COMMUNICATIONS

ALLIANCE LTD

INDUSTRY GUIDELINE

MOBILE NUMBER PORTABILITY- IT SPECIFICATION PART 2: ARCHITECTURE AND MESSAGING REQUIREMENTS

G573.2:2009

G573.2:2009 Mobile Number Portability - IT Specification Part 2: Architecture and Messaging Requirements

First published as ACIF G573.2:2001
Second edition as ACIF G573.2:2003
Third edition as ACIF G573.2:2004
Fourth edition ACIF G573.2:2005

Communications Alliance Ltd (formerly Australian Communications Industry Forum Ltd) was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

TABLE OF CONTENTS

1	GENERAL	2
	1.1 Purpose	2
	1.2 Scope	2
	1.3 2009 Revision	2
2	ACRONYMS AND DEFINITIONS	3
	2.1 Acronyms	3
	2.2 Definitions	4
3	ASSUMPTIONS	8
4	MESSAGING PLATFORM	9
	4.1 Architecture Framework	9
	4.2 Topology	10
5	MESSAGING NODE REQUIREMENTS	11
	5.1 Transport Protocol	11
	5.2 Message Definitions	11
	5.3 Messaging Protocol	12
	5.4 Security	15
6	REFERENCES	20
APPENDIX		21
A	COMMUNICATIONS CONTROL MESSAGE DTDS	21
B	COMMUNICATIONS CONTROL MESSAGE DATA DICTIONARY	25
C	CONFIGURABLE PARAMETERS	26
D	MESSAGE TYPES	27
E	RETURN CODES	28
PARTICIPANTS		29

1 GENERAL

1.1 Purpose

This document is Part 2 of the three-part MNP IT Specification. The purpose of this document is to specify the requirements for the Messaging Nodes of the MNP Messaging Platform. The Messaging Nodes are part of the technical infrastructure for the electronic exchange of MNP messages between the Participants involved in MNP.

Each Participant must implement its Messaging Node in compliance with the specified requirements to ensure inter-operability.

MNP IT Specification– Part 1: Transaction Analysis Specification (G573.1:2009) covers the application layer. ***MNP IT Specification- Part 3: Common Network*** (G573.3:2009) covers the Common Network requirements.

1.2 Scope

This document covers the requirements for the Messaging Nodes of the MNP Messaging Platform at the Messaging Layer, including the:

- transport protocol for message transfer;
- messaging protocol for reliable message exchange;
- definitions of the messages that can be exchanged between the Participants; and
- security standards and mechanisms for safeguarding the messages and the Participants systems and networks.

This document does not cover the application layer and network layer requirements.

1.3 2009 Revision

In 2009, the Mobile Number Portability Code was revised. At that time all associated Mobile Number Portability documents were republished as Communications Alliance documents to reflect the change of organisational name from ACIF. Where relevant any references to other documents have also been updated.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

For the purposes of the Guideline

ACIF

Australian Communications Industry Forum

CA

Certification Authority

CN

Common Name

CRL

Certificate Revocation List

DN

Domain Name

DNS

Domain Name System

DTD

Document Type Definition

HTTP

Hyper Text Transfer Protocol

IP

Internet Protocol

LDAP

Lightweight Directory Access Protocol

MNP

Mobile Number Portability

Root CA

Root Certification Authority

SSL

Secure Socket Layer

TCP

Transmission Control Protocol

XML

eXtensible Mark-up Language

2.2 Definitions

For the purposes of this Guideline, the following definitions apply:

Annual Compliance Audit

means a review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

Application Transaction

means a transaction that originates in the Application Layer

Application Layer

means the layer that represents the Business Application capabilities of each of the Participants in MNP for the initiation, processing, and reporting of the MNP transactions that are specified in Part 1 of this Specification.

Authorised Relying Party

means a recipient of a digitally signed message who is authorised to rely on a certificate to verify the digital signature on a message.

Certification Authority

means an organisation that issues certificates. The CA authenticates the certificate owner's identity and the services that the owner is authorised to use. It also manages the issuance of new certificates and revokes certificates from unauthorised users who are no longer authorised to use them. A CA is considered to be trusted when a user accepts any certificate issued by that CA as proof of the certificate owner's identity.

Certificate Practice Statement

means a statement of the practices which a CA employs in issuing certificates and managing the life-cycle of such certificates.

Certificate Revocation List

means a list maintained by the CA of all certificates that are revoked, but not expired. A certificate may be revoked because the user's private key is assumed to be compromised, the user is no longer certified by this CA, or the CA's private key is assumed to be compromised. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates' serial

numbers, and the specific times and reasons for suspension and revocation.

Client Certificate

means a certificate authenticating a network client and signed by a CA. It contains the client's Public Key.

Common Name

means a field of an X.509 certificate used for matching against the DN when validating the certificate.

Common Network

means a transmission network that interconnects all the Participants and provides a common network layer service for use on the platforms of all the Participants.

Digital Certificate

means a digital representation of information in a data structure used in a public key system to bind a particular authenticated individual to a particular Public Key which at least:

1. identifies the CA issuing it;

2. names or identifies its subscriber;

3. contains the subscriber's Public Key;

4. identifies its operational period; and

5. is digitally signed by the CA issuing it.

Digital Signature

means the unique information appended to a transaction used to sign the data.

Document Type Definition

means the description of the structure and the rules a document must satisfy for an XML document type. The DTD comprises the formal declaration of the elements that make up a document, their mutual coherence, meaning and documentation as drawn up for a document type (or document or information model). That is, it lists a number of element names, which elements can appear in combination with other ones, what attributes are available for each element type, etc. that, as a collection, defines the legal structure, elements, and attributes that are available for use in a document that complies to the DTD.

Domain Name

means the fully qualified name of a machine, including the hostname and domain

Domain Name System

means a data query service which translates DNs to IP addresses, and vice versa.

eXtensible Mark-up Language

means the widely used standard from the World Wide Web Consortium (W3C) that facilitates the interchange of data between computer applications. XML is similar to the language used for Web pages, the HyperText Markup Language (HTML), in that both use mark-up codes (tags). Computer programs can automatically extract data from an XML document, using its associated DTD as a guide.

Host Certificate

means a certificate containing a machines Domain Name in the CN field.

NOTE: Also known as a SSL Certificate

Hyper Text Transfer Protocol

means a protocol (utilising TCP) to transfer hypertext requests and information between servers and browsers to request a document and transfer its contents.

Internet Protocol

means a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network. IP is a connectionless, best-effort packet switching protocol. It is often linked to TCP, which assembles the packets once they have been delivered to the intended location.

Internet Protocol Address

means the unique number that identifies a networked system so that it may communicate via Internet Protocols. It consists of four numbers separated by periods. Most often, each part of the IP address is a number between 0 and 225; however, the first number must be less than 224 and the last number cannot be 0. IP addresses are logically divided into two parts: the network (similar to a telephone area code), and the system on the network (similar to a phone number).

Lightweight Directory Access Protocol

means a client-server protocol that supports interactive access to X.500 directory servers, i.e. database servers or other systems that provide information (e.g. digital certificate) about an entity whose name is known.

Participant

means those parties involved in MNP including any Carrier, CSP or PSS that interconnects with the PIPN to either send or receive Porting transactions.

Private Key

means a key used in asymmetric cryptography that belongs to an individual entity and is not made public, only being used by its owner. This is the key used for making digital signatures and is used to encrypt messages that only the corresponding Public Key can decrypt. The Private Key is also used to decrypt messages that were encrypted by the corresponding Public Key.

Public Key

means a key used in asymmetric cryptography that belongs to an individual entity and is distributed publicly. The Public Key is used to verify a digital signature created by the corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files that can then be decrypted with the corresponding Private Key.

Root Certification Authority

means the top level CA in a hierarchy of such authorities. A CA that is directly trusted by an end–entity.

NOTE: This term is not meant to imply that a Root CA is necessarily at the top of any hierarchy, simply that the CA in question is trusted directly.

RSA PKCS#7

means a standard that describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

Secure Socket Layer

means a protocol developed by Netscape Communications to provide security and privacy over the Internet. The protocol supports server and client authentication and maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

Server Certificate

means a certificate that attests to the identity of an organisation that uses a secure web server to serve data. A Server Certificate must be associated with a key pair. With this certificate a Participant can ensure that they are communicating with the right server.

Transmission Control Protocol

means the session-oriented streaming transport protocol which provides sequencing, error detection and correction, flow control, congestion control and multiplexing. TCP enables two computers to establish a connection and exchange information. TCP guarantees delivery of data and also guarantees that information packets will be delivered in the same order in which they were sent.

3 ASSUMPTIONS

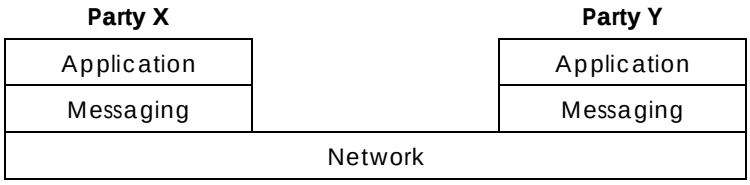
Security is required to be provided at the messaging layer.

4 MESSAGING PLATFORM

4.1 Architecture Framework

The MNP messaging platform is derived from a framework of a simple three-layer system architecture as shown in Table 1 below.

TABLE 1
MNP System Architecture



The Application layer represents the business application capabilities of each of the Participants for the initiation, processing, and reporting of the MNP transactions that are specified in Part 1 of this Specification.

The Messaging layer provides the messaging capabilities for the business applications of the Participants to reliably communicate and exchange MNP transaction messages.

The Network layer provides the capabilities for inter-connectivity between the Participants and for the carriage of the messages exchanged between the Participants.

The combination of the Messaging layer and the Network layer forms the Messaging Platform for MNP.

4.2 Topology

The Messaging Platform for MNP will have a topology as shown in Figure 1 below.

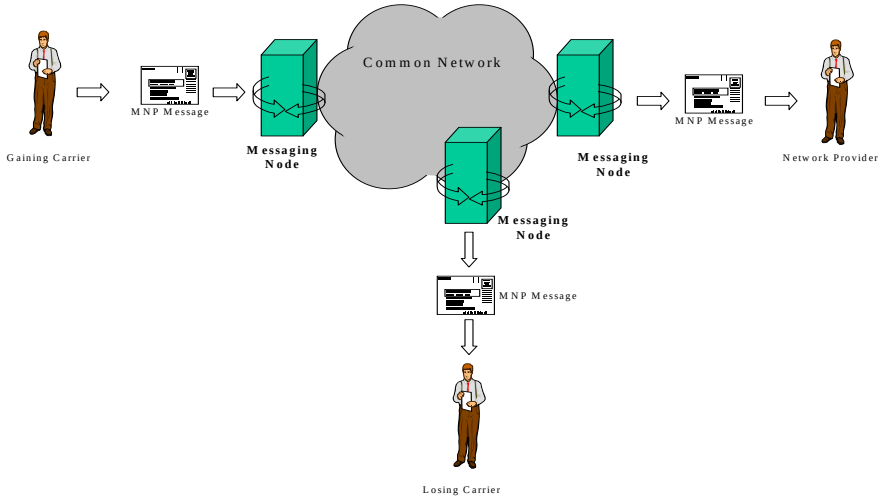


FIGURE 1
Messaging Platform Topology

A Messaging Node must be implemented and deployed by each of the Participants.

All Messaging Nodes must connect to a Common Network, which is an IP routed network that provides any-to-any access at the IP level for and between all the Messaging Nodes.

5 MESSAGING NODE REQUIREMENTS

5.1 Transport Protocol

Hyper Text Transfer Protocol (HTTP) must be the transport protocol to be used for message transfer between the Messaging Nodes of the Participants.

The protocol implementation must be compliant with the specification in the RFC 1945 HTTP/1.0, with the following additional constraints:

- Content-Length in the HTTP message header must always be populated with the actual length of the HTTP message;
- Content-Type in the HTTP message header must always be populated with "application/pkcs7-signature"; and
- There must only be one XML message per HTTP request or response.

5.2 Message Definitions

5.2.1 Message Category

Two categories of messages must be exchangeable between the Messaging Nodes of the Participants:

- Communication Control messages – These messages originate from the Messaging Layer and include the Receipt Acknowledgment, Node Ready and Node Inactive messages; and
- Application Transaction messages – These messages originate from the application layer and include the Port messages as identified in the IT Specification.

5.2.2 Logical Message Structure

The logical structure of the messages to be exchanged between the Messaging Nodes must consist of:

- One and only one Message Header element; and
- Zero, one or many XML Data elements.

The Message Header element must be the first element in each message.

5.2.2.1 Message Header Element

The Message Header element must consist of the following:

- MessageId – This is an identifier that uniquely identifies a message, as defined in the Data Dictionary in this document. This is a logical field

that is not present in the DTD and is formed by concatenating MessageType, RequestID, SendingParty, and TimeStamp.

- SendingParty – This is an identifier that identifies the Involved Party issuing the message.
- DestinationParty – This is an identifier that identifies the Involved Party to which the message is directed.
- TimeStamp – This is the time the message was first issued to one thousandth of a second, except in the ReceiptAcknowledgment message where it will be the TimeStamp of the message being acknowledged.

To ensure uniqueness of MessageId, no two messages must have the same MessageId value.

A message must be deemed a duplicate if it's MessageId is the same as that of a previously received message.

5.2.2.2 Message Data Element

The Message Data element must consist of the attributes that are required to carry the message data. The Message data must be compliant with the Messaging Layer DTD specified in Appendix A of this document, and compliant with the Application Layer DTD as specified in Part 1 of this IT Specification appropriately.

5.2.3 Message Format

Each of the messages to be exchanged between the Messaging Nodes of the Participants must be formatted as an XML document complying to the XML 1.0 standard.

The Communication Control messages must be in the format of the Communication Control Message DTD as defined in the Appendix A of this document.

The Application Transaction messages must be in the format of the Port Message DTD as defined in – Part 1 of this Specification.

5.2.4 Message Data Dictionary

The Data Dictionary for the Application Transaction messages must be as defined in Part 1 of this Specification.

The Data Dictionary for the Communication Control messages must be as defined in Appendix B of this document.

5.3 Messaging Protocol

5.3.1 Node Status

A Messaging Node of a Participant must maintain a Partner Table to identify the Messaging Nodes of all other Participants with whom it exchanges messages.

The Partner Table must contain Node Status to indicate the status of readiness to receive messages, of the Messaging Nodes of all Participants.

A Messaging Node of a Participant which is ready to receive messages must have its Node Status marked as Ready. A Messaging Node of a Participant which is not ready to receive messages must have its Node Status marked as Inactive.

The Node Status of the Messaging Node of a Participant must be initialised to Ready, following the completion of necessary bilateral agreements and registration.

5.3.2 Send Message

Messaging Nodes of the Participants must use the HTTP/1.0 POST operation to send messages to each other.

A message must only be sent to a Messaging Node of a Participant when it has a Node Status of Ready.

Each Messaging Node must send messages for different Participants independently of each other, so that any delay in the sending of a message to one Participant does not delay the sending of a message to another Participant.

The messaging protocol between two Participants is conversational, however Participants may implement parallel conversations.

A message must be resent if the sending node does not receive a Receipt Acknowledgment message, which must be returned within the body of the HTTP/1.0 “200 OK” synchronous response to the POST operation by the intended receiving node after it has received the message, following the elapse of a TimeoutToRetry as defined in Appendix C of this document.

The sending node must queue the message if it fails to receive a Receipt Acknowledgment message after retrying a MaxRetry as defined in Appendix C of this document.

Following the queuing of a message, the sending node must mark the Node Status as Inactive for the Messaging Node that is the intended receiving node of the queued message.

5.3.3 Receive Message

Upon receipt of a message, the receiving node must acknowledge the receipt of the message by returning a Receipt Acknowledgment message within the body of the HTTP/1.0 “200 OK” synchronous response to the POST operation.

Receipt Acknowledgment message must be returned irrespective of whether the received message is an original or a duplicated message. An original message is a message that has not been received before. A duplicated message is one that has already been received previously.

The Receipt Acknowledgment message must indicate whether the received message is:

1. accepted as an original message;

2. accepted as a duplicate message;

3. rejected because it is not a well formed and valid XML document;

4. rejected because it fails digital signature authentication; and

5. rejected because the digital signature does not match the Sending Party.

The Receipt Acknowledgment message must be used to acknowledge receipt of other messages only and not of itself. The Receipt Acknowledgment message must not be acknowledged upon receipt.

If a message is rejected at the messaging layer, then the message is considered as not received at the application layer.

If a message is accepted as a duplicate message, then the message must not be presented to the application layer so as to avoid rejection or duplication of processing.

5.3.4 Advise Ready Status

The Messaging Node of a Participant must advise the Messaging Nodes of other Participants of its Ready status by sending to them a Node Ready message upon the following events:

1. when it first becomes active and ready to receive messages from the other nodes;

2. when it returns to the active and ready state after an outage; and

3. a HeartbeatInterval, as defined in Appendix C of this document, has elapsed since the last Node Ready message was sent (this avoids checking on activity with other Participants).

A Messaging Node must mark the Node Status of other Messaging Nodes in its Partner Table as Ready, when their Node Ready messages have been received.

A Messaging Node must send the messages queued in persistent store for another Messaging Node following a change in Node Status, from Inactive to Ready, of that Messaging Node.

5.3.5 Advise Inactive Status

When a Participant wishes to cease receiving messages from another Participant, its Messaging Node must send a Node Inactive message to the Messaging Node of the other Participant.

Each of the Messaging Nodes must mark the Node Status of the Messaging Nodes in its Partner Table as Inactive when their Node Inactive messages have been received.

Messages intended for a Messaging Node must be queued to a persistent store following a change of Node Status of that Messaging Node to Inactive.

5.3.6 Configurable Parameters

The following parameters must be configurable so as to enable a change in value (e.g. for better performance) without the need for program code change:

- TimeoutToRetry;
- MaxRetry; and
- HeartbeatInterval.

5.4 Security

The security for safeguarding the messages in transit and the Participants' systems and networks must be based on the use of Digital Certificate, Digital Signature and Secure Socket Layer (SSL) mechanisms.

5.4.1 Digital Certificate

Digital Certificates to be used by the Participants must comply with version 3 of the X.509 standard.

Each Digital Certificate must chain to a Certification Authority (CA) that is recognised as a trusted Certification Authority for MNP purposes. A list of recognised CAs is available on the Communications Alliance web site at http://www.commsalliance.com.au.

The minimum requirements for a CA to be recognised include:

(a) It must have a published Certification Practice Statement (CPS) and operate according to generally accepted and developing industry standards including the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) WebTrust Program for Certificate Authorities and ANS X9.79:2001 PKI Practices and Policy Framework;

(b) It must have its operations and practices audited annually by an accredited independent public accounting firm;

(c) It must publish a CRL, keep the CRL up to date at no less frequent than daily, and make the CRL available for access by the Participants at no charge;

(d) It must secure its certificate signing operations and management by employing hardware protected cryptographic equipment, commonly known as Hardware Security Module (HSM) or Cryptographic Signing Unit (CSU), and applying appropriate procedural and employee controls; and

(e) It must confirm that the holder of an SSL Server certificate is the registered owner of or is otherwise authorised to use the Domain Name identified in the certificate; that the holder is an organisation which exists through the use of third party entity proofing service or database, or organisational documentation issued by or filed with the applicable government; and that the holder authorised the certificate application and the person who submitted the application on the holder's behalf was authorised to do so.

X509v3 conforming certificates are permitted to contain extensions. According to the x509v3 standard, these extensions MAY be ignored by participating systems, apart from extensions marked as CRITICAL. For this reason, only X509v3 Key Usage and X509v3 Basic Constraints extensions MAY be marked CRITICAL, and SHOULD be respected by participating nodes. No other CRITICAL extensions are permitted.

All Digital Certificates must have a key pair with a length of 1024 bit RSA. The Digital Certificates used with the SSL mechanism must be SSL Sever certificates. Each SSL Server certificate must identify the host by its fully qualified Domain Name in the Common Name field.

The same SSL Sever certificate and key pair must be used by both the SSL server and SSL client of the SSL mechanism.

The Digital Certificates used with the Digital Signature mechanism must be of a type that identifies an organisation, organisational role or host server, and not an individual person. Each Digital Certificate must contain a Common Name that is stable (does not change) between certificate renewals.

All Participants must, in an initial exchange, provide the Common Names in the Digital Certificates that are to be used with the SSL and Digital Signature mechanisms. The Common Name information forms the configuration information for name-based check by Participants and must not change frequently.

When a Digital Certificate is to be renewed or replaced, and if any part of the Common Name is to be changed, prior notice of

at least 6 weeks must be provided to all other Participants to facilitate timely systems changes.

Organisations using a proxy server must ensure that the complete certificate chain of the signer, up to and including the certificate of the recognised root Certification Authority, must be present on the proxy server.

5.4.2 Digital Signature

The Digital Signature mechanism must comply with version 1.5 of the RSA PKCS#7 standard.

Prior to being encrypted and sent, a message must be digitally signed in compliance with the PKCS#7 CMS standard.

The digitally signed message must be a PKCS#7 signature object that encapsulates the original unsigned message (ie. Implicit signature must be used). The following PKCS#7 options must be used to ensure maximum compatibility:

(a) ContentType of the PKCS#7 signature object must be signed data;

(b) Content of the signed data must be unencrypted data (ie. plain XML text);

(c) Content must be signed by one and only one signer, namely the sending party;

(d) The signature message digest algorithm must be SHA-1;

(e) The complete certificate chain of the signer, up to and including the certificate of the recognised root Certification Authority, must be present;

(f) A CRL is not required but its presence will not prevent normal operation;

(g) A single SignerInfo object corresponding to the signer must be present;

(h) The optional unauthenticatedAttributes and AuthenticatedAttributes fields must not be used.

NOTE: In the absence of an industry standard, the certificate chain of the Digital Certificate used to sign messages may be sent in any order.

Participants must perform the following validations prior to accepting a digitally signed message:

(a) The Digital Certificate of the message signer must not have expired, must chain to an MNP recognised CA, and must have the issuer's digital signature on the Digital Certificate validated by the issuer's public key;

(b) The Common Name in the Digital Certificate of the message signer must match with the Common Name that was provided by the message signer Participant in an initial exchange or subsequent renewal. At a minimum the country, state, organisation and Common Name must match with the country, state, organisation and Common Name that were provided by the message signer Participant; and

(c) The digital signature of the message signer is validated by the signer's public key.

NOTE: A pre-validation sort of the certificate chain may be required to validate the Digital Certificate used to sign messages.

Each Participant must use a Digital Certificate in accordance with the requirements specified in Digital Certificate section above. SSL Server certificates meeting these requirements must be accepted.

5.4.3 Secure Socket Layer

The SSL mechanism must comply with version 3.0 of the SSL Standard. To ensure maximum compatibility, the following options must be used:

(a) Both client and server must be authenticated;

(b) Public key cryptography in compliance with RSA must be used with authentication and key exchange;

(c) Data must be encrypted with block cipher in compliance with DES;

(d) Data encryption must use 128 bit RCA or 2 – Key - 3DES (168 bit) with setting given as SSL_RSA_WITH_3DES_EDE_CBC_SHA or SSL_RSA_WITH_RC4_128_SHA; and

(e) SHA-1 hash algorithms must be used.

SSL server authentication by the SSL client must include the following validations:

(a) The Digital Certificate of the SSL server must not have expired, must chain to an MNP recognised CA, and must have the issuer's digital signature on the Digital Certificate validated by the issuer's public key; and

(b) The Common Name in the Digital Certificate of the SSL server must match with the fully qualified domain name in the URL of the SSL connection request.

SSL client authentication by the SSL server must include the following validations:

(a) The Digital Certificate of the SSL client must not have expired, must chain to an MNP recognised CA, and must have the issuer's digital signature on the Digital Certificate validated by the issuer's public key; and

(b) The Common Name in the Digital Certificate of the SSL client must match the Common Name that was provided by the client Participant in an initial exchange or subsequent renewal.

6 REFERENCES

Publication	Title
Industry Codes	
C570:2009	Mobile Number Portability
Industry Guidelines	
G573.1:2009	Mobile Number Portability - IT Specification Part 1: Transaction Analysis
G573.3:2009	Mobile Number Portability - IT Specification Part 3: Common Network
G579:2009	Mobile Number Portability Operations Manual
SSL standard	SSL standard is http://wp.netscape.com/eng/ssl3/draft302.txt

APPENDIX

A Communications Control Message DTDS

A1 ReceiptAcknowledment DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Receipt Acknowledgment DTD-->
<!ELEMENT ReceiptAcknowledgment (MessageHeader, ReturnStatus)>
<!ELEMENT MessageHeader (EMPTY)>
<!ATTLIST MessageHeader MessageType CDATA #REQUIRED
                        RequestID CDATA #REQUIRED
                        SendingParty CDATA #REQUIRED
                        DestinationParty CDATA #REQUIRED
                        TimeStamp CDATA #REQUIRED>
<!ELEMENT ReturnStatus (ReturnCode, Description)>
<!ELEMENT ReturnCode (#PCDATA)>
<!ELEMENT Description (#PCDATA)>
```

NOTE: The MessageType field must contain the code that identifies the Receipt Acknowledgment message, and the RequestID field must contain the value of the RequestID field in the message that is being acknowledged. The TimeStamp field must contain the value of the TimeStamp field in the message that is being acknowledged.

A2 NodeReady DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Node Ready DTD-->
<!ELEMENT NodeReady (MessageHeader)>
<!ELEMENT MessageHeader (EMPTY)>
<!ATTLIST MessageHeader MessageType CDATA #REQUIRED
                        RequestID CDATA #REQUIRED
                        SendingParty CDATA #REQUIRED
                        DestinationParty CDATA #REQUIRED
                        TimeStamp CDATA #REQUIRED>
```

A3 NodeInactive DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Node Inactive DTD-->
<!ELEMENT NodeInactive (MessageHeader)>
<!ELEMENT MessageHeader (EMPTY)>
<!ATTLIST MessageHeader MessageType CDATA #REQUIRED
                        RequestID CDATA #REQUIRED
                        SendingParty CDATA #REQUIRED
                        DestinationParty CDATA #REQUIRED
                        TimeStamp CDATA #REQUIRED>
```

A4 Message Examples

The examples below demonstrate the use of the Communication Control messages in the following scenarios:

- **Scenario 1** - Party "0002" sends a NodeReady message to Party "0001". Note that a Receipt Acknowledgment for the NodeReady message is to be returned by Party "0001" but is not provided in the example.
- **Scenario 2** - The GMC (identified as "0001") sends a Port Notification message to the LMC (identified as "0002"). The Messaging Node of the LMC automatically uses the ReceiptAcknowledgment message to confirm the receipt of the Port Notification message.
- **Scenario** 3 - Party "0002" sends a NodeInactive to Party "0001". Note that a Receipt Acknowledgment for the NodeInactive message is to be returned by Party "0001" but is not provided in the example.

A.4.1 Scenario 1

Node Ready Message

```
<NodeReady>
      <Message Header
            MessageType= "NR"
            RequestID= "00012000122500000001"
            SendingParty= "0002"
            DestinationParty= "0001"
            TimeStamp= "2000122509013410"
      />
</NodeReady>
```

A.4.2 Scenario 2

Port Notification Message – GMC to LMC

```
<PortMessage>
      <MessageHeader
            MessageType= "PN"
            RequestID= "00012000122500000001"
            SendingParty= "0001"
            DestinationParty= "0002"
            TimeStamp= "2000122509083010"
      />
      <CustomerIdentity
            MSN= "0412411229"
            CADate= "20001130"
            <CustomerReference
                  AccountReference= "888777666"
            />
      />
<InvolvedParty
            GainingCSP= "0011"
            GainingMC= "0001"
      />
      <AuditTrail
            ATParty= "0011"
            ATMessageType= "PN"
            ATTimeStamp= "2000122509043010"
            ATParty= "0001"
            ATMessageType= "PN"
            ATTimeStamp= "2000122509083010"
      />
</PortMessage>
```

Receipt Acknowledgement Message

```
<ReceiptAcknowledgement>
      <Message Header
            MessageType= "ACK"
            RequestID= "00012000122500000001"
            SendingParty= "0002"
            DestinationParty= "0001"
            TimeStamp= "2000122509083010"
      />
      <ReturnStatus
```

```
            ReturnCode= “001”
            Description= “Original message received”
      />
</ ReceiptAcknowledgement>
```

A.4.3 Scenario 3

Node Inactive Message

```
<NodeInactive>
      <Message Header
            MessageType= “NR”
            RequestID= “00012000122500000002”
            SendingParty= “0002”
            DestinationParty= “0001”
            TimeStamp= “2000122509103410”
      />
</NodeInactive>
```

B Communications Control Message Data Dictionary

Attribute Name	Length/Format	Description
Description	CHAR(48)	A textual description of the Return Code. Valid values are specified in Appendix E of this document.
DestinationParty	NUM(4)	An ID identifying the party to which a message is directed. This is an industry standard 4 digit ID attached to each party – e.g. 0001 = Optus, 0002 = Telstra. A list of all Australian MCs/NPs and MCSPs and their respective IDs is maintained by Communications Alliance and is available on its website http://www.commsalliance.com.au.
EPID	NUM(4)	A unique identifier for Mobile Carriers, Mobile Carriage Service Providers, and Network Providers. Maintained by Communications Alliance and is available on its website. http://www.commsalliance.com.au
MessageId		This is a unique identifier for a message and consists of MessageType, RequestID, SendingParty and TimeStamp
MessageType	CHAR(10)	This is a code to identify a message type. This forms the first part of MessageId. This is mandatory on all messages. Valid values are specified in Appendix D of this document.
RequestID	NUM(21)	This is a system generated transaction identifier that is created by the originator of the message. This is used to uniquely identify an Application Transaction at the application layer, and to uniquely identify a Communication Control message at the messaging layer. This forms the second part of MessageId. This is mandatory on all messages. Value must be in the format of CSPIDCCYYMMDDnnnnnnnnn. For example, 000120001113000000001.
ReturnCode	NUM(3)	A code identifying the status of a received message. Valid values are specified in Appendix E of this document.
ReturnStatus		This provides the status of a received message and consists of ReturnCode and Description.
SendingParty	NUM(4)	An ID identifying the party to which a message is directed. This is an industry standard 4 digit ID attached to each party – e.g. 0001 = Optus, 0002 = Telstra. A list of all Australian MCs/NPs and MCSPs and their respective Ids is maintained by Communications Alliance and is available on its website. http://www.commsalliance.com.au
TimeStamp	NUM(17)	The time the message was first issued to one thousandth of a second. This forms the third part of MessageId. Mandatory on all messages. Value must be in the format of CCYYMMDDHHMMSSNNN.

C Configurable Parameters

Parameter	Value
TimeoutToRetry	90 seconds
MaxRetry	3
HeartbeatInterval	30 minutes

D Message Types

Valid MessageType values for the Application Transaction messages are specified in Part 1 of this Specification.

Valid MessageType values for the Communication Control messages are specified in the table below.

Message	Message Type
Receipt Acknowledgment	ACK
Node Ready	NR
NodeInactive	NI

These communication control MessageTypes are reserved and must not be used in Application Transaction messages.

E Return Codes

ReturnCode	Description
001	Original message received
002	Duplicate message received
003	Invalid XML message received
004	Digital signature fails to authenticate
005	Digital signature does not match Sending Party

PARTICIPANTS

The Working Committee responsible for the revisions made to this Guideline consisted of the following organisations and their representatives:

Organisation	Representative
ACCC	Grant Young
Optus	Gary Smith
Paradigm.One	Dev Gupta
Pivotel	Robert Sakker
Telstra	Mark Podzuweit
Telstra	Ray Pearson
Vodafone Hutchison Australia	Alexander R. Osborne
Vodafone Hutchison Australia	Meri Rowlands
Vodafone Hutchison Australia	Arti Sharma

This Working Committee was chaired by Alexander R. Osborne. Visu Thangavelu of Communications Alliance provided project management support.

Communications Alliance was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507