



MDM/R File Transfer Services and Web Services

Configuration Workbook

Version 1.0

October 15, 2008

Table of Contents

1	INTRODUCTION.....	2
1.1	PURPOSE.....	2
1.2	ASSUMPTIONS	2
1.3	RELATED DOCUMENTS	2
1.4	DEFINITION OF TERMS.....	2
2	MDM/R OVERVIEW AND CONCEPTS.....	4
2.1	MDM/R FILE TRANSFER SERVICES (FTS)	5
2.1.1	<i>Protocol</i>	5
2.1.2	<i>AS2 ID Assignment</i>	5
2.1.3	<i>Connectivity between the MDM/R and MDM/R service recipients</i>	5
2.1.4	<i>File Types Transported by FTS</i>	5
2.1.5	<i>Encryption and Digital Signatures</i>	6
2.1.6	<i>Authorization to Submit Files to the MDM/R</i>	6
2.1.7	<i>MDM/R FTS Processing</i>	6
2.1.8	<i>Recertification of Security Certificates</i>	7
2.2	MDM/R WEB SERVICES	7
2.2.1	<i>Protocol</i>	7
2.2.2	<i>Connectivity between the MDM/R and MDM/R service recipients</i>	7
2.2.3	<i>MDM/R Web Services Request Types</i>	8
2.2.4	<i>Encryption and Digital Certificates</i>	8
2.2.5	<i>Authorization to Submit MDM/R Web Service Requests to the MDM/R</i>	9
3	GUIDANCE FOR SELECTING AS2 SOFTWARE.....	10
3.1	AS2 SOFTWARE.....	10
3.2	OTHER CONSIDERATIONS	10
3.2.1	<i>AS2 File Name Preservation</i>	10
4	GETTING STARTED	11
4.1	MDM/R ENVIRONMENTS	11
4.1.1	<i>Sandbox Environment</i>	11
4.1.2	<i>Quality Assurance Environment</i>	11
4.1.3	<i>Production Environment</i>	11
4.1.4	<i>Disaster Recovery Environment</i>	11
4.2	NETWORK OVERVIEW	11
4.3	EXCHANGING CONFIGURATION INFORMATION.....	12
4.4	ESTABLISHING CONNECTION.....	13
4.4.1	<i>Selection and procurement of an AS2 software package</i>	13
4.4.2	<i>Exchange of configuration information with the IESO</i>	13
4.4.3	<i>Installation of the AS2 package and Firewall configuration</i>	14
4.4.4	<i>Testing with the IESO</i>	14
5	AS2 CONFIGURATION.....	15
6	DIGITAL CERTIFICATE SETTINGS	18

1 Introduction

1.1 Purpose

The intent of this document is to help you understand the framework for file transfer and web services with the MDM/R.

It provides an overview of the File Transfer Services (FTS) capability and describes the specific information that you will need to configure your systems and to test connectivity. During enrolment there will be an information exchange for gathering the settings required for successful connectivity.

1.2 Assumptions

Unless otherwise indicated, all references to “we”, “us” and “our” shall mean a reference to both the IBM Canada and the Independent Electricity System Operator (IESO) acting in its capacity as the Smart Metering Entity (SME).

You are responsible for selecting, acquiring, installing, configuring and operating your own AS2 software.

If you wish to make use of the web service interface, you will be required to implement your own application server capable of initiating the requests and handling the responses.

1.3 Related Documents

Document Title
<i>MDM/R Detailed Design (SME_DEC_9001)</i>
<i>MDM/R Reports Technical Specifications (SME_SPEC_0001)</i>
<i>MDM/R Technical Interface Specifications (IESO_SPEC_9027)</i>
<i>MDM/R Service Recipient – FTS and Web Services Configuration Form (SME_FORM_0014)</i>
<i>MDM/R Configuration Template for FTS and Web Services (SME_TPL_0001)</i>

1.4 Definition of Terms

Terms used within this document have been defined in Table 1.1 below.

Table 1.1 – Definitions

TERM	Description
AMI	AMI means the Advanced Metering Infrastructure, it includes the meter, Advanced Metering Communication Device (AMCD), Local Area Network (LAN), Advanced Metering Regional Collector (AMRC), Advanced Metering Control Computer (AMCC), Wide Area Network (WAN), and related hardware, software, and connectivity required for a fully functioning data collection system. An AMI does not include the MDM/R.
AMI Operator	

TERM	Description
AS2	AS2 means Applicability Statement 2 and is a specification of the Electronic Data Interchange over the Internet (EDIINT) working group of the Internet Engineering Task Force (IETF).
Billing Agent	
Billing Quantity	Refers to consumption data that has been through VEE and Framing and is ready for use in billing.
Customer Contracted Agents (CCA)	An organization that has been retained to operate on behalf of an end user.
File Transfer Service or FTS	The service which manages the transfer of files between the MDM/R and LDCs and/or the LDC's authorized agents.
Framing	The process by which interval data is assembled into Billing Quantities.
Framing Structure	Framing Structure means a parameter that denotes the method by which Meter Reads are assembled into Billing Quantities by the MDM/R.
LDC	Means a Local Distribution Company, which is an LDC, as defined in the Ontario Energy Board Act, 1998
Meter Read	Is a number generated by a meter that reflects cumulative electricity consumption at a specific point in time. (The Meter Read and related data will be reported to the MDM/R at a specific Service Delivery Point.)
MDM/R	Means the meter data management and meter data repository functions within which Meter Reads are processed to produce Billing Quantity data and the storage of data for future use.
MDMR Service Recipient	Any organization that has registered as an official MDM/R participant. This includes LDCs, AMI Operators, Billing Agents, Retailers or Customer Contracted Agents.
Operational Service Provider (OSP)	The party with primary responsibility for operating the MDM/R on behalf of the Smart Metering Entity. This role is currently fulfilled by IBM Canada as of the date of publication of this document.
Organization ID	A unique Identifier for an organization that will be assigned within the MDM/R during the registration process. Examples of organizations include LDC, billing agents, AMI operators and Retailers.
Retailer	
SSL	Secure Sockets Layer - A cryptographic protocol which provides secure communications on the Internet.
SOAP	Simple Object Access Protocol – A protocol for exchanging XML based messages over computer networks normally using Http.
VEE	Means Validation, Estimating and Editing of Meter Reads to identify and account for missed and inaccurate Meter Reads to derive billing data. The algorithm to complete VEE identifies gaps in Meter Reads and rebuilds consumption based on historical trending and averaging.
Web Services	Means the web service interface provided by the MDM/R to authorized parties allowing connection to dynamic websites to serve their customers.
WPG	WebSphere Partner Gateway - provides the platform for the MDM/R to manage the business to business (B2B) transactions for file transfer and translations

2 MDM/R Overview and Concepts

This section describes the system-to-system interactions with the MDM/R through the MDM/R File Transfer Services (FTS) and through web services.

FTS is the component that provides the capability for secure file transfer between your systems and the MDM/R. Local Distribution Companies (LDCs), AMI operators and billing agents are all entities allowed to exchange files with the MDM/R.

The MDM/R web services interface is a synchronous interface between your systems and the MDM/R. This interface allows service recipients (LDCs, AMI operators, billing agents, retailers and customer contracted agents) to build websites with dynamic, real-time access. It allows access to customer consumption data and daily billing quantity data, for a specified timeframe, for one service delivery point (SDP) at a time.

The MDM/R V1.0 solution footprint (below) illustrates the interactions with the MDM/R through FTS and web services.

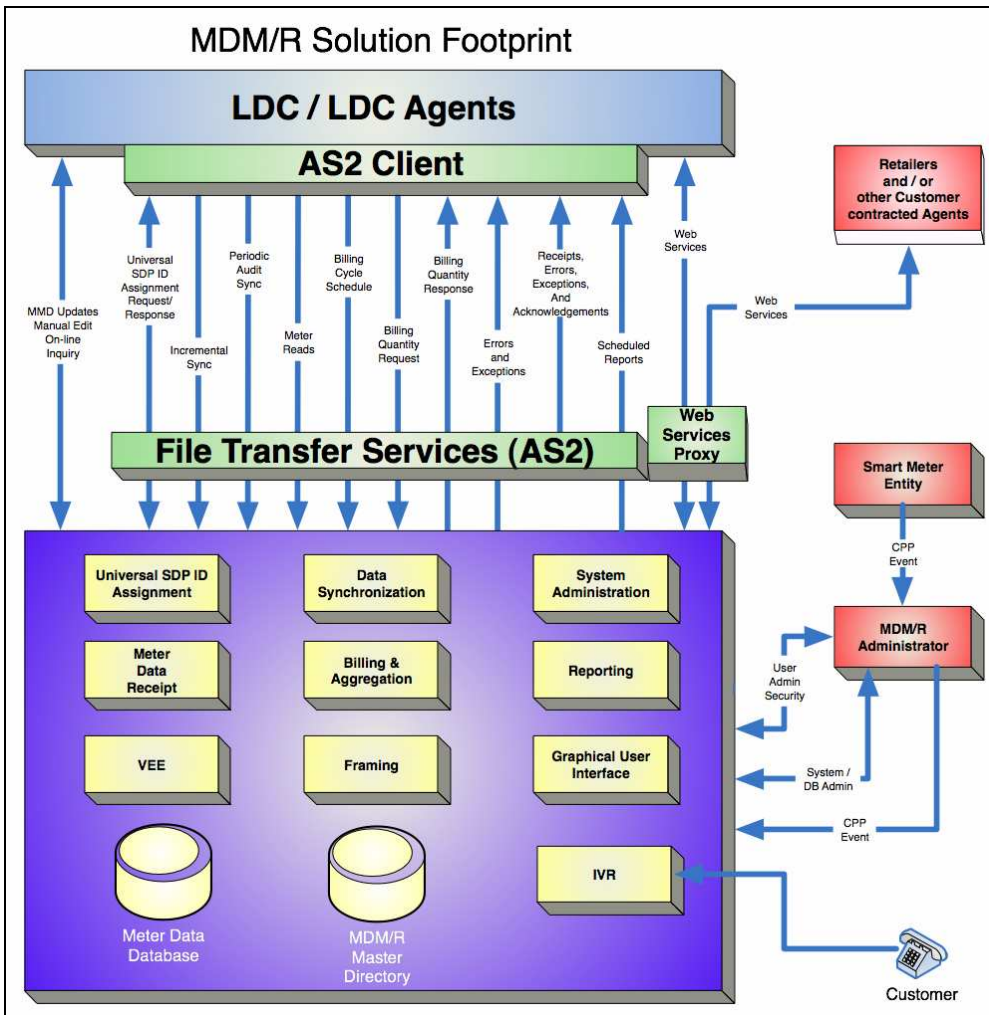


Figure 2.1: MDM/R V1.0 Solution Footprint

2.1 MDM/R File Transfer Services (FTS)

2.1.1 Protocol

FTS uses the *Use of Applicability Statement 2* (AS2) protocol for all file exchanges. You will require your own AS2 software and are free to select from the list of approved products. Guidelines for selection are provided in Section 3.

AS2 is a specification of the Electronic Data Interchange over the Internet (EDIINT) working group of the Internet Engineering Task Force (IETF). It was designed to support the secure movement of business data across the internet using established internet protocols such as HTTP and HTTPS. It concerns itself with the movement of the file, not the content of the file.

FTS provides secure transfer of files, receipts, and optional compression through the use of the AS2 protocol. The protocol requires that both ends of the file exchange support AS2.

The AS2 protocol includes the concept of a Message Disposition Notice (MDN) that is returned to the sender of a file. The MDM/R FTS uses the MDN to inform you of the result of processing of the file. The format and content of the MDN will vary with the AS2 package.

2.1.2 AS2 ID Assignment

AS2 IDs are used within the AS2 software to identify the sending and receiving organizations. The MDM/R implementation of the AS2 protocol will use the Organization ID as the AS2 ID for each MDM/R service recipient. The Organization ID is a unique identifier within the MDM/R and will be issued by the Smart Metering Entity (SME) during the registration and enrolment process.

Your Organization ID will be used in your AS2 software as the AS2 ID for each of the MDM/R environments. The MDM/R itself will have multiple Organization IDs (see section 4.2 Network Overview for details). Your systems will exchange files via FTS with three MDM/R environments, each with their own Organization ID.

The MDM/R environments are:

- Production – used for production operations
- Quality Assurance – used for System Integration Testing (SIT) and Qualification Testing (QT) through the registration and enrolment process.
- Sandbox – used for optional unit testing through the registration and enrolment process and for the regression testing of new releases once in production operations.

The Organization ID of each of these MDM/R environments will be provided by the SME during the registration and enrolment process.

2.1.3 Connectivity between the MDM/R and MDM/R service recipients

FTS connectivity between your application server and the MDM/R will be accomplished via the internet. You are responsible for procuring internet connectivity that allows connectivity to the MDM/R. We are not responsible for supporting the MDM/R service recipients AS2 software as our responsibility ends with the MDM/R's AS2.

2.1.4 File Types Transported by FTS

The Technical Interface Specifications document (IESO_SPEC_9027) describes the files, their content, and format. This specification can be found at 'http://www.smi-ieso.ca/Technical_Interfaces'.

Files that arrive at the MDM/R for processing that do not meet this specification will be rejected and a notification will be returned to you.

2.1.5 Encryption and Digital Signatures

Files for exchange with the MDM/R involve digital signing prior to transmission. The signed files are transmitted using a mutually authenticated SSL connection. This allows for mutual authentication by the sender and receiver. The SSL encryption and digital signature requires the exchange of self signed digital certificates between your application server and the MDM/R. The exchange of these 'keys' or digital certificates is explained further in section 6 of this document and will be performed during the registration and enrolment process.

2.1.6 Authorization to Submit Files to the MDM/R

FTS verifies that the organization submitting every file is a registered MDMR service recipient and is authorized to submit the file. This is true whether the file is submitted by the LDC or by an agent organization on behalf of an LDC.

Authorization is established during the registration and enrolment process through the submission of MDM/R Registration Application Forms (SME_FORM_0003) and LDC Organizational Relationships and Authority Delegation forms (SME_FORM_0006) available at 'http://www.smi-ieso.ca/Manuals_Procedures'.

For example, if the LDC called Acme Hydro has out-sourced the operation of its AMI to Ace AMI Operations Inc., then it will be necessary for Ace AMI Operations to send meter read data to the MDM/R on behalf of Acme Hydro. This is enabled through the completion of the following steps:

- Acme Hydro and Ace AMI Operations Inc. must both become registered MDM/R service recipients by each submitting an MDM/R Registration Application Form;
- Acme Hydro must authorize Ace AMI Operations to submit files through FTS on its behalf by submitting an LDC Organizational Relationships and Authority Delegation form

2.1.7 MDM/R FTS Processing

The functionality provided by FTS is described in the following sections.

2.1.7.1 AS2 Processing

AS2 processing is implemented on the MDM/R side of the FTS interface using IBM Websphere Partner Gateway. You are free to choose any approved AS2 product to meet your business needs. Failures and error situations occurring during AS2 processing are communicated back to you through the use of the Message Disposition Notice (MDN). The MDN is typically displayed to the users through an AS2 Management console. Direct examination of the MDN file is not required.

2.1.7.2 Message Disposition Notice (MDN)

A MDN is the internet messaging format used to convey an electronic, informational receipt. It is used by AS2 software implementations at either end of a connection to inform the other of the results of a file transfer.

The content and format of an MDN is defined in RFC 3798 which forms part of the AS2 specification.

Typically, MDNs are not viewed or manipulated directly by a user. They are used by the AS2 software implementation in functions such as the management console to provide the administrator or user with a view of the status of any given operation.

MDN notification is limited to the scope of the AS2 processing. Once a file transfer has completed AS2 processing further notification of outcomes must be handled through independent messages.

2.1.7.3 Post AS2 Processing by MDM/R FTS

The MDM/R FTS validates the following during its post AS2 processing:

- File name syntax
- The AS2_ID, ORG_ID_1 and ORG_ID_2
- Confirmation that the organization has the authority to submit the file type

Failure and error situations are communicated back through the FTS processing failure reports. These responses are specified in the MDM/R Reports Technical Specifications (SME_SPEC_0001).

2.1.8 Recertification of Security Certificates

2.1.8.1 Responsibility:

The security certificates used for connectivity between the MDM/R and your systems have an expiry date. It is your responsibility to track when these certificates expire and take pro-active steps to renew them before they do, in order to avoid disruption to your business activities.

2.1.8.2 Timeframe:

A minimum of one month prior to the expiration date of each security certificate, you must notify us through IESO Customer Relations that your security certificate is about to expire. Such notice should clearly identify:

- the Organization ID you are referring to;
- the specific security certificate(s) involved and the exact date(s) of their expiration; and
- a contact person for the recertification activity.

2.1.8.3 Recertification action:

You should also work with your certificate provider to generate a re-certified security certificate. Once the certificate has been generated, you must notify IESO Customer Relations, and the IESO will arrange for an appointment between you and the OSP to perform a connectivity testing session using the new certificate. The OSP will also send an email confirming your appointment time and requesting for you to send the new certificate. The new certificates should be sent by email to the address provided by the OSP.

2.2 MDM/R Web Services

2.2.1 Protocol

MDM/R web services encompass server to server communications between your application server and the MDM/R. MDM/R web services uses SOAP (Simple Object Access Protocol) for exchanging XML-based messages. The MDM/R web service interface is delivered using FTS; however it does not use the AS2 protocol. You are not required to use AS2 software to implement MDM/R web services.

2.2.2 Connectivity between the MDM/R and MDM/R service recipients

The MDM/R web services implementation provided by the MDM/R uses HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). The network connection between you and the MDM/R is a mutually authenticated SSL session.

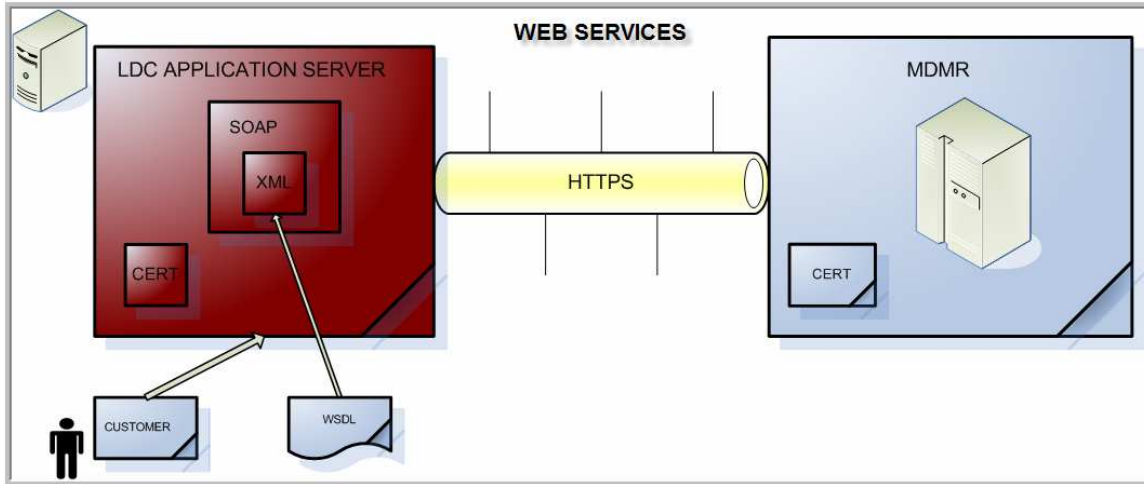


Figure 2-1 – MDM/R Web Services High Level Architecture Diagram

Figure 2-1 above illustrates the high level architecture of the web services solution offered by the MDM/R. Those wishing to make use of the web service interface are required to implement an application server that will request the web service and process the response.

The format of the web service request and corresponding response is fully defined in the *MDM/R Technical Interface Specifications (IESO_SPEC_9027)*. Building and testing the application server is the responsibility of the LDC or requesting organization. The implementation of web services is optional. Therefore, the testing of web services can be completed independently of System Integration Testing (SIT) and Qualification Testing (QT).

Web services testing is allowed in the production environment as it is a read only service and has no ability to change or edit data in the MDM/R.

2.2.3 MDM/R Web Services Request Types

Four request types can be made using Web Services:

Request Type	Description
MP01	Cumulative Consumption Report
MP02	TOU Consumption Report
MP03	Interval Reads Request
MP04	Interval Reads and TOU Consumption Request

Table 2- 1 – MDM/R Web Services Request Types

Table 2- 1 shows the four request types available. The *Technical Interface Specifications (IESO_SPEC_9027)* provides the detail on how to create each of these request types.

2.2.4 Encryption and Digital Certificates

Similar to FTS, the MDM/R web service interface will utilize digital certificates. You can use the same self signed certificate for web services as FTS if you already have FTS connectivity. Alternatively, you can create and exchange new certificates to be used solely by your web services application. If you do not have FTS connectivity with the MDM/R, you will have to create and exchange certificates with us prior to use. In either case, the self signed certificate that is generated by the organization requesting MDM/R Web Services must specify the LDC’s MDM/R Organization ID in the CN of the certificate.

2.2.5 Authorization to Submit MDM/R Web Service Requests to the MDM/R

We will enable MDM/R web services during the registration and enrolment process for each LDC. You can develop, configure, test and utilize web services anytime after connectivity testing.

The LDC controls the access to customer consumption data and daily billing quantity data and is responsible for authorizing access to other MDM/R service recipients. Web service access to this data is granted for each SDP by the LDC. The LDC will identify organizations authorized to access the data using the synchronization process. Web service requests will return information to authorized organizations and will return an error to unauthorized organizations.

3 Guidance for Selecting AS2 Software

3.1 AS2 Software

If you will be exchanging files with the MDM/R you must procure, install and configure software that provides AS2 functionality.

The AS2 software is used both to exchange files with the MDM/R and to manage the operational aspects of the exchanges such as error logs, notifications, retries, etc.

The AS2 software must be interoperable with the FTS implementation. An independent third party interoperability testing group, Drummond Group, provides interoperability testing of AS2 software and provides a listing of the AS2 software providers that have been certified as interoperable. You are responsible for obtaining AS2 software from one of the vendors of the current Drummond Group AS2 interoperability testing certification list.

Please refer to the Drummond Group web site for the most recent list of AS2 certified software vendors.

<http://www.drummondgroup.com/html-v2/as2-companies.html>

The MDM/R FTS is a part of the MDM/R solution. However, your AS2 software is not part of the MDM/R FTS. It is installed, operated, maintained and supported by you.

3.2 Other Considerations

This section contains any additional considerations that may arise as a result of ongoing connectivity testing between different AS2 software products.

3.2.1 AS2 File Name Preservation

FTS uses the original file name from the sender's side in order to route the file within the MDM/R.

Original file names however do not always survive processing by AS2 software. A common convention known as, "file name preservation," places the original file name of the file being transmitted in the Content-Disposition field of the "S/MIME bodyPart" header. It should be noted however, that this is not used by all types of AS2 implementations.

Because of these problems, the specification of each interface file that is supported by the MDM/R requires the placement of the file name in the first record of the file in a specific format. The FTS also sets the file name in the expected header when returning a file. By placing the file name in the first record of the file, both systems will be able to determine what to do with the file should the name change during transit. The specifications for each file type are documented in the MDM/R Technical Interface Specifications (IESO_SPEC_9027).

4 Getting Started

4.1 MDM/R Environments

During the enrolment process, an organization will establish connections to all test environments, the sandbox, QA, production and the disaster recovery environment. Each connection is configured and tested separately.

4.1.1 *Sandbox Environment*

The sandbox environment is available for optional unit testing of interface files and for testing connectivity through the use of digital certificates during the enrolment process. The sandbox environment will also be used for regression testing of new releases and functionality once you have entered the production environment.

4.1.2 *Quality Assurance Environment*

The Quality Assurance (QA) environment is used to perform final testing prior to moving changes into production. This is also the environment you will perform SIT and Qualification Testing (QT) in before going into the production environment.

4.1.3 *Production Environment*

The production environment will be the environment used to support the MDM/R's production operations.

4.1.4 *Disaster Recovery Environment*

The disaster recovery environment is only used in the event that the production environment is not usable. The process of switching from the production environment to the disaster recovery environment has been designed to be transparent. However in order to ensure that infrastructure, like firewalls, have been correctly configured both on the MDM/R side and on your side the connection to the disaster recovery environment is tested during enrolment. Other than connectivity testing, this environment is not used for any other business purpose during the normal course of MDM/R operations.

4.2 Network Overview

You have the option to choose the number of environments required to support the connection to the three MDM/R environments. Figure 4-1 below depicts the scenario where you have one environment to connect to the three MDM/R environments. You may also use three environments to connect to the MDM/R's three environments.

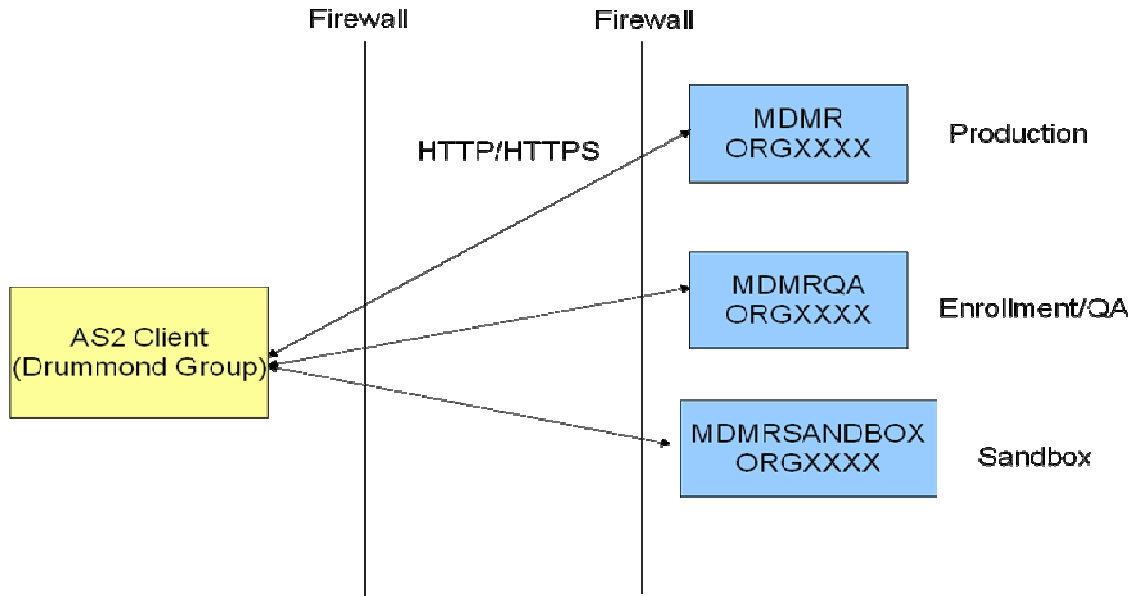


Figure 4-1 – Connection to Multiple MDM/R Environments

Each MDM/R environment will be identified by a unique MDM/R Organization ID. You will have one Organization ID regardless of the number of environments you decide upon.

4.3 Exchanging Configuration Information

The system configuration information exchanged between our organizations is confidential.

During registration prior to connectivity testing, we will send the OSP's confidential system configuration information to each LDC in a form called the Meter Data Management and Repository FTS and Web Services Configuration Template. The service recipients who will be installing an AS2 client must send their corresponding confidential system configuration information to us using an FTS and Web Services Configuration form (SME_FORM_0014).

MDM/R FTS and Web Services Configuration Template

The configuration template contains the following information that you will need to configure your firewall and AS2 software:

1. Participant AS2 ID

The AS2 ID to be used in your AS2 configuration is the MDM/R's Organization ID. We have different IDs for the sandbox, QA and production environments.

2. Inbound public IP address

This is the IP address that is used by the MDM/R to receive files. This address should be used in your firewall configuration for communication to us. Each MDM/R environment will have a unique IP address.

3. Inbound DNS name – FTS Connectivity

This DNS name is the corresponding DNS name for the inbound public IP address identified in number 2 above. Each MDM/R environment will have a unique DNS name. When configuring your AS2 software, you should use DNS names instead of the actual IP address. The use of DNS names will allow the transparent switchover to the disaster recovery system in the event of a business interruption resulting in a loss of the MDM/R production site. You should send files to the MDM/R inbound DNS name.

4. Inbound DNS name – Web Services

This DNS name is the corresponding DNS name to be used by the Web Service application for the submission of web service requests. These are the DNS names to be used within the WSDL.

5. Inbound Ports

The OSP's firewall will be configured to listen on these ports only.

6. Outbound public IP address

Files sent from the MDMR will appear to come from this IP address. Each MDM/R environment will have a unique IP address.

We will send the MDM/R's digital certificates when we send you the AS2 Configuration Template.

MDMR FTS and Web Services Configuration Form (SME_FORM_0014)

Use this form to return your configuration information to the IESO prior to connectivity testing so that we can complete our firewall and FTS configuration:

1. Outbound public IP Address

This is the IP Address that you will use to send files to the MDM/R. If you have different sandbox, QA and production systems then include all applicable outbound IP addresses.

2. Inbound public IP Address

This is the IP Address you will use to receive files via FTS. If you have different sandbox, QA and production systems then include all applicable inbound IP addresses.

3. Inbound Ports

These are the firewall ports that you will configure to listen. We recommend that the inbound ports be selected from 80, 443 or between 56000 and 60000.

4. AS2 URLs

These are the URLs that you have configured for inbound traffic using http and https protocols.

5. Web Services

These are the IP addresses of the servers that will be used by you to host your Web Services application.

Email us your digital certificates when you submit your configuration form.

4.4 Establishing Connection

The establishment and testing of FTS connectivity with the MDM/R is referred to as connectivity testing. The steps required to complete connectivity testing, at a high level, are:

4.4.1 Selection and procurement of an AS2 software package

Section 3 of this document provides a series of selection guidelines for consideration when selecting an AS2 software package. You should determine the configuration of your environment(s) to support testing, SIT, QA, and eventual production operations with the MDM/R

4.4.2 Exchange of configuration information with the IESO

The exchange of information with the IESO is accomplished via:

- o Completion and submission of the MDMR FTS and Web Services Configuration Form (SME_FORM_0014), and

- o Your receipt of the MDMR FTS and Web Services Configuration Template

You are required to create and exchange digital certificates with us at this time.

4.4.3 Installation of the AS2 package and Firewall configuration

Once the exchange of information has been completed you can proceed to configure your firewall(s) to allow the exchange of files with the MDM/R and install and configure your AS2 software. Although the settings required by each compatible software package cannot be anticipated, Section 5 of this document provides guidance to configuring the AS2 software settings. The AS2 Configuration Template provides the MDM/R's confidential information required for firewall configuration and AS2 software configuration.

4.4.4 Testing with the IESO

The process of testing the connection to each of the MDM/R's environments will be done in 3 stages. This process is referred to as connectivity testing.

- In the first stage, standard connectivity will be established using the HTTP protocol without digital signatures.
- In the second stage, the protocol will be changed to HTTPS.
- In the third stage, digital signing will be added. The second and third stages require the use of digital certificates.

Prior to connectivity testing, you must exchange information with us to allow for:

- Firewall changes on both sides to allow connectivity
- The configuration of the AS2 software on both sides to allow for the exchange of files.

Additional information on connectivity testing can be found in the testing guide on the main IESO website at the following location:

http://www.ieso.ca/imoweb/pubs/training/smartmetering/Testing_Cutover.pdf

5 AS2 Configuration

This section is to be used as a guide when configuring your AS2 software for each of the MDM/R environments (Sandbox, QA, and Production).

Referenced requirements will be provided to you in the MDMR FTS and Web Services Configuration Template. Each MDM/R environment will have a unique value.

Where there is no requirement, configurations can be made to suit your organization's environment. The table below describes the required AS2 parametric settings that you must use.

Table 5-1 Required AS2 parametric settings

Parameter	Description	Requirement
Participant Name	The name that is used as to identify the MDMR environment in your AS2 client	Provide a full name with no spaces.
<i>Document Receipt Protocol</i>		
Parameter	Description	Requirement
HTTP	HTTP protocol (no SSL)	Required.
HTTPS	HTTPS protocol (secure using SSL).	Required
<i>Capabilities</i>		
Parameter	Description	Requirement
Protocol HTTP	Indicates whether "raw" documents (i.e. non-AS2 packaged content) can be sent or received. When off for sending, all documents dropped in the Send directory will be moved to the Error directory when transmitting the document. When off for receiving, documents which are received without AS2 packaging are placed in the receive error directory for the participant.	Sending and receiving non AS2 packaged content with http is not allowed.
Participant AS2 ID (MDM/R Environment ORGID)	The AS2 ID, which is required by the AS2 packaging standard. If any documents are to be AS2 packaged for transmission, then this value must be supplied. This value will be supplied to you.	Reference 1 (AS2 Configuration Template)
Content Type	Only transmission or receipt of AS2 Binary packaged documents is supported by the MDM/R FTS. This usually requires that the content type be explicitly stated.	Binary Send: Allow Binary Receive: Allow Binary Content

Parameter	Description	Requirement
		Type: octet-stream
<i>Inbound AS2</i>		
Parameter	Description	Requirement
Basic Authentication Required	The MDM/R does not use basic authentication.	Not allowed
User Name	The user name for Basic Authentication	Leave Blank
Password	The password for Basic Authentication	Leave Blank
Identify the Partner	The method for which a partner is identified. The MDM/R requires the AS2 ID and not basic authentication.	Use AS2 ID
<i>Outbound AS2</i>		
Destination Address	The address or DNS name where outbound AS2 documents are sent.	Reference 3 (AS2 Configuration Template)
Basic Authentication Required	The MDM/R does not use basic authentication.	Not allowed
User Name	The user name for Basic Authentication	Leave Blank
Password	The password for Basic Authentication	Leave Blank
Request MDN	This option is for specifying whether a Message Disposition Notification (MDN) is required as proof of receipt for outbound AS2 documents.	Required
Synchronous or Asynchronous	Select whether outbound AS2 documents will be sent synchronously or asynchronously.	Asynchronous
HTTP or HTTPS	Select whether the HTTPS or HTTP protocol is to be used with outbound AS2 documents.	HTTPS
Request Signed MDN	This option is for specifying if a digitally signed MDN is required as proof of receipt for outbound AS2 documents.	Required

Parameter	Description	Requirement
Sign Documents	This digitally signs outbound AS2 documents. It is the user's responsibility to ensure that the appropriate digital certificate is loaded prior to sending Signed/Encrypted documents. If the appropriate certificate is not loaded, document transmission will fail.	Required
Encrypt Documents	This option is for the encryption of outbound AS2 documents.	Do not encrypt
Compress Documents	This is to compress outbound AS2 documents.	Do not compress

6 Digital Certificate Settings

This section provides the details required to create digital certificates that allow the secure transport of your files being transferred. Below are the requirements for your digital certificate.

Settings	Required
Self signed certificate (includes CA)	Yes *
Thumbprint Algorithm	SHA1
Format	Encoded binary X.509
Extension	DER (Note: you may need to rename an encoded binary X.509 to be DER instead of CER)
Public Certificate filename format	ORGXXXXX_CERT_YYYYMMDD##.der
Expiration	Determine based on your IT security policy
Subject: Common Name (CN) Field	Your MDM/R Organization ID. This will be used by FTS to authenticate your identity.

* Note: When viewing the certificate it may have a red X that says the certificate authority (CA) is not trusted. This is allowed. If it has a yellow exclamation mark, you likely have not included the CA certificate. This will not work as it is not self signed.

Please email your certificate to the IESO Market Entry department, at Market.Entry@ieso.ca, when you submit your AS2 configuration form. You may use one certificate across all your environments, or you may use one per environment. Using one certificate is easier to manage and simplifies connectivity test on setup and on expiration. It is up to you which you would like to use. There is the potential of production downtime when you choose to have one per environment. The MDM/R uses one per environment.