Western Australian Electricity Market
Build Pack
Infrastructure User Guide

July 2008

DOCUMENT RELEASE INFORMATION

Client	Metering Services
Project Name	WAEM Build Pack
Document Number	Published version # 5361762 Source version #4923679
Document Title	Infrastructure User Guide
Revision Status	2.1

Document prepared by:

Western Power
ABN 18540492861

Prepared by: Metering Services	Reviewed by OR Approved by::
Name (prepared by)	Name (reviewed/approved by)
WAEM Build Pack Working Group	Metering Services Manager

Document history

Version	Date	Changes
2.0	6 Nov 2006	Initial version
2.1	27 Jul 2008	Updated as part of Build pack V2.1 revision Change document references to revised Build Pack documents Update Terms & Definitions Clarify file naming specifications Clarify infrastructure set-up, availability and testing processes

Table of Contents

1 Introduction

1.1 Purpose

Note: In this document a reference to “Code Participants” excludes the Network Operator unless stated otherwise.

The purpose of the document is to provide registered Code Participants with a guide to the infrastructure required for system level integration with the Network Operator. The document gives an overall description on the integration service setup, and the likely configuration required by the Code Participant. The document will describe the setup and testing of the communication layer only between the Network Operator and the Code Participant as this ensures the infrastructure has been established correctly. For detailed information regarding the waeXML messages and the business processes, please refer to the Western Australian Build Pack - Standing Data and Customer Transfer Procedures; B2B Procedures.

1.2 Commencement

This document comes into operation in accordance with the Electricity Industry Customer Transfer Code 2004 Communication Rules and the Electricity Industry Metering Code 2005.

1.3 Overview and Structure

This document contains the following Sections:

Section 2 of this document provides an Overview of the Infrastructure
Section 3 of this document describes the Setup
Section 4 of this document describes the System Administration

1.4 Interpretation

This document is to be interpreted in accordance with Sections 1.4 (1) of the Customer Transfer Code and Metering Code.

1.5 Related Documents

This document should be read in conjunction with the other documents contained within the Western Australian Electricity Market Build Pack, as defined in the Western Australian Electricity Market Build Pack – Usage Guidelines.

1.6 Terms and Definitions

The following table lists the acronyms and definitions that are used in this document:

Term	Definition
aseXML	Australian Standard Electricity Extensible Markup Language. A standard for Energy Transactions in XML. It is XML schema designed to accommodate the necessary transactions required to operate the energy market.
B2B	Business to Business. Interactions between two or more independent business entities
Certification	In the context of this document, certification is official acceptance from the Network Operator that a code participant's system meets all requirements to connect to the market participant gateway.
Code Participant	In the context of this document, a code participant is a participant in the WA electricity market with rights to transact electronically with other participants, according to the rules defined in the Metering Code build pack.
FTPS	A secure version of the file transfer protocol (FTP)
Hokey-Pokey	Colloquial name for MSATS File Exchange Protocol
Market participant gateway	The FTP gateway between market participants and the Network Operator, through which all Transactions are exchanged.
Message	A waeXML envelope for the transportation of transactions or acknowledgements. In the WAEM each message is contained in a discrete file, and can only contain one waeXML transaction, transaction acknowledgement or message acknowledgement.
Message Acknowledgement	A waeXML element sent by the recipient of a message to its sender.
MSATS File Exchange protocol	The file transfer and acknowledgement protocol used in the NEM to ensure delivery and receipt of transactions between participants in the NEM. In the WA market, a simplified version of this protocol has been adopted, to support delivery and receipt of transactions between the Network Operator and other code participants.
Network Operator	In the context of this document, Western Power.
Production environment	Refers to all IT system components provided by the Network Operator to support the delivery and receipt of transactions between the Network Operator and other code participants.
SSL	Secure Sockets Layer. Provides for encrypted transmission of documents over the internet, and authentication using x509 certificates.
Testing environment	Refers to all IT system components provided by the Network Operator to support the testing of transaction delivery and receipt processes, prior to those processes being implemented into the production environment.
Transaction	A waeXML element used for the one-way exchange of information between applications with communicating end systems.

Term	Definition
Transaction Acknowledgement	A waeXML element sent by the recipient of a transaction to its sender. The transaction acknowledgement allows tracking of the transaction's progress and flags the receiver's commitment to process it. It may also be used to carry error information with regards to the corresponding transaction.
XSD	XML Schema Definition. This is an XML based language used to describe and control XML document content.
waeXML	Western Australian Electricity Extensible Mark-up Language. This is based on aseXML Version 17 but it includes Western Australian specific definitions.

2 Overview

The model, to be used for B2B system level integration between Code Participants and the market operator, will be based around the use of waeXML over Secure FTP (FTPS). It is not expected that all Code Participants will use this model/technique. This option is recommended for any Code Participants that may be expecting a high number of transactions, or looking for a streamlined, cost effective automated process. The Metering Service Centre (Web Portal) is an alternate solution for Code participants with low transaction volumes (see Web Portal Functional Specification). The Network Operator will not supply any other method of communication other than waeXML over Secure FTP or the Metering Service Centre. The code participant is obliged to use one of those two methods.

waeXML controls all business transaction functions, such as identification, timing, acknowledgment, transaction duplicate handling, etc to facilitate the communication between Code Participants and the Network Operator. (Note, waeXML documents are generally handled by individual business back end systems. This area will not be the focus of this document).

This document will discuss the waeXML transport mechanism for the B2B environment. It will elaborate on what will be provided by the Network Operator and the system requirements of the Code participant. It will also describe system availability, initial set-up and test procedures.

2.1 Stakeholders

The following stakeholders in the process and related infrastructure are responsible in some way for administration, management and operations:

Network Operator — While also a Code Participant, the Network Operator is acting as the message coordinator and facilitates various transactions e.g. customer transfers. The Network Operator is a central source for all information regarding connection points and meter readings.

Code Participants — As defined in Clause 1.2 of the Electricity Industry Metering Code 2004, refers to any party that is required to comply with the code.

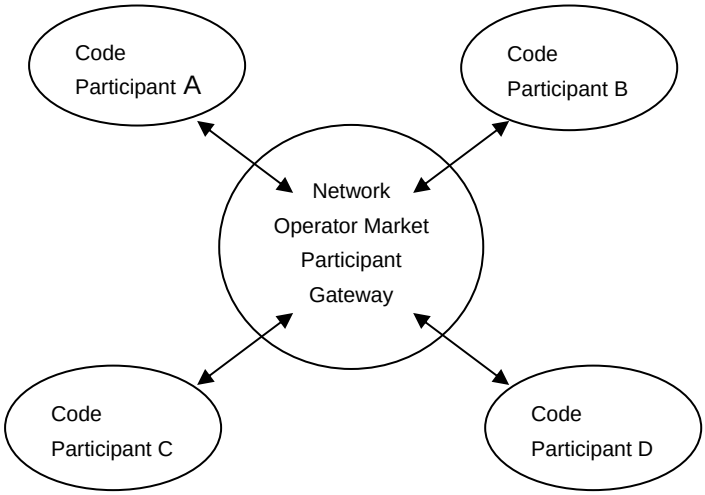
2.2 Topology

The Network Operator will act as the gateway with all messages from all Code Participants being either sent to or sent from them. Each message is either:

1) sent from the Network Operator to one Code Participant; or

2) from one Code Participant to the Network Operator; or

3) the Network Operator may send a different transaction (e.g. transfer notification) to one Code Participant as a result of processing a transaction sent by another Code Participant.



2.3 High Level Process

A waeXML transaction exchange will result in several messages being sent and received by the Code Participant and the Network Operator. Each message may contain a single message acknowledgement, one or more transactions, or one or more transaction acknowledgments.

Any message, sent or received as part of the transaction exchange, will be required to conform to one of these two processes:

1) A Code Participant sending a message to the Network Operator

2) A Code Participant retrieving a message from the Network Operator.

2.3.1 Sending a Message

The Code Participant will “FTP Put” the message file into their allocated inbox (i.e. inbox to the Network Operator) using the certificate and user-id password provided by the Network Operator to that Code Participant. The Code Participant will remove the message file on receipt (detection) of a corresponding message acknowledgement in their allocated outbox (i.e. outbox from the Network Operator).

All message files should be limited in size according to Section 4.8 Size of aseXML Messages in WA B2B Procedures: Technical Delivery Specification.

To ensure that message files are not read in a partially written state, each message file is to be "Put" with a .tmp extension and renamed to .zip or .ack (as appropriate) when the file "Put" is complete.

2.3.2 Retrieving a Message

The Code Participant will "FTP Get" the message file from their allocated outbox (i.e. outbox from the Network Operator) using a certificate and user-id password provided by the Network Operator. The Code Participant acknowledges receipt of the message file by placing (FTP Put) a message acknowledgment into their allocated inbox (i.e. inbox to the Network Operator).

The Code Participant and the Network Operator will be required to interrogate their FTPS outbox frequently to "poll" for existence of messages. Unless otherwise agreed with the Network Operator, the frequency of "polling" must be no more than once per 120 seconds and a no less than once per 30 minutes, to ensure that the transaction integrity (message response time) is maintained at all times (see the WA B2B Procedures: Technical Delivery Specification document for more detail regarding message and transaction response times).

The Code Participant should retrieve all messages. Therefore, if more than one message file is waiting to be retrieved, it is expected that the Code Participant will initiate a series of "FTP Get" requests within the "polling" period. Unless otherwise agreed with the Network Operator, the Code Participant must single-stream requests for messages, i.e. multi-threading requests are not to be performed.

Messages that are not retrieved will be visible in the View Messages function of the Metering Service Centre (Web Portal) – with the exception of transaction acknowledgments and message acknowledgments.

All message files should be limited in size according to Section 4.8 Size of aseXML Messages in WA B2B Procedures: Technical Delivery Specification.

To ensure that message files are not read in a partially written state, the "Get" must be restricted to message files with an extension of .zip or .ack.

2.3.3 Archiving of Messages

Messages sent by the Code Participant to the Network Operator, will not be archived by the Network Operator for retrieval by the Code Participant. But, the Network Operator may choose to archive the messages for their own purposes. Similarly, Code Participants are expected to provide their own message archiving processes for sent messages if it is deemed necessary to keep archives as part of their business process.

Messages retrieved from the Network Operator by the Code Participant, will not be archived by the Network Operator for retrieval by the Code Participant. But, the Network Operator may choose to archive the messages for their own purposes. Similarly, Code Participants are expected to provide their own message archiving processes for retrieved messages if it is deemed necessary to keep archives as part of their business process.

Note: Messages that are processed through Metering Service Centre (Web Portal) View Messages function can be archived. The Network Operator will provide each Code Participant with access to an ARCHIVE directory within their allocated outbox (i.e. outbox from Network Operator). The Network Operator may, at its discretion, delete a message

from the ARCHIVE directory if it is older than a defined age (initially 90 days). Code Participants should not rely on retention of messages in the archive directory.

2.4 The Technical Environment

Two environments will be described, the Network Operator's environment and the Code Participant's environment.

2.4.1 The Network Operators Environment

The Network Operator will provide FTPS server facilities, which will host the Code Participant's inbox and outbox, for both the production and testing environments. The FTPS server facility is capable of supporting 128-bit SSL connections. The server supports "explicit ssl" but not "implicit ssl" connections.

To facilitate access to that server, the Network Operator will provide the following to the Code Participant:

1) Digital certificates to facilitate secure access to the production and testing environments;

2) User-ids and passwords for authentication;

3) The network name and port of the production and testing FTPS server facilities; and

4) A set of FTPS commands to confirm that the FTPS interface is accessible from the Code Participant site.

The Code Participant will provide the following to the Network Operator:

1) A request to use the FTPS B2B interface.

2.4.2 The Code Participant's Environment

The Code Participant will not be required to provide any specific infrastructure. It is expected that Code Participants will put in place any necessary system of their own design.

Code participants will require an SSL compatible FTP client to access the FTPS server hosted by the Network Operator. Non-SSL access is not supported. The client should be capable of generating and importing SSL certificates.

To provide strengthened transaction security, the Network Operator may, in agreement with a Code Participant, establish additional controls which must then be supported by that Code participant's environment.

2.4.3 SSL and Certificates

The SSL session will require both the client and the server to exchange certificates. Each client will need to have a valid signed certificate issued by the Network Operator.

To obtain a valid client certificate, the participant will need to generate a public/private key pair and forward the associated certificate signing request to the Network Operator. On receipt of the request, the Network Operator will sign the request, which will generate a new certificate. The newly generated certificate will be sent back to the participant and should be imported into the participant's FTP client. This certificate should be used for all subsequent connections to the FTP server.

The FTP server will supply a certificate when an SSL connection is made. This certificate will be made available to the participant prior to the initial connection being made, at which point the participant must import the certificate and add it to their list of trusted authorities.

2.4.4 Establishing the FTP session

The following describes the process of establishing the FTP session.

- The client will make the initial connection to the server and request that an SSL connection is made. This communication should be of the type “explicit ssl” (eg. AUTH SSL), not “implicit ssl”.
- The server will send the client its certificate and public key and request a certificate from the client.
- The client will compare the certificate from the server against its trusted authorities database. If the certificate is listed, the session will continue.
- If the certificate is listed, the client will then use the server public key to encrypt a session key. The client will then send the session key and its own certificate to the server.
- The server will compare the client certificate against its own trusted authorities database and will then either accept or reject the connection. If the connection is accepted the server will decrypt the client session key using the server public key and send a success message to the client. This will open a secure data channel for the FTP session to proceed.

The user login will occur following the successful exchange of certificates.

2.4.5 FTP commands

Login:

```
sFTP codeparticipant@FTPs.networkoperator-secure
[enter password]
```

Obtain messages intended for Code Participant:

Navigate to outbox (i.e. Network Operator outbox to Code Participant):

```
cd out
```

Obtain files from “out” directory:

```
ls

[perform get on each file]
get filename.zip

quit
```

Send messages intended for Network Operator:

Navigate to inbox (i.e. Network Operator inbox from Code Participant):

```
cd in
```

Place files into “in” directory:

```
put filename.tmp
```

For files containing a transaction or transaction acknowledgement:

```
rename filename.tmp filename.zip
```

For files containing message acknowledgements:

```
rename filename.tmp filename.ack

quit
```

Delete messages:

Navigate to inbox (i.e. Network Operator inbox from Code Participant):

```
cd in
```

Delete files from the “in” directory:

```
delete filename.zip

or

delete filename.ack

quit
```

2.4.6 Testing and Production

Multiple server and/or ports will be provided to separate the testing environment from the production environment. The Network Operator and the Code Participant will be required to provide the necessary information (e.g. network name, port, user-id etc) for both environments, as described in Section 4.1 Schedule of Availability.

The production environment will include scheduled maintenance periods. For more information regarding this and the periods, refer to Section 4.1 Schedule of Availability.

The testing environment will only be provided via mutual agreement between the Network Operator and Code Participants. For more information regarding this, refer to Section 4.1 Schedule of Availability.

2.5 Administration

To gain access to the B2B Service the Code Participant should contact their Access Account manager. The following details will be need to be provided for each intended user:

- Contact position title
- Contact name
- Contact email address

- Phone
- Email address for planned outage notification
- Company
- Market participant code

2.6 Certification

The Network Operator will award the Code Participant with certification to interface with the market participant gateway after formal sign-off, by confirming that all tests were performed successfully. Infrastructure sign-off will entail the following:

1) Confirmation of a successful connection by the Code Participant to the market participant gateway.

2) Confirmation of a successful “Put” of a message and subsequent message clean-up by the Code Participant

3) Confirmation of a successful “Get” of a message, “put” of message acknowledgement and subsequent clean-up by the Code Participant

4) Confirmation of a successful “Get” of multiple messages, put of message acknowledgements and subsequent clean-up by the Code Participant

5) Confirmation of the implementation of a suitable polling frequency for the “Get” message request. For more information, refer to Section 2.3.2 - Retrieving a Message of this document.

This certification is limited to the infrastructure only. The Code Participant will ensure transaction integrity and compliance with the XML schemas in line with the specifications described in the Standing Data and Customer Transfer Procedures, B2B Procedures.

2.7 File Naming

The file naming convention assists in the identification and prioritization of messages.

Messages containing transactions or transaction acknowledgements have a suffix of .xml, but for transport are compressed into a message file of the same name but with a .zip suffix. For example:

```
message.xml
```

is compressed in a message file:

```
message.zip
```

Messages containing message acknowledgements are not compressed, and have the same filename as the corresponding message but with an .ack suffix. For example:

```
message.zip
```

is acknowledged with a message acknowledgement file:

```
message.ack
```

All filenames must be in lower case to allow for consistent processing by all participant systems.

2.7.1 Files to the Network Operator

The file naming structure is as follows:

```
0         1         2         3
12345678901234567890123456789012345.xxx
-------------------------------------
ttttpfffffffcccccccuuuuuuuuuuuuuu.xxx
```

where the above codes translate as:

tttt =	Transaction group (e.g. cats, sord, mtrd, nmid, etc)
p =	transaction priority (h=high, m=medium, l=low)

The last 30 characters uniquely identify the transaction and the from and to participants:

fffffff =	8 character for the "From" participant code, right padding with "_" (e.g. wpntwrks, abcd____)
ccccccc =	8 characters for the "To" participant code, right padding with "_" (e.g. wpntwrks, abcd____)
uuuuuuuuuuuuuu =	up to 14 characters to uniquely identify the transaction (e.g. date and unique id as follows 20061228_00001, or another unique id. The id can contain numbers, letters, dashes and underscores.)

The file extension identifies the file type:

xxx =	3 character file extension (xml=uncompressed message file, zip=compressed messge file, ack=message acknowledgement file, tmp=partially written file)

Sample file name examples:

```
sordmabcd____wpntwrks20061228_00002.zip   ← Service order request from Abcd
nmidmabcd____wpntwrks20061228_00001.zip   ← NMI Discovery request from Abcd
mtrdhabcd____wpntwrks20061228_00003.zip   ← MDN transaction ack from Abcd
```

2.7.2 Files from Network Operator

File names from the Network Operator to Code Participants will follow a similar but alternate file naming structure:

The primary driver for a detailed file naming specification is the Metering Service Centre (Web Portal), which requires informative file names to minimise performance overheads when displaying file lists.

Proposed file name for outbound Transaction and MessageAcknowledgement Files:

Originating Transaction and TransactionAcknowledgement:

```
0         1         2         3
12345678901234567890123456789012345.xxx
-------------------------------------
ttttpgggnnnnnnnnnnn_yyyymmdduuuuuuu.zip
ttttptxa_trans_ack__yyyymmdduuuuuuu.zip
```

Message Ack is identical file name with .ack extension:

```
0         1         2         3
12345678901234567890123456789012345.xxx
-------------------------------------
ttttpgggnnnnnnnnnnn_yyyymmdduuuuuuu.ack
ttttptxa_trans_ack__yyyymmdduuuuuuu.ack
```

Where

tttt = Transaction Group
p = Priority (h, m, l)
ggg = Transaction Type within Transaction Group (letters of the alphabet)
nnnnnnnnnnn = NMI (eg. 80010001111) if single NMI file
"mdn_nem12__" if NEM12
"mdn_nem13__" if NEM13
"_nmi_na____" if no NMI or multiple NMI
yyyymmdd = year, month, day (this is the date transaction/message was generated in the senders system)
uuuuuuu = unique identifier up to 9,999,999 each day (this can be an integer, can be zero padded and can be used as an indicator of the order in which messages were generated)

Transaction	Group	Type	Priority
NMIDiscoveryRequest	nmid	ndq	Medium
NMIDiscoveryResponse	nmid	ndr	Medium
NMIStandingDataRequest	nmid	sdq	Medium
NMIStandingDataResponse	nmid	sdr	Medium
NMIStandingDataNotification – Partial	nmid	sdp	Medium
NMIStandingDataNotification – Full	nmid	sdf	Medium
MessageAcknowledgement	msgs	msg	Same priority as the initiating Transaction
TransactionAcknowledgement	**	txa	Same priority as the initiating Transaction
MeterDataNotification	mtrd	mdn	High
+ MeterDataNotification (Meter Data History)	mtrd	mdh	High
+ MeterDataNotification (Meter Data Verify)	mtrd	mdv	High
MeterDataMissingNotification (request)	mtrd	mdm	High
MeterDataVerifyRequest	mtrd	mvq	High
ServiceOrderRequest	sord	soq	Medium
ServiceOrderResponse	sord	sor	Low
WAElectricityCustomerTransferRequest	cats	ctq	High
WAElectricityCustomerTransferResponse	cats	ctr	Low
WAElectricityCustomerTransferNotification	cats	ctn	Low
WAElectricityCustomerTransferCancelRequest	cats	ctc	High
CustomerDetailsNotification	cust	cdn	Low
CustomerDetailsRequest	cust	cdq	Low

Transaction	Group	Type	Priority
AmendMeterRouteDetails/AmendSiteAccessDetails	site	acn	Medium
AmendMeterRouteDetails/AmendSiteAddressDetails	site	aan	Low

Note: msg acks have identical file name to the message being acknowledged
\+ Only for Metering Service Centre (Web Portal)
** transaction acknowledgments have same group as originating transaction

Sample file name examples:

```
sordmsor8001000111112006122800000002.zip  <--- Service order response to Abcd
custltxa_trans_ack___20061228000002.zip  <--- CDN transaction ack to Abcd
```

3 Setup

This section describes the detailed steps required to ensure that the B2B setup process between the Code Participant and Network Operator infrastructure is implemented correctly. The following steps are recommended:

1) Register for access

2) Exchange required information e.g. security, technical details etc (see Section 2.4.1 The Network Operators Environment.)

3) Establish suitable communications link that supports FTPS to and from the Network Operator

4) Confirm access to FTPS server (Testing Environment)

5) Establish and test full B2B integration (Testing Environment)

6) Confirm access to FTPS server (Prod Environment)

7) Establish full B2B integration (Prod Environment).

3.1 Registration and Access

To register for access to the B2B Service, please follow the business process described in Section 2.5 Administration. Once access has been authorised, the Network Operator will send the following items to the Code Participant.

1) Certificates for the Testing and Production environments;

2) Command Line to confirm Testing and Production environment access;

3) User-IDs and Passwords; and

4) Other connection information as required.

3.2 Information Required

The following information is required for the Code Participants to successfully establish the B2B interfaces.

waeXML (XSDs) – http://www.westernpower.com.au/mainContent/workingWithPower/NetworkAccessServices/MeteringCodeCommunicationsRules.html

Standing Data and Customer Transfer Procedures, B2B Procedures

WA B2B Processes: Participant Build Pack

3.3 Confirming Access

Use the Command Lines to test the connection to the Network Operator. The initial test should be to execute a "Login" request in the Test environment. This will confirm that basic network connectivity can be achieved enabling the Code Participant to confirm the hostname, login/password that they were provided with as part of the registration process. If the login is unsuccessful, please contact the Network Operator.

If the connection was successful, proceed by testing the "FTPS Get" (secure) service in the Test environment. This will confirm that the certificate and other credentials are correct.

If further tests are required, the Command Lines can be used to send and receive test messages in the Test environment.

3.4 FTPS Functions

The FTPS service supports the MSATS File Exchange Protocol (previously known as Hokey-Pokey), which is used in the NEM. The WA implementation of the MSATS File Exchange Protocol is a point-to-point protocol between Western Power and market participants, whereas the NEM implementation is a multi-point protocol between market participants through the MSATS hub. The point-to-point protocol uses .ack files, whereas the multi-point protocol uses .ack and .ac1 files for message acknowledgement. The code participant is required to use the MSATS File Exchange Protocol communications protocol if not utilising the Metering Service Centre, the Network Operator will not make any other protocol available.

Refer to B2B Procedures: Technical Delivery Specification section 3, Transaction Model for details on the MSATS File Exchange Protocol as used by the WA market participant gateway.

4 System Administration

4.1 Schedule of Availability

4.1.1 Production Environment

Code participants will be able to send or receive market transactions using either the Web Portal or the market participant gateway. The infrastructure and applications used to support these requirements will run within the Network Operator's environment and be subject to controlled maintenance windows.

The Network Operator will notify each Code Participant (via the Code Participant's pre-defined email address for planned outage notification) of planned system outages, giving notice of at least 1 business day. The Network Operator will schedule this work to occur

outside of normal business hours (8:00am – 5:00pm WST Monday – Friday) wherever possible.

The Network Operator will provide each Code Participant with at least 1 hours notice of planned outages that need to occur urgently within normal business hours. These changes will be limited to break-fix patches that are required to maintain optimal market operation.

The Network Operator will notify each Code participant as soon as possible when an unplanned outage occurs (indicating estimated down-time) and also when market participant gateway services are restored.

The Network Operator and the Code Participants need to be able to send and receive messages 24 hours a day, 7 days a week. To aid in this process, the Network Operator and Code Participants must provide a contact point or person 24 hours a day, 7 days a week to assist in resolving technical issues.

Code participants can raise technical and business issues to the Network Operator via the contact number on the Retailer and Generator Portal web page:

`http://www.westernpower.com.au/mainContent/workingWithPower/NetworkAccessServices/RetailerGeneratorPortal.html`

4.1.2 Testing Environment

4.1.2.1 Testing of changes and upgrades to the market participant gateway

For upgrades to the market participant gateway, periods of availability will be published by the Network Operator, to allow all Code Participants to perform testing in a controlled manner. This is not to be used by Code Participants to perform back office functional testing, but only to be used for end–to-end integration tests between the Network Operator and the Code Participants.

In consultation with Code Participants the Network Operator will facilitate industry-wide testing and will be required to prepare an Industry Testing Strategy in accordance with he timeframes agreed through the market consultation process.

4.1.2.2 Testing of changes and upgrades to Cade Participant systems

A Code Participant may request the testing environment to be made available as part of their own system testing strategy. Where predefined Network Operator activity is needed to completed the test cases, the Code Participant must give notice to the Network Operator as per the following table:

Estimated person days of Network Operator activity	**Notice to be given**
0 days	10 business days
1-2 days	10 business days
2-5 days	20 business days
6-20 days	2 months
20+ days	3 months

Following due notice given to the Network Operator, the Code Participant will be required to specify the cases being tested, the NMIs to be loaded into the testing environment and the Network Operator action to be taken on each test case.

The Nework Operator and Code Particpant will work together to establish a reasonable commercial arrangement to meet the cost of testing using the testing environment.

4.2 Disaster Recovery

The Network Operator has a schedule of standard backup processes that cover the Network Operator systems, including the market participant gateway. In the event of a disaster (e.g. hardware failure), standard recovery processes would be used to get the required systems operational within the mandated two business days.

Should the recovery process extend to the limit of two days the Network Operator will consult with Code participants so as to determine the most appropriate transfer of data to clear any backlog.