_Format_in_DIrect_Model OMA-MC-2009-0089R04-CR_Location_Data_Format_in_Indirect_Model OMA-MC-2009-0091R02-CR-MC-1-and-3-Messaging OMA-MC-2009-0136-CR_Plain_Text_Recognizable_Format_and_DMF OMA-MC-2009-0137-CR_http_and_https_URI_schemes_support OMA-MC-2009-0138R01- CR_Telephone_Number_String_and_Tel_URI_Scheme_Recognition OMA-MC-2009-0145R01-CR_email_address_recognition OMA-MC-2009-0151R01-CR_for_TS_miscellaneous_sections
	03 Dec 2009	Cover page, 2, 3, 5, 7, 8, 10, Appendix	Implemented Agreed Changes: OMA-MC-2009-0133R02-CR_MC1_Code_Resolution_Text OMA-MC-2009-0146R02-CR_to_TS_Data_Format. OMA-MC-2009-0156R01-CR_QR_Code_Symbology_Specification OMA-MC-2009-0157-CR_Editorial_changes__for_Chapter_7
	31 Jan 2010	Cover Page, 3, 5, 7, 10, Appendix	Updated document to 2010 TS Template, Implemented Agreed Changes: OMA-MC-2009-0183- CR_Business_Card_Data_Format_for_Direct_Model.zip OMA-MC-2009-0191R02- CR_Consolidated_QR_Code_and_Data_Matrix_Symbology_Specification OMA-MC-2009-0195R02-CR_TS_MC_Interfaces

Document Identifier	Date	Sections	Description
	05 Mar 2010	Cover Page, 3, 5 - 10, Appendix	Implemented Agreed Changes: OMA-MC-2010-0008-CR_Property_Value_of_Direct_Code_DMF.doc OMA-MC-2010-0009R02-CR_Proposed_changes_in_section_6.1.doc OMA-MC-2010-0011R01-CR_Quiet_Zone_and_Module_Width.doc OMA-MC-2010-0016-CR_Proposed_Changes_to_Align_TS_with_AD_Arch_Models.doc OMA-MC-2010-0021R01-CR_Plain_Text_Messages_and_Control_Characters.doc OMA-MC-2010-0024R02-CR_Recognition_of_overlapping_Recognizable_Formats.doc Editorial Updates: "CCH" changed to "Split-CMP-Parent" "CRS" changed to "Split-CMP-Child" Moved Sections 5.2.1 – 5.2.3 to 9.1.1 – 9.1.3 as agreed in Sorrento
	02 Apr 2010	Cover Page, 5, 7, 8, 10, Appendix	Implemented Agreed Changes: OMA-MC-2010-0013R04-CR_Proposed_changes_in_sections_8.1_through_8.2.doc OMA-MC-2010-0014-CR_Proposed_changes_in_section_10.3.doc OMA-MC-2010-0033R01-CR_Structured_Append_Mode_Additional_Specifications.doc OMA-MC-2010-0036R02-CR_Email_Linkage_Data_Format.doc OMA-MC-2010-0037-CR_Bookmark_Data_Format_for_Direct_Code.doc
	20 May 2010	Cover Page, 2, 3, 5, 6, 7, 8, 10, Appendix	Implemented Agreed Changes: OMA-MC-2010-0038R03-CR_Proposed_changes_in_section_10.6 OMA-MC-2010-0039R03-CR_Proposed_changes_in_section_10.7 OMA-MC-2010-0040R04-CR_Proposed_changes_in_section_10.4 OMA-MC-2010-0041R04-CR_Proposed_changes_in_section_10.3 OMA-MC-2010-0045R01-CR_Symbol_Contrast_and_Lighting OMA-MC-2010-0051-CR_Proposed_structure_for_section_8 OMA-MC-2010-0057R03-CR_Proposed_changes_to_10.1 OMA-MC-2010-0064-CR_Direct_Code_Editorials OMA-MC-2010-0069-CR_CR_Editorial_clean_up_for_Direct_Code_related_sections Editorial Updates: Grouped error messages and mapping table into one section under 10.2 As per OMA-MC-2010-0076-MINUTES_04May2010_CC status review. The completed actions are: Section 2: All references to the NFC data format, identifier, etc., should be removed from the MC documents (NDEF, NFRIC, SPRTD, TEXTRTD and URIRTD). Section 5.2: Should be removed, but discussion is covered in the Provisioning section. Section 5.3: Remove. Section 6.2: Remove. Fujitsu (Alan) will review this again in order to update or remove this section. Section 7.1.2.3: Remove. Section 7.1.3 – Table 1 needs to be finished. – Change "OMA-Indirect" to "OMA" Section 7.2.1: Editor's Note is gone. Section 7.2.4.1: Editor's Note is gone. Section 10.1.1: Location Information (AP on TIM; see bullets at the end of this discussion). Section 10.2: Table 10 has "occurrence" field, but not in the other tables. (TS Editor to make sure consistency throughout).

Document Identifier	Date	Sections	Description
	23 June 2010	Cover Page, 8, 9, 10, Appendix	Implemented Agreed Changes: OMA-MC-2010-0015R04-CR_Text_for_Section_9.5 OMA-MC-2010-0072R02-CR_Code_transfer_procedures OMA-MC-2010-0073R01-CR_Code_resolution_procedures OMA-MC-2010-0082R01- CR_MC_4_and_MC_6_Tracking_Report_Messages OMA-MC-2010-0084R01-CR_code_resolution_worst_case_scenario OMA-MC-2010-0086R01-CR_addr_description_change
	13 July 2010	General update; added new materials for Appendices B and H	Implemented Agreed CRs: OMA-MC-2010-0056R04-CR_MC_3_Interface_Security.zip OMA-MC-2010-0092R01-CR_Tracking_in_code_resolution_procedures.zip OMA-MC-2010-0093-CR_Character_Set_for_Direct_Code_Display.zip OMA-MC-2010-0094-CR_SCR_Direct_Code.zip OMA-MC-2010-0097-CR_Guideline_for_Direct_Code_Authors.zip OMA-MC-2010-0098R01- CR_addr_description_change_in_MC_3_RESOLVE_ICI_REQUEST.zip OMA-MC-2010-0101R02- CR_Alignment_of_Tracking_and_Reporting_Text.zip OMA-MC-2010-0102-CR_Reporting_by_Applications.zip OMA-MC-2010-0103R01-CR_MCC_User_Profile_Data.zip OMA-MC-2010-0106R01-CR_Indirect_Code_Data_Format.zip OMA-MC-2010-0109-CR_Removal_of_timer_related_procedures.zip OMA-MC-2010-0110-CR_TS_online_edits_by_the_group.zip OMA-MC-2010-0112-CR_Alignment_of_Sections_2_and_3.zip Updated Table of Content including appendix figures & tables. Corrected section numbering and applied minor editorial clean-up; international English spell-check for consistency.
	02 August 2010	Cover Page, 10	Implemented Agreed CRs: OMA-MC-2010-0116R02-CR_MC_1_and_3_Interface_Responses (incl. R&A comments) OMA-MC-2010-0117-CR_addr_description_change_in_section_10.7.1.1 OMA-MC-2010-0125R01-CR_Updates_to_10.6.1.1_and_10.8.3.1 Editorial Updates as per 0114-MINUTES: Ensured consistency of 'Occurrences' column in section 10 Ensured consistency of "Parameter" column in section 10 Removed Editorial Notes that have been resolved Added latency related note for each interface Added Indirect Code disclaimer at start of section 10
	12 August 2010	Cover Page, 8, 9, 10, Appendix	Implemented Agreed CRs: OMA-MC-2010-0081R01- CR_TS_details_for_MC_Service_Policy_attributes_repository_decision_and_enforcement OMA-MC-2010-0120-CR_Correction_in_Section_9.5.1.2 OMA-MC-2010-0122-CR_Updates_to_Section_9.5_and_8.4 OMA-MC-2010-0126R02-CR_TS_Section_9.1_clean_up OMA-MC-2010-0127R01-CR_changes_to_count_related_texts OMA-MC-2010-0137- CR_Sect_8.1_Indirect_Code_Data_Format_update_and_other_TS_clean_up_ OMA-MC-2010-0138-CR_MCC_to_Home_CMP_authentication Editorial Updates as per CR 137: Ensured use of "user personal data" vs "subscriber profile information" and "personal data information" Ensured addition of "location information" to all statements of use permission being required
	23 August 2010	Cover Page, 2, 8, 9, 10, Appendix	Implemented Agreed CRs: OMA-MC-2010-0144-CR_Add_content_description_in_MC_3_response OMA-MC-2010-0146-CR_TransactionID_Consistency OMA-MC-2010-0148-CR_MC_4_and_MC_6_Message_Consistency OMA-MC-2010-0134R01-INP_CR_Updates_to_8.1.3.1.2_and_9.3.1 OMA-MC-2010-0143R01-CR_Remove__user__from_MC_3_request OMA-MC-2010-0145R01- CR_Discuss_optout_and_other_parameters_in_MC_1_request OMA-MC-2010-0147R01- CR_contentdescription_in_code_resolution_procedures OMA-MC-2010-0130R02-CR_Guideline_for_MLA_ecosystem OMA-MC-2010-0131R02-CR_Simplification_of_section_8.2

Document Identifier	Date	Sections	Description
	29 August 2010	Cover Page, Appendix	Implemented Agreed CR: OMA-MC-2010-0151R01-CR_SCR_tables_for_Indirect_Codes Update to Appendix D examples as per minutes Minor editorial changes – spelling/grammar check
	30 August 2010	Cover Page, Appendix	Corrected figure reference in Appendix G Added Change History for 29-Aug-2010
	31 August 2010	Cover Page, Appendix B	Corrected some SCR tables with the group's input Removed unused templates
	04 October 2010	All	Resolved editorial CONRR comments with the exception of: A052 – Awaiting clarification from author A103 – Will be closed by CR to A171 A125 – AP for TIM A126 – AP for TIM A133 – To be done during last TS pass A135 – To be done during last TS pass A136 – To be done during last TS pass A171 – CR will be provided to resolve A171 (E) and A172 (T) A190 – AP for TIM A222 – Awaiting feedback from Fujitsu A223 – Awaiting feedback from Fujitsu
	18 October 2010	All	Addressed offline comments against editorial CONRR comment resolution Resolved remaining editorial CONRR comments Further editorial updates: • All MUSTs changed to SHALLs for consistency • All unnecessary mentions of split-CMP deployment were removed Implemented agreed changes for Technical comments as per CONRR: A184, A222, A223, A057, A001, A169, A202, A108, A174, A112, A114, A203, A205, A207, A173 Implemented Agreed CRs: OMA-MC-2010-0160R01-CR_MC_TS_Informative_Appendix_E OMA-MC-2010-0164R02-CR_CONRR_Comment_A001 OMA-MC-2010-0173-CR_CONRR_comment_A090 OMA-MC-2010-0174-CR_CONRR_comments_A109_A111_A115_and_A119 (Change 1 & 2 only) OMA-MC-2010-0175-CR_CONRR_comment_A084 OMA-MC-2010-0178-CR_CONRR_comment_A117 OMA-MC-2010-0179-CR_RIM_Comment_A167 OMA-MC-2010-0180-CR_RIM_Comment_A164 OMA-MC-2010-0181R02-CR_RIM_Comment_A165 OMA-MC-2010-0182R01-CR_RIM_Comment_A166 OMA-MC-2010-0183R02-CR_CONRR_Comment_A125_A126_A127_A143_A189_A190 OMA-MC-2010-0184-CR_Comment_101 OMA-MC-2010-0185-CR_RIM_Comment_A172 OMA-MC-2010-0189-CR_MC_TS_A234_Resolution OMA-MC-2010-0190-CR_CONRR_Comment_A130
	26 October 2010	Cover Page, 8, 10	Implemented agreed CRs: OMA-MC-2010-0165R07-CR_CR_CONRR_Comment_A002 OMA-MC-2010-0195R01-CR_Proposed_changes_to_Sections_10.1_and_10.2 OMA-MC-2010-0196R01-CR_Section_8.3.2_rewrite_based_on_CR0195 OMA-MC-2010-0198-Status Code for Tracking Report Messages
	02 November 2010	All	Updated Appendix B – SCR Tables Editorial cleanup: Capitalization of defined terms Removal of overarching normative language Removal of mentions of "preferred language"

Document Identifier	Date	Sections	Description
	04 November 2010	All	Editorial Updates: - Aligned TS definitions with those in RD and AD - SCR Table update - Global check to capitalize defined terms - Minor edits to Section 3 and Appendix D - SCR Table updates: o Corrected mis-numbered or missing numbers in the rows o Filled in missing section references o Removed informational rows (e.g., "Home CMP", or "MCR") o Added Abbreviations to all SCR Table headings
	05 November 2010	Cover sheet	Updated date following online edits from the group on the 2010-11-04 CC.
Candidate Version: OMA-TS-MC-V1_0	30 Nov 2010	All	Status changed to Candidate Status by TP ref # OMA-TP-2010-0475-INP_MC_V1_0_ERP_for_Candidate_Approval

Appendix B. Static Conformance Requirements

Static Conformance Requirements (SCRs) are normative. The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for MC Enabler Client

Section B.1 covers Static Conformance Requirements for the MC Enabler Client component (i.e., Mobile Code Client 'MCC').

B.1.1 MCC Support for Symbologies (QR/DM)

Item	Function	Reference	Requirement
MC-QR-C-001-M	Symbologies : QR Code as defined in ISO/IEC 18004:2006	Section 5.1.1	
MC-QR-C-002-M	Support QR Code Model 2	Section 5.1.1.1	MC-QR-C-001-M
MC-QR-C-003-M	support Versions 1 to 10	Section 5.1.1.2	MC-QR-C-001-M
MC-QR-C-004-O	Versions 11 or higher	Section 5.1.1.2	MC-QR-C-001-M
MC-QR-C-005-M	Support Error Correction Levels, L, M, Q and H, for all the mandatory Versions	Section 5.1.1.3	MC-QR-C-001-M
MC-QR-C-006-M	Support the specified Modes and the combination of it as defined 5.1.1.4.	Section 5.1.1.4	MC-QR-C-001-M
MC-QR-C-007-M	support any combination the modes in Section 5.1.1.4	Section 5.1.1.4	MC-QR-C-001-M and MC-QR-C-006-M
MC-QR-C-008-M	Minimum Conformance Characters Set for Direct Code Display, MCCSDCD	Section 5.1.1.5	MC-QR-C-001-M
MC-QR-C-009-M	QR Code symbol with a Quiet Zone that is equal to or larger than 4X wide on all four sides	Section 5.1.1.6	MC-QR-C-001-M
MC-QR-C-010-O	QR Code symbol with a Quiet Zone that is equal to 3X wide on all four sides	Section 5.1.1.6	MC-QR-C-001-M
MC-QR-C-011-M	support Structured Append mode to enable up to 16 QR Code symbols to be concatenated	Section 5.1.1.7	MC-QR-C-001-M
MC-QR-C-012-M	Support a mechanism that allows the user to exit from the process of capturing multiple QR Code symbols	Section 5.1.1.7	MC-QR-C-001-M
MC-DM-C-013-M	Symbologies :support Data Matrix as defined in ISO/IEC 16022:2000	Section 5.1.2	
MC-DM-C-014-M	support Data Matrix type ECC 200	Section 5.1.2.1	MC-DM-C-012-M
MC-DM-C-015-M	support Data Matrix symbol sizes up to 52x52 modules, including the rectangular symbols	Section 5.1.2.2	MC-DM-C-012-M
MC-DM-C-016-O	Data Matrix ECC 200 symbol sizes of 64x64 or larger	Section 5.1.2.2	MC-DM-C-012-M
MC-DM-C-017-M	Support the Encodation Schemes as specify Section 5.1.2.3 for Data Matrix	Section 5.1.2.3	MC-DM-C-012-M
MC-DM-C-018-M	support any combination of the encodation schemes for Data Matrix	Section 5.1.2.3	MC-DM-C-012-M

Item	Function	Reference	Requirement
MC-DM-C-019-M	Read a Data Matrix symbol with a Quiet Zone that is equal to or larger than 1X wide on all four side	Section 5.1.2.4	MC-DM-C-012-M
MC-DM-C-020-M	support Structured Append to enable up to 16 Data Matrix symbols to be concatenated	Section 5.1.2.5	MC-DM-C-012-M
MC-DM-C-021-M	Support a mechanism that allows the user to exit from the process of capturing multiple Data Matrix symbols	Section 5.1.2.5	MC-DM-C-012-M
MC-DM-C-022-O	Minimum Conformance Characters Set for Direct Code Display, MCCSDCD	Section 5.1.3	MC-DM-C-012-M

B.1.2 MCC Support of Character Set for Direct Code Display (CSD)

Item	Function	Reference	Requirement
MC-CSD-C-001-M	this specification is tested or elaborated for displaying the data of Direct Code for QR and Data Matrix	Section 5.1.3	MC-QR-C-001-M and MC-QR-C-012-M

B.1.3 MCC Support for Direct Code Resolution (DIR)

Item	Function	Reference	Requirement
MC-DIR-001-M	Display plain text and Recognizable Formats that are specified in the Recognizable Format section	Section 7.1	
MC-DIR-002-M	Replace an unprintable-control-character by an appropriate printable character	Section 7.1	MC-DIR-001-M
MC-DIR-003-M	Direct MC Format (DMF) is identified by Identifier followed by ":", and is a collection of Properties and Delimiter	Section 7.1.2.1	MC-DIR-001-M
MC-DIR-004-M	Property-Values escaped according to the rule defined in Section 7.1.2.2.	Section 7.1.2.1	MC-DIR-003-M
MC-DIR-005-M	Certain characters used in the a parameter of Property, i.e. ",", ";", ":", and "\", SHALL be denoted by using the escape sequence with a backslash "\"	Section 7.1.2.2	MC-DIR-003-M
MC-DIR-006-M	Recognise http: and https: URI schemes as the Recognizable Formats	Section 7.2.1.1	MC-DIR-001-M
MC-DIR-007-M	Support the of OMA-URI [OMAURI] with clarifications	Section 7.2.1.1	MC-DIR-006-M
MC-DIR-008-M	Recognise http and https format that may exist in: Plan text, with other Recognizable Formats and inside of other Recognizable Format	Section 7.2.1.1	MC-DIR-006-M
MC-DIR-009-M	When http: or https: URI appears in other Recognizable Formats listed in Table 10 conduct recognition based on the rules that are specified in Section 7.3	Section 7.2.1.1	MC-DIR-006-M

Item	Function	Reference	Requirement
MC-DIR-010-M	Display the recognised http and https URIs with other data such as plain text messages	Section 7.2.1.2	MC-DIR-001-M
MC-DIR-011-M	make such a http and https URI selectable by the user for invocation	Section 7.2.1.2	MC-DIR-001-M
MC-DIR-012-M	provide means for the user to choose one of http and https URI if multiple URIs are recognised	Section 7.2.1.2	MC-DIR-001-M
MC-DIR-013-M	Display http and https URIs in texts so that the user is able to see the URIs before invoking a browser;	Section 7.2.1.2	MC-DIR-001-M
MC-DIR-014-M	If a URI is selected and clicked by the user, invoke a browser with the URI to be passed to the browser	Section 7.2.1.2	MC-DIR-006-M
MC-DIR-015-O	make the URIs available for other applications such as registering them into a bookmark in	Section 7.2.1.2	MC-DIR-006-M
MC-DIR-016- O	invoked application is terminated the control will go back to the MCC if it is possible	Section 7.2.1.2	
MC-DIR-017 –M	Recognise a Telephone-Number-String as a Recognizable Format	Section 7.2.2.1	
MC-DIR-018 –M	Recognise the Telephone-Number-String as a Recognizable Format that may exist alone, in the middle of a plain text message, with other Recognizable Format, or inside of other Recognizable Format	Section 7.2.2.1	MC-DIR-017 -M
MC-DIR-019 -M	When a Telephone-Number-String appears in other Recognizable Formats that are specifically listed Table 10, conduct recognition based on the rules that are specified in Section 7.3	Section 7.2.2.1	MC-DIR-017 -M
MC-DIR-020-O	Recognise the “tel:” scheme as a Recognizable Format [RFC 3966].	Section 7.2.2.2	
MC-DIR-021 -M	Display the recognised format telephone number by the specifications 7.2.2.1 or 7.2.2.2 with any other data such as plain text messages and/or other Recognizable Formats	Section 7.2.2.3	MC-DIR-017 -M and/or MC-DIR-020-M
MC-DIR-022 –M	Make the format that represents a telephone number by the specifications 7.2.2.1 or 7.2.2.2 if selectable by the user for initiating a voice call, sending an SMS / MMS message or other types of communications	Section 7.2.2.3	MC-DIR-017 -M and/or MC-DIR-020-M
MC-DIR-023 –M	If multiple Recognizable Formats that represent telephone numbers by the specifications Section 7.2.2.1 or 7.2.2.2 are recognised, and provide means for the user to choose one from them;	Section 7.2.2.3	MC-DIR-017 -M and/or MC-DIR-020-M
MC-DIR-024 -M	make the telephone number obtained from the Recognizable Format that represents a telephone number by the specifications 7.2.2.1 or 7.2.2.2 available for other applications such as saving it into a contact book	Section 7.2.2.3	MC-DIR-017 -M and/or MC-DIR-020-M

Item	Function	Reference	Requirement
MC-DIR-025 -M	Recognise a Mailbox as the Recognisable Format	Section 7.2.3.1	
MC-DIR-026 –M	Mailbox SHALL follow the definition in [RFC2822]. With exceptions defined in Section 7.2.3.1	Section 7.2.3.1	MC-DIR-025 -M
MC-DIR-027 –M	No used in a Mailbox Any white spaces or comments	Section 7.2.3.1	MC-DIR-026 -M
MC-DIR-028 –M	name-addr, display-name follow the same syntax as that of local-part	Section 7.2.3.1	MC-DIR-026 -M
MC-DIR-029 -M	Recognise a Mailbox as a Recognizable Format that my exist alone, in the middle of a plain text message, with other Recognizable Format, or inside of other Recognizable Format	Section 7.2.3.1	MC-DIR-025 –M and MC-DR-001-M
MC-DIR-030 –M	When a Mailbox appears in other Recognizable Formats that are specifically listed in Table 10, conduct recognition based on the rules that are specified in Section 7.3	Section 7.2.3.1	MC-DIR-025 -M
MC-DIR-031 –M	Display the Mailbox with any other data such as plain text messages and/or other Recognizable Formats;	Section 7.2.3.2	MC-DIR-025 –M and MC-DR-001-M
MC-DIR-032 –M	Make the Mailbox selectable by the user for invoking an email client application, with the Mailbox being inserted as the destination in the email application.	Section 7.2.3.2	MC-DIR-025 -M
MC-DIR-033 –M	If multiple Mailboxes are recognised, provide means for the user to choose one from them;	Section 7.2.3.2	MC-DIR-025 -M
MC-DIR-034 –O	Make the Mailbox available for other applications such as saving it into a contact book in the device if the user wishes.	Section 7.2.3.2	MC-DIR-025 -M
MC-DIR-035 –M	The definition of MECARD syntax is based on the DMF Definition in Section 7.1.2, with the clarifications that listed in Section 7.1.2	Section 7.2.4.1	
MC-DIR-036 –M	Recognise MECARD: as a Recognizable Format	Section 7.2.4.1	MC-DIR-035 -M
MC-DIR-037 -M	Do not recognise MECARD: as a Recognised Format when MECARD: is found embedded within another Recognizable Format.	Section 7.2.4.1	MC-DIR-035 -M
MC-DIR-038 –M	Ignore any Property that is found in the MECARD but is not included in this table 2	Section 7.2.4.1	MC-DIR-035 -M
MC-DIR-039 –M	All the Properties have one Property-Value, respectively	Section 7.2.4.1	MC-DIR-035 -M
MC-DIR-040 –M	characters; comma, “,”, semicolon, “;”, colon, “:”, and back slash, “\”, is escaped as defined in Section 7.1.2.1 using a back slash, “%x5C”	Section 7.2.4.1	MC-DIR-035 -M
MC-DIR-041 –M	If the following characters; comma, “,”, semicolon, “;”, colon, “:”, and back slash, “\”, that need to be escaped are found without being escaped in the Property, be ignored.	Section 7.2.4.1	MC-DIR-040 -M

Item	Function	Reference	Requirement
MC-DIR-042 –M	SHALL support the N Property	Section 7.2.4.2	MC-DIR-035 -M
MC-DIR-043 –M	N Property is recognised as the name of the person associated with the MECARD.	Section 7.2.4.2	MC-DIR-042 –M and MC-DIR-035 -M
MC-DIR-044 –M	SHALL recognise as many N Properties as it can process	Section 7.2.4.2	MC-DIR-042 –M and MC-DIR-035 -M
MC-DIR-045 –M	The N Properties that exceed the maximum number of the MCC's processing capability is ignored.	Section 7.2.4.2	MC-DIR-042 –M and MC-DIR-035 -M
MC-DIR-046 –O	Support the SOUND Property.	Section 7.2.4.3	MC-DIR-035 -M
MC-DIR-047 -M	Recognised as the sound annotation for the name of the person associated with the MECARD.	Section 7.2.4.3	MC-DIR-035 –M and MC-DIR-046 -M
MC-DIR-048 –M	Recognise as many SOUND Properties as it can process.	Section 7.2.4.3	MC-DIR-035 –M and MC-DIR-046 -M
MC-DIR-049 –M	The SOUND Properties that exceed the maximum number of the MCC's processing capability is ignored.	Section 7.2.4.3	MC-DIR-035 –M and MC-DIR-046 -M
MC-DIR-050 –M	support the TEL Property	Section 7.2.4.4	MC-DIR-035 –M
MC-DIR-051 –M	the TEL Property -Value comply to the definition of Telephone-Number-String, as defined in Section 7.2.2	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-052 –M	The Property-Value of the TEL Property is recognised as the telephone number associated with the MECARD.	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-053 –M	If more than one TEL Property is found, the MCC recognise as many TEL Properties as it can process.	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-054 –M	The TEL Properties that exceed the maximum number of the MCC's processing capability is ignored	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-055 –M	Recognise the Property-Value in the TEL Property by itself, if it complies with the definition, as the telephone number associated with the MECARD and provide the functions that are defined in Section 7.2.2.	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-056 –M	provide a means to the user to be able to choose which the MECARD or the telephone number, is to be invoked	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-057 -M	If multiple TEL Properties are found, the MCC provide all functions for all the telephone numbers that the MCC is capable of supporting.	Section 7.2.4.4	MC-DIR-035 –M and MC-DIR-050 -M
MC-DIR-058 –M	support the EMAIL Property	Section 7.2.4.5	MC-DIR-035 –M
MC-DIR-059 –M	EMAIL Property-Value comply to the definition of the Mailbox, as defined in Section 7.2.3.	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M
MC-DIR-060 –M	Property-Value of the EMAIL Property SHALL be recognised as the electronic mail address associated with the MECARD.	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M

Item	Function	Reference	Requirement
MC-DIR-061 –M	If more than one EMAIL Property is found, the MCC recognise as many EMAIL Properties as it can process. The EMAIL Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M
MC-DIR-062 –M	The EMAIL Properties that exceed the maximum number of the MCC's processing capability is ignored	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M
MC-DIR-063 –M	Recognise the Property-Value in the EMAIL Property by itself, if it complies with the above definition, as the electronic mail address associated with the MECARD and provide the functions that are defined in Section 7.2.3.	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M
MC-DIR-064 –M	Provide a means to the user to be able to choose the MECARD or the EMAIL Property-Value the electronic mail address, is to be invoked.	Section 7.2.4.5	MC-DIR-035 –M and MC-DIR-058 –M
MC-DIR-065 -M	If multiple EMAIL Properties are found, the MCC is to provide all the functions for all the electronic mail addresses that the MCC is capable of supporting.	Section 7.2.4.5	MC-DIR-034 –M and MC-DIR-058 –M
MC-DIR-066 –M	Support the BDAY Property	Section 7.2.4.6	MC-DIR-035 –M
MC-DIR-067 –M	The Property-Value of the BDAY Property is recognised as the date of birth associated with the MECARD.	Section 7.2.4.6	MC-DIR-035 –M and MC-DIR-066 -M
MC-DIR-068 –M	If more than one BDAY Property is found, the MCC recognise as many BDAY Properties as it can process.	Section 7.2.4.6	MC-DIR-035 –M and MC-DIR-066 -M
MC-DIR-069 –M	The BDAY Properties that exceed the maximum number of the MCC's processing capability is ignored	Section 7.2.4.6	MC-DIR-035 –M and MC-DIR-066 -M
MC-DIR-070 -M	The string of characters in the BDAY Property-Value is string of 8 characters consisting of ASCII characters, "%x30-39". The first 4 represent the year, the next 2 represent the month, and the last 2 represent the day of the birth, respectively.	Section 7.2.4.6	MC-DIR-035 –M and MC-DIR-066 -M
MC-DIR-071 –M	If there are more than 8 characters found in BDAY Property-Value the excessive characters is set to NULL	Section 7.2.4.6	MC-DIR-035 –M and MC-DIR-066 -M
MC-DIR-072 –M	Support the ADR Property.	Section 7.2.4.7	MC-DIR-035 –M
MC-DIR-073 –M	Property-Value of the ADR Property is recognised as the physical delivery address associated with the MECARD.	Section 7.2.4.7	MC-DIR-034 –M and MC-DIR-072 -M
MC-DIR-074 –M	If more than one ADR Property is found, the MCC recognise as many ADR Properties as it can process.	Section 7.2.4.7	MC-DIR-035 –M and MC-DIR-072 -M
MC-DIR-075 –M	The ADR Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.	Section 7.2.4.7	MC-DIR-035 –M and MC-DIR-072 -M
MC-DIR-076 –M	Support the NOTE Property.	Section 7.2.4.8	MC-DIR-035 –M

Item	Function	Reference	Requirement
MC-DIR-077 –M	Property-Value of the NOTE Property is recognised as the supplemental information or a comment associated with the MECARD	Section 7.2.4.8	MC-DIR-035 –M and MC-DIR-076 -M
MC-DIR-078 –M	If more than one NOTE Property is found, the MCC recognise as many as it can process.	Section 7.2.4.8	MC-DIR-035 –M and MC-DIR-076 -M
MC-DIR-079 –M	The NOTE Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored.	Section 7.2.4.8	MC-DIR-035 –M and MC-DIR-076 -M
MC-DIR-080 –M	Support the URL Property.	Section 7.2.4.9	MC-DIR-035 –M
MC-DIR-081 –M	Property-Value SHALL comply with the definition of the http: and https:, as defined in Section 7.2.1.	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-082 -M	Property-Value of the URL Property SHALL be recognised as the http: and https: URI schemes associated with the MECARD.	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-083 –M	MCC recognise as many http: and https URL Properties as it can process.	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-084 –M	The http: and https URL Properties that exceed the maximum number of the MCC's processing capability SHALL be ignored	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-085 –M	recognise the Property-Value in the http: and https URL Property by itself, if it complies to the above definition, as the http: and https: URI schemes associated with the MECARD and provide the functions that are defined in Section	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-086 –M	provide a means to the user to be able to choose which one, i.e., the MECARD or the http: and https URI scheme, is to be invoked	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-087 –M	If multiple http: and https URL Properties are found MECARD, the MCC SHALL provide these functions for all the URI schemes that the MCC is capable of supporting	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-088 –M	DMF Definition, Section in the http: and https URI scheme certain characters denoted by using the escape sequence with a backslash "\"	Section 7.2.4.9	MC-DIR-035 –M and MC-DIR-080 -M
MC-DIR-089 –M	support the NICKNAME Property	Section 7.2.4.10	MC-DIR-035 –M
MC-DIR-090 –M	Property-Value of the NICKNAME Property be recognised as the nick name of the person associated with the MECARD.	Section 7.2.4.10	MC-DIR-035 –M and MC-DIR-089 -M
MC-DIR-091 –M	If more than one NICKNAME Property is found, the MCC SHALL recognise as many NICKNAME Properties as it can process.	Section 7.2.4.10	MC-DIR-035 –M and MC-DIR-089 -M
MC-DIR-092 –M	The NICKNAME Properties that exceed the maximum number of the MCC's processing capability is ignored.	Section 7.2.4.10	MC-DIR-035 –M and MC-DIR-089 -M
MC-DIR-093 –M	If MECARD is chosen by the user, an appropriate application invoked to store the data contained in the MECARD to a phone book on the device	Section 7.2.4.11	MC-DIR-035 –M

Item	Function	Reference	Requirement
MC-DIR-094 –M	the Property-Values of TEL, EMAIL, and URL Properties, as defined in Sections 7.2.2 , 7.2.3 and 7.2.1, respectively recognised as Recognizable Formats and offer the functions that are specified in the respective sections of this specification in addition to recognizing the MECARD itself	Section 7.2.4.11	MC-DIR-035 –M
MC-DIR-095 –M	Display to the user and provide a means of selecting a Recognizable Formats and select the desired application	Section 7.2.4.11	MC-DIR-035 –M
MC-DIR-096 –M	MEBKM syntax is based on the DMF Definition in Section 7.1.2 with the clarifications	Section 7.2.5.1	MC-DIR-001-M
MC-DIR-097 –M	recognise MEBKM: as a Recognizable Format MEBKM: as a Recognised Format when MEBKM: is found embedded within another Recognizable Format.	Section 7.2.5.1	MC-DIR-096 -M
MC-DIR-098 -M	Do not recognise MEBKM: as a Recognised Format when MEBKM: is found embedded within another Recognizable Format.	Section 7.2.5.1	MC-DIR-096 -M
MC-DIR-099 –M	Ignore any Property that is found in the MEBKM but is not included in this Table 4.	Section 7.2.5.1	MC-DIR-096 -M
MC-DIR-100-M	The following characters; comma, “,”, semicolon, “;”, colon, “:”, and back slash, “\”, is escaped as defined in Section 7.1.2.1 using a back slash, “%x5C”, if such a character needs to be included in the Property-Value of MEBKM	Section 7.2.5.1	MC-DIR-096 -M
MC-DIR-101 –M	If the following characters; comma, “,”, semicolon, “;”, colon, “:”, and back slash, “\”, in the Property-Value need to be escaped are found without being escaped in the Property of MEBKM it is ignored	Section 7.2.5.1	MC-DIR-096 -M
MC-DIR-102 –M	MEBKM support the TITLE Property.	Section 7.2.5.2	MC-DIR-096 -M
MC-DIR-103 –M	Property-Value of the TITLE Property is recognised as the title associated with the MEBKM.	Section 7.2.5.2	MC-DIR-096 –M and MC-DIR-102 -M
MC-DIR-104 –M	MEBKM support the URL Property	Section 7.2.5.3	MC-DIR-096 –M
MC-DIR-105 –M	MEBKM URL Property-Value SHALL comply with the definition of the http: and https:, as defined in Section 7.2.1.	Section 7.2.5.3	MC-DIR-096 –M
MC-DIR-106 -M	MEBKM URL Property is recognised as the http: and https: URI schemes associated with the MEBKM.	Section 7.2.5.3	MC-DIR-096 –M
MC-DIR-107 –M	Recognise Property-Value in the URL Property by itself, if it complies with definition, the http: and https: URI schemes associated with the MEBKM, and provide the functions that are defined in Section 7.2.1	Section 7.2.5.3	MC-DIR-096 –M
MC-DIR-108 –M	SHALL provide a means to the user to be able to choose which one, i.e., the MEBKM or the URI scheme, is to be invoked.	Section 7.2.5.3	MC-DIR-096 –M

Item	Function	Reference	Requirement
MC-DIR-109 –M	Section 7.1.2 DMF Definition, certain characters in the URI scheme is denoted by using the escape sequence with a backslash “	Section 7.2.5.3	MC-DIR-096 –M
MC-DIR-110 –M	If MEBKM is chosen an appropriate application invoked to store the data contained in the MEBKM to a bookmark registry on the device.	Section 7.2.5.4	MC-DIR-096 –M
MC-DIR-111 –M	Property-Value of URL Property as a Recognizable Format in addition to recognizing the MEBKM itself, and offer the functions that are specified in Section 7.1.2.2 in addition to that for the MEBKM.	Section 7.2.5.4	MC-DIR-095 –M
MC-DIR-112 –M	With MEBKM provide the user with a means of selecting which application is to be invoked, for recognizable format and the MEBKM	Section 7.2.5.4	MC-DIR-095 –M
MC-DIR-113 -M	MATMSG syntax is based on the DMF Definition in Section 7.1.2 with clarifications	Section 7.2.6.1	
MC-DIR-114 –M	Recognise MATMSG: as a Recognizable Format.	Section 7.2.6.1	MC-DIR-113 -M
MC-DIR-115 –M	MCC SHALL NOT recognise MATMSG: as a Recognised Format when MATMSG: is found embedded within another Recognizable Format.	Section 7.2.6.1	MC-DIR-113 -M
MC-DIR-116 –M	Ignore any Property that is found in the MATMSG format but is not included in this table 6.	Section 7.2.6.1	MC-DIR-113 -M
MC-DIR-117 –M	following characters; comma, “,”, semicolon, “;”, colon, “:”, and back slash, “\”, are escaped as defined in Section 7.1.2.1 using a back slash, if these character needs to be included in the Property-Value MATMSG.	Section 7.2.6.1	MC-DIR-113 -M
MC-DIR-118-M	If characters; comma, “,”, semicolon, “;”, colon, “:”, that need to be escaped are found without being escaped in the Property, they SHALL be ignored	Section 7.2.6.1	MC-DIR-113 -M
MC-DIR-119 –M	Support the TO Property in MATMSG	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-120 –M	TO Property-Value in MATMSG comply with the definition of the Mailbox, as defined in Section 7.2.3	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-121 –M	Recognise each Property-Value of the TO Property as a Mailbox associated with the MATMSG.	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-122-M	If more than one TO Property is found, recognise as many TO Properties as it can process as a group.	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-123 –M	Any TO Properties over and above the maximum number that can be processed as a group SHALL be ignored	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-124 –M	displayed the MATMSG be as an actionable string of characters that is familiar to users in the desired language,	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-125 –M	display each individual TO Property-Value as an actionable string of characters, to the extent that the MCC can process.	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-126 –M	insert the group of recognised TO Property-Values into the destination address fields of an application,	Section 7.2.6.2	MC-DIR-113 -M

Item	Function	Reference	Requirement
MC-DIR-127 –M	Individual TO Property-Values, the MCC behavior is defined in Section 7.2.3.2	Section 7.2.6.2	MC-DIR-113 -M
MC-DIR-128 –M	Support the SUB Property in MATMSG.	Section 7.2.6.3	MC-DIR-113 -M
MC-DIR-129 –M	SUB Property is recognised as the subject of the message associated with the MATMSG.	Section 7.2.6.3	MC-DIR-113 -M
MC-DIR-130 –M	If present, the Property-Value of the SUB Property inserted in the subject field of the application, if MATMSG is selected and invoked.	Section 7.2.6.3	MC-DIR-113 -M
MC-DIR-131 –M	support the BODY Property in MATMSG	Section 7.2.6.4	MC-DIR-113 -M
MC-DIR-132 –M	Property-Value of the BODY Property recognised as the body of the message associated with the MATMSG.	Section 7.2.6.4	MC-DIR-113 -M
MC-DIR-133 –M	Property-Value of the BODY Property is inserted in the body field of the application, if MATMSG is selected and invoked.	Section 7.2.6.4	MC-DIR-113 -M
MC-DIR-134 –M	Provide the user with a means of selecting any one of the actionable strings, i.e., the MATMSG or an individually displayed TO Property-Value.	Section 7.2.6.5	MC-DIR-113 -M
MC-DIR-135 –M	In MATMSG if one of the actionable strings is selected by the user, an appropriate application is invoked.	Section 7.2.6.5	MC-DIR-113 -M
MC-DIR-136 –M	In MATMSG if one of the actionable strings is selected by the user the data in the format that is selected inserted in the respective fields of the application.	Section 7.2.6.5	MC-DIR-113 -M
MC-DIR-137 –M	Recognise MELOC: as the Recognizable Format	Section 7.2.7.1	
MC-DIR-138 –M	Do not recognise MELOC: as the Recognised Format when the MELOC: is found in other Recognizable Format.	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-139 –M	ADR Property-Value input of 100 bytes data	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-140 –M	BLD Property-Value input of 1 bytes data	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-141 –M	FLR Property-Value input of 4 bytes data	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-142 –M	Room Property value 4 bytes	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-143 –M	GEO Property value 17 bytes		
MC-DIR-144 –M	ALT Property-Value input of 4 bytes data	Section 7.2.7.1	MC-DIR-137 -M
MC-DIR-145 –M	display the MELOC with other data such as plain text messages and/or other Recognizable Formats;	Section 7.2.7.2	MC-DIR-137 -M
MC-DIR-146 –M	If multiple Recognizable Formats are recognised, the MCC SHALL provide means for the user to choose one from them.	Section 7.2.7,2	MC-DIR-137 -M
MC-DIR-147 –M	The MCC SHALL make such a format selectable by the user for initiating the appropriate application e. g. map, indoor routing, workforce tracking et	Section 7.2.7.2	MC-DIR-137 -M

Item	Function	Reference	Requirement
MC-DIR-148 –M	If telephone number and an email address are overlapping select the email address as the first priority Recognizable Format	Section 7.3	
MC-DIR-149 –M	IF telephone number and an email address are overlapping recognise a partial string that does not overlap with the string representing the email address if the telephone number defined in 7.2.3.1.	Section 7.3	
MC-DIR-150 –M	overlapping Recognizable Formats are found : select the email address as the first priority Recognizable Format if the email address starts with a telephone number	Section 7.3	
MC-DIR-151 -M	overlapping Recognizable Formats are found: select the Recognizable Format whose first character starts closest to the beginning of the Data String as the first priority Recognizable Format.	Section 7.3	
MC-DIR-152 –M	overlapping Recognizable Formats are found: display the actionable image of the first priority Recognizable Format.	Section 7.3	

B.1.4 MCC Support for Indirect Code Data Format (IDF)

Item	Function	Reference	Requirement
MC-IDF-C-001-M	Indirect Code data format SHALL follow Table 11.	Section 8.1	
MC-IDF-C-002-M	ICI SHALL start at immediately after the Version-Number field and end just before the ICI-DT-Separator field.	Section 8.1	MC-IDF-C-001-M
MC-IDF-C-003-M	ICI-DT-Separator SHALL only be present if and only if there is Display-Text to follow	Section 8.1	MC-IDF-C-001-M
MC-IDF-C-004-M	A new major version number should be used and SHALL be one higher than the latest major version number.	Section 8.1	MC-IDF-C-001-M
MC-IDF-C-005-M	The Code-Marker SHALL contain the format as described in Section 6.1 to indicate that the Mobile Code is an Indirect Code	Section 8.1.1	
MC-IDF-C-006-M	The Version-Number version number of this specification	Section 8.1.2	MC-IDF-C-001-M
MC-IDF-C-007-M	The most significant 4 bits indicate the major version number	Section 8.1.2	MC-IDF-C-001-M
MC-IDF-C-008-M	The least significant 4 bits indicate the minor version number	Section 8.1.2	MC-IDF-C-001-M
MC-IDF-C-009-M	For this specification, this field contains the value “%x10”.	Section 8.1.2	MC-IDF-C-001-M
MC-IDF-C-010-M	The Indirect Code Identifier (ICI) SHALL comprise of the following format Table 35	Section 8.1.3	MC-IDF-C-001-M
MC-IDF-C-011-M	The ICI SHALL consist of two major fields:	Section 8.1.3	MC-IDF-C-001-M

Item	Function	Reference	Requirement
MC-IDF-C-012-M	The length of the ICI field SHALL NOT be more than 36 octets	Section 8.1.3	
MC-IDF-C-013-M	The Length-Indicator SHALL be 4-bit long and contains a 1-hex digit value that indicates the length of the Remaining-Part-of-Routing-Prefix field	Section 8.1.3.1.1	
MC-IDF-C-014-M	The Registry-ID SHALL be assigned by OMNA	Section 8.1.3.1.2	
MC-IDF-C-015-M	A Registry-ID SHALL have a fixed length of 3-hex digits	Section 8.1.3.1.2	
MC-IDF-C-016-M	The value "%x000" SHALL be reserved.	Section 8.1.3.1.2	
MC-IDF-C-017-M	The value "%x001" SHALL be used by OMNA to assign Routing-Prefix directly	Section 8.1.3.1.2	
MC-IDF-C-018-M	The range of values from %x002 to %xFFF SHALL be assigned by OMNA	Section 8.1.3.1.2	
MC-IDF-C-019-M	Remaining-Part-of-Routing-Prefix SHALL be assigned by OMNA or a Registry-ID Recipient to a Resolving CMP	Section 8.1.3.1.3	
MC-IDF-C-020-M	Remaining-Part-of-Routing-Prefix SHALL be equal to the value in the Length-Indicator field + 1	Section 8.1.3.1.3	
MC-IDF-C-021-M	Each octet in the Remaining-Part-of-Routing-Prefix SHALL contain any value from %x00 to %xFF, except %x04	Section 8.1.3.1.3	
MC-IDF-C-022-M	Resolution-Identifier SHALL be assigned by the Resolving CMP for purposes of resolving each ICI	Section 8.1.3.2	
MC-IDF-C-023-M	Resolution-Identifier SHALL be assigned by the Resolving CMP for purposes of resolving each ICI	Section 8.1.3.2	
MC-IDF-C-024-M	The ICI-DT-Separator SHALL be equal to %x04 to indicate the presence of Display-Text that follows immediately after the ICI.	Section 8.1.4	
MC-IDF-C-025-O	Display-Text MAY be present after the ICI and, when present, is preceded immediately by the ICI-DT-Separator	Section 8.1.5	
MC-IDF-C-026-M	The Display-Text, when present, SHALL contain the text string to be displayed on the mobile device	Section 8.1.5	
MC-IDF-C-027-M	The MCC processes the Display-Text that SHALL contain only the following ASCII characters: %x20-7E, %x0A (LF) and %x0D (CR).	Section 8.1.5	

B.1.5 MCC Configuration (CFG)

Item	Function	Reference	Requirement
MC-CFG-C-001-M	MCC installation, provisioning or updating, the MCC SHALL be configured on the mobile device in order to use the MC Enabler	Section 9.1.1	

Item	Function	Reference	Requirement
MC-CFG-C-002-M	If MCC supports resolution of Indirect Codes, the following minimum parameters SHALL be configured in the MCC: • Network Address of the Home CMP	Section 9.1.1	
MC-CFG-C-003-O	If MCC supports resolution of Indirect Codes, the following charging-related parameters MAY be configured in the MCC: • Tracking Address of the tracking server at the Home CMP	Section 9.1.1	
MC-CFG-C-004-M	MCC SHALL support the ability for the user to enter and store user personal data on an 'Opt-in' basis	Section 9.2	Method of entering user personal data is out-of-scope
MC-CFG-C-005-M	The following user personal data SHOULD be supported at minimum: a) Age b) Gender c) Postal Code/Zip Code d) Household Income	Section 9.2	
MC-CFG-C-006-M	MCC to insert available data information and location information in the MC-1-RESOLVE_ICI_REQUEST message and MC-4-TRACKING_REPORT message	Section 9.2.1	
MC-CFG-C-007-M	The user SHALL be able to 'Opt-in' or 'Opt-out' for each (or all) MC-1-RESOLVE_ICI_REQUEST message and MC-4-TRACKING_REPORT message	Section 9.2.1	

B.1.6 MCC Support for Security (SEC)

Item	Function	Reference	Requirement
MC-SEC-C-001-O	This section describes an optional solution that MAY be used to authenticate the MCC to the Home CMP, which comprises of the following procedures	Section 9.3.1	
MC-SEC-C-002-M	used to authenticate the MCC to the Home CMP; if supported, the following procedures SHALL apply:	Section 9.3.1	

B.1.7 MCC Support for Code Resolution (CR)

Item	Function	Reference	Requirement
MC-CR-C-001-M	If the "Display-Text" (as specified in Section 8.1.5) is present, the MCC will display that text	Section 8.2.2.1	
MC-CR-C-002-M	The MCC parse the Indirect Code as specified in Section 8.1 to extract the ICI value as the "ici" parameter and the Version-Number as the "enablerver" parameter	Section 8.2.2.1	

Item	Function	Reference	Requirement
MC-CR-C-003-M	The request contain the following mandatory parameters as specified in Table 15: “ici”, “appid”, “enablerver”, “clientid”, “optout”	Section 8.2.2.1	
MC-CR-C-004-O	The request contain the following of the optional parameters as specified in Table 15: “btype”, “networkidhome”, “networkidroam”	Section 8.2.2.1	
MC-CR-C-005-O	If the “optout” parameter is FALSE and the data is available on the MCC, then the request contain the following optional parameters as specified in Table 15	Section 8.2.2.1	
MC-CR-C-006-M	Otherwise, the MCC will not send any of these mentioned parameters.	Section 8.2.2.1	
MC-CR-C-007-M	If the MC-ERROR message is received, the MCC SHALL display an appropriate text	Section 8.2.2.1	
MC-CR-C-008-M	If the MC-1-RESOLVE_ICI_RESPONSE message is received, the MCC will perform the following	Section 8.2.2.1	
MC-CR-C-009-M	If the “contentdescription” (as specified in Table 16) is present, the MCC SHALL display the data to the user	Section 8.2.2.1	
MC-CR-C-010-M	If the “tracking-address” parameter (as specified in Tables 16) is present, the MCC SHALL invoke tracking for the specified ICI using the received parameter	Section 8.2.2.1	
MC-CR-C-011-M	Otherwise, it SHALL invoke tracking for the specified ICI using the pre-provisioned tracking address on the MCC	Section 8.2.2.1	

B.1.8 MCC Support for Tracking & Reporting Procedures (TRP)

Item	Function	Reference	Requirement
MC-TRP-C-001-M	In order to track chargeable events, the MCC send the MC-4-TRACKING_REPORT message to the Home CMP over the MC-4 interface	Section 8.4.2.1	
MC-TRP-C-002-M	The MC-4-TRACKING_REPORT message contain at least the Indirect Code Identifier and an identifier of the MCC	Section 8.4.2.1	
MC-TRP-C-003-M	If a “trackingaddress” is present in the MC-1-RESOLVE_ICI_RESPONSE message sent from the Home CMP to the MCC, the MCC SHALL send the MC-4-TRACKING_REPORT message to the indicated “trackingaddress”	Section 8.4.2.1	
MC-TRP-C-004-M	If a “trackingaddress” is not present but the *trackingindicator* is set to “true” in the MC-1-RESOLVE_ICI_RESPONSE message sent from the Home CMP to the MCC, the MCC send the MC-4-TRACKING_REPORT message	Section 8.4.2.1	

B.1.9 MCC Support for Interface (INT1) MC-1

Item	Function	Reference	Requirement
MC-INT1-C-001-M	The MC-1 interface support the following REST APIs	Section 10.3	
MC-INT1-C-002-M	The MC-1-RESOLVE_ICI web service request SHALL be made as specified below:	Section 10.3.1.1	
MC-INT1-C-003-M	The URL in the request SHALL be the MC-1-RESOLVE_ICI_REQUEST_URL that is currently configured in the MCC	Section 10.3.1.1	
MC-INT1-C-004-M	The parameters marked "Mandatory" in the Table 15 below SHALL be present in the request	Section 10.3.1.1	
MC-INT1-C-005-O	The parameters marked "Optional" in the Table 15 below MAY be present in the request	Section 10.3.1.1	
MC-INT1-C-006-M	The "cc" SHALL be present when the "post" is present	Section 10.3.1.1	
MC-INT1-C-007-M	If the "income" or "age" contains a free text phrase but the "language" is not present, the default language, English, SHALL apply.	Section 10.3.1.1	

B.1.10 MCC Support for Interface (INT4) MC-4

Item	Function	Reference	Requirement
MC-INT4-C-001-M	The MC-4-TRACKING_REPORT web service request SHALL be made as specified below	Section 10.6.1.1	
MC-INT4-C-002-M	The URL in the request SHALL be one of	Section 10.6.1.1	
MC-INT4-C-003-M	The parameters marked "Mandatory" in Table 23 below SHALL be present in the request	Section 10.6.1.1	
MC-INT4-C-004-O	The parameters marked "Optional" in Table 23 below MAY be present in the request.	Section 10.6.1.1	
MC-INT4-C-005-M	If "usagestatistics" is present it SHALL be structured according to the format in Table 24.	Section 10.6.1.1.1	

B.2 SCR for MC Enabler Server

Section B.2 covers Static Conformance Requirements for the following MC Enabler Server components (also referred to as 'network elements' in the TS):

- Code Management Platform (CMP).
- CMP-Split-Parent (where applicable).
- CMP-Split-Child (where applicable).
- MC Registry (MCR), where applicable.

B.2.1 Home CMP Configuration (CFG)

Item	Function	Reference	Requirement

Item	Function	Reference	Requirement
MC-CFG-S-001-M	Home CMP MAY support the ability for the user to enter and store user personal data on an 'Opt-in' basis	Section 9.2	Method of entering user personal data is out-of-scope
MC-CFG-S-002-M	The following user personal data SHOULD be supported at minimum: a) Age b) Gender c) Postal Code/Zip Code d) Household Income	Section 9.2	
MC-CFG-S-003-M	Home CMP to insert available user personal data information and location information in the MC-3-RESOLVE_ICI_REQUEST message and MC-6-TRACKING_REPORT message	Section 9.2.1	
MC-CFG-S-004-M	The user SHALL be able to 'Opt-in' or 'Opt-out' for each (or all) MC-3-RESOLVE_ICI_REQUEST message and MC-6-TRACKING_REPORT message	Section 9.2.1	
MC-CFG-S-005-M	If user personal data or location information is available and stored locally on the Home CMP, it SHALL be possible for the Home CMP to insert available user personal data	Section 9.2.2	
MC-CFG-S-006-M	If user personal data or location information has been entered and stored in the Home CMP, the user SHALL be able to 'Opt-in' or 'Opt-out'	Section 9.2.2	

B.2.2 Network Element Support for Security (SEC)

Item	Function	Reference	Requirement
MC-SEC-S-001-O	Secure, dedicated & managed physical or logical transport connections (i.e. ranging from Layer 1 TDM to Layer 2/3 VPNs) between the requestor and responder network elements (i.e. CMPs or MCR) nay be used.	Section 9.3.2	
MC-SEC-S-002-M	When insecure or shared transport connections are used (e.g. public Internet connection) between the requestor and responder network elements, the following security measures SHALL be used	Section 9.3.2	
MC-SEC-S-003-M	All communications between requestor and responder network elements SHALL use https	Section 9.3.2	
MC-SEC-S-004-M	As part of the initial registration process, an "apikeyid" and an "apikey" SHALL be generated and provided by the responder network element	Section 9.3.2	
MC-SEC-S-005-M	SHALL concatenate the "tid", "ici" values – making it unique for each request/response, thus safe from spoofing	Section 9.3.2	
MC-SEC-S-006-M	SHALL use the concatenated value to generate a HMAC hash using the "apikey" provided by the responder network element.	Section 9.3.2	

Item	Function	Reference	Requirement
MC-SEC-S-007-M	The requestor network element SHALL include the "apikeyid" and the above signature as part of every request to the responder network element	Section 9.3.2	
MC-SEC-S-008-M	The responder network element uses the "apikeyid" to retrieve the security information associated with the requestor network element (i.e., the stored "apikey") and SHALL validate the signature before proceeding to execute the request.	Section 9.3.2	
MC-SEC-SC-009-M	If authentication in step (e) fails, the responder network element SHALL not execute the request	Section 9.3.2	
MC-SEC-SC-010-M	SHALL return an appropriate error status.	Section 9.3.2	
MC-SEC-SC-011-M	A secure ICI SHALL have the same Routing-Prefix field as that of the original ICI	Section 9.3.3	
MC-SEC-SC-012-M	The routing of a Secure ICI SHALL NOT be changed if any portion of the Resolution-Identifier field of the original ICI is changed. This particular recommendation only applies to transferred ICIs because non-transferred ICI can be routed on the Routing Prefix of the ICI	Section 9.3.3	
MC-SEC-SC-013-M	The maximum length of any Secure ICI SHALL NOT exceed 36 octets, the maximum length of the ICI field	Section 9.3.3	
MC-SEC-SC-014-M	Any octet after the Routing-Prefix part of any Secure ICI SHALL NOT contain the value "%x04", the ICI-DT-Separator	Section 9.3.3	
MC-SEC-SC-015-M	When a Secure ICI scheme is used, it SHOULD be used for all the non-transferred ICIs under a particular Routing Prefix or for all the transferred ICIs under the same ICI block	Section 9.3.3	

B.2.3 CMP Support for Indirect Code Data Format (IDF)

Item	Function	Reference	Requirement
MC-IDF-S-001-M	The Length-Indicator SHALL be 4-bit long and contains a 1-hex digit value that indicates the length of the Remaining-Part-of-Routing-Prefix field	Section 8.1.3.1.1	
MC-IDF-S-002-M	A Registry-ID SHALL have a fixed length of 3-hex digits and with the following specific details:	Section 8.1.3.1.2	
MC-IDF-S-003-M	The value "%x000" SHALL be reserved	Section 8.1.3.1.2	
MC-IDF-S-004-M	The length of the Remaining-Part-of-Routing-Prefix SHALL be equal to the value in the Length-Indicator field + 1	Section 8.1.3.1.3	
MC-IDF-S-005-M	Each octet in the Remaining-Part-of-Routing-Prefix SHALL contain any value from %x00 to %xFF, except %x04	Section 8.1.3.1.3	
MC-IDF-S-006-M	Resolution-Identifier SHALL contain any value from %x00 to %xFF, except %x04	Section 8.1.3.2	

B.2.4 Support for Code Resolution (CR)

Item	Function	Reference	Requirement
MC-CR-S-001-M	If the "ici" is hosted on it, it will follow the procedures specified in Section 8.2.2.5.2	Section 8.2.2.2	
MC-CR-S-002-M	in the case of a Split-CMP-Parent, where the "ici" is hosted on a Split-CMP-Child served by it, it will follow the procedures specified in Section 8.2.2.5.3.	Section 8.2.2.2	
MC-CR-S-003-M	If the Home CMP has the routing information for the specified "ici", it will follow the procedures specified in Section 8.2.2.5.3.	Section 8.2.2.2	
MC-CR-S-004-M	Otherwise, if the Home CMP is configured to query an MCR, it will follow the procedures specified in Section 8.2.2.5.4	Section 8.2.2.2	
MC-CR-S-005-M	the Home CMP set the 'status" to "MC_CANNOT_RESOLVE_ICI" and send the MC-ERROR message as specified in Section 10.2.2 to the MCC	Section 8.2.2.2	
MC-CR-S-006-M	If the "ici" is hosted on it, it will follow the procedures specified in Section 8.2.2.5.2	Section 8.2.2.3	
MC-CR-S-007-M	Otherwise, in the case of a Split-CMP-Parent where the "ici" is hosted on a Split-CMP-Child served by it, it SHALL follow the procedures specified in Section 8.2.2.5.3	Section 8.2.2.3	
MC-CR-S-008-M	Otherwise, if the Remote CMP has the routing information for the specified "ici", it SHALL follow the procedures specified in Section 8.2.2.5.3.	Section 8.2.2.3	
MC-CR-S-009-M	Otherwise, if the Remote CMP is configured to query an MCR, it SHALL follow the procedures specified in Section 8.2.2.5.4	Section 8.2.2.3	
MC-CR-S-010-M	Otherwise, the Remote CMP SHALL set the 'status" to "MC_CANNOT_RESOLVE_ICI" and send the MC-ERROR message as specified in Section 10.2.2 to the requestor CMP	Section 8.2.2.3	
MC-CR-S-011-M	Otherwise, the MCR will retrieve the network address associated with the ICI in the "ici" and generate the MC-2-ROUTE_ICI_RESPONSE as specified in Table 20 in Section 10.4.1.2	Section 8.2.2.4	
MC-CR-S-012-M	The MCR send the MC-2-ROUTE_ICI_RESPONSE message to the CMP	Section 8.2.2.4	
MC-CR-S-013-M	If the CMP is the Home CMP and does not support tracking of ICIs as specified in Section 8.4, it set the "trackingindicator" to 0	Section 8.2.2.5.1	
MC-CR-S-014-M	The "trackingaddress" will not be present in the MC-1-RESOLVE_ICI_RESPONSE message	Section 8.2.2.5.1	
MC-CR-S-015-M	if the CMP is the Home CMP and supports tracking as specified in Section 8.4 and the specified ICI is to be tracked, the Home CMP SHALL set the "trackingindicator" to 1	Section 8.2.2.5.1	

Item	Function	Reference	Requirement
MC-CR-S-016-M	If the "trackingaddress" is present in an MC-3-RESOLVE_ICI_RESPONSE message it SHALL include the "trackingaddress" received in the MC-3-RESOLVE_ICI_RESPONSE message	Section 8.2.2.5.1	
MC-CR-S-017-M	Home CMP is interested in receiving tracking information, it prepend its designated tracking server address to the received "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE message	Section 8.2.2.5.1	
MC-CR-S-018-M	Otherwise, the Home CMP set the "trackingaddress" parameter to the received "trackingaddress" value, subject to local policy	Section 8.2.2.5.1	
MC-CR-S-019-M	If the "trackingaddress" is not present in an MC-3-RESOLVE_ICI_RESPONSE message, it set the "trackingaddress" to the appropriate address	Section 8.2.2.5.1	
MC-CR-S-020-M	as specified in Section 8.4 and the specified ICI is to be tracked, the CMP prepend its designated tracking server address to the received "trackingaddress" parameter	Section 8.2.2.5.1	
MC-CR-S-021-M	the MC-3-RESOLVE_ICI_RESPONSE message, the Remote CMP set the "trackingaddress" to its designated tracking server address when it wants to track the ICI	Section 8.2.2.5.1	
MC-CR-S-022-M	non-Home Resolving CMP that is interested in receiving tracking information set the "trackingaddress" to its designated tracking server address	Section 8.2.2.5.1	
MC-CR-S-023-M	Based on the MC Service Policy conditions, if any, as specified in Section 8.2.3, the Resolving CMP follow the error handling procedures in Sections 10.2.2	Section 8.2.2.5.2	
MC-CR-S-024-M	Otherwise, the Resolving CMP follow the procedures specified in Section 8.2.2.5.1 to set the parameters for ICI tracking	Section 8.2.2.5.2	
MC-CR-S-025-M	The Resolving CMP generate the MC-1-RESOLVE_ICI_RESPONSE message as specified in Table 16 if it is the Home CMP	Section 8.2.2.5.2	
MC-CR-S-026-M	otherwise, it SHALL generate the MC-3-RESOLVE_ICI_RESPONSE as specified in Table 22 and send the message to the requestor CMP.	Section 8.2.2.5.2	
MC-CR-S-027-O	The request contains the following optional parameters as specified in Table 21: "apikeyid", "signature", "addr".	Section 8.2.2.5.3	
MC-CR-S-028-M	The request contain all parameters present in the incoming Code Resolution request message that are relevant to the Code Resolution	Section 8.2.2.5.3	
MC-CR-S-029-M	the request contain additional user personal data and location information if they are available in the Home CMP.	Section 8.2.2.5.3	

Item	Function	Reference	Requirement
MC-CR-S-030-M	The CMP send the MC-3-RESOLVE_ICI_REQUEST message to the Remote CMP and wait for the response	Section 8.2.2.5.3	
MC-CR-S-031-M	Otherwise, the CMP follow the procedures specified in Section 8.2.2.5.1 to set the parameters for ICI tracking	Section 8.2.2.5.3	
MC-CR-S-032-M	The CMP generate the MC-1-RESOLVE_ICI_RESPONSE message as specified in Table 16	Section 8.2.2.5.3	
MC-CR-S-033-M	otherwise, it generate the MC-3-RESOLVE_ICI_RESPONSE as specified in Table 22 and send the message to the requestor CMP.	Section 8.2.2.5.3	
MC-CR-S-034-M	Otherwise, the CMP use the returned "addr" (as specified in Table 20) to identify the Remote CMP to receive the Code Resolution request and follow the procedures in Section 8.2.2.5.3	Section 8.2.2.5.4	

B.2.5 Resolving CMP Support for Service Policy Management (SPM)

Item	Function	Reference	Requirement
MC-SPM-C-001-M	Code Resolution request validity period of the ICI, if specified, SHALL comprise of a 'START-DATE-TIME' and an 'END-DATE-TIME'.	Section 8.2.3.1	
MC-SPM-C-002-M	Code Resolution request geographic area origin of the ICI, if specified, SHALL comprise of either one, or both, of the following geographic location identification information	Section 8.2.3.1	
MC-SPM-C-003-M	If the arrival time as above falls within the range of the validity period policy conditions as specified in Section Section 8.2.3.1	Section 8.2.3.2	
MC-SPM-C-004-M	If the arrival time as above falls outside of the range the validity period policy conditions as specified in Section (1) stored for the ICI, or range of ICIs, then Code Resolution SHALL NOT be completed and an appropriate MC-ERROR message SHALL be returned	Section 8.2.3.2	
MC-SPM-C-005-M	f the geographic location identification information received as above falls within the range of geographic area origin policy conditions as specified in Section 8.2.3.1 (2) stored for the ICI, or range of ICIs, then Code Resolution be completed and the information retrieved	Section 8.2.3.2	
MC-SPM-C-006-M	If the geographic location identification information received as above falls within the range of geographic area origin policy conditions as specified in Section 8.2.3.1 (2) stored for the ICI, or range of ICIs, then Code Resolution be completed and the information retrieved.	Section 8.2.3.2	
MC-SPM-C-007-M	then Code Resolution will not be completed	Section 8.2.3.2	MC-SPM-C-011-M

Item	Function	Reference	Requirement
MC-SPM-C-008-M	appropriate MC-ERROR message SHALL be returned	Section 8.2.3.2	MC-SPM-C-011-M and MC-SPM-C-012-M

B.2.6 Support for Code Transfer Procedures (CTP)

Item	Function	Reference	Requirement
MC-CTP-S-001-M	The old Resolving CMP mark "confirmation pending" for the to-be-transferred out ICI or ICI block.	Section 8.3.2.1.1	
MC-CTP-S-002-M	he old Resolving CMP SHALL mark "transfer out confirmed" for the transferred-out ICI or ICI block or remove information related to the transferred-out ICI or ICI block	Section 8.3.2.1.2	
MC-CTP-S-003-M	case of the old Resolving CMP, it SHALL generate the MC-5-TRANSFER_CONFIRMATION_RESPONSE message as specified in section 10.7.2.2 and send the message to the MCR	Section 8.3.2.1.2	
MC-CTP-S-004-M	In the case of the old resolving Split-CMP-Child, it SHALL generate the MC-6-TRANSFER_CONFIRMATION_RESPONSE message as specified in section 10.8.2.2	Section 8.3.2.1.2	
MC-CTP-S-005-M	the old Split-CMP-Parent store the token or replace the stored token with the value in the "token" received from the request for the ICI or ICI block indicated in the received "ici" or "icibk"	Section 8.3.2.2.1	
MC-CTP-S-006-M	The old Split-CMP-Parent generate the MC-5-CODE_TRANSFER_REQUEST message as specified in section 10.7.1.1, send the message to the MCR and wait for the response.	Section 8.3.2.2.1	
MC-CTP-S-007-M	SHALL mark "pending confirmation" for the to-be-transferred-out ICI or ICI block	Section 8.3.2.2.1	
MC-CTP-S-008-M	SHALL mark "transfer out confirmed, pending notification" for the transferred-out ICI or ICI block	Section 8.3.2.2.2	
MC-CTP-S-009-M	Otherwise, process the received MC-6-TRANSFER_CONFIRMATION_RESPONSE message. The old Split-CMP-Parent mark "transferred out" for the transferred-out ICI or ICI block	Section 8.3.2.2.3	
MC-CTP-S-010-M	the MCR SHALL set the "status" to "MC_UNAUTHORISED" and send the MC-ERROR message to the requestor CMP as specified in Section 10.2.3	Section 8.3.2.3.1	
MC-CTP-S-011-M	SHALL store the token or replace the stored token for the to-be-transferred ICI or ICI block indicated by the "ici" or "icibk	Section 8.3.2.3.1	

Item	Function	Reference	Requirement
MC-CTP-S-012-M	the received token does not match the stored token, the MCR set the "status" to "MC_CT_TOKEN_MISMATCH" and send the MC-ERROR message to the requestor CMP as specified in Section 10.2.3.	Section 8.3.2.3.1	
MC-CTP-S-013-M	The MCR update the network address associated with the ICI or ICI block indicated in the "ici" or "icibk" with that in the received "addr"	Section 8.3.2.3.1	
MC-CTP-S-014-M	The MCR remove the stored token for the transferred ICI or ICI block	Section 8.3.2.3.1	
MC-CTP-S-015-M	The MCR generate the MC-5-CODE_TRANSFER_RESPONSE message as specified in Section 10.7.1.2 and send the message to the requestor CMP	Section 8.3.2.3.1	
MC-CTP-S-016-M	If the old Split-CMP-Parent and new Split-CMP-Parent involved in the Code Transfer are the same, the MCR mark "transfer completed" or "normal" or remove any flag for the transferred ICI or ICI block	Section 8.3.2.3.1	
MC-CTP-S-017-M	Otherwise, the MCR mark "transferred, pending notification" for the transferred ICI or ICI block	Section 8.3.2.3.1	
MC-CTP-S-018-M	The MCR execute the Code Transfer confirmation procedures described in Section 8.3.2.3.2	Section 8.3.2.3.1	
MC-CTP-S-019-M	The MCR executes the Code Transfer confirmation procedures described in Section 8.3.2.3.2	Section 8.3.2.3.1	
MC-CTP-S-020-M	Otherwise, process the received MC-5-TRANSFER_CONFIRMATION_RESPONSE message. The MCR mark "transferred and confirmed" or "normal" or remove any flag for the transferred ICI or ICI block	Section 8.3.2.3.2	
MC-CTP-S-021-M	The new Resolving CMP update the database with the transferred-in ICI or ICI block and information on the MCP and how to resolve the ICI or ICI block	Section 8.3.2.4.1	
MC-CTP-S-022-M	the new Split-CMP-Parent set the "status" to "MC_CT_TOKEN_MISMATCH" and send the MC-ERROR message to the new resolving Split-CMP-Child as specified in Section 10.2.3	Section 8.3.2.5.1	
MC-CTP-S-023-M	The new Split-CMP-Parent update the database for the transferred in ICI or ICI block with the identification of the new resolving Split-CMP-Child	Section 8.3.2.5.1	
MC-CTP-S-024-M	The new Split-CMP-Parent generate the MC-6-CODE_TRANSFER_RESPONSE message as specified in Section 10.8.1.2 and send the message to the new resolving Split-CMP-Child	Section 8.3.2.5.1	
MC-CTP-S-025-M	The new Split-CMP-Parent mark "transferred, pending notification" for the transferred ICI or ICI block	Section 8.3.2.5.1	

Item	Function	Reference	Requirement
MC-CTP-S-026-M	If the new Split-CMP-Parent needs not inform the MCR about the intra-Split-CMP-Parent Code Transfer, it remove the stored token for the transferred ICI or ICI block	Section 8.3.2.5.1	
MC-CTP-S-027-M	The new Split-CMP-Parent store the value in the "token" received from the request for the ICI or ICI block indicated in the "ici" or "icibk	Section 8.3.2.5.1	
MC-CTP-S-028-M	The new Split-CMP-Parent mark "pending report to MCR" for the transferred ICI or ICI block	Section 8.3.2.5.1	
MC-CTP-S-029-M	Otherwise, process the received MC-5-CODE_TRANSFER_RESPONSE message. The new Split-CMP-Parent remove the "pending report to MCR" flag and remove the stored token for the transferred ICI or ICI block	Section 8.3.2.5.1	
MC-CTP-S-030-M	Otherwise, the new Split-CMP-Parent store the value in the "token" and the ICI or ICI block indicated in the "ici" or "icibk" in the received request.	Section 8.3.2.5.1	
MC-CTP-S-031-M	SHALL update the database with the transferred-in ICI or ICI block and the identification of the new resolving Split-CMP-Child	Section 8.3.2.5.1	

B.2.7 CMP Support for Tracking & Reporting Procedures (TRP)

Item	Function	Reference	Requirement
MC-TRP-S-001-M	If the Home CMP supports tracking and reporting it SHALL set the "trackingindicator" to "true" in the MC-1-RESOLVE_ICI_RESPONSE	Section 8.4.2.2	
MC-TRP-S-002-M	Otherwise, the "trackingindicator" SHALL be set to "false".	Section 8.4.2.2	
MC-TRP-S-003-M	the Home CMP SHALL include the "trackingaddress" parameter in the MC-1-RESOLVE_ICI_RESPONSE message and set it to its designated tracking address(es)	Section 8.4.2.2	
MC-TRP-S-004-M	Each "trackingaddress" fragment SHALL have the following format	Section 8.4.2.2	
MC-TRP-S-005-M	Upon reception of the MC-4-TRACKING_REPORT message, the tracking server as designated by the Home CMP able to remove and/or anonymise some data elements in the tracking report	Section 8.4.2.3	
MC-TRP-S-006-M	If multiple CMPs (or Split-CMPs/Parents) were involved in Code Resolution, the tracking server as designated by the Home CMP send the tracking report to the "trackingaddress" received in the MC-3- RESOLVE_ICI_RESPONSE	Section 8.4.2.3	
MC-TRP-S-007-O	Home CMP may remove this tracking address fragment if the Home CMP does not have business agreements with this entity.	Section 8.4.2.3	

Item	Function	Reference	Requirement
MC-TRP-S-008-M	When there are multiple CMPs (or Split-CMPs/Parents) involved in Code Resolution, the "trackingaddress" in the MC-3-RESOLVE_ICI_RESPONSE represent a combination of the tracking address	Section 8.4.2.4	
MC-TRP-S-009-M	Each "trackingaddress" fragment SHALL have the following format	Section 8.4.2.4	MC-TRP-S-010-M
MC-TRP-S-010-O	Under certain circumstances (e.g. as mandated by community restrictions) the [REMOTE_CMPx_TRACKING_ADDRESS]	Section 8.4.2.4	
MC-TRP-S-011-O	Under certain circumstances, some or all [REMOTE_CMPx_TRACKING_ADDRESS_URL] fragments MAY point to a commonly designed neutral 3rd party	Section 8.4.2.4	
MC-TRP-S-012-M	If the Remote CMP is interested in receiving tracking information for the specified ICI and is also the Resolving CMP, the Remote CMP (or Split-CMP-Child where applicable) SHALL set the "trackingaddress" parameter in the MC-3-RESOLVE_ICI_RESPONSE to its designated tracking address(es)	Section 8.4.2.4	
MC-TRP-S-013-M	is not interested in receiving tracking information for the specified ICI and is not the Resolving CMP, it SHALL set the "trackingaddress" parameter of the outgoing MC-3-RESOLVE_ICI_RESPONSE message to the "trackingaddress"	Section 8.4.2.4	
MC-TRP-S-014-M	If the Remote CMP is interested in receiving tracking information for the specified ICI and is also the Resolving CMP, the Remote CMP (or Split-CMP-Child where applicable) SHALL set the "trackingaddress	Section 8.4.2.4	
MC-TRP-S-015-M	Upon reception of the MC-6-TRACKING_REPORT message, the tracking server as designated by the Remote CMP (or Split-CMP-Parent) be able to remove and/or anonymise some data elements in the tracking report	Section 8.4.2.5	
MC-TRP-S-016-M	The tracking server as designated by the Remote CMP (or Split-CMPs-Parent) use URL redirection to send the tracking report to the next entity in the reporting path	Section 8.4.2.5	
MC-TRP-S-017-O	The tracking server as designated by the Remote CMP may remove this tracking address fragment if the Remote CMP does not have business agreements with this entity.	Section 8.4.2.5	

B.2.8 General Interface Considerations (GIC)

Item	Function	Reference	Requirement

Item	Function	Reference	Requirement
MC-GIC-C-001-M	Each MC interface SHALL expose a REST API [REST] web service	Section 10.1	
MC-GIC-C-002-M	Http POST SHALL be used for MC-4-TRACKING _REPORT and MC-6- TRACKING_ REPORT messages	Section 10.1	
MC-GIC-C-003-M	The URL used SHALL always point to one of the MC Enabler network components: the CMP (or Split-CMP-Parent or Split-CMP-Child where applicable) or the MCR	Section 10.1	
MC-GIC-C-004-M	All string parameters containing special characters or spaces SHALL be UTF-8 URL encoded	Section 10.1	
MC-GIC-C-005-M	The root element of all these XML documents SHALL be “envelope	Section 10.1	
MC-GIC-C-006-M	The USER_AGENT text string in the HTTP header SHALL be transmitted unchanged in the requests.	Section 10.1	
MC-GIC-C-007-M	Each REST API response SHALL be in the form of a XML 1.0 document delivered using the http protocol:	Section 10.1	
MC-GIC-C-008-M	Unless otherwise specified, the http header information SHALL contain the 200 OK HTTP status code for all requests that were completed	Section 10.1	
MC-GIC-C-009-M	The HTTP 204 NO CONTENT status code SHALL be used in response to the MC-4-TRACKING_REPORT and MC-6-TRACKING_REPORT messages that were successfully received	Section 10.1	
MC-GIC-C-010-M	The root element of all these XML documents SHALL be “envelope	Section 10.1	
MC-GIC-C-011-M	Each MC web service SHALL have a distinct URL for the request based on the type of web service	Section 10.1	
MC-GIC-C-012-M	The MC Enabler components (the MCC, the CMP and the MCR) SHALL support the parsing of XML 1.0 documents.	Section 10.1	

B.2.9 Error Handling (EH)

Item	Function	Reference	Requirement
MC-EH-S-001-M	In case of an unsuccessful execution of the requested MC web service, the response contain an “mc-error” element as specified in Table 13.	Section 10.2	
MC-EH-S-002-M	The responder network component SHALL set the “status” to	Section 10.2.1	
MC-EH-S-003-M	If the responder network component supports loop-prevention and detects looped routing, it set the “status” to “MC_TOO_MANY_HOPS”	Section 10.2.2	

Item	Function	Reference	Requirement
MC-EH-S-004-M	MC_CANNOT_RESOLVE_ICI" if the requestor is an MCC. The responder network component SHALL NOT forward the newly received Code Resolution request	Section 10.2.2	
MC-EH-S-005-M	This action SHALL also be done for the requestor associated with the previously received Code Resolution request	Section 10.2.2	
MC-EH-S-006-M	If the responder network component is the Resolving CMP that supports Secure ICI and the "ici" in the received Code Resolution request is a Secure ICI that fails the authentication check, it SHALL set the "status" to "MC_ FRAUDULENT_ICI"	Section 10.2.2	
MC-EH-S-007-M	The responder network component SHALL set the "status" to "MC_CANNOT_RESOLVE_ICI" if the Code Resolution request cannot be completed for any other reason not specified in Sections 10.2.1 and 10.2.2 (e.g., no routing information) for the ICI in the received "ici".	Section 10.2.2	
MC-EH-S-008-M	The responder network component SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.	Section 10.2.2	
MC-EH-S-009-M	If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following: SHALL set the "status" to "MC_CANNOT_RESOLVE_ICI".	Section 10.2.2	
MC-EH-S-010-M	If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following: SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.	Section 10.2.2	
MC-EH-S-011-M	If the MC-ERROR message with the correct "tid" is received, the responder network component performs the following: SHALL set the "status" to	Section 10.2.2	
MC-EH-S-012-M	If the MC-ERROR message with the correct "tid" is received, the responder network component performs the following SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.	Section 10.2.2	
MC-EH-S-013-M	The responder network component SHALL set the "status" to	Section 10.2.3	
MC-EH-S-014-M	The responder network component SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.	Section 10.2.3	

Item	Function	Reference	Requirement
MC-EH-S-015-M	If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following: SHALL set the "status" to "MC_CT_NOT_AVAILABLE"	Section 10.2.3	
MC-EH-S-016-M	If the "tid" in the received positive response or MC-ERROR message does not match with the "tid" in the sent request, the responder network component performs the following SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor.	Section 10.2.3	
MC-EH-S-017-M	If the MC-ERROR message with the correct "tid" is received, the responder network component SHALL perform the following: SHALL set the "status" to	Section 10.2.3	
MC-EH-S-018-M	SHALL generate the MC-ERROR message as specified in Table 13 and return the message to the requestor. If the MC-ERROR message with the correct "tid" is received, the responder network component SHALL perform the following	Section 10.2.3	

B.2.10 Support for Interface (INT1) MC-1

Item	Function	Reference	Requirement
MC-INT1-S-001-M	The MC-1 interface support the following REST APIs	Section 10.3	
MC-INT1-S-002-M	The URL in the request SHALL be the MC-1-RESOLVE_ICI_REQUEST_URL that is currently configured in the MCC	Section 10.3.1.1	
MC-INT1-S-003-M	The parameters marked "Mandatory" in the table below SHALL be present in the request	Section 10.3.1.1	
MC-INT1-S-004-O	while the others MAY be present in the request.	Section 10.3.1.1	
MC-INT1-S-005-M	The "cc" SHALL be present when the "post" is present	Section 10.3.1.1	
MC- INT1-S-006-M	The resolved content as specified in Section 10.3.1.2.1	Section 10.3.1.2	
MC- INT1-S-007-M	URL specifying a location to which to send tracking data. Home CMP have full control over this parameter	Section 10.3.1.2	
MC-INT1-S-008-M	In the case of a successful execution of the MC-1-RESOLVE_ICI web service, the response SHALL contain a "codecontentset" element in the root "envelope" element as specified in Table 17	Section 10.3.1.2.1	
MC-INT1-S-009-M	The resolved content items as specified below in Table 18. One or more "codecontent" elements SHALL be present.	Section 10.3.1.2.1	
MC-INT1-S-010-M	The MC-1-RESOLVE_ICI web service error SHALL be made as specified below	Section 10.3.1.3	

Item	Function	Reference	Requirement
MC-INT1-S-011-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.	Section 10.3.1.3	
MC-INT1-S-012-M	The "tid" SHALL NOT be present	Section 10.3.1.3	

B.2.11 Support of Interface (INT2) MC-2

Item	Function	Reference	Requirement
MC-INT2-S-001-M	The MC-2 interface support the following REST API	Section 10.4	
MC-INT2-S-002-M	The URL in the request SHALL be the MC-2-ROUTE_ICI_REQUEST_URL that is currently configured in the CMP	Section 10.4.1.1	
MC-INT2-S-003-M	The parameters marked "Mandatory" in Table 19 below be present in the request	Section 10.4.1.1	
MC-INT2-S-004-O	The parameters marked "Optional" in Table 19 below May be present in the request	Section 10.4.1.1	
MC-INT2-S-005-M	The "apikeyid" is used by the MCR to retrieve security information associated with the requestor CMP	Section 10.4.1.1	
MC-INT2-S-006-M	When using digital signatures for authentication, the "signature" field be present and contain the signature calculated by the requestor CMP	Section 10.4.1.1	
MC-INT2-S-007-M	The parameters marked "Optional" in Table 20 below SHALL be present in the response	Section 10.4.1.2	
MC-INT2-S-008-O	The parameters marked "Mandatory" in Table 20 below May be present in the response.	Section 10.4.1.2	
MC-INT2-S-009-M	The "addr" SHALL be present when the MCR has the routing information for the ICI or ICI block.	Section 10.4.1.2	
MC-INT2-S-010-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.	Section 10.4.1.3	
MC-INT2-S-011-M	The "tid" SHALL be present and SHALL be copied from the "tid" in the request	Section 10.4.1.3	
MC-INT2-S-012-M	One of the possible "status" errors below SHALL be included:	Section 10.4.1.3	

B.2.12 Support of Interface (INT3) MC-3

Item	Function	Reference	Requirement
MC-INT3-S-001-M	The MC-3 interface SHALL support the following REST API	Section 10.5	
MC-INT3-S-002-M	The URL in the request SHALL be the MC-3-RESOLVE_ICI_REQUEST_URL that is provided by the Remote CMP	Section 10.5.1.1	
MC-INT3-S-003-M	The parameters marked "Mandatory" in the Table 21 below SHALL be present in the request	Section 10.5.1.1	

Item	Function	Reference	Requirement
MC-INT3-S-004-O	The parameters marked “Optional” in Table 21 below MAY be present in the request	Section 10.5.1.1	MC-INT3-S-004-M
MC-INT3-S-005-M	The “clientid” is used for identifying an instance of the MCC installation on the specific device. This parameter is generally used by the Home CMP only	Section 10.5.1.1	
MC-INT3-S-006-M	The “apikeyid” is used by the responder CMP to retrieve security information associated with the requestor CMP	Section 10.5.1.1	
MC-INT3-S-007-M	When using digital signatures for authentication, the “signature” field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2	Section 10.5.1.1	
MC-INT3-S-008-M	It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range	Section 10.5.1.1	
MC-INT3-S-009-M	The “income” provides the household income information. A value, when provided, is tied to the currency associated with the “cc”.	Section 10.5.1.1	
MC-INT3-S-010-M	The MC-3-RESOLVE_ICI web service response SHALL be made as specified below	Section 10.5.1.2	
MC-INT3-S-011-M	The parameters marked “Mandatory” in Table 22 below SHALL be present in the response	Section 10.5.1.2	
MC-INT3-S-012-O	The parameters marked “Optional” in Table 22 below MAY be present in the response	Section 10.5.1.2	
MC-INT3-S-013-M	The resolved content as specified in Section 10.3.1.2.1. This element SHALL be present on successful resolution of the “ici”	Section 10.5.1.2	
MC-INT3-S-014-M	URL specifying a location to which to send tracking data. Home CMP	Section 10.5.1.2	
MC-INT3-S-015-M	The MC-3-RESOLVE_ICI web service error SHALL be made as specified below	Section 10.5.1.3	
MC-INT3-S-016-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.5.1.3	
MC-INT3-S-017-M	The “tid” SHALL be present and SHALL be copied from the request	Section 10.5.1.3	

B.2.13 Support for Interface (INT4) MC-4

Item	Function	Reference	Requirement
MC-INT4-S-001-M	The MC-4 interface SHALL support the following REST APIs:	Section 10.6.	
MC-INT4-S-002-M	The URL in the request SHALL be one of:	Section 10.6.1	
MC-INT4-S-003-M	The parameters marked “Mandatory” in the Table 23 below SHALL be present in the request	Section 10.6.1	
MC-INT4-S-004-O	while the others MAY be present in the request	Section 10.6.1	

Item	Function	Reference	Requirement
MC-INT4-S-005-M	Usage information as detailed in Section 10.6.1.1.1. At least one of either the "usagestatistics" or "usagecount" parameter SHALL be present.	Section 10.6.1	
MC-INT4-S-006-M	It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range (e.g., 22-55) or a free text phrase (e.g., "young" or "retired") in the language associated with "cc" up to 20 octets long.	Section 10.6.1	
MC-INT4-S-007-M	It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with "<" or ">" (e.g., <30,000 or >100,000) or a free text phrase	Section 10.6.1	
MC-INT4-S-008-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.6.1.2	
MC-INT4-S-009-M	The "tid" SHALL NOT be present	Section 10.6.1.2	
MC-INT4-S-010-M	One of the possible "status" errors below SHALL be included	Section 10.6.1.2	

B.2.14 Support of Interface (INT5) MC-5

Item	Function	Reference	Requirement
MC-INT5-S-001-M	The MC-5 interface SHALL support the following REST APIs:	Section 10.7	
MC-INT5-S-002-M	The URL in the request SHALL be the MC-5-CODE_TRANSFER_REQUEST_URL that is currently configured in the CMP	Section 10.7.1.1	
MC-INT5-S-003-M	The parameters marked "Mandatory" in Table 25 below SHALL be present in the request	Section 10.7.1.1	
MC-INT5-S-004-O	The parameters marked "Optional" in Table 25 below MAY be present in the request.	Section 10.7.1.1	
MC-INT5-S-005-M	Either "ici" or "icibk" but not both SHALL be present in the request	Section 10.7.1.1	
MC-INT5-S-006-M	The "addr" SHALL be present in the request that is sent by the new CMP (or the Split-CMP-Parent when applicable)	Section 10.7.1.1	
MC-INT5-S-007-M	The "addr" SHALL NOT be present in the request that is sent by the old CMP (or the Split-CMP-Parent when applicable).	Section 10.7.1.1	
MC-INT5-S-008-M	The "apikeyid" is used by the MCR to retrieve security information associated with the requestor CMP (or Split-CMP-Parent when applicable),	Section 10.7.1.1	
MC-INT5-S-09-M	When using digital signatures for authentication, the "signature" field SHALL be present and contain the signature calculated by the requestor CMP	Section 10.7.1.1	
MC-INT5-S-10-M	The parameters marked "Mandatory" in the table below SHALL be present in the response	Section 10.7.1.2	

Item	Function	Reference	Requirement
MC-INT5-S-11-M	while the others MAY be present in the response	Section 10.7.1.2	
MC-INT5-S-12-M	The “tid” SHALL be present and SHALL be copied from the “tid” in the request	Section 10.7.1.2	
MC-INT5-S-13-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.7.1.3	
MC-INT5-S-14-M	The “tid” SHALL be present	Section 10.7.1.3	
MC-INT5-S-15-M	e copied from the “tid” in the request	Section 10.7.1.3	
MC-INT5-S-16-M	One of the possible “status” errors below SHALL be included:	Section 10.7.1.3	
MC-INT5-S-17-M	The MC-5-TRANSFER_CONFIRMATION web service MAY be used by the MCR to inform the old CMP	Section 10.7.2	
MC-INT5-S-18-M	The URL in the request SHALL be the MC-5-TRANSFER_CONFIRMATION_REQUEST_URL that is currently configured in the MCR	Section 10.7.2	
MC-INT5-S-19-M	The parameters marked “Mandatory” in Table below SHALL be present in the request while the others MAY be present in the request	Section 10.7.2	
MC-INT5-S-020-O	The parameters marked “Optional” in Table below MAY be present in the request	Section 10.7.2	
MC-INT5-S-021-M	Either “ici” or “icibk” but not both SHALL be present in the request	Section 10.7.2	
MC-INT5-S-022-M	The “apikeyid” is used by the MCR to retrieve security information associated with the requestor CMP	Section 10.7.2	
MC-INT5-S-023-M	When using digital signatures for authentication, the “signature” field SHALL be present and contain the signature calculated by the requestor CMP (or Split-CMP-Parent, where applicable) as described in Section 9.3.2.	Section 10.7.2	
MC-INT5-S-024-M	The parameters marked “Mandatory” in the Table 28 below SHALL be present in the response	Section 10.7.2.2	
MC-INT5-S-025-M	while the others MAY be present in the response.	Section 10.7.2.2	
MC-INT5-S-026-M	The “tid” SHALL be copied from the “tid” in the request	Section 10.7.2.2	
MC-INT5-S-027-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.7.2.3	
MC-INT5-S-028-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected.	Section 10.7.2.3	
MC-INT5-S-029-M	The “tid” SHALL be present	Section 10.7.2.3	
MC-INT5-S-030-M	SHALL be copied from the “tid” in the request	Section 10.7.2.3	
MC-INT5-S-031-M	One of the possible “status” errors below SHALL be included	Section 10.7.2.3	

B.2.15 Support of Interface (INT6) MC-6

Item	Function	Reference	Requirement
MC-INT6-S-001-M	The MC-6 interface SHALL support the following REST API	Section 10.8	
MC-INT6-S-002-M	The URL in the request SHALL be the MC-6-CODE_TRANSFER_REQUEST_URL that is currently configured in the Split-CMP-Child	Section 10.8.1.1	
MC-INT6-S-003-M	The parameters marked “Mandatory” in Table 29 below SHALL be present in the request	Section 10.8.1.1	
MC-INT6-S-004-O	The parameters marked “Optional” in Table 29 below MAY be present in the request.	Section 10.8.1.1	
MC-INT6-S-005-M	Either “ici” or “icibk” but not both SHALL be present in the request.	Section 10.8.1.1	
MC-INT6-S-006-M	The “apikeyid” is used by the responder CMP to retrieve security information associated with the requestor CMP	Section 10.8.1.1	
MC-INT6-S-007-M	When using digital signatures for authentication, the “signature” field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2.	Section 10.8.1.1	
MC-INT6-S-08-M	The parameters marked “Mandatory” in Table 30 below SHALL be present in the response	Section 10.8.1.2	
MC-INT6-S-09-O	The parameters marked “Optional” in Table 30 below MAY be present in the response	Section 10.8.1.2	
MC-INT6-S-010-M	The “tid” SHALL be present and SHALL be copied from the “tid” in the request	Section 10.8.1.2	
MC-INT6-S-011-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.8.1.3	
MC-INT6-S-012-M	The “tid” SHALL be present and SHALL be copied from the “tid” in the request.	Section 10.8.1.3	
MC-INT6-S-013-M	The MC-6-TRANSFER_CONFIRMATION web service MAY be used by the old Split-CMP-Parent to inform the old Split-CMP-Child about the successful transfer of an ICI or ICI block	Section 10.8.2	
MC-INT6-S-014-M	The MC-6-TRANSFER_CONFIRMATION web service request SHALL be made as specified below	Section 10.8.2.1	
MC-INT6-S-015-M	The URL in the request SHALL be the MC-6-TRANSFER_CONFIRMATION_REQUEST_URL that is currently configured in the Split-CMP-Parent.	Section 10.8.2.1	
MC-INT6-S-016-M	The parameters marked “Mandatory” in Table 31 below SHALL be present in the request	Section 10.8.2.1	
MC-INT6-S-017-O	The parameters marked “Optional” in Table 31 below MAY be present in the request	Section 10.8.2.1	
MC-INT6-S-018-M	Either “ici” or “icibk” but not both SHALL be present in the request.	Section 10.8.2.1	

Item	Function	Reference	Requirement
MC-INT6-S-019-M	The “apikeyid” is used by the responder CMP to retrieve security information associated with the requestor CMP	Section 10.8.2.1	
MC-INT6-S-020-M	When using digital signatures for authentication, the “signature” field SHALL be present and contain the signature calculated by the requestor CMP as described in Section 9.3.2	Section 10.8.2.1	
MC-INT6-S-021-M	The parameters marked “Mandatory” in Table 32 below SHALL be present in the response	Section 10.8.2.2	
MC-INT6-S-022-O	The parameters marked “Optional” in Table 32 below MAY be present in the response	Section 10.8.2.2	
MC-INT6-S-023-M	The “tid” SHALL be present and SHALL be copied from the “tid” in the request.	Section 10.8.2.2	
MC-INT6-S-024-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.8.2.3	
MC-INT6-S-025-M	The “tid” SHALL be present and SHALL be copied from the “tid” in the request	Section 10.8.2.3	
MC-INT6-S-026-M	One of the possible “status” errors below SHALL be included:	Section 10.8.2.3	
MC-INT6-S-027-M	The URL in the request SHALL be the MC-6-TRACKING_URL associated with the recipient CMP as received by the sender CMP in the MC-3_RESOLVE_ICI_RESPONSE	Section 10.8.2.3	
MC-INT6-S-028-M	The parameters marked “Mandatory” in Table below SHALL be present in the request	Section 10.8.3.1	
MC-INT6-S-029-O	The parameters marked “Optional” in Table 33 below MAY be present in the request.	Section 10.8.3.1	
MC-INT6-S-030-M	Usage information as detailed in Section 10.8.3.1.1. At least one of either the “usagestatistics” or “usagecount” parameter SHALL be present.	Section 10.8.3.1	
MC-INT6-S-031-M	It SHALL contain a numeric value for an exact age (e.g., 35), two values separated by a dash indicating a range (e.g., 22-55) or a free text phrase	Section 10.8.3.1	
MC-INT6-S-032-M	It SHALL contain a numeric value for an exact income (e.g., 50,000), two values separated by a dash indicating a range (e.g., 35,000-75,000), a value with “<” or “>” (e.g., <30,000 or >100,000) or a free text phrase	Section 10.8.3.1	
MC-INT6-S-033-M	Provides the number of times the resolved content has been accessed. At least one of either the “usagestatistics” or “usagecount” parameter SHALL be present.	Section 10.8.3.1	
MC-INT6-S-034-M	The MC-ERROR message defined in Section 10.2 SHALL be returned when a failure is detected	Section 10.8.3.2	
MC-INT6-S-035-M	The “tid” SHALL NOT be present	Section 10.8.3.2	
MC-INT6-S-036-M	One of the possible “status” errors below SHALL be included	Section 10.8.3.2	

Appendix C. Best Practices of Character Set for Direct Code Display of QR Code (Informative)

This section summarises some best practices in the industry for character sets that are used for Direct Code.

C.1 Japan

Instead of ISO/IEC 18004:2006 [QR], JIS X 0510 [JIS X 0510] is normatively referenced by all Japanese QR Code implementations. JIS X 0510 contains the same specifications as those of ISO/IEC 18004:2006 [QR] except for minor points. One of the differences is that JIS X 0510 defines the default character set to be JIS X 0201 (8-bit character set) [JIS X 0201] and JIS X 0208 (Shift JIS) [JIS X 0208].

The following features are mandated in addition to those that are specified in 5.1.1.

- [JIS X 0201] must be the character set to be used for Byte mode,
- Kanji mode as defined by [QR] must be supported, and
- Any combination of those specified in 5.1.1.4 and Kanji mode must be supported.

Appendix D. MC Interfaces (Informative)

This appendix contains MC Interface web service examples.

D.1 Examples of MC-1-RESOLVE_ICI web service

D.1.1 Example 1

Request:

http://resolver.acme-home.com/?ici=P812345612345&appid=1234&enablerver=%x10&clientid=5678&optout=true

Response:

```
<? xml version="1.0" encoding="UTF-8" ?>
<envelope>
        <MC-1-RESOLVE_ICI_RESPONSE>
                <codecontentset>
                        <codecontent>
                                <type>http://www.acontentschema.com/URL</type>
                                <contentelement>
                                        {...content as described by the content schema...}
                                </contentelement>
                        </codecontent>
                </codecontentset>
                <trackingindicator>FALSE</trackingindicator>
        </MC-1-RESOLVE_ICI_RESPONSE>
</envelope>
```

D.1.2 Example 2

Request:

http://resolver.acme-home.com/?ici=
P812345612345&appid=1234&enablerver=%x10&clientid=5678&btype=DM&optout=false&
cc=us&post=11111&age=45&income=50000&gender=male&locationinfo=43.7000,-
79.5000&networkidhome=310120&networkidroam=40436

Response:

```
<? xml version="1.0" encoding="UTF-8" ?>
<envelope>
        <MC-1-RESOLVE_ICI_RESPONSE>
                <codecontentset>
                        <codecontent>
                                <type>http://www.acontentschema.com/URL</type>
                                <title>Homepage</title>
                                <contentelement>
                                        {...content as described by the content schema...}
                                </contentelement>
                        </codecontent>
                </codecontentset>
                <contentdescription>Link to OMA homepage</contentdescription>
                <trackingindicator>TRUE</trackingindicator>
                <trackingaddress>
                        http://www.cmp1.com/tracking?t2=http://www.cmp2.com/metrics/2009?t3=http://www.cmp3.net/report
                </trackingaddress>
        </MC-1-RESOLVE_ICI_RESPONSE>
</envelope>
```

D.2 Examples of MC-3-RESOLVE_ICI web service

D.2.1 Example 1

Request:

http://resolver.acme-remote.com/?tid=512345&ici=P812345612345&clientid=5678

Response:

```
<? xml version="1.0" encoding="UTF-8" ?>

<envelope>
        <MC-3-RESOLVE_ICI_RESPONSE>
                <tid>512345</tid>
                <codecontentset>
                        <codecontent>
                                <type>http://www.acontentschema.com/URL</type>
                                <contentelement>
                                        {...content as described by the content schema...}
                                </contentelement>
                        </codecontent>
                </codecontentset>
        </MC-3-RESOLVE_ICI_RESPONSE>
</envelope>
```

D.2.2 Example 2

Request:

http://resolver.acme-remote.com/?tid=512345&ici=
P812345612345&clientid=5678&apikeyid=613a333a7b693a303b733a3132383a22674378dba9f3251&signature=ac99f1ecfc
179c8226ee9e137da80337 &cc=us&post=11111&age=45&income=50000&gender=male&locationinfo=43.7000,-
79.5000&networkidhome=310120&networkidroam=40436

Response:

```
<? xml version="1.0" encoding="UTF-8" ?>
<envelope>
        <MC-3-RESOLVE_ICI_RESPONSE>
                <tid>512345</tid>
                <codecontentset>
                        <codecontent>
                                <type>http://www.acontentschema.com/URL</type>
                                <title>Homepage</title>
                                <contentelement>
                                        {...content as described by the content schema...}
                                </contentelement>
                        </codecontent>
                </codecontentset>
                <contentdescription>Link to OMA homepage</contentdescription>
                <trackingaddress>
                        http://www.cmp2.com/metrics/2009?t3=http://www.cmp3.net/report
                </trackingaddress>
        </MC-3-RESOLVE_ICI_RESPONSE>
</envelope>
```

Appendix E. Best Practices for making Mobile Code reading successful (Informative)

In order to provide the users with successful reading experiences of the mobile codes that are specified in this specification, the players that constitute the ecosystems need to satisfy certain requirements that are specific to each player. There are fundamentally three players:

a) Hardware Developers: Device vendors and optical component vendors (lenses, cameras, etc);

b) MCC Developers: Those who develop the MCC software. They may develop the MCC: i) inside a device vendor who may have influence on or control of the hardware design, or ii) independent of a device vendor targeting at various devices from different device vendors that are available in the market; and

c) Publishers: Those who publish mobile codes on printed materials or computer displays.

This informative appendix aims to highlight key requirements relevant to aspects of Mobile Code generation and reading from the perspectives of the players as above. Further to this informative appendix, [NTTDOCOMOGUIDE] and [NTTDOCOMOFUNC] also provide recommendations for Mobile Code generation and reading.

E.1 Quiet Zone

The requirement of a Quiet Zone pertains to:

i) The performance of an algorithm that reads a symbology and is implemented in the MCC; and,
ii) The size of the Quiet Zone that is provided for a printed mobile code by a Publisher so that the symbology is successfully read by a MCC.

1	Requirement: Quiet Zone		
Player		**Relevance**	**Recommendation**
(a)	Hardware Developers	Not directly	None
(b)	MCC Developers	YES	Normative (Sections 5.1.1.6 and 5.1.2.4)
(c)	Publishers	YES	Informative (Appendix E1.3)

E.1.1 Hardware Developers

No requirements.

E.1.2 MCC Developers

The requirements for Quiet Zones are specified normatively in Sections 5.1.1.6 and 5.1.2.4. It should be noted that these requirements are essential for developing a successful MCC.

E.1.3 Publishers

It is important for Publishers to provide a sufficiently large Quiet Zone width when printing a QR Code or a Data Matrix symbol, so that the width is supported by the performance of the MCC that is used for reading the mobile code. It must be matching with the requirements that are addressed by the MCC Developer.

(1) QR Code

In Japan where the QR Code has been ubiquitously adopted and used, 4X or larger Quiet Zones are recommended for printed QR Code symbols. However, even a device that meets this requirement may fail to read the symbology. Thus, it is recommended for the Publishers to confirm if their printed QR Code symbols are successfully read by the targeted devices before publishing the codes. In case where the printed symbol of the created code is not recognised, it is recommended to make the width of the Quiet Zone larger for printing.

(2) Data Matrix

1X or larger Quiet Zones are mandated for printed Data Matrix symbols. However, it has been found with commercial implementations of Data Matrix reading software that a larger Quiet Zone of at least 2X significantly increases reading performance and tolerance against difficult reading conditions (as e.g. low lighting, skew angle, blur due to imperfect focus, etc.). An even stronger enlarged Quiet Zone is beneficial for Data Matrix symbols with large (logical) dimensions beyond 26x26 cells. Thus, it is recommended for the Publishers to use a Quiet zone of at least 2X for Data Matrix symbols up to 26x26 cells and a Quiet Zone of 4X for Data Matrix symbols of size 32x32 and higher. It is also recommended, to confirm if their printed Data Matrix symbols are successfully read by the targeted devices before publishing the codes. In case where the printed symbol of the created code is not recognised, it is recommended to make the width of the Quiet Zone larger for printing.

E.2 The minimum module width X

The requirement of the minimum module width X pertains to:

i) The performance of the optics, such as lenses, cameras, etc., for appropriately capturing an image of a symbology that has the smallest module width ; and,

ii) The minimum module width that a Publisher can use to print a mobile code on printed materials or computer displays, so that the symbology is successfully read by a MCC.

2	Requirement: Minimum Module Width X		
Player		**Relevance**	**Recommendation**
(a)	Hardware Developers	YES	Informative (Appendix E2.1)
(b)	MCC Developers	Not directly	None
(c)	Publishers	YES	Informative (Appendix E2.3)

E.2.1 Hardware Developers

The scanning technology that is used in devices implementing the OMA MCC, including cameras, lenses, optics, etc. shall be able to read QR Code symbols and Data Matrix symbols of which module width X is 0.25 mm or larger.

E.2.2 MCC Developers

No requirements.

E.2.3 Publishers

It is important for Publishers to provide a sufficiently large module width when printing a QR Code symbol or a Data Matrix symbol so that the module width is supported by the performance of the optics developed by the Hardware Developer.

(1) QR Code

Based on the experiences in Japan where the QR Code has been ubiquitously adopted and used, module widths larger than 0.28mm are recommended for printed QR Code symbols. However, a QR Code with a module width that is sufficiently larger than this minimum module width may not be successfully read by a device due to various reasons. Thus, it is recommended for the Publishers to confirm if their printed codes are successfully read by the targeted devices before publishing the codes. In case where the printed symbol of the created mobile code is not recognised, it is recommended to make the module width larger for printing.

(2) Data Matrix

Module widths larger than 0.28mm are recommended for printed Data Matrix symbols. However, a Data Matrix symbol with a module width that is sufficiently larger than this minimum module width may not be successfully read by a device due to various reasons. Thus, it is recommended for the Publishers to confirm if their printed code symbols are successfully read by the targeted devices before publishing the codes. In case where the printed symbol of the created mobile code is not recognised, it is recommended to make the module width larger for printing.

E.3 Symbol Contrast

Symbol Contrast is the difference of reflectance between the light module (a module that the reflectance is high) and the dark module (a module that the reflectance is low) in the symbol. When a mobile code symbol is to be recognised with the camera, the larger the Symbol Contrast, the easier the recognition of the symbol becomes. Conversely, it is more difficult to recognise a mobile code symbol if the Symbol Contrast is smaller. Hence, it is important to recommend the minimum Symbol Contrast that the recognition is expected to be successful.

The requirement of Symbol Contrast pertains to the following 3 elements:

i) The performance of the optics, such as lenses, cameras, etc., for appropriately capturing an image of a printed symbology of which Symbol Contrast is equal to or larger than what is specified;

ii) The performance of the algorithm to read a symbology, which is implemented in the MCC; and

iii) The minimum Symbol Contrast that a Publisher can use to print a mobile code symbol on printed materials or computer displays, so that the symbol is successfully read by the MCC.

1	Requirement: Symbol Contrast		
Player		**Relevance**	**Recommendation**
(a)	Hardware Developers	Yes	Informative
(b)	MCC Developers	Yes	Informative
(c)	Publisher	Yes	Informative

E.3.1 Hardware Developers

It is important for Hardware Developers to develop optics with enough performance for such Symbol Contrast that is used by Publishers when printing a QR Code symbol or a Data Matrix symbol.

Based on the experiences in Japan where the QR Code has been ubiquitously adopted and used, the scanning technology that is used in devices implementing the MCC, including cameras, lenses, optics, etc. shall be able to read QR Code symbols and Data Matrix symbols whose Symbol Contrast is 45% or larger.

E.3.2 MCC Developers

It is recommended for MCC Developers to implement an appropriate image correction (or contrast correction) in the MCC for the purpose of improving the code recognition performance for printed mobile code symbols whose Symbol Contrast is 45% or larger.

E.3.3 Publishers

It is important for Publishers to provide a sufficiently large Symbol Contrast when printing a QR Code symbol or a Data Matrix symbol, so that the Symbol Contrast is sufficiently larger than the minimum Symbol Contrast that is supported by the devices that implement the MCC and are used for reading the mobile code.

Based on the experiences in Japan, the Symbol Contrast of printed mobile code symbols shall be 55% or larger.

However, a mobile code symbol with a Symbol Contrast that is sufficiently larger than the minimum Symbol Contrast may not be successfully read by a device. Thus, it is recommended for the Publishers to confirm if their printed codes are successfully read by the targeted devices before publishing the codes. In case where the printed symbol of the created mobile code is not recognised, it is recommended to increase the Symbol Contrast for printing.

Note: The measurement methodology and grading of the Symbol Contrast are standardised by ISO/IEC15415 [ISO/IEC15415]. The Symbol Contrast 55% or more corresponds to the grade B in the ISO standard, and is recommended as the OMA standard when a mobile code symbol is printed. However, when printing a mobile code symbol, the Symbol Contrast varies according to the various conditions of the printing materials; for example, the quality of the paper (newspapers, magazines, posters, fliers, etc.), the printing methods, and the colours of ink to be used. Therefore, the Symbol Contrast 45% or more that gives enough margins to 55% is recommended for the Hardware Developers to support. This is based on the experiences in Japan, which has been proven to be successful.

E.4 Lighting

When a mobile code symbol is to be recognised with the camera, the environmental condition (Lighting) of the place in which the symbols is captured by the camera critically influences the performance of the recognition. It is assumed that the MCC needs to capture and recognise mobile code symbols indoors as well as outdoors. The indoor Lighting varies. Hence, it is necessary to set up some guidelines for the Lighting conditions for successful recognition, so that the devices that implement the MCC are able to successfully recognise the mobile codes under such an environmental condition.

The requirement of Lighting pertains to the following two performances:

i) The performance of the optics, such as lenses, cameras, etc., for appropriately capturing an image of a mobile code symbol under a given Lighting condition; and

ii) The performance of the algorithm to read a symbology, which is implemented in the MCC.

1	Requirement: Lighting		
Player		**Relevance**	**Recommendation**
(a)	Hardware Developers	Yes	Informative
(b)	MCC Developers	Yes	Informative
(c)	Publisher	No	None

E.4.1 Hardware Developers

Based on the experiences in Japan, the scanning technology that is used in the devices implementing the MCC, including cameras, lenses, optics, etc. shall be able to read QR Code symbols and Data Matrix symbols under the condition of 30lx-5000lx in the illuminance. Especially, it is recommended to recognise the symbols under the condition of 200lx-1200lx in the illuminance.

It is recommended for the devices to have a capability to be able to illuminate the symbols by some means, e.g., the photo-light etc., when recognition of the symbol is difficult under the low illumination conditions.

E.4.2 MCC Developers

It is recommended for MCC Developers to implement an appropriate image correction (or illumination correction) in the MCC for the purpose of improving the code recognition performance for printed mobile code symbols under the conditions of 30lx-5000lx in the illuminance.

E.4.3 Publishers

No requirements.

Note: The standard of Lighting of indoor work space is standardised by ISO 8995 [ISO 8995-1].

Appendix F. A Structured Append Mode Implementation Example (Informative)

This Appendix describes an Informative note for a Structured Append mode implementation example.

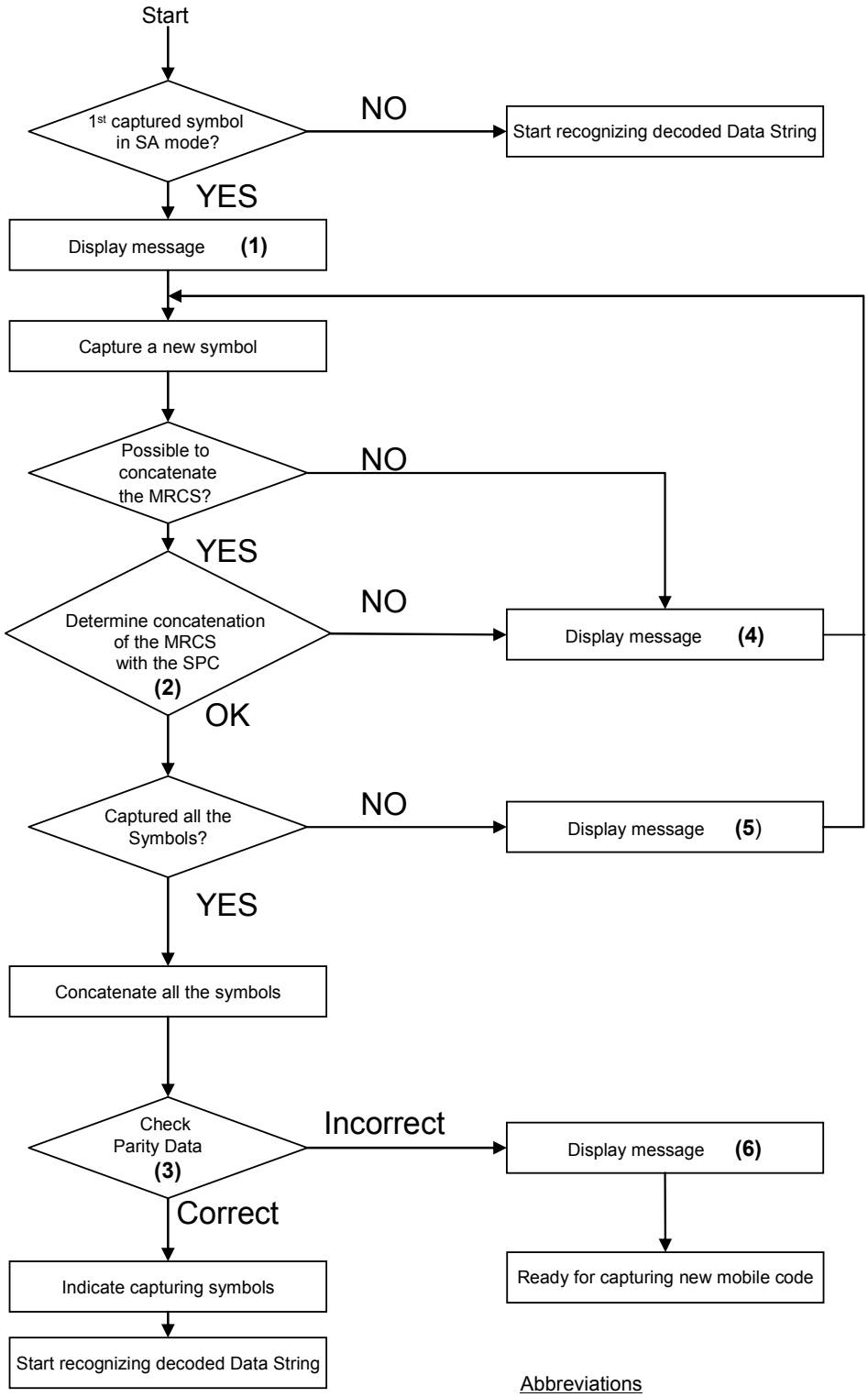
The Structured Append mode, as specified by 5.1.1.7 for QR Code and 5.1.2.5 for Data Matrix, is used to split the encoding of the data from a message over a number of symbols. All of the symbols require to be read and the data message needs to be reconstructed in the correct sequence. This mode is typically used in case where the data size exceeds the capacity of the limit of one symbol.

Structured Append mode requires the user to capture multiple symbols one after another based on instructions from the MCC to the user.

The following flow chart describes an example of such a capturing process of multiple symbols that are in the Structured Append mode. The flow chart describes an example implementation that has been developed for QR Code. While there are minor differences in the specifications of the Structured Append modes for QR Code and Data Matrix, the overall process is very similar. The differences due to the original ISO specifications are described in the notes.

One of the important design issues is that the user should always be able to terminate the process anytime wherever the step may be. This is defined in the respective normative sections.

F.1 Flow Chart



Abbreviations
SA: Structured Append
MRCS: Most recently captured symbol
SPC: Symbol(s) previously captured

(1) Display the fact that the first captured symbol uses the Structured Append mode. Prompt the user to capture the next symbol. Display the number of remaining symbols to be captured, and the number of the total number of all the symbols.

(2) Determine concatenation of the most recently captured symbol with the symbol(s) previously captured based on the Parity Data and the Symbol Sequence Indicator.

Refer to Chapter 7 of [QR] for determining valid concatenation of QR Code.

Refer to Section 5.6 of [DATAMARTIX] for determining valid concatenation of Data Matrix.

Note that "the Parity Data" is not defined in the symbol syntax of Data Matrix. Therefore, the process (2) is based only on the Symbol Sequence Indicator in the case of Data Matrix. In addition, the process (3) is not necessary for decoding a Data Matrix code of the Structured Append mode.

(3) Refer to Chapter 7 of [QR] for checking the Parity Data.

Note that the process (3) is not necessary for decoding a Data Matrix code of the Structured Append mode, since Data Matrix does not define “the Parity Data”.

(4) Indicate that the symbol most recently captured is not possible to be concatenated, and prompt the user to start capturing a next symbol. Discard the symbol that is not possible to be concatenated. Indicate that the symbol is already captured, if the symbol most recently captures has already been captured before.

(5) Prompt the user to start capturing a next symbol. Display the number of remaining symbols to be captured, and the number of the total number of all the symbols.

(6) Indicate that the symbols (or the mobile code) are not possible to be concatenated, and go back to starting state which is ready for capturing new mobile codes.

As defined normatively in Section 5.1.1.7, and Section 5.1.2.5, the MCC must support a mechanism that allows the user to exit from the process of capturing multiple QR Code symbols or Data Matrix symbols, wherever and whenever the user may be in the process of capturing these symbols if the user wishes to do so.

Appendix G. Code Resolution Worst Case Scenario (Informative)

G.1 Introduction

This section describes the worst case scenario in resolving an ICI. The purpose is to show that many CMPs and MCRs may be involved and how the Code Resolution request or response is routed.

G.2 Message Flows

Figure 1 shows the message flows in resolving an ICI. In this scenario, the specified ICI is not hosted on the Home CMP and a Split-CMP-Child, instead of a CMP, resolves the specified ICI. In this scenario, the Remote CMPs are involved in routing the MC-3-RESOLVE_ICI_REQUEST message where the Remote CMPx provides services to the Home CMP and the Remote CMPy provides services to the Split-CMP-Parent of the Resolving Split-CMP-Child and Remote CMPx and Remote CMPy each queries an MCR for routing information.

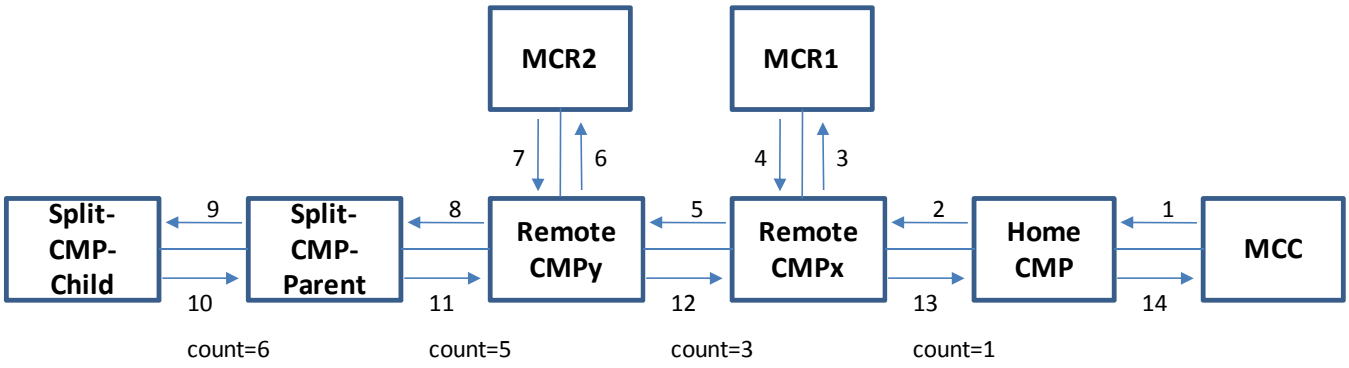


Figure 1: Message Flows in Resolving an ICI in the Worst Case Scenario

The steps in resolving the specified ICI are described below:

1. The MCC sends the MC-1-RESOLVE_ICI_REQUEST message to the Home CMP.
2. The Home CMP sends the MC-3-RESOLVE_ICI_REQUEST message to the Remote CMPx.
3. The Remote CMPx sends the MC-2-ROUTE_ICI_REQUEST message to the MCR1.
4. The MCR1 returns the MC-2-ROUTE_ICI_RESPONSE message to the Remote CMPx.
5. The Remote CMPx sends the MC-3-RESOLVE_ICI_REQUEST message to the Remote CMPy.
6. The Remote CMPy sends the MC-2-ROUTE_ICI_REQUEST message to the MCR2.
7. The MCR2 returns the MC-2-ROUTE_ICI_RESPONSE message to the Remote CMPy.
8. The Remote CMPy sends the MC-3-RESOLVE_ICI_REQUEST message to the Split-CMP-Parent of the Resolving Split-CMP-Child.
9. The Split-CMP-Parent sends the MC-3-RESOLVE_ICI_REQUEST message to the Split-CMP-Child.
10. The Split-CMP-Child returns the MC-3-RESOLVE_ICI_RESPONSE message to the Split-CMP-Parent.
11. The Split-CMP-Parent returns the MC-3-RESOLVE_ICI_RESPONSE message to the Remote CMPy.
12. The Remote CMPy returns the MC-3-RESOLVE_ICI_RESPONSE message to the Remote CMPx.
13. The Remote CMPx returns the MC-3-RESOLVE_ICI_RESPONSE message to the Home CMP.
14. The Home CMP returns the MC-1-RESOLVE_ICI_RESPONSE message to the MCC.

G.3 Discussion

Figure 1 shows that several CMPs (or the Split-CMP-Parents when applicable) can be involved in routing the Code Resolution request and two MCRs can be queried to retrieve the routing information for resolving an ICI. Also not shown in Figure 1, the Domain Name System (DNS) is used to retrieve the IP address associated with the hostname in the http URL of the Code Resolution request when no cached information is available. Therefore, the timers at the MCC and CMPs (or the Split-CMP-Parents when applicable) would need to consider the worst-case scenario. Since several CMPs (or the Split-CMP-Parents when applicable) may be involved, a loop due to the incorrect routing information at some of the involved CMPs (or the Split-CMP-Parents when applicable) could be formed; therefore, it is recommended that the CMPs (or the Split-CMP-Parents when applicable) support some loop-prevention mechanisms.

Appendix H. Guideline for Direct Code Authors (Informative)

Scope: This Appendix explains how to make Direct Codes that can be recognised by Mobile Code Client (MCC) applications that are compliant with the OMA MC Enabler specification. The content in this Appendix is informational; in case of any discrepancies between descriptions in this guideline and the MC technical specification, the normative sections of the specification always supersedes this guideline.

Audience: The targeted audience of this Appendix is the authors who want to create Direct Codes that will be recognised by the mobile phones implementing the MCC.

H.1 Introduction

A Direct Code is able not only to display the text stored in the code but also to offer other various actionable features. They are enabled by mobile phones with cameras that implement the MCC specified in this specification.

For example, you can encode your contact information, phone numbers, and/or email addresses into a Direct Code, and publish the encoded Direct Code on your business cards or on your web pages for convenient access. The intended users will capture the symbol image of the Direct Code that you published, using their mobile phones with cameras, and will be able to read the information or use the data that you encoded in the Direct Code. Figure 2 shows the overall concept of the Direct Code recognition.

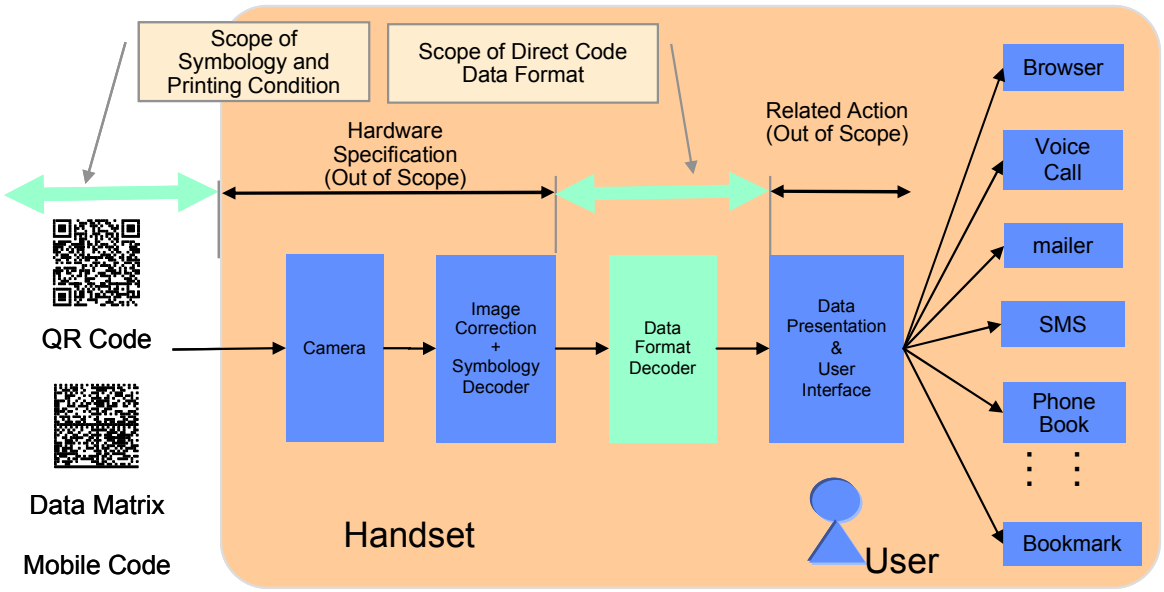


Figure 2: Overall Concept of the Direct Code Recognition

There are two aspects that are explained in this Appendix:

(1) **Data Format Aspect:** To offer various functions, the data format encoded in Direct Codes is defined. In the mobile phones that have captured the symbol images of your Direct Code, the following steps are executed:

- The symbology, i.e., QR Code or Data Matrix, is decoded;
- The data format encoded in your Direct Code is decoded and recognised; and
- Various functions related to the data format are invoked.

The data formats and the functions related to the data formats for Direct Codes are further explained later.

(2) **Symbology Aspect**: In order to provide the readers of your Direct Codes with successful reading experiences, the specifications of symbology that is used in the Direct Codes and printing condition of the Direct Codes are important. These aspects are further explained later.

In order to facilitate the recognition of Direct Codes, the performances of the camera (including lenses, optics) and the code recognition software is also important. These aspects are not discussed herein as they are dependent on the specific mobile phone implementation.

H.2 Creating Direct Codes

(1) Function and syntax

A Data String for a Direct Code contains human readable plain text messages and data formats that are specified by this specification and are recognised by the MCC. Such a data format is defined as a Recognizable Format. The plain text messages and Recognizable Formats may appear in a Data String of a Direct Code in any order or in any number of occurrences within the physical limitation of the symbols. One of the main objectives for introducing the dedicated syntaxes for Direct Codes that is specified in this specification is to reduce the size of the physical symbols. Since printed Direct Codes are required to fit into a small footprint to make it useful in the market, the content has to be compact enough.

The Recognizable Format has the following types, each of which enables specific functions, respectively:

- Telephone Number String Recognition and Tel URI Scheme (Finds telephone numbers and enables the reader to initiate a voice call or send an SMS message).
- Web access (Finds a URL and enables launching a web browser to access the URL).
- Mail address recognition (Finds email addresses and enables invoking an email application).
- Business Card Recognition :MECARD (Registers contact data to a phone book).
- Bookmark Recognition :MEBKM (Registers a URL data into a bookmark registry).
- E-mail linkage data format recognition :MATMSG (Enables launching an email application and inserting the data in appropriate fields of the application).

(2) How to make a Direct Code

A Direct Code is created using the following procedures.

You will:

a) Create a Data String that includes a plain text message and/or Recognizable Formats (web addresses, phone numbers, email addresses, business cards, bookmarks or just text…etc).

b) Generate a Direct Code using the Data String and save the image.

c) Print the image of the Direct Code on a paper or publish it on a website for distribution.

Your user will:

d) Scan the Direct Code with your camera phone. The image may be scanned from a printed material, on a computer monitor, or on a mobile device's screen.

e) Use the recognised results for further actions.

(3) How to determine the symbol size of a Direct Code

You can choose different sizes for the Direct Code depending on what you want to do with it.

The readability of a Direct Code may vary from a device to a device. For example, the distance from which the reader scans the symbol image is very important. Also you need to consider the suitable size of the published symbol to be scanned. For example, will the symbol be published on a computer screen, on a paper, etc? The basic rules is that you need to test reading your published Direct Code symbols using as many intended devices as possible before publishing the Direct Code for your intended users.

H.3 Syntax of Plain Text Message and Recognisable Format

You encode a plain text message and/or data that complies with a Recognizable Format into a Direct Code, and the users will scan the Direct Code. The data will appear in the mobile phone as it was typed and with added functionality. The user will be able to click the data and pass the data to an appropriate application. For example, clicking on the URL will launch the browser with that URL.

A Direct Code uses plain text (printable characters) messages and/or Recognizable Formats.

- The plain text messages help human readability and facilitate creation of a Direct Code. Plain text messages are displayed to the user as they are written and not processed any further by the MCC. They may be in any human language such as English, Spanish, French, Italian, Arabic, Chinese, Korean, Japanese, etc. Note that support of various language character sets other than the ASCII code character set is subject to the mobile phone implementations, while this specification is flexible enough to support a variety of character sets.

- Recognizable Formats are defined in the specification of the Direct Code, and recognised by the MCC. They enable causing certain actions by displaying the recognition results to the user along with the messages if any. A string of text to which a specific function is allocated in Recognizable Format is displayed as an actionable string (a highlighted, selectable and clickable string). Options to select and/or to invoke an application are offered for the user. The invocation typically involves the user's intervention, e.g., menu selection and/or confirmation, etc.

A Direct Code may contain an arbitrarily number of plain text messages and Recognizable Formats in an arbitrary order as shown in Figure 3.

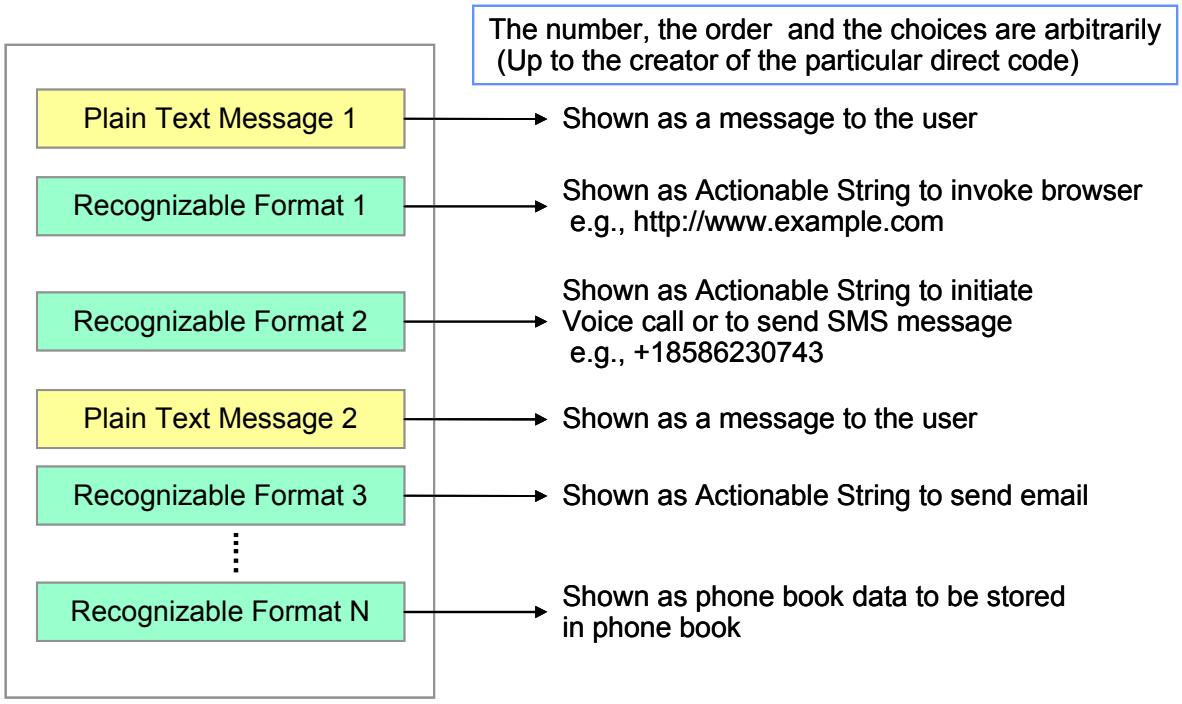


Figure 3: A Conceptual Data String Structure Example

A Recognizable Format has two types of syntax, both of which are based on plain text, i.e., (i) the syntax using plain text of specific forms, and (ii) the syntax using a common format named Direct MC Format (DMF) that is defined for specifying Recognizable Formats in this specification.

- Recognizable Formats using plain text:
  - Telephone Number String Recognition and Tel URI Scheme,
  - Web access, and
  - Mail address recognition.
- Recognizable Formats using DMF:
  - Business Card Recognition,
  - Bookmark Recognition, and
  - E-mail linkage data format recognition.

Note that the Recognizable Formats using plain text may be used inside of a Recognizable Format using DMF. The details are explained in the next section, respectively.

H.3.1 Recognisable Formats Using Plain Text

H.3.1.1 Telephone Number String Recognition and Tel URI Scheme

(1) Use case

A string of the following format is recognised as a telephone number, and displayed as an actionable string.

The user may select the telephone number for initiating a voice call, sending an SMS / MMS message or other types of communications. Such communications may include initiating a push-to-talk call, a video phone call, etc, whichever may be available on the device.

A Telephone-Number-String may contain visual separators. Visual separators are allowed to only help readability for humans. They are removed when the telephone number is used for initiating a phone call or sending an SMS/MMS message.

(2) Format

A Telephone-Number-String consists of phone digits, “+”, “*”,”#”, and it may contain visual separators.

	Supported Phone Number Representations	Examples
1	Both Local Numbers and Global Numbers	Local number: 1-858-623-0743 Global number: +1-858-623-0743
2	Both with and without a TEL: scheme	1-858-623-0743 TEL: 1-858-623-0743
3	Allow visual separators	1-858-623-0743 1 858 623 0743 1 85 86 23 07 43

Table 35: Example of Telephone Number Representations

- Visual separators
  - Support the following characters

    “(“ “)“ “.“ “-“ “/“ SP

    Up to 4 consecutive series of any permutation of visual separators are recognised as visual separators.
- Examples
  - 1-858-623-0743
  - 1 858 623 0743
  - 1 85 86 23 07 43
  - 1(858)623-0743
  - 1/858/623/0743
  - 1. 858. 623.0743
  - 18586230743

The types of Telephone-Number-String that are recognised by MCC:

- String-1 Recognises without TEL:,
  - If a telephone number string starts with “+” or any number, the recognizable range of its length is 10 to 26 digits.
- String-2 Recognises special numbers
  - If a telephone number string starts with “*” or “#”, the recognizable range of its length is 5 to 26 digits.
- String-3 Recognises with TEL:
  - If a telephone number string starts with “TEL:”, the recognizable range of its length is 3 to 26 digits.

There is a chance that a string of digits that appears as a part of plain text message but may not be intended to be a phone number may be recognised as a phone number. However, this is not a big issue because the user will be able to ascertain the correct meaning from the context of the message before the user initiates a call. It is recommended that you fully test the Direct Code before printing. It is recommended that you avoid using expressions that may confuse your users.

(3) Examples

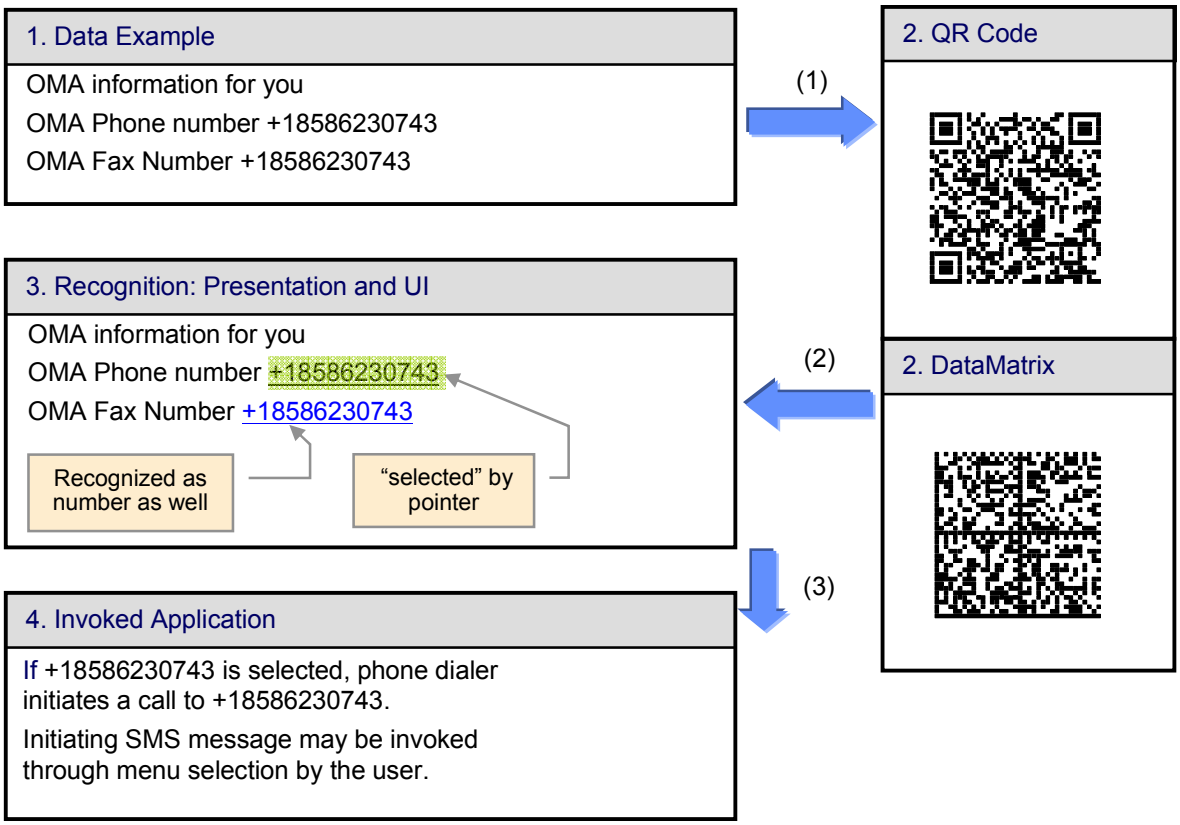


Figure 4: Example of Telephone Number String Recognition

H.3.1.2 Web Access

(3) Use case

The http scheme is widely used for interacting with Web resources using Hypertext Transfer Protocol.

The string of the following format is recognised as a URL, and displayed as an actionable string. If user selects this actionable string, a browser is invoked.

(2) Format

A text string that starts by http: or https: is recognised as a URL.

(3) Examples

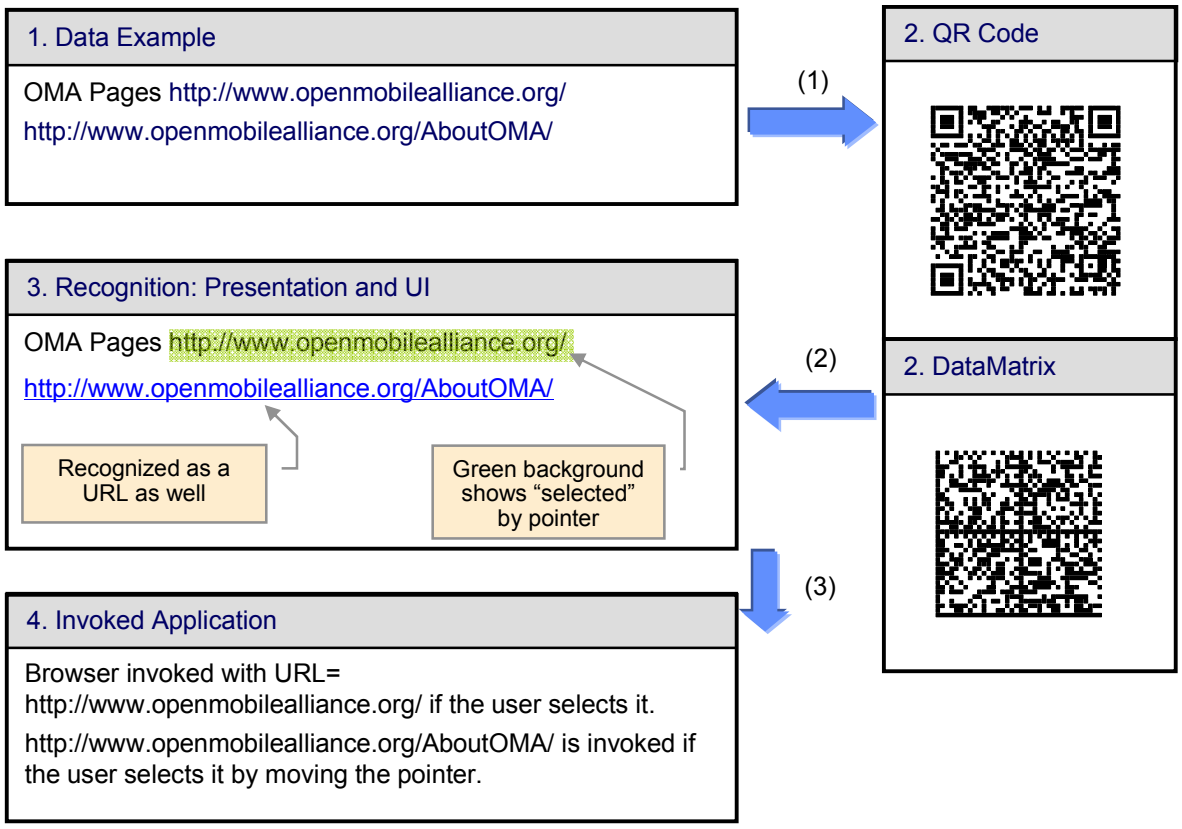


Figure 5: Example of Web Access

H.3.1.3 Mail Address Recognition

(1) Use case

An email address identifies an email box to which email messages may be delivered. An email address on the Internet looks like, for example, jsmith@example.com and is usually read as "jsmith at example dot com".

The string of the following format is recognised as an email address, and displayed as an actionable string. If the user selects this actionable string, an email client application is invoked.

(4) Format

A character string including @ is recognised as an email address.

(5) Examples

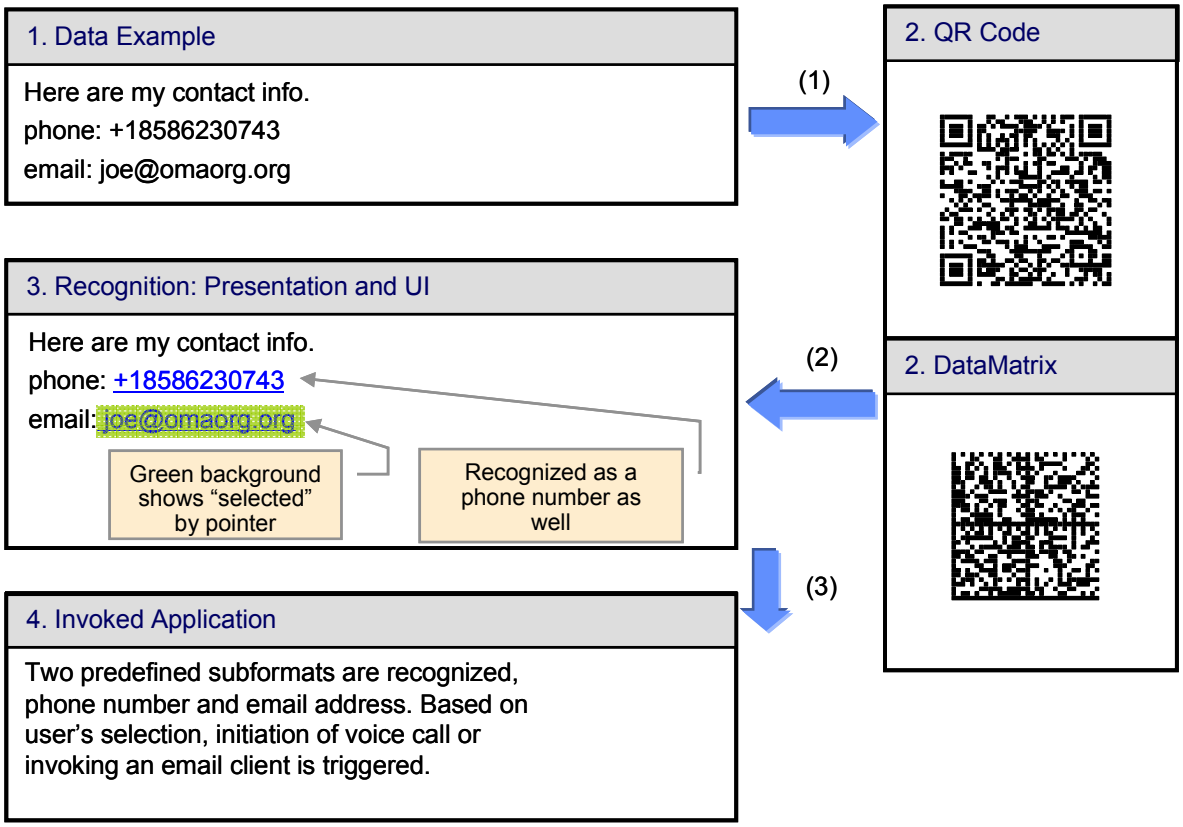


Figure 6: Example of Mail Address Recognition

H.3.2 Recognizable Formats using DMF

H.3.2.1 DMF Common Syntax

All the Recognizable Formats based on a DMF are formatted as shown below:

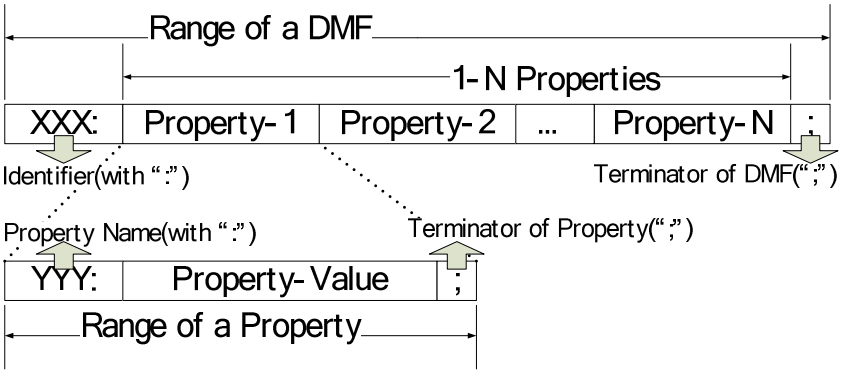


Figure 7: Data Structure of a DMF Format

(1) Identifier

The MCC identifies the DMF contents by its Identifier. The MCC will process the DMF data from the Identifier to the terminator character of the DMF (';') as one content. If the terminator character is not found, the DMF content will be ignored.

(2) Property (Property-Name and Property-Value)

A DMF format may contain zero or more Property(s). Each Property must be ended with one termination character, (';').

The allowed Property-Values depend on the content (i.e. Identifier).

Each Property-Value is recommended not to be NULL.

Note that Recognizable Formats using plain text which are appearing inside of a Property-Value of a Recognizable Format using DMF content are recognised as well. For example, joe@omaorg.org, being inserted in a Property-Value of a DMF format, is recognised as an email address and is shown as an actionable string in addition to the recognition of the DMF format itself.

The following table shows the range of allowed characters for each Property-Value for the DMF formats that are specified in this specification.

Identifier Name	Property Name	ASCII Character							Other Character set
		Digit	Alphabet	New Line	SPACE	"-"	Another Printable	Escape sequence	
		0x30 - 0x39	0x41-0x5a 0x61-0x7a	0x0a,0 x0d	0x20	0x2d	0x21-0x2b 0x2e-0x2f 0x3c-0x40 0x5b 0x5d-0x60 0x7b-0x7e	",", ";", ":", "\"	
MECARD	N	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
	SOUND	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
	TEL	Yes	"tel" only	N/A	Yes	Yes	"+","*",”#”,"(",")",”,”,"/"	":"	N/A
	EMAIL	Yes	Yes	N/A	N/A	Yes	partially	N/A	N/A
	BDAY	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	ADR	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	NOTE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	URL	Yes	Yes	N/A	N/A	Yes	partially	Yes	N/A
	NICKNAME	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
MATMSG	TO	Yes	Yes	N/A	N/A	Yes	partially	N/A	N/A
	SUB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	BODY	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MEBKMK	TITLE	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
	URL	Yes	Yes	N/A	N/A	Yes	partially	Yes	N/A

Table 36: Available Character Set for Property-Value

(i) Other Character Set:

While this specification is flexible enough to support various international character sets in addition to the ASCII character sets, actual support of such character sets is an implementation specifics of each mobile phone. If the character sets other than ASCII are expected to be used, please investigate the language support situation of your target mobile phones and the market that you want to target at.

(ii) Escape sequence:

In Property-Value, special characters (‘:’,’;’,’,’,’\’) must be escaped (ex. ‘\:’, ‘\;’,’\,’,’\\’).

For example, http://www.openmobilealliance.com must be denoted as http\://www.openmobilealliance.com.

(iii) Characters for an Identifier Name and a Property Name:

Only Digits, Alphabets, and “-” as shown in Table 36 are allowed for the characters to be used for an Identifier Name and a Property Name.

NOTE:

Here are a couple of points that you should be careful about when you create a data format to be recognised as a DMF:

- After the terminator of a Property, (“;”), CR/LF (a carriage return, 0x0d, and a line feed, 0x0a) must NOT be attached. Such a format is NOT recognised as a DMF.
- If the terminator, (“;”) is not attached at the end of the format, the format is not recognised as a DMF.
- If all the Property-Values of all the Properties are NULL, the format is not recognised as a DMF.
- If a format has no Property, the format is not recognised as an appropriate DMF.

H.3.2.2 Business Card (phone book) Recognition

(1) Use case

The Business card recognition enables a Recognizable Format based on a DMF to encode contact information that can be printed on usual business cards. Business cards have limited physical spaces that may be used for printing a 2 dimensional code. Furthermore, the physical size of business cards themselves has a limited physical space. Hence, the data format is required to be capable of supporting smaller sizes with essential data up to larger sizes with more data (generally, larger data requires physically larger symbols).

(2) Format

This function requires a MECARD for the Identifier and Properties as shown in Table 37. The MECARD Identifier is an essential element for this structure that must be present. All of the Properties are optional. All or some of the Properties may be included to be present depending on the data to be encoded.

Identifier Name	Actionable?	Description
MECARD	Yes	MECARD may be displayed using any string, e.g., "Add to phone book". The display text is subject to the implementation of a mobile phone. If this is selected, the data in the MECARD is to be stored in the phone book.
Property Name	**Actionable?**	**Description**
N	No	The name of the person associated with the MECARD.
SOUND	No	A sound annotation for the name of the person associated with the MECARD.
TEL	Yes	A telephone number associated with the MECARD. If multiple telephone numbers are needed, use multiple TEL properties. If this actionable string is selected, a phone call is initiated as shown in G.3.
EMAIL	Yes	An electronic mail address associated with the MECARD. If multiple email addresses are needed, use multiple EMAIL properties. If this actionable string is selected, an email application is invoked as shown in G.3.
BDAY	No	The date of birth associated with the MECARD. This value is a string of 8 characters

		consisting of ASCII characters "0"-"9", representing the year (first 4 characters), the month (next 2 characters), the day (last 2 characters) of the birth, respectively.
ADR	No	The physical delivery address associated with the MECARD.
NOTE	No	Supplemental information or a comment associated with the MECARD.
URL	Yes	A URL associated with the MECARD. If this actionable string is selected, a web browser is invoked to access the page designated by the URL as shown in G.3.
NICKNAME	No	A nick name of the person associated with the MECARD.

Table 37: Identifier and Properties of the MECARD

(3) Examples

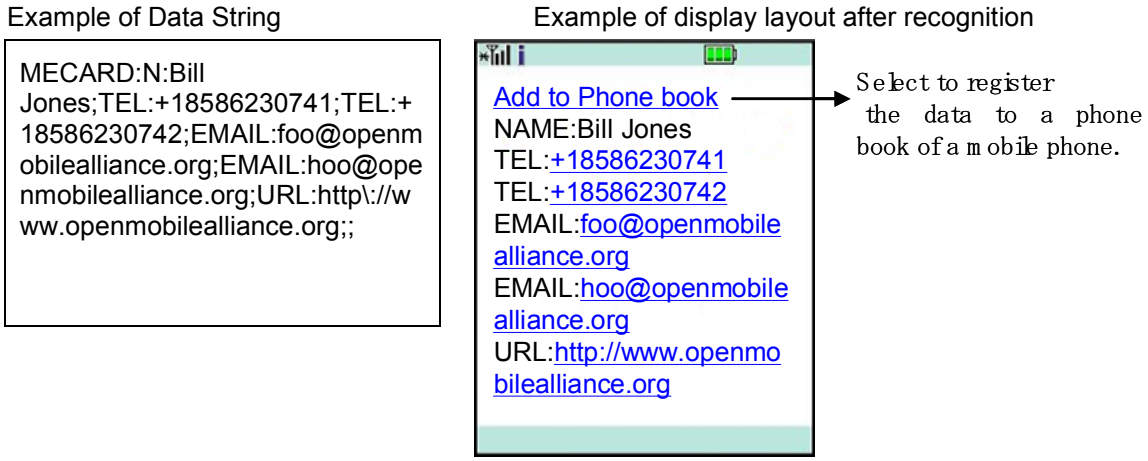


Figure 8: Example of MECARD Content

H.3.2.3 Bookmark Recognition

(1) Use case

The Bookmark Recognition enables a Recognizable Format based on a DMF to encode a URL with a title that can be stored in the book mark registry of a mobile phone, so that the user can visit the URL easily.

(2) Format

This function requires a MEBKM for the Identifier and Properties as shown in Table 38. The MEBKM Identifier is an essential element for this structure that must be present. All the Properties are optional. All or some of the Properties may be included to be present depending on the data to be encoded.

Identifier Name	Actionable?	Description
MEBKM	Yes	MEBKM may be displayed using any string, e.g., “Add to Bookmark”. The display text is subject to the implementation of a mobile phone. If this is selected, the data in the MEBKM is to be stored in the bookmark registry.
Property Name	**Actionable?**	**Description**
TITLE	No	A Title text associated with the MEBKM
URL	Yes	A URL associated with the MEBKM

Table 38: Identifier and Properties of the MEBKM

(3) Examples

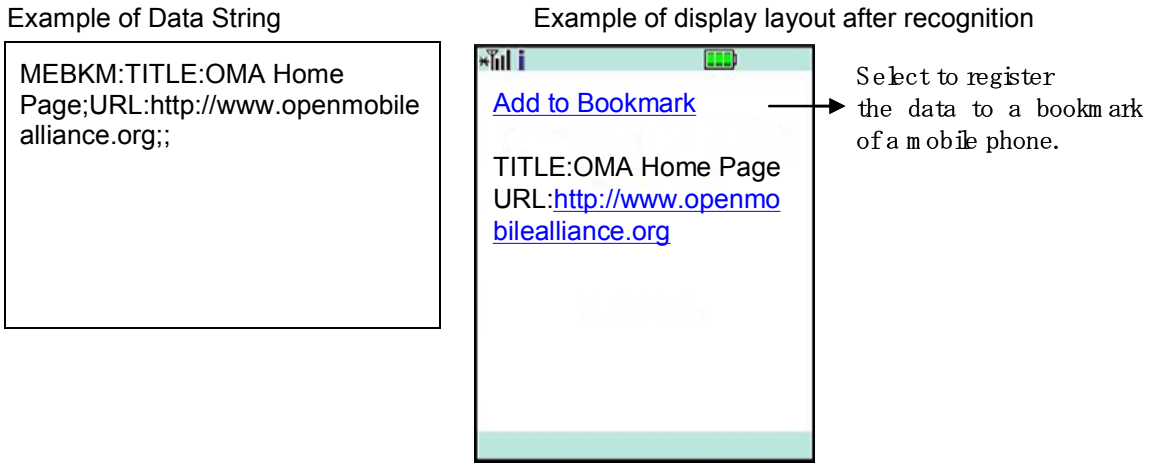


Figure 9: Example of MEBKM Content

H.3.2.4 E-Mail Linkage Data Format

(1) Use case

The E-Mail Linkage Data Format enables a Recognizable Format based on a DMF to encode email addresses with other messages that can invoke an email client. You can fill the subject and/or the body of the email.

(2) Format

This function requires a MATMSG for the Identifier and Properties as shown in Table 39. The MATMSG Identifier is an essential element for this structure that must be present. The TO Property is also an essential element that must be present in the MATMSG structure. The SUB and the BODY Properties are optional. The SUB or BODY Properties may be included to be present depending on the data to be encoded.

Identifier Name	Actionable?	Description
MATMSG	Yes	MATMSG may be displayed by using any string e.g., “Create Email”. The display text is subject to the implementation of a mobile phone. If this is selected, an email application is invoked and the data in the MATMSG is inserted in the respective field of the email.
Property Name	**Actionable?**	**Description**
TO	Yes	One electronic mail address associated with the MATMSG that will be inserted in the destination address field of an email application. If multiple addresses are needed, insert multiple TO properties. The maximum number of TO properties that can be recognised by a mobile phone is subject to the implementation. TO property itself is actionable. Thus if the TO property is clicked by the user, an email application is invoked with the email address being filled in the destination field. But the other data in the MATMSG is not filled in the application.
SUB	No	A subject of the message associated with the MATMSG that will be inserted in the subject field of an email application.
BODY	No	A body of the message associated with the MATMSG that will be inserted in the body field of an email application.

Table 39: Identifier and Properties of the MATMSG

(3) Examples

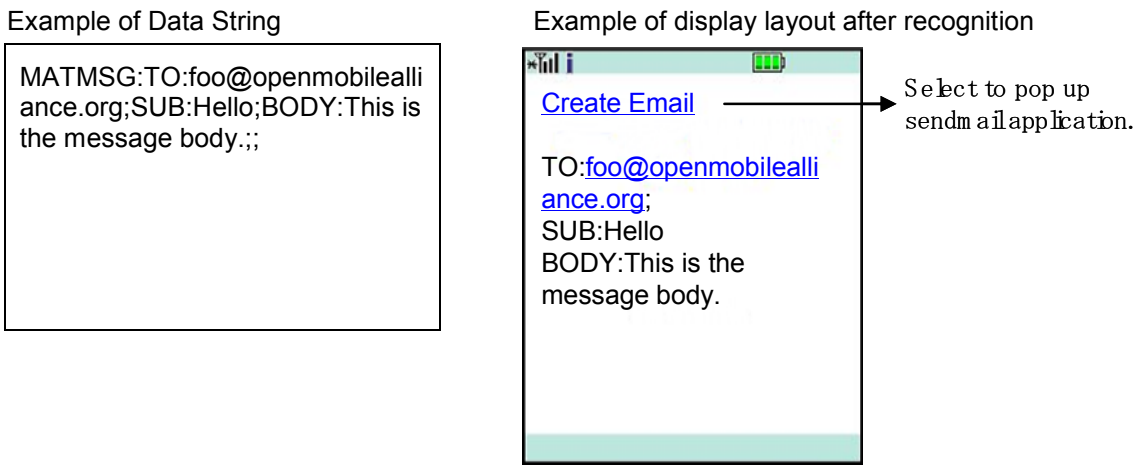


Figure 10: Example of MATMSG Content

H.4 Plain Text and Recognizable Formats

A Direct Code may contain plain text messages and multiple Recognizable Formats. The total data size must be smaller than the physical limitation of the Direct Code. Details of Recognizable Format syntaxes are described in Section H.2 and H.3.

The following figure shows an example of a Direct Code that includes plain text messages and 6 different types of Recognizable Formats. It also shows an example of the display image of the Direct Code and actions after recognition of the Direct Code. If a data string is recognised as a Recognizable Format, it is shown as an actionable string (underlined and highlighted string in this example) to indicate that can invoke a related action. If the user selects one of the actionable strings, the selected action is invoked. In addition, a Direct Code allows Recognizable Formats using plain text to be present in the Property-Value of a Recognizable Format using DMF. If a Recognizable Format using plain text is recognised in a Recognizable Format using DMF, the former is also shown as an actionable string.

In this example, an MECARD Recognizable Format (using DMF) contains 5 Recognizable Formats using plain text (telephone-number-string, mail address, web access), and all of them are shown as actionable strings. When the user chooses the “Add to Phone Book” actionable string, the set of data (telephone numbers, email address, and Homepage address) will be processed and stored in the phone book. On the other hand, when the user chooses the “+1858623074” actionable string in the MECARD Recognizable Format, possible actions which use the phone number such as “Make Phone Call” or “Send SMS” will be displayed, e.g., as a menu, and prompted.

NOTE: In the following example of Data String, CR/LFs are added after character “:” and “;” of Recognizable Formats using DMF for only helping your readability. In the actual Direct Code, such CR/LFs must NOT be present.

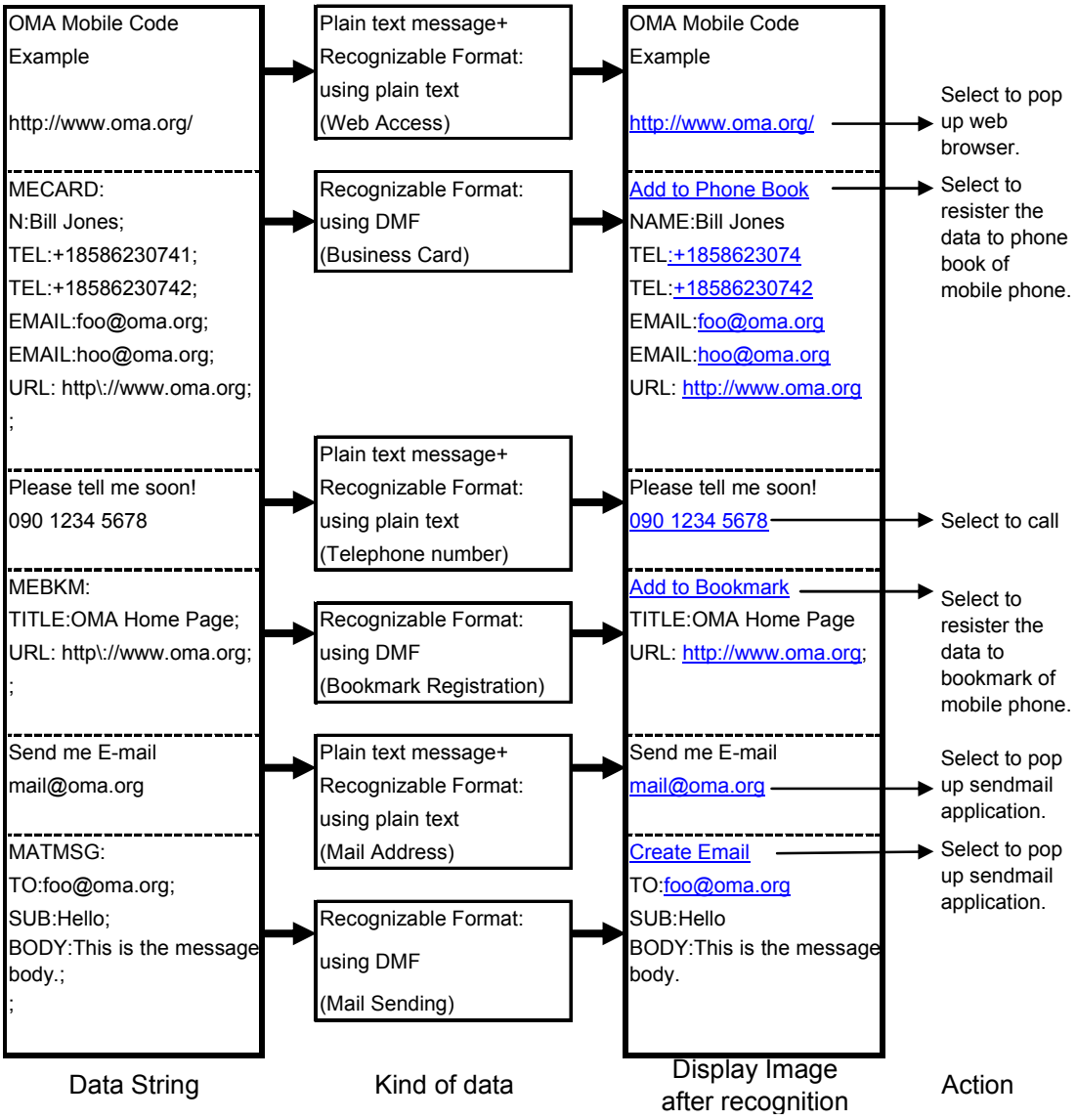


Figure 11: Example of Data String and Processing Procedure

H.5 Selection of two-dimensional Code format

A Direct Code supports both QR Code and Data Matrix as a two-dimensional barcode. Either code may be selected and used depending on the content of service, the targeted regions for service deployment, and the targeted mobile phones.

The specification of each two-dimensional barcode that can be used as Direct Code is as follows.

An appropriate symbol size and the error correction level must be selected according to the content of service and the targeted mobile phones.

(1) QR Code specification:

Item	Specification	Note
Model	Model 2	
Versions (Symbol size)	Versions 1 to 10	
Error Correction Levels	L, M, Q, H	M is Recommended

Table 40: Specification of QR Code Symbology

(2) Data Matrix specification:

Item	Specification	Note
Type	ECC200	
Symbol size	from 10x10 modules up to 52x52 modules	

Table 41: Specification of Data Matrix Symbology

H.6 Printing Condition

Printing conditions of Direct Codes are not specified. But in order to provide the users with successful reading experiences of Direct Codes, the following explains the recommended conditions to print a Direct Code.

NOTE: It is also recommended to confirm if printed Direct Code symbols are successfully read by the targeted mobile phones before publishing the Direct Codes. In case where the printed Direct Code symbol is not recognised, it is recommended to change the printing condition.

H.6.1 Quiet Zone

A Quiet Zone is a region which must be free of all other markings, surrounding the symbol on all four sides. When the Quiet Zone is wider, the recognition of the Direct Code is easier. Therefore, the following conditions are recommended (X: Minimum Module Width). In case where the printed Direct Code symbol is not recognised by the targeted mobile phones, it is recommended to make the width of the Quiet Zone larger for printing.

(1) QR Code

4X or larger Quiet Zones are recommended for printed QR Code symbols.

(2) Data Matrix

2X or larger Quiet Zones are recommended for printed Data Matrix symbols up to 26x26 modules.

4X or larger Quiet Zones are recommended for printed Data Matrix symbols over 32x32 modules.

H.6.2 Minimum Module Width

When a Module Width is too small, it becomes impossible to recognise the Direct Code because it is impossible to resolve it with the camera. Therefore, the following conditions are recommended. In case where the printed Direct Code symbol is not recognised by the targeted mobile phones, it is recommended to make the module width larger for printing.

(1) Common in QR Code and Data Matrix

A Module Width larger than 0.28mm is recommended for printed Direct Code symbols.

H.6.3 Contrast

A Symbol Contrast is the difference of reflectance between the light module (a module that the reflectance is high) and the dark module (a module that the reflectance is low) in a Direct Code symbol. When a Direct Code symbol is to be recognised with the camera, the larger the Symbol Contrast, the easier the recognition of the symbol becomes. Therefore, the following conditions are recommended. In case where the printed Direct Code symbol is not recognised by the targeted mobile phones, it is recommended to increase the Symbol Contrast for printing.

(1) Common for QR Code and Data Matrix

The Symbol Contrast of printed Direct Code symbols is recommended to be 55% or larger.

H.6.4 Example of Symbol Size versus Data Length

Table 40 and Table 41 show the symbol sizes based on the minimum printing module width of 0.28mm for QR Code and Data Matrix, respectively. The minimum printing module width of 0.28mm is recommended in this specification. Considering this table, you can select an appropriate symbol size depending on the needs of your data size and services.

* Not including quiet zone

Version	Module	Size(mm)* (X=0.28mm)	Error Correction	Number of characters			
				Numeric	Alphanumeric	Binary	Kanji
1	21×21	**5.88**	L	41	25	17	10
			M	34	20	14	8
			Q	27	16	11	7
			H	17	10	7	4
2	25×25	**7.00**	L	77	47	32	20
			M	63	38	26	16
			Q	48	29	20	12
			H	34	20	14	8
3	29×29	**8.12**	L	127	77	53	32
			M	101	61	42	26
			Q	77	47	32	20
			H	58	35	24	15
4	33×33	**9.24**	L	187	114	78	48
			M	149	90	62	38
			Q	111	67	46	28
			H	82	50	34	21
5	37×37	**10.36**	L	255	154	106	65
			M	202	122	84	52
			Q	144	87	60	37
			H	106	64	44	27
6	41×41	**11.48**	L	322	195	134	82
			M	255	154	106	65
			Q	178	108	74	45
			H	139	84	58	36
7	45×45	**12.60**	L	370	224	154	95
			M	293	178	122	75
			Q	207	125	86	53
			H	154	93	64	39
8	49×49	**13.72**	L	461	279	192	118
			M	365	221	152	93
			Q	259	157	108	66
			H	202	122	84	52
9	53×53	**14.84**	L	552	335	230	141
			M	432	262	180	111
			Q	312	189	130	80
			H	235	143	98	60
10	57×57	**15.96**	L	652	395	271	167
			M	513	311	213	131
			Q	364	221	151	93
			H	288	174	119	74

Table 42: QR Symbol Size with Minimum Module Width (X=0.28mm)

* Not including quiet zone

Module	Size(mm)* (X=0.28mm)	Number of characters		
		Numeric	Alphanumeric	Byte
10×10	**2.80**	6	3	1
12x12	**3.36**	10	6	3
14x14	**3.92**	16	10	6
16x16	**4.48**	24	16	10
18x18	**5.04**	36	25	16
20x20	**5.60**	44	31	20
22x22	**6.16**	60	43	28
24x24	**6.72**	72	52	34
26x26	**7.28**	88	64	42
32x32	**8.96**	124	91	60
36x36	**10.08**	172	127	84
40x40	**11.20**	228	169	112
44x44	**12.32**	288	214	142
48x48	**13.44**	348	259	172
52x52	**14.56**	408	304	202

Table 43: Data Matrix Symbol Size with Minimum Module Width (X=0.28mm)

Appendix I. MLA-based Example Implementation (Informative)

Scope: This Appendix describes an example of a MLA-based community of CMPs where a subset of this specification is implemented. The content in this Appendix is Informative.

Multi-lateral Arrangement (MLA) in this specification is defined as: "An arrangement amongst specific CMPs (including Split-CMP-Parents, where applicable) that are not associated with any Mobile Code Registry, in which the parties agreed to support each other in a multi-lateral way in order to manage sub-allocation of MC Routing Prefixes as well as discovery and updates thereof; details of such MLAs are not specified in the MC Enabler TS."

I.1 Description of a MLA-based Implementation

Ref: MC AD, Section 5.2.1, "Note 1 - Mobile Code Registry (MCR) and its exposed interfaces MC-2 and MC-5 are optional. Alternatively, if CMP belongs to a multi-lateral arrangement (MLA) with other CMPs, equivalent functionalities to the MCR can be achieved; details of MLAs are not specified in this enabler."

This MLA-based implementation example describes a basic case of Mobile Codes system (see Section 8.2.2). The main feature of this implementation illustrates an alternative means through which the MCR functionalities (i.e. sub-allocation of MC Routing Prefixes and discovery & updates of them) are achieved.

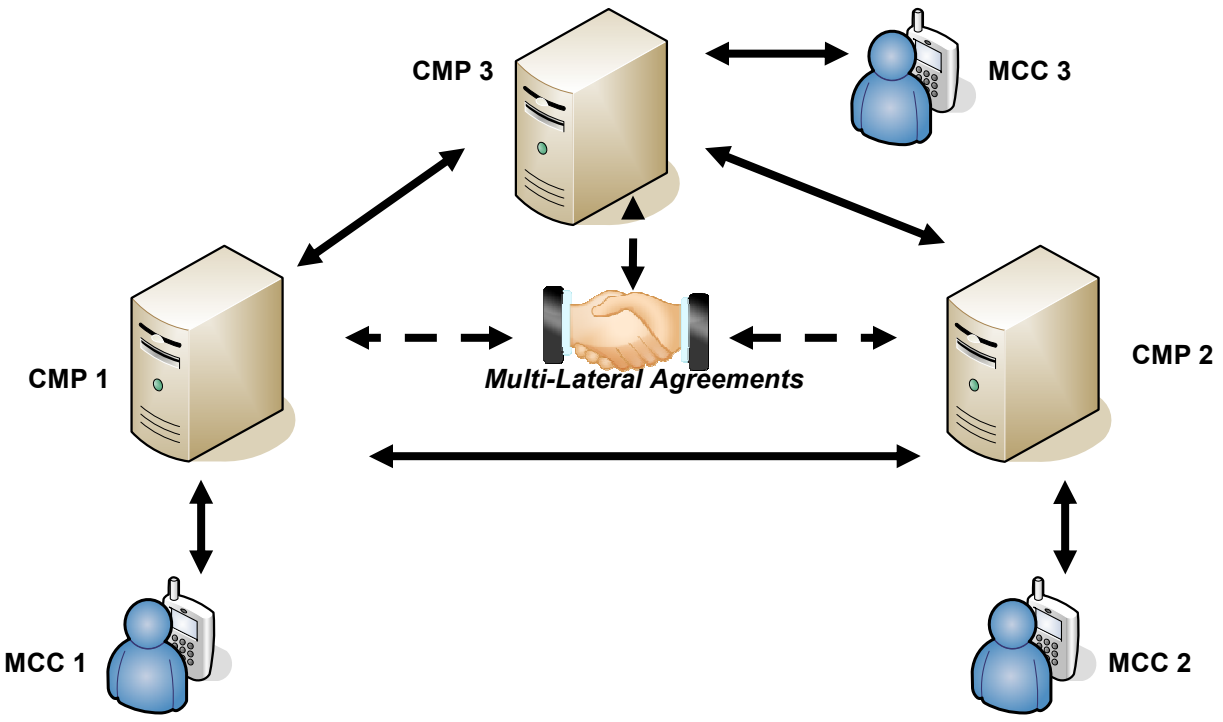


Figure 12: CMPs in a MLA-based Implementation

I.2 CMP Routing Prefix Assignment & Updates within the MLA

This MLA example takes the following actions to achieve CMP Routing Prefix assignments and updates within the MLA through off-line exchange of information:

- First, an entity within the community of CMPs in the MLA is designated as the Registry-ID Recipient. This may be, for example, the largest CMP service provider in a geographical or market region within that MLA.
- Next, the Registry-ID Recipient applies for and obtains a Registry-ID from OMNA.
- The Registry-ID Recipient then performs the following functions:
  - Using the Registry-ID, generate unique Routing Prefixes as specified in Section 8.1 and distribute them amongst the participant CMPs.
  - Maintain a MLA-routing table (shared amongst all CMPs within the MLA) that associates the Routing Prefix with the current network address of the participant CMP that it was assigned to. This includes updates provided by the participant CMPs when their network addresses change.
  - Periodically (or when this table changes), distribute the MLA-routing table amongst the participant CMPs to ensure routing information is kept up-to-date: this normally includes prior-testing to ensure the accuracy of the routing information. This table may be distributed in a variety of forms (e.g., emailed as a delimited text file).
- The participant CMPs will, on receipt of an update of the MLA-routing table, update their internal registry cache accordingly.

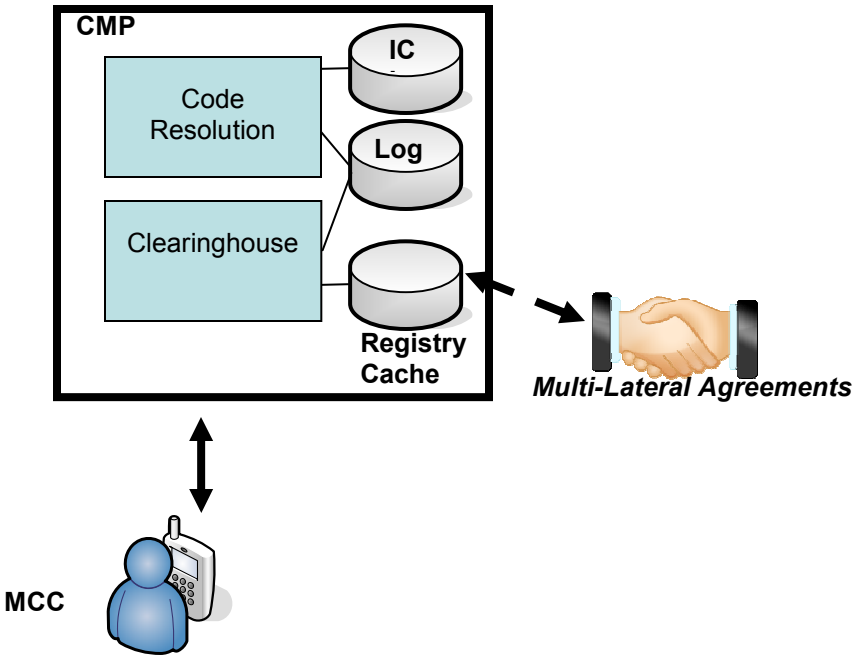


Figure 13: Updating the CMP's Registry Cache in a MLA-based Implementation

I.3 Remote CMP Code Resolution Procedures within the MLA

In this example MLA implementation, the participant CMPs follow the Code Resolution procedures as below:

- Code Resolution as described in Section 8.2:

- Using its internal registry cache, the Home CMP determines the network address of the Remote/Resolving CMP for the ICI.
- The Home CMP then forwards the MC-3-RESOLVE_ICI_REQUEST message to the Remote/Resolving CMP through the MC-3 Interface.

Appendix J. Secure ICI Scheme Example (Informative)

This section describes a specific scheme to create, process and verify the Secure ICI for two non-transferred ICIs. This scheme applies standardized encryption and signature algorithms to the Resolution Identifier (RI) part of the ICI to effectively protect the RI from being altered. The encrypted RI is further split into two parts so that only one part is carried in the Secure ICI to guarantee more security because the attacker does not have sufficient cryptographic information to launch an attack to change data in the Secure ICI without being detected and also to ensure that the length of the Secure ICI does not exceed 36 octets, the maximum allowable ICI length.

J.1 General Procedures to Create a Secure ICI

The general procedures to create a Secure ICI for a non-transferred ICI that does not specify any type of encryption and hashing algorithm is described below and in Figure K-1.

1. Use a RSA Private Key and Public Key pair.
2. Encrypt the "Resolution Identifier" of the ICI with the RSA Private Key to obtain the Encrypted RI (ERI). ERI is now a binary data.
3. Calculate the Hash on the ERI with the RSA Public Key to obtain the ERI Hash (ERIH).
4. Encode the ERI in Base 64 format to obtain ERI_B64. This ensures that none of the octets in the ERI_B64 contains the value "%x04".
5. Split the ERI_B64 into two parts, the ERI_B64_Part_One and ERI_B64_Part_Two.
6. Create an index for the ERI part ("ERX") that is used to correlate the two ERI_B64 parts.
7. Create the Secure ICI by concatenating the newly calculated ERX followed by the ERI_B64_Part_One after the Routing Prefix.
8. The Secure ICI is used as the ICI to generate the Indirect Code using the appropriate symbology.
9. The ERI_B64_Part_Two, ERX and ERIH are stored together with the associated ICI mapping information at the Resolving CMP. Storing the original ICI is optional.

The whole process can be done at the Resolving CMP, or steps #1 through #8 can be done by the MCP that then provides the ERI_B64_Part_Two, ERX and ERIH to the Resolving CMP in step #9.

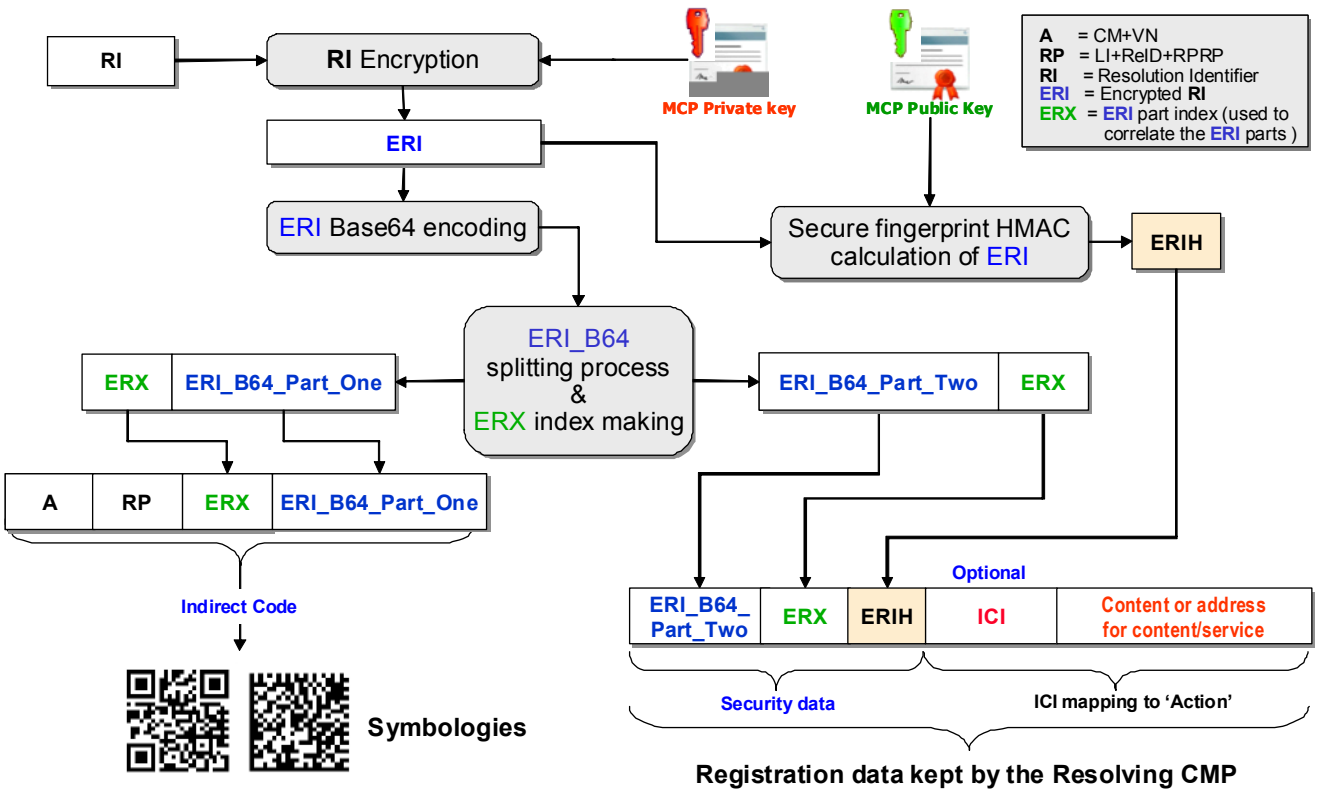


Figure 14: General Procedures to Create a Secure ICI

J.2 General Procedures to Verify a Secure ICI

It is assumed that the information in the Secure ICI allows the Code Resolution request that contains the Secure ICI to be routed by the non-Resolving CMP(s) (or the Split-CMP-Parent(s) when applicable) to the Resolving CMP when the guidelines in Section 9.3.3 are followed. Figure K-2 shows how the Secure ICI in the Code Resolution request is used for routing by the non-Resolving CMP(s) (or the Split-CMP-Parent(s) when applicable) and how it is verified by the Resolving CMP. The procedures below start when the Resolving CMP retrieves the Code Resolution request.

1. Verify if the received ICI is a Secure ICI.
    a. If NOT, go to the standard resolution process.
    b. If YES, continue.
2. Extract the RI part from the Secure ICI.
3. Identify the ERX and the ERI_B64_Part_One in the RI part.
4. Use the ERX to find the ERI_B64_Part_Two and associated ERIH.
    a. If ERI_B64_Part_Two cannot be found at the Resolving CMP, an error is detected and error process is invoked.
    b. If ERI_B64_Part_Two can be found, continue.
5. Concatenate the ERI_B64_Part_One and the ERI_B64_Part_Two to obtain the Full_ERI_B64.
6. Decode the Full_ERI_B64 to obtain the Received_ERI.
7. Calculate the hash of the Received_ERI with the RSA Public Key to obtain the Received_ERIH.
8. Compare the Received_ERIH with the ERIH.
    a. If the two are not the same, an error is detected and error process is invoked.
    b. If the two are the same, continue.
9. The procedures below depend on if the original ICI must be verified or not and if it is stored by the Resolving CMP.

a. If the original ICI does not need to be verified by the Resolving CMP against the received one:
   i. Use the ERX to retrieve the corresponding ICI mapping information to return the Code Resolution response.

b. If the original ICI, previously stored, needs to be verified by the Resolving CMP against the received one:
   i. Decrypt the Received_ERI with the RSA Public Key to obtain the Calculated RI (CRI).
   ii. Use the ERX to retrieve the previously stored ICI.
   iii. Prepend the received RP to CRI to obtain the Received_ICI and compare it with the stored ICI.
      – If the two are not the same, an error process is invoked.
      – If the two are the same, use the stored ICI mapping information to return the Code Resolution response.

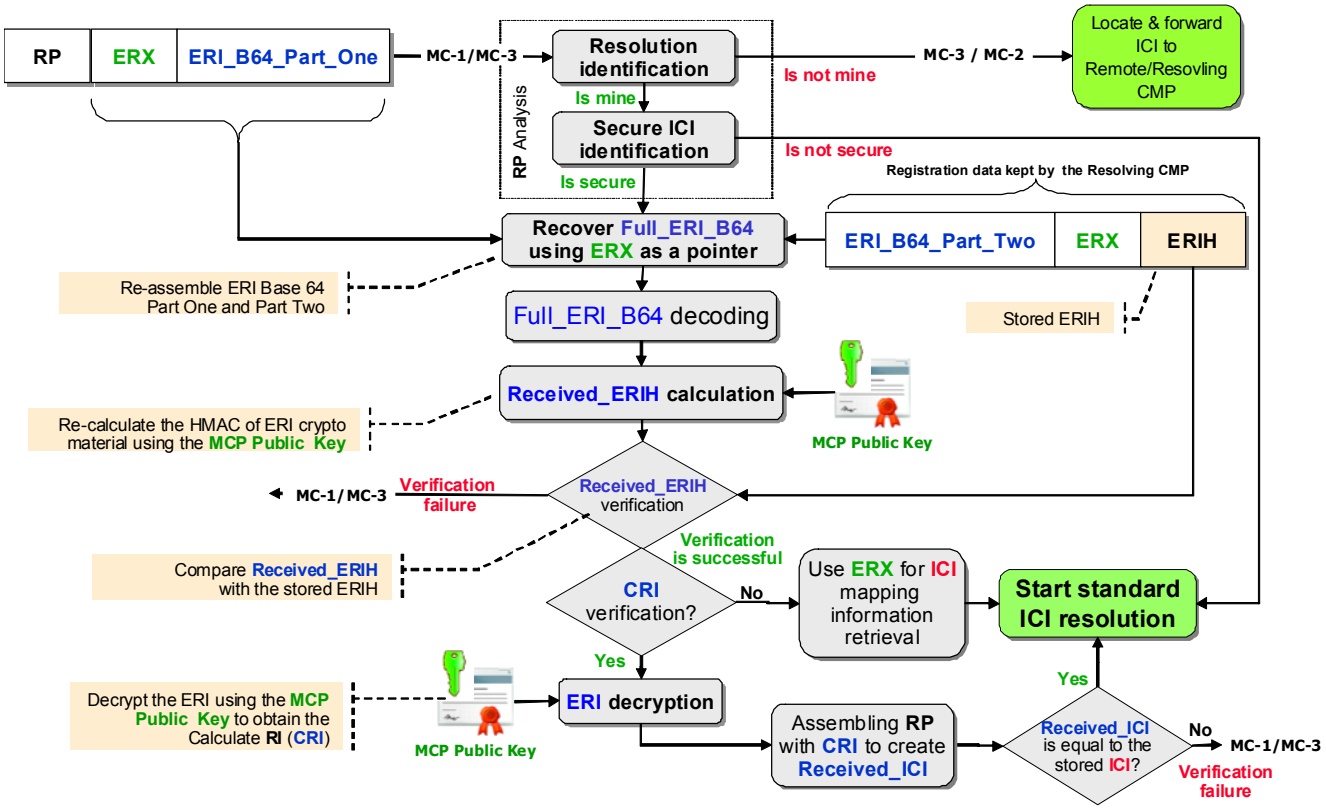


Figure 15: General Procedures to Verify a Secure ICI

J.3 Specific Examples

In the three examples below, "Public-key cryptography", "Hash-based Message Authentication Code" [RFC2104] and the "Splitting Feature" in the RFC 4868 [RFC4868] are used where RFC 4868 specifies as truncation value nnn/2 bits of the resulting hash bits, where nnn corresponds to the output bit length of the algorithm (e.g., HMAC-SHA-nnn/2).

The advantages of using the RSA digital signature methodology to encrypt the Resolution Identifier portion of the ICI with the MCP's Private Key and sign it using the HMAC signature algorithm with the MCP's Public Key, are:

- The MCP can protect the ICI authenticity in two ways, by encrypting the Resolution Identifier with its Private Key and by signing the resulting crypto information using HMAC signature algorithm and its Public Key.

- The Resolving CMP can verify the authenticity of a received Resolution Identifier using only the MCP's Public Key, both to verify the signature of crypto information and to decrypt it. (Note that the MCP's Public Key may be managed by its Resolving CMP on behalf of the MCP, subject to the business agreements between them.)
- Holding only the Public Key does not allow anyone to:
    - Deduce the full Resolution Identifier
    - Encrypt any valid Resolution Identifier to produce a valid ICI

Two examples are shown below to show the suitability of the scheme described above. Both examples have the maximum ICI length of 36 octets. Example #1 has the minimum length for the Routing Prefix (3 octets) and maximum length for the Resolution Identifier (33 octets), and Example #2 has the maximum length for the Routing Prefix (18 octets) and a length of 18 octets for the Resolution Identifier, Note that in the two examples, the lengths of the original ICI and the Secure ICI are the same to prove that this scheme works even when the original ICI has the maximum length of 36 octets.

Example #1 – 1,024 RSA key size with 3-octet Routing Prefix and 33-octet Resolution Identifier

---- Start of the Original ICI ----

a) The first two octets that correspond to the 1 hex digit Length-Indicator (value is %x0) and 3 hex digits Registry-ID (value is assumed to be %x002) = 0002 in hex digits

b) Remaining-Part-of-Routing-Prefix (RPRP) = 1 (1 character/octet)

c) Resolution-Identifier (RI) = 000000000000000000000000000000001 (33 characters/octets)

The original ICI = %x0002 followed by characters 100000000000000000000000000000001 (36 characters/octets)

---- End of the Original ICI ----

---- Start of Encryption Procedures ----

a. Create the RSA Private Key and Public Key pair for 1,024-bit encryption.

   i. Private Key (612 hex digits):
   613a333a7b693a303b733a3132383a22674378dba9f3251a164f09d268e7bbc2067ecd9b2de77c33915ba7ce18ea0a49f634c5926b0dff01a2920aa0117
   22d03312745235d9e7c4b7fae154108fe5c91e9691b4b30bc280a2afd76f9b6b52d2a383b3ead85069d404bf747a514cc044d789819367efd73e793deca
   b6d72cf4940deed13b5f75e7d852be19c6ca91199e223b693a313b733a3132383a2221f58676e56bbd41a71729b8276792fed5c6ffb848eee3ecbc18bb7
   87b51bfc1c0235bac078aad34de962049b745fa3964dc157bdcb8a334cfac1175dc2791e686c29fdcffc49b6554b65b64b37eeab4ae988e1c2a6a342cda0
   1563e8e7d28e732b6324267aac0b63d0c26e6f3f4d9fffb0edb833b0521969a71b1614d635970223b693a323b733a373a2270726976617465223b7d

   ii. Public Key (356 hex digits):
   613a333a7b693a303b733a3132383a22674378dba9f3251a164f09d268e7bbc2067ecd9b2de77c33915ba7ce18ea0a49f634c5926b0dff01a2920aa0117
   22d03312745235d9e7c4b7fae154108fe5c91e9691b4b30bc280a2afd76f9b6b52d2a383b3ead85069d404bf747a514cc044d789819367efd73e793deca
   b6d72cf4940deed13b5f75e7d852be19c6ca91199e223b693a313b733a333a22010001223b693a323b733a363a227075626c6963223b7d

b. Encrypt the RI with the RSA Private Key to obtain the 1,024-bit ERI (in 256 hex digits):
   de403e0a0e0641bb96a29599a493078cd0160bc0823f57dba8df0a2895adb50c426fe0a878ec918bb37ee8c133a33b7d40740f8e8a73d07f37d5a820916ac81a
   a1e9abb189f63e26f9877631cb721ef274eafb46462648e1babd4ef6e5f2ae97a9d74b21ce263426839d7f77e963016b5b482251223ce9fc2e2722f34c7c9a42

c. Create ERI HMAC (HMAC-SHA-256/2) using the RSA Public Key to obtain the 128-bit ERIH (in 32 hex digits): ac99f1ecfc179c8226ee9e137da80337

d. Encode the ERI in Base64 to obtain the ERI_B64 (172 ASCII characters):
   3kA+Cg4GQbuWopWZpJMHjNAWC8CCP1fbqN8KKJWttQxCb+CoeOyRi7N+6MEzozt9QHQPjopz0H831aggkWrIGqHpq7GJ9j4m+Yd2MctyHvJ06
   vtGRiZI4bq9Tvbl8q6XqddLIc4mNCaDnX936WMBa1tIIlEiPOn8Lici80x8mkI=

e. Split ERI_B64 into two parts

   i. ERI_B64_Part_One = 3kA+Cg4GQbuWopWZpJMHjNAWC8CC (Length = 28 characters)

   ii. ERI_B64_Part_Two =
   P1fbqN8KKJWttQxCb+CoeOyRi7N+6MEzozt9QHQPjopz0H831aggkWrIGqHpq7GJ9j4m+Yd2MctyHvJ06vtGRiZI4bq9Tvbl8q6XqddLIc4mNCa
   DnX936WMBa1tIIlEiPOn8Lici80x8mkI= (Length = 144 characters)

f. Assign an ERI Part Index (ERX): **07a60** (Length = 5 characters/octets) equal to 31,328 in decimal value.

   Note: The ERX should have a proper length to uniquely correlate each Secure ICI with its original ICI.

g. Create Secure ICI (RP + ERX + ERI_B64_Part_One): %x0002 followed by characters 107a603kA+Cg4GQbuWopWZpJMHjNAWC8CC (Length = 36 octets with 16.3% of crypto material in the ICI)

h. Create Registration Data (ERI_B64_Part_Two | ERX | ERIH | Original-ICI | ICI-mapping-information): P1fbqN8KKJWttQxCb+CoeOyRi7N+6MEzozt9QHQPjopz0H831aggkWrIGqHpq7GJ9j4m+Yd2MctyHvJ06vtGRiZI4bq9Tvbl8q6XqddLIc4mNCaDnX936WMBa1tIIlEiPOn8Lici80x8mkI=|07a60|ac99f1ecfc179c8226ee9e137da80337|%xf002 followed by characters1000000000000000000000000000000001|http://my_site/index.asp

---- End of Encryption Procedures ----

---- Start of Decryption Procedures ----

a. Identify the ERX and ERI_B64_Part_One in the received Secure ICI.

b. Use ERX to retrieve the ERI_B64_Part_Two.

c. Assemble ERI_B64_Part_One and ERI_B64_Part_Two to obtain the Full_ERI_B64: 3kA+Cg4GQbuWopWZpJMHjNAWC8CCP1fbqN8KKJWttQxCb+CoeOyRi7N+6MEzozt9QHQPjopz0H831aggkWrIGqHpq7GJ9j4m+Yd2MctyHvJ06vtGRiZI4bq9Tvbl8q6XqddLIc4mNCaDnX936WMBa1tIIlEiPOn8Lici80x8mkI=

d. Decode the Full_ERI_B64 to obtain the Received_ERI (in hex digits): de403e0a0e0641bb96a29599a493078cd0160bc0823f57dba8df0a2895adb50c426fe0a878ec918bb37ee8c133a33b7d40740f8e8a73d07f37d5a820916ac81aa1e9abb189f63e26f9877631cb721ef274eafb46462648e1babd4ef6e5f2ae97a9d74b21ce263426839d7f77e963016b5b482251223ce9fc2e2722f34c7c9a42

e. Create from the Received_ERI the HMAC (HMAC-SHA-256/2) using the RSA Public Key to obtain the Received_ERIH (32 hex digits): ac99f1ecfc179c8226ee9e137da80337

f. Compare the Received_ERIH with the stored ERIH:

i. The HMAC test is Positive (Received_ERIH == stored ERIH).

g. Decrypt the binary Received_ERI using the RSA Public Key to obtain the Calculated RI (CRI): 000000000000000000000000000000001 (33 characters)

---- End of Decryption Procedures ----

The Received_ICI (received RP + CRI) = %x0002 followed by characters 1000000000000000000000000000000001

Example #2 – 1,024 RSA key size with 18-octet Routing Prefix and 18-octet Resolution Identifier

---- Start of the Original ICI ----

a) The first two octets that correspond to the 1 hex digit Length-Indicator (value is %xF) and 3 hex digits Registry-ID (value is assumed to be %x002) = f002 in hex digits

b) Remaining-Part-of-Routing-Prefix (RPRP) = 0000000000000001 (16 characters/octets)

c) Resolution-Identifier (RI) = 000000000000000001 (18 characters/octets)

The original ICI = %xF002 followed by characters 000000000000000100000000000000001 (36 characters/octets; or 4 hex digits plus 34 characters)

---- End of the Original ICI ----

---- Start of Encryption Procedures ----

a. Use the same RSA Private Key and Public Key pair from example #1.

b. Encrypt the RI with the RSA Private Key to obtain the 1,024-bit ERI (in 256 hex digits): 6efb2c8e67499e826ee365348667cd3dd150cedf99feb8145c24eaa9399e1627db2e8c65cacacb0aed18747df7c04dbd89ec9528a02a3efa736e1641e6c8ed74e5c253bea1d9ec2f5db93811bdc6579966cb963bf4f501d47684c7f0f5010440a3f27b3dc055b19d64995c1efbff0c2ffbd38282ae10c51b68689ae4a0dec66e

c. Calculate ERI HMAC (HMAC-SHA-256/2) using the RSA Public Key to obtain the 128-bit ERIH (in 32 hex digits): fcf31945d2001848d02740031d2bdf5f

d. Encode the ERI in Base64 to obtain the ERI_B64 (172 ASCII characters): T6Hczh6YO4N37wGwA3kxUHKKpDWUTbwaR/TLTS9BWvwnt8YurRqxdob2aHU64+Ix74VR06RPVQBCbEqQB2yRNjgLyHwJ7CQzfdwxROaGaZbPuZ/3muESnBx+dXDXnC8VYHI53V2eMOYRtJ4li2jgOcol59ftssQq4JZV8wOsKiQ=

e. Split ERI_B64 into two parts

   i. ERI_B64_Part_One = T6Hczh6YO4N37 (13 characters)

   ii. ERI_B64_Part_Two = wGwA3kxUHKKpDWUTbwaR/TLTS9BWvwnt8YurRqxdob2aHU64+Ix74VR06RPVQBCbEqQB2yRNjgLyHwJ7CQzfdwxROaGaZbPuZ/3muESnBx+dXDXnC8VYHI53V2eMOYRtJ4li2jgOcol59ftssQq4JZV8wOsKiQ= (159 character)

f. Assign an ERI Part Index (ERX): ca200 (Length = 5 characters/octets) equal to 827,904 in decimal value

g. Create the Secure ICI (RP + ERX + ERI_B64_Part_One): %xF002 followed by characters 0000000000000001ca200T6Hczh6YO4N37 (Length = 36 octets with 7.6% of crypto material in the ICI)

h. Create Registration Data (ERI_B64_Part_Two | ERX | ERIH | Original-ICI | ICI-mapping-information): wGwA3kxUHKKpDWUTbwaR/TLTS9BWvwnt8YurRqxdob2aHU64+Ix74VR06RPVQBCbEqQB2yRNjgLyHwJ7CQzfdwxROaGaZbPuZ/3muESnBx+dXDXnC8VYHI53V2eMOYRtJ4li2jgOcol59ftssQq4JZV8wOsKiQ=|ca200|fcf31945d2001848d02740031d2bdf5f|%xf002 followed by characters00000000000000001000000000000000001|http://my_site/index.asp

---- End of Encryption Procedures ----

---- Start of Decryption Procedures ----

a. Identify the ERX and ERI_B64_Part_One in the received Secure ICI.

b. Use ERX to retrieve the ERI_B64_Part_Two.

c. Assemble ERI_B64_Part_One and ERI_B64_Part_Two to obtain the Full_ERI_B64: T6Hczh6YO4N37wGwA3kxUHKKpDWUTbwaR/TLTS9BWvwnt8YurRqxdob2aHU64+Ix74VR06RPVQBCbEqQB2yRNjgLyHwJ7CQzfdwxROaGaZbPuZ/3muESnBx+dXDXnC8VYHI53V2eMOYRtJ4li2jgOcol59ftssQq4JZV8wOsKiQ=

d. Decode the Full_ERI_B64 to obtain the Received_ERI (in hex digits): 4fa1dcce1e983b8377ef01b003793150728aa435944dbc1a47f4cb4d2f415afc27b7c62ead1ab17686f668753ae3e231ef8551d3a44f5500426c4a90076c9136380bc87c09ec24337ddc3144e6866996cfb99ff79ae1129c1c7e7570d79c2f15607239dd5d9e30e611b49e258b68e039ca25e7d7edb2c42ae09655f303ac2a24

e. Create from the Received_ERI the HMAC (HMAC-SHA-256/2) using the RSA Public Key to obtain the Received_ERIH (32 hex digits): fcf31945d2001848d02740031d2bdf5f

f. Compare the Received_ERIH with the stored ERIH:

   i. The HMAC test is Positive (Received_ERIH == stored ERIH).

g. Decrypt the binary Received_ERI using the RSA Public Key to obtain the Calculated RI (CRI): 0000000000000001 (18 characters)

---- End of Decryption Procedures ----

The Received_ICI (received RP + CRI) = %xF002 followed by characters 00000000000000001000000000000000001