

MDM/R I.T. Workshop

October 19, 2010



Purpose



- To provide you with a comprehensive overview of the Meter Data Management Repository File Transfer Services (MDM/R FTS) and Web Services.
- This overview will include an inventory of practical business considerations and associated information technology components that will bridge your organization to the MDM/R.

Objectives



- Provide overall knowledge of the technical components of the MDM/R FTS communications layer, including the associated requirements of the Applicability Standard 2 (AS2) protocol that governs it.
- Familiarize you with the technical requirements needed for, and the information available through, Web Services.
- Specifically outline the major technical and business issues that your organization will need to address.

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

Topics

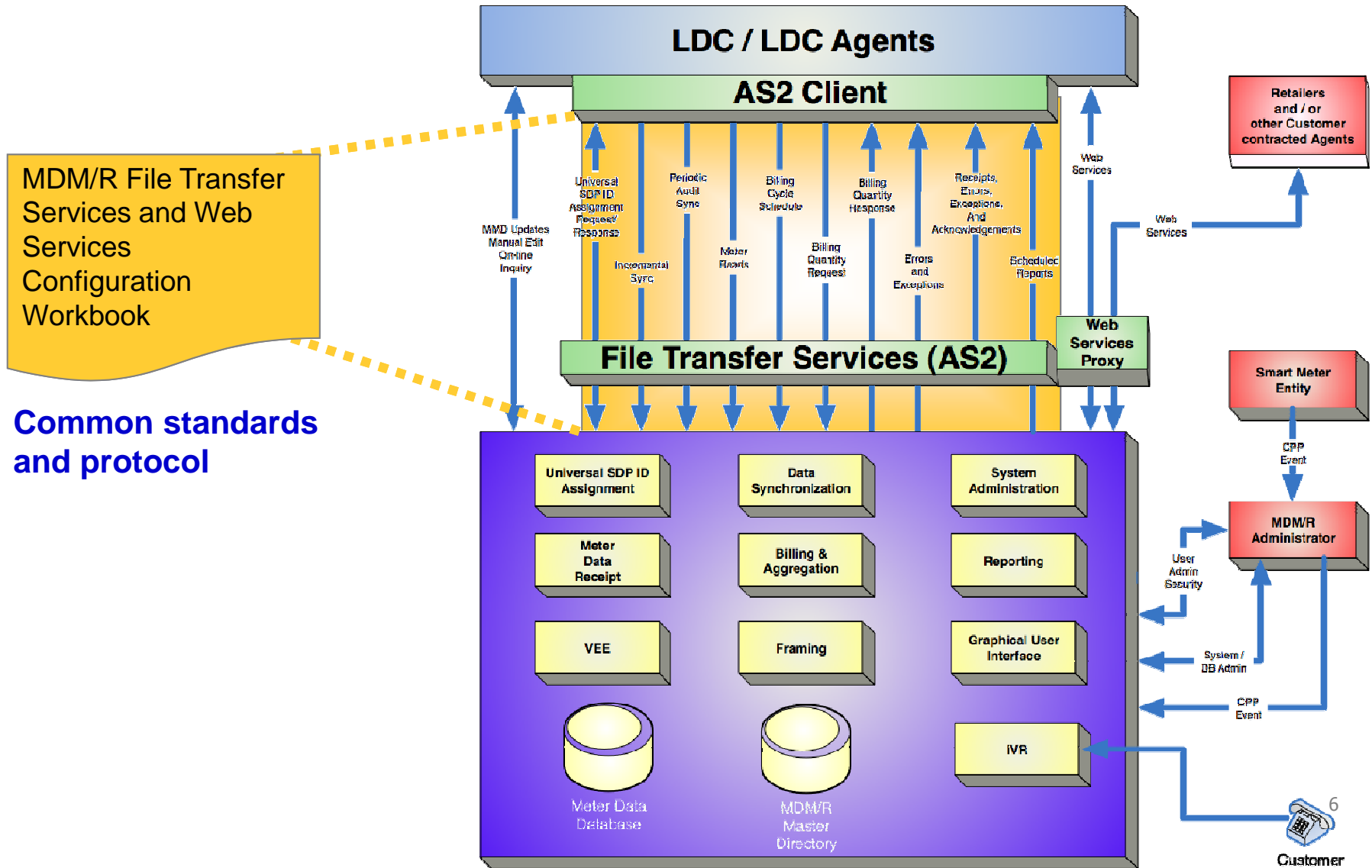
- **File Transfer Services**
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example

- **Web Services**
 - Information available
 - Technical requirements
 - Lessons Learned

- **Q&A**

File Transfer Services Overview

MDM/R Solution Footprint

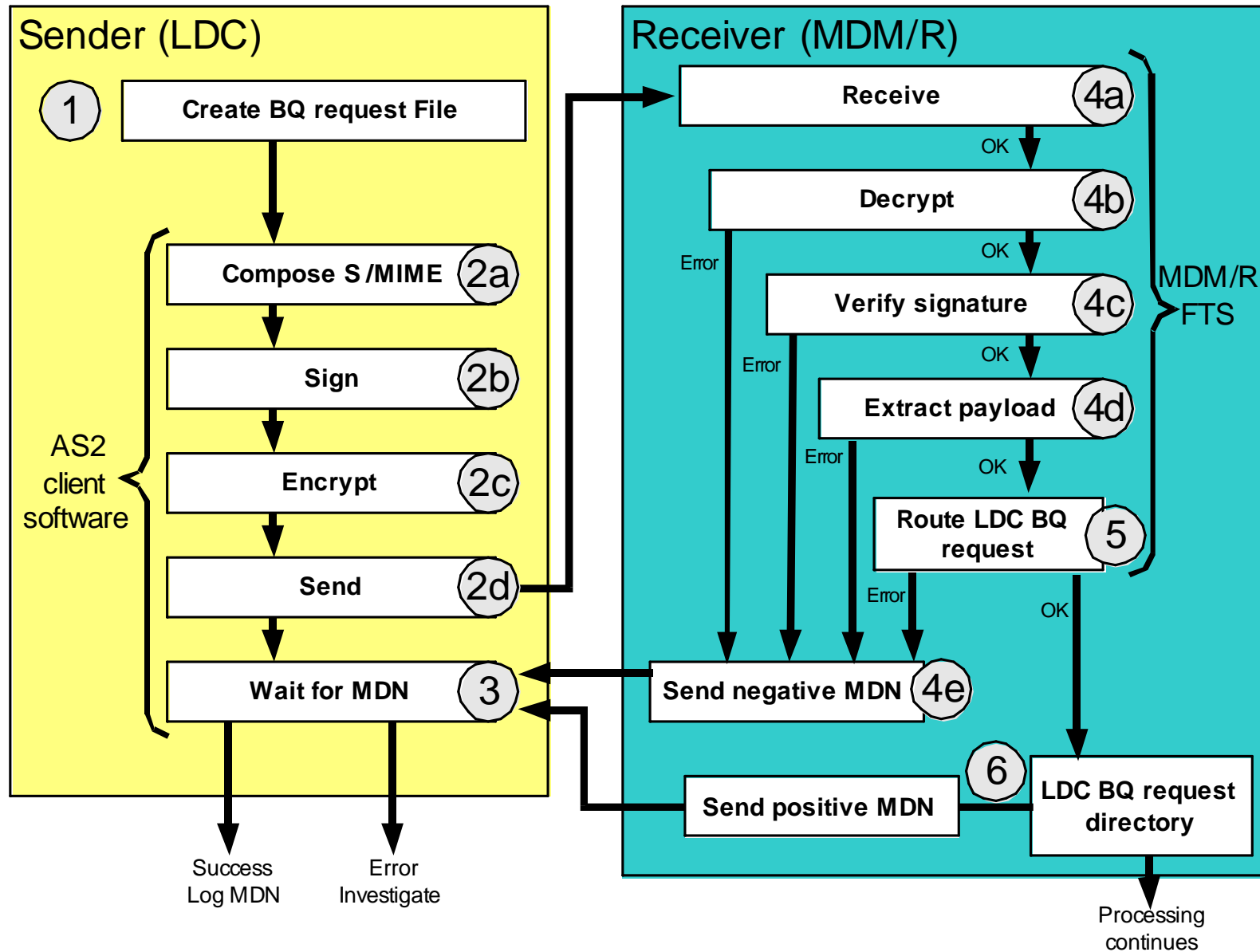


File Transfer Services Overview



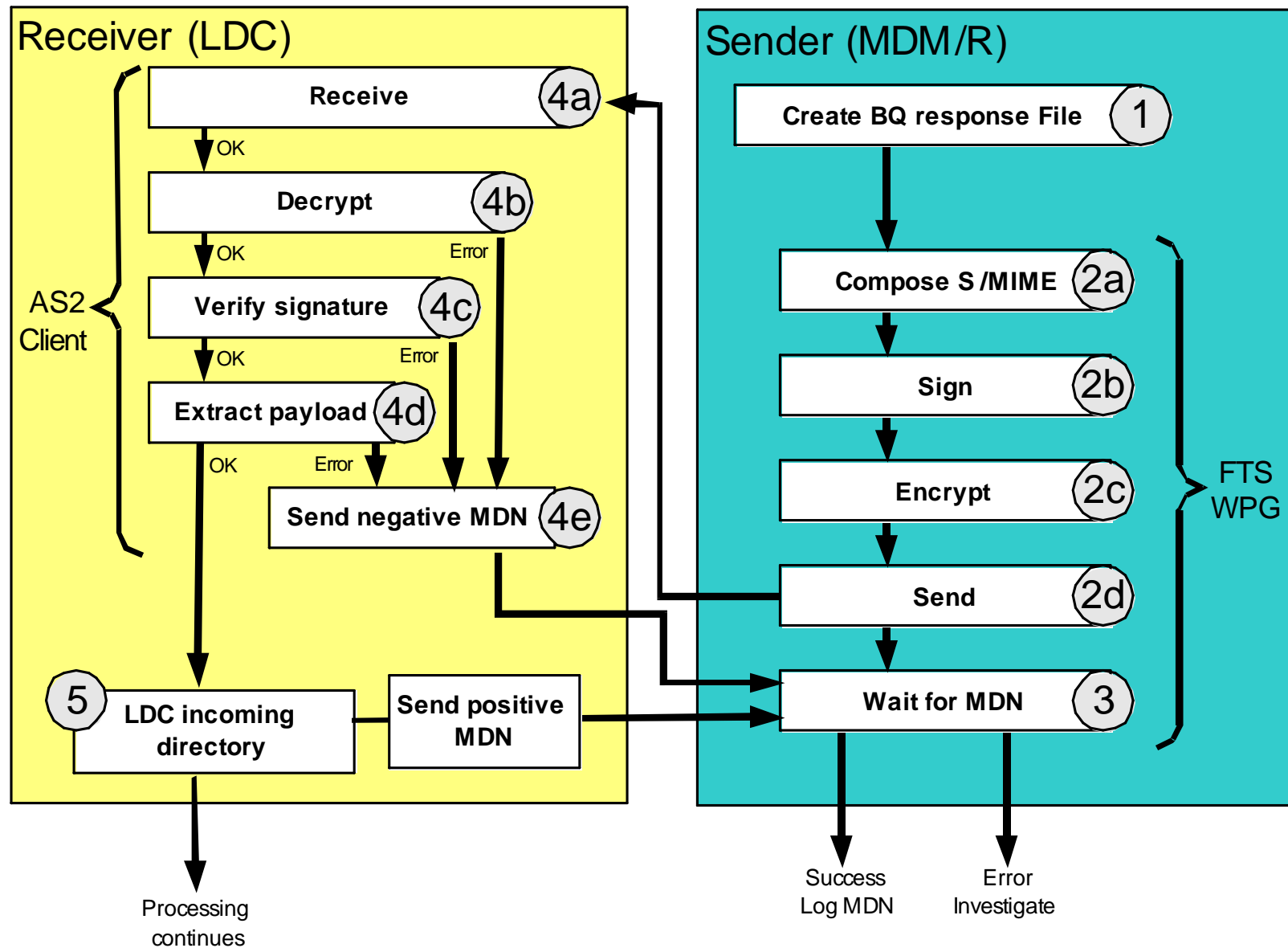
- Business to Business (“B2B”) integration model – Document (File) exchange
- “Closed Community” confined to Organizations registered by the SME.
- Registered LDC’s, AMI Operators and Billing agents can exchange files with the MDM/R (in future looking at adding Retails)
- All files move through MDM/R FTS
- Files digitally signed

MDM/R FTS Processing LDC to MDM/R



MDM/R FTS Processing

MDM/R to LDC



File Transfer Services Overview



- The *MDM/R Technical Interface Specifications* document defines the naming and content of each file
 - Each organization has its own set of directories on the MDM/R FTS side
 - MDM/R FTS relies on the file name and AS2 envelope to route files correctly
 - MDM/R FTS does not touch the application content of the files

Topics

- **File Transfer Services**
 - Brief overview of MDM/R FTS
 - **File naming**
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example

- **Web Services**
 - Information available
 - Technical requirements
 - Lessons Learned

- **Q&A**

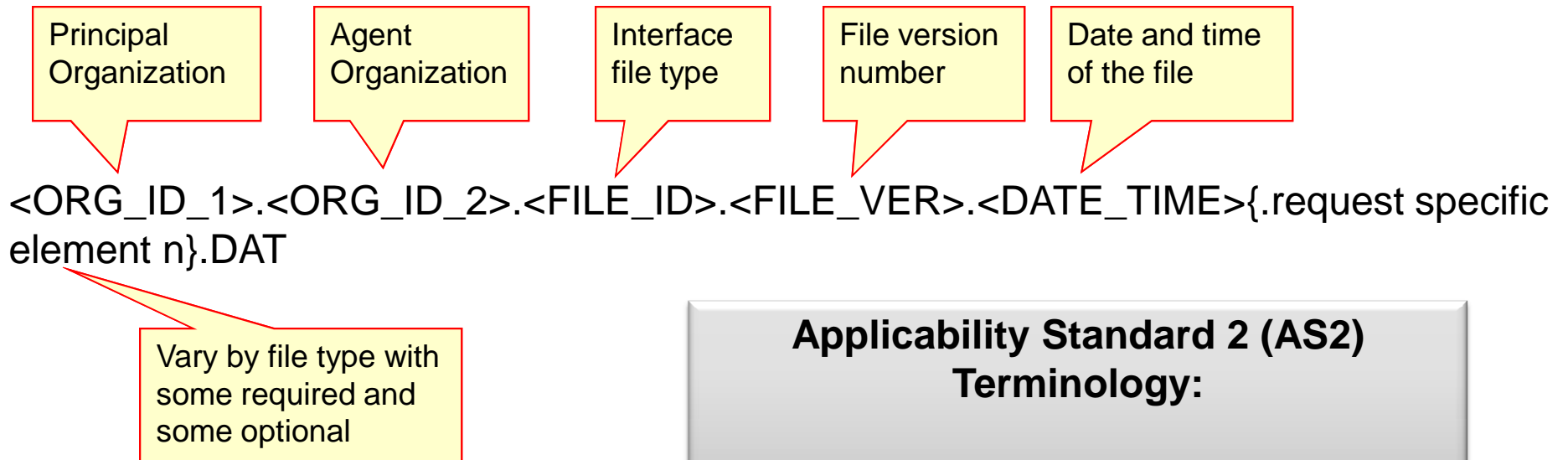
MDM/R FTS File Naming

- Each file type and file name is specified in the Technical Interface Specifications document
 - Name of the file is generated by the source system before it is sent
 - Name of the file also embedded in the first record of each file
- File name is made up of:
 - Mandatory elements – must be present in specified order
 - Optional elements – may be present and vary by file type
 - Mandatory suffix or extension – ‘.DAT’
- File name is case sensitive
- Elements are separated by a dot ‘.’
- File name elements may contain letters (A-Z, a-z) and numbers (0-9)

File Transfer Services

File Name Elements

- All interface files sent to and from the MDM/R follow a specific naming convention:



Applicability Standard 2 (AS2) Terminology:

Within the realm of File Transfer Services and the attendant AS2 Protocol, each registered MDM/R Organization is referred to as a “Community Participant”.

MDM/R FTS File Naming Mandatory Elements



- **ORG_ID_1 (Organization ID)**
 - 8 character string assigned to a Community Participant during registration with the MDM/R
 - Identifies the Community Participant to whom the file applies
 - ORG_ID_1 will be the LDC's MDM/R ORG ID

- **ORG_ID_2 (Agent Organization ID)**
 - 8 character string assigned to a Community Participant during registration with the MDM/R
 - Identifies the Community Participant sending/receiving the file
 - ORG_ID_2 will be the MDM/R ORG ID of the LDC or the LDC's designated Operator/Agent

Sample File Names

LDC submits and receives their own files



- Universal SDP ID Request/Response
 - ORG11111.**ORG11111**.1000.00.20070214221345.DAT
 - ORG11111.**ORG11111**.2000.00.20070214224545.DAT

- Synchronization
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.00.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.01.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.02.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.03.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.04.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.05.01.DAT
 - ORG11111.**ORG11111**.3000.01.20070214221345.cdcdcd.07.01.DAT

- Meter Reads
 - ORG11111.**ORG11111**.7100.00.20070214221345.DAT

- Billing Quantity Request/Response
 - ORG11111.**ORG11111**.5000.00.20070214221345.DAT
 - ORG11111.**ORG11111**.6000.00.20070214224545.DAT

Sample File Names

Agent submits and receives files for the LDC



- Universal SDP ID Request/Response
 - ORG11111.**ORG22222**.1000.00.20070214221345.DAT
 - ORG11111.**ORG22222**.2000.00.20070214224545.DAT

- Synchronization
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.00.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.01.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.02.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.03.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.04.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.05.01.DAT
 - ORG11111.**ORG22222**.3000.01.20070214221345.cdcdcd.07.01.DAT

- Meter Reads
 - ORG11111.**ORG33333**.7100.00.20070214221345.DAT

- Billing Quantity Request/Response
 - ORG11111.**ORG22222**.5000.00.20070214221345.DAT
 - ORG11111.**ORG22222**.6000.00.20070214224545.DAT

MDM/R FTS File Naming Mandatory Elements



- **FILE_ID (File Type Identifier)**
 - 4 digit value
 - Identifies the file contents
 - Valid values defined by *Technical Interface Specifications* document

- **FILE_VER (File Version Number)**
 - 2 digit value to define multiple versions of one file type
 - File version number defined in the *Technical Interface Specifications* document

- **DATE_TIME (Date and time)**
 - 14 character string of format 'YYYYMMDDHHMMSS'
 - HH is 24 hour clock format (Eastern Standard Time)
 - Has business meaning beyond file creation date and time
 - Multiple files in one set must have the same value for DATE_TIME

MDM/R FTS File Naming Request Specific Elements



- The following file types do not have any request specific elements
 - Universal SDP ID Assignment Request (FILE_ID 1000)
 - Universal SDP ID Assignment Response (FILE_ID 2000)
 - Billing Quantity Request (FILE_ID 5000)
 - Billing Quantity Response (TOU/ CPP & Periodic) (FILE_ID 6000)
 - Billing Quantity Response – (Hourly) (FILE_ID 6100)
 - Billing Quantity Response (Demand) (FILE_ID 6200)
 - Billing Cycle Schedule (FILE_ID 8000)
 - Aggregated Settlement Data (FILE_ID 9000)
 - Data Aggregation Contributors File (FILE_ID 9100)

MDM/R FTS File Naming Request Specific Elements



- Periodic Audit Synchronization (FILE_ID 3000) and Incremental Synchronization (FILE_ID 4000) both require 3 request specific elements
 - **TX_ID** is a 6 character transaction identifier
 - Defined by the sender
 - Uniquely identifies a single Periodic Audit or Incremental Synchronization
 - Ties together the files that make up a Periodic Audit or Incremental Synchronization

MDM/R FTS File Naming Request Specific Elements



- Periodic Audit and Incremental Synchronization (cont'd)
 - **FILE_NO** is a 2 digit value identifying each of the 7 files that make up a Periodic Audit or Incremental Synchronization file set:
 - 00 – Manifest
 - 01 – Asset
 - 02 – Premise
 - 03 – Service Agreement
 - 04 – Parameter
 - 05 – Relationship
 - 06 – (Not Used)
 - 07 – Component SDP Data Files (only required for virtual SDP functionality)

MDM/R FTS File Naming Request Specific Elements



- Periodic Audit and Incremental Synchronization (cont'd)
 - **SEGMENT_NO** is a 2 digit value, starting with '01' for each file in the file set. The SEGMENT_NO does not have to be sequential.

MDM/R FTS File Naming Request Specific Elements

- Sample Synchronization File names:

Premise File Type (unsegmented)

ORG11111.ORG11111.3000.01.20070214221345.cdcdcd.02.01.DAT

Service Agreement File Type (segmented)

ORG11111.ORG11111.3000.01.20070214221345.cdcdcd.03.01.DAT

ORG11111.ORG11111.3000.01.20070214221345.cdcdcd.03.02.DAT

cdcdcd	TX_ID, uniquely identifies synchronization file set
02 & 03	FILE_ID, identifies synchronization file type
01 & 02	SEGMENT_NO, allows to break up a synchronization file type

MDM/R FTS File Naming

Request Specific Elements



- Meter Read Interface – Sensus (FILE_ID 7000)
- Meter Read Interface – Elster (FILE_ID 7100)
- Meter Read Interface – Trilliant (FILE_ID 7200)
- Meter Read Interface – Tantalus (FILE_ID 7300)

SEGMENT_NO

- SEGMENT_NO is an optional 10 character alphanumeric value that represents a file segment number.
- The purpose of this element is to allow an LDC to segment a large Meter Read data transmission for the same DATE_TIME into multiple Meter Read data files.
- The segment numbers for multiple files for the same DATE_TIME may take any alphanumeric value without relationship to each other.

MDM/R FTS File Naming Request Specific Elements



- **Sample Meter Read File name, no request specific element**
ORG11111.ORG11111.7100.01.20070214221345.DAT
- **Sample Meter Read File name, request specific element**
ORG11111.ORG11111.7000.00.20080504221345.**UM129**.DAT
ORG11111.ORG11111.7000.00.20080504221345.**QP46294765**.DAT

UM129 & **QP46294765** – SEGMENT_NO, allows large meter read files with the same date/time to be segmented

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

AS2 File Name Preservation Issue

- Original file name is preserved through the use of headers in the S/MIME format
- AS2 specification is not explicit on the requirement to preserve the file name
- Testing revealed the following about the AS2 Client, “WebSphere Partner Gateway Express”:
 - It does preserve the original file name when sending a file
 - It does not preserve the original file name when receiving a file
 - For example:
 - Send: ORG11111.ORG11111.7100.00.20070214221345.DAT
 - Receive: 3825898928733.txt

AS2 File Name Preservation Issue

- Other AS2 client packages may not preserve the original file name when sending and/or receiving a file
- These problems make it impossible for the receiver to preserve/restore the original file name from the sender
 - MDM/R FTS relies on the file name to route the file for processing within the MDM/R
 - This may also be a problem for LDC and their agents' systems

AS2 File Name Preservation Issue



- The solution to this issue, is to store the file name in a File Name record in both inbound and outbound files
 - If necessary, MDM/R FTS can use the stored file name to properly direct processing of the inbound files
 - MDM/R Service Recipients whose AS2 client does not preserve the file name upon receipt must add logic in their system to extract the file name from the file name header within the file

AS2 File Name Preservation Issue

Header Record Example



This is an example of a typical file with the File Name Header Record containing the file name.

<FTSFN>ORG12345.ORG12345.DC04.00.20070823062620.DAT</FTSFN>

Missing Reads Detail Report

ORG12345

2007-08-23 06:25:17 GMT-05:00

Utility Id|SDP Id|Universal SDP Id|Meter Id|Channel Ref|Last Interval End Time|Service
Connected Flag

ORG12345|00013806|12345678|SR 12345|1-FVWZ|2007-08-22 00:00:00|Y
ORG12345|00014314|23456789|SR 24680|1-FVES|2007-08-22 00:00:00|Y
ORG12345|00013804|87654321|SR 35791|1-FUWE|2007-08-22 00:00:00|Y
ORG12345|00013801|98765432|SR 97531|1-FTS4|2007-08-22 00:00:00|Y
ORG12345|00013810|24680135|SR 13579|1-FVAF|2007-08-22 00:00:00|Y

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - **What is needed?**
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

AS2 Software Package



- Each file going to or from the MDM/R must go via the AS2 protocol
- Each organization needs to:
 - Choose and purchase an AS2 software package that is best suited to their needs, keeping in mind the possible issue of file name preservation
 - Learn the package
 - Install and configure
 - Register and enroll with the Smart Metering Entity
 - Operate and maintain their AS2 software

Choose and Purchase an AS2 Software Package



- Commercial AS2 implementations are available from many vendors
- AS2 package chosen must interoperate with the current MDM/R FTS implementation
- Drummond Group maintains an AS2 Interoperability Product Directory
 - Tests implementation against the AS2 specification
 - Directory can be found at <http://www.drummondgroup.com/html-v2/as2-companies.html>
 - Approved vendor products as of June 2, 2009 included on next slide
 - Anyone procuring an AS2 client to interface with the MDM/R should ensure it is an approved vendor product at the time of purchase

Drummond Group AS2 Interoperability Product Directory as of June 2, 2009



- Axway, Synchrony Gateway Interchange V5.6.1 / Synchrony Endpoint Activator V5.6.1
- Axway, Synchrony Gateway V6.11
- Boomi, Boomi AS2 Transport 3.3
- Cleo Communications Inc., VersaLex™ v4.0 tested in VLTrader™ v4.0
- EDS, EDS*ELIT AS2 Connector version 4.1
- EXTOL International, Inc., EXTOL Secure Engine V5R2 tested in EXTOL Secure V5.3.2
- GXS, Inc., AS2 Engine v4.6
- IBM, IBM WebSphere Partner Gateway v6.2
- Inovis, BizManager 3.2
- Microsoft, BizTalk Server 2009
- /n software, IP*Works! EDI/AS2 v8.1
- nuBridges, Inc., nuBridges Exchange Enterprise 2.5
- nuBridges, Inc., nuBridges Exchange i 3.2
- nuBridges, Inc., nuBridges Exchange C.S. 3.4
- SEEBURGER AG, SEEBURGER EDI INT AS2 Adapter version 6.3.2 tested with BIS 6.3.2
- Sterling Commerce, Sterling Standards Library v5.3 as tested in Gentran Integration Suite/Multi-Enterprise Financial Gateway v4.3
- Sterling Commerce, Connect:Enterprise UNIX v2.4
- Sterling Commerce, Sterling Information Broker v4.4
- TIBCO Software Inc. , TIBCO BusinessConnect™ v5.2 AS2 Transport v5.2.1 as tested in TIBCO BusinessConnect™ v5.2

Selection Considerations

- **Business point of view**
 - Implementation of interfaces to and from the MDM/R
 - How will the software package relate to existing business systems?
 - What test systems will be used?
- **IT infrastructure point of view**
 - How does the package fit with your existing IT standards
 - Security
 - Package pre-requisites such as operating system
 - Connectivity to MDM/R Sandbox, Enrolment, Disaster Recovery and Production systems
- **Operations point of view**
 - Day-to-day operations of the software package
 - Troubleshooting and vendor support
 - Interaction with the MDM/R

Installation and Initial Configuration

- Identify where in the network the AS2 server will sit
 - Possible options:
 - DMZ with direct connection
 - Secure zone with proxy connection
 - Rely on the software vendor's best practices recommendations
- Plan and execute software implementation
 - Change window for installation activities
 - Allow time for any required vendor support
- Initial Configuration consists of:
 - Configurations outlined in vendor documentation; and,
 - Additional configurations outlined in the *MDM/R FTS and Web Services Configuration Workbook*

Operate and Maintain

- Integrate AS2 package into operations routine
 - Provide for vendor support of chosen AS2 package
 - Establish escalation procedures
 - Monitoring and troubleshooting procedures
- Establish daily file movement schedules based on MDM/R timelines and organizational needs

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - **When is it needed?**
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

When is it needed?

- AS2 software package is required to perform any testing with the MDM/R
 - AS2 software package must be purchased and implemented prior to Connectivity testing
 - Connectivity testing must be completed prior to Unit and Enrolment testing in any of the MDM/R environments

Topics

- **File Transfer Services**
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - **How is it implemented?**
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example

- **Web Services**
 - Information available
 - Technical requirements
 - Lessons Learned

- **Q&A**

How is it Implemented?

- To establish a connection between your organization and the MDM/R
 - Register with the Smart Metering Entity (SME)
 - Review of *MDM/R File Transfer Services and Web Services Configuration Workbook* (SME_MAN_9001).
 - Complete the *MDM/R FTS and Web Services Configuration Form* (SME_FORM_0014)
 - Provides information such as:
 - AS2 identifiers, Self signed certificates, Contact information
 - Conduct AS2 Connectivity Test

Registration Form

Part 3 – AS2, Web Services and Firewall Configuration

We need these values to configure the firewall and file transfer service (FTS) of the MDM/R for connection to your AS2 and Web Services software.

	Inbound Ports	Sandbox	█
		QA	█
		Production	█
AS2 URLs	Sandbox	http://	█
		https://	█
	QA	http://	█
		https://	█
	Production	http://	█
		https://	█

Registration Form – Important Points

- AS2 URLs
 - These are the URLs that the MDM/R Service Recipient has configured for inbound traffic using http and https protocols

- Inbound Ports
 - These are the firewall ports that the MDM/R service recipient will configure to listen. It is recommended that the inbound ports be selected from 80,433, or 56000-60000

How is it Implemented?

Connectivity Test Prerequisites

- *Understand Public Key Infrastructure (PKI)*
You should have an understanding of private and public keys, how digital certificates work, what digital signatures are.
- *Manage and install key pairs*
You should review your AS2 documentation about how to generate keystore, keypair and public certificates.
- *Implement and configure firewall rules*
You should be able to configure your network to allow two way traffic between MDM/R and LDC systems.
- *Install and Manage AS2 client*
You should be familiar with how to install and configure your AS2 with the requirements outlined in the MDM/R FTS and Web Services Configuration Workbook.

How is it Implemented?

Technical Requirements – Digital Certificates



- To get authenticated and access MDM/R Web Services, LDCs must present their digital certificate to the IESO in a “.DER” format (Binary DER data format).
 - If an LDC needs to convert the certificate format to “.DER” from another format (for example, “.PEM” or “.CER”), free tools (e.g.: openssl) are available and should properly convert the file
- When LDC generates self-signed certificate, three files are generated:
 - Keystore file – stores the public/private key used for authentication
 - Keypair file – contains the public and corresponding private key information
 - Certificate file – this is the certificate itself
- Highly Recommended to use Self Signed Certificates

How is it Implemented?

Pre-Connectivity Testing Tips and Recommendations

- You are recommended to install the same keypair for **both** inbound and outbound security settings
- After loading a new keypair to the inbound or outbound, restart the service.
- Involve AS2 technical support staff on the connectivity test. You may find it helpful to invite your AS2 technical support staff on the connectivity conference call to help resolve any unexpected configuration issues.

How is it Implemented?

More Pre-Connectivity Testing Tips and Recommendations

- You are required to allow SSL encryption for sender/recipient authentication and digital signature for message authentication within your AS2 client. Do not enable content encryption.
- You are recommended to use the same certificate for both digital signature and SSL encryption.
- For the digital certificate you send to us, you are recommended to provide one digital certificate that will be installed on the MDM/R production, QA and sandbox environments.

How is it Implemented?

■ AS2 Connectivity Test

- The objective of the test is to ensure communication channels are established between the desired MDM/R and LDC environments using the LDC's selected AS2 software
- Test interface files are exchanged during the test
 - Inbound and outbound
 - Use of a “ping file” – blank file with file type '0000'
 - Ping file should contain the FTS file header record
- Allow sufficient time to set up and configure your AS2 client prior to Connectivity Testing

How is it Implemented?

Connecting to multiple environments



- LDCs and their agents will require an AS2 connection between the MDM/R testing and production environments
- May wish to connect from different testing environments to the MDM/R Testing Environments
- There are 3 MDM/R Environments
 - Sandbox – used for unit and regression testing
 - Enrollment – used for enrollment testing activities
 - Production

How is it Implemented?

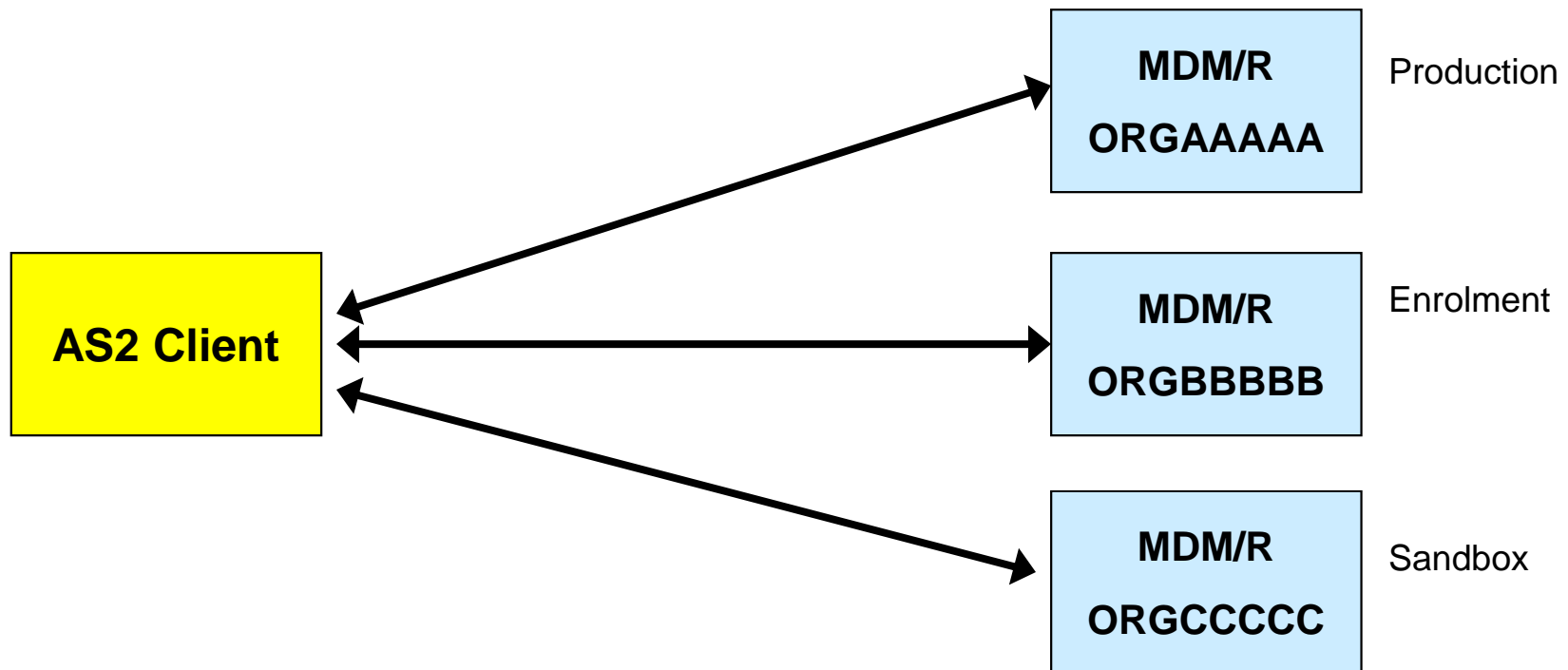
Connecting to multiple environments



- Will require a means to request Universal Service Delivery Point (USDP) ids from Production for testing purposes
 - USDP id request is just the assignment of a reference number, not the creation of the asset
 - USDP id's persist across all environments
 - When performing Unit and Enrollment testing – a request will be made for a block of USDPs to be used for testing – these USDPs will be made available in all MDM/R environments

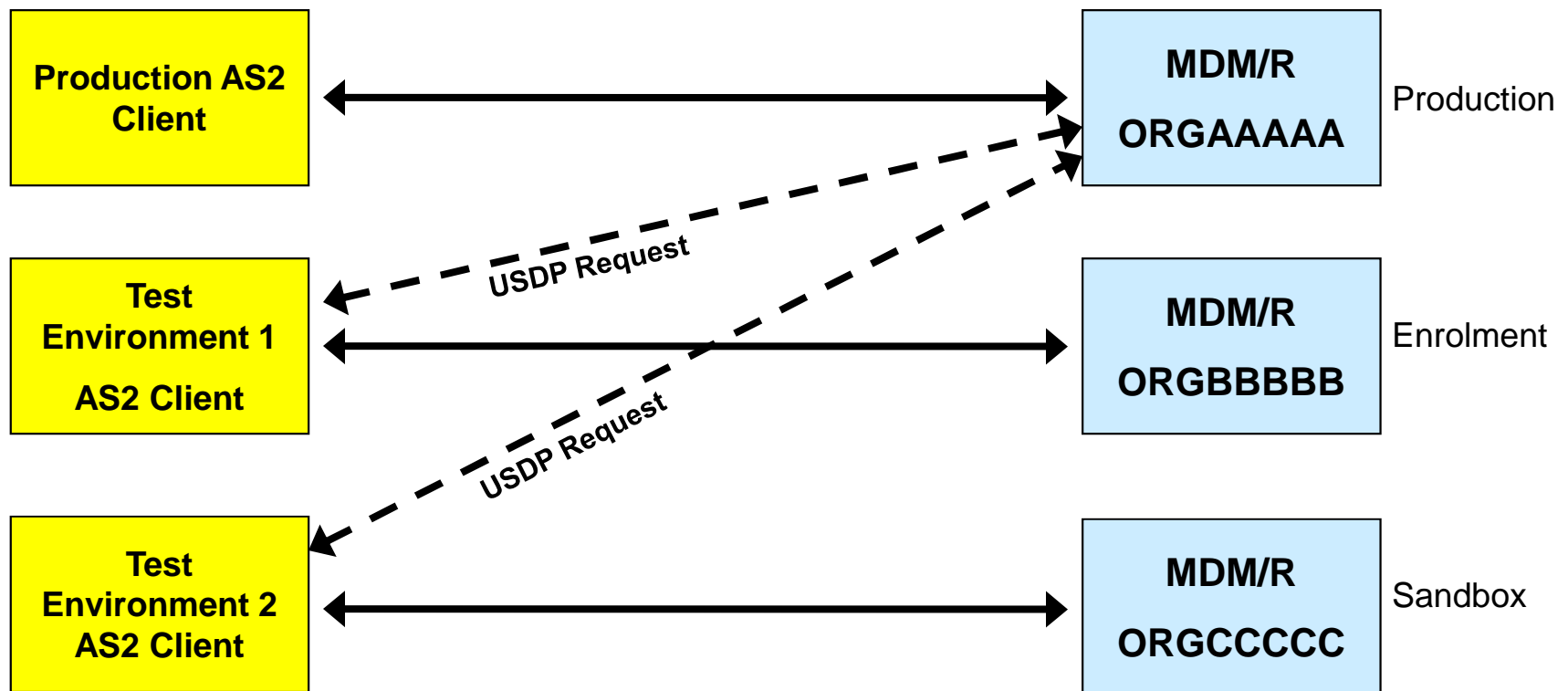
How is it Implemented?

Example of one AS2 client connecting to all MDM/R environments:



How is it Implemented?

Example of multiple LDC AS2 clients connecting to one or more MDM/R Environments:



Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - **Who is responsible for what?**
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

Who is responsible for what?

- MDM/R Operational Service Provider (IBM) is responsible for operation of MDM/R FTS
- Each organization is responsible for operation of its AS2 Client(s)
- Each organization is responsible for its own connectivity to the public internet
- AS2 protocol makes it clear to both parties where a given file is when problems arise
- The support organizations of the MDM/R Operational Service Provider and the LDCs will work together to troubleshoot and resolve problems

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - **Lessons Learned**
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

Lessons Learned



- Plan connectivity testing carefully
 - Connectivity testing should be conducted using all the final AS2 servers and configurations intended for ongoing operations
 - Any switches of servers after connectivity testing has been completed will require retesting of the new configurations and will need to be factored into your integration timeline.

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - **Secondary Agents Example**

- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned

- Q&A

Secondary Agents – Problem Statement



- How can an LDC have two organizations identified with “AMI Operator” type capabilities for a single SDP in addition to the LDC themselves?:
 - The defined AMI Agent organization will submit meter read files and receive data collection reports via FTS. (GUI access)
 - The secondary organization will re-submit meter read files and would receive data collection reports, VEE processing reports and billing reports via FTS. (GUI access)
 - The LDC may also submit meter read files and receive all reports via FTS. (GUI access)

What the MDM/R Supports



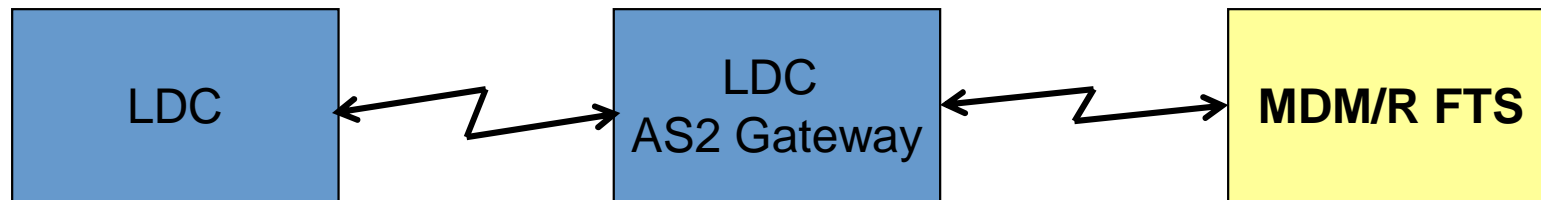
- LDC can only define one AMI Operator service provider for each Service Delivery Point (SDP).
- The AMI Operator and the LDC both have full capability for all AMI Operator functions.
 - Each of these organizations can access the MDM/R FTS by hosting its own unique AS2 gateway that it uses to receive data collection reports and submit meter read files.
- Additional authorized organizations can be registered as AMI Operators and can host their own AS2 gateway.
 - If they are not defined as the AMI Operator for any Service Delivery Points, they will be able to receive data collection reports but they will not be able to submit meter read files through their own AS2 gateway.

What the MDM/R Doesn't Support



- The MDM/R has no provision to name another organization as a secondary AMI Operator service provider for a Service Delivery Point (SDP) and share the services between the primary defined and secondary service provider.

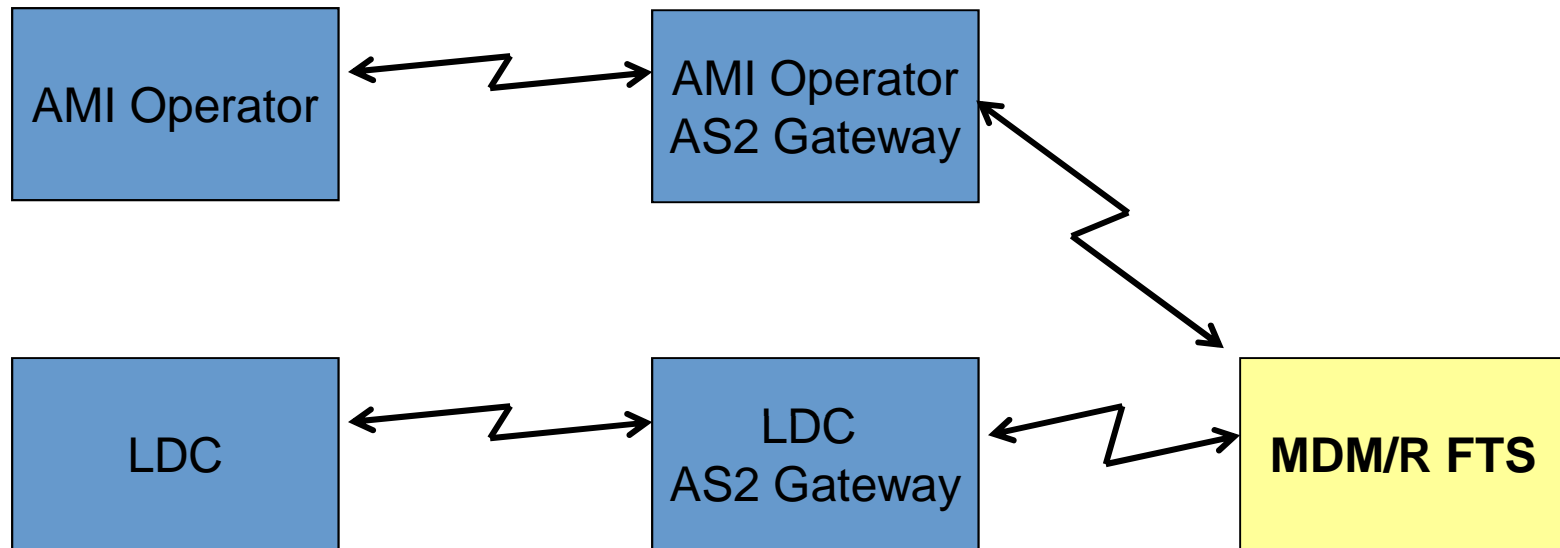
Example: LDC as its Own AMI Operator and Billing Agent



The LDC is registered as the AMI Operator.

All data is exchanged using the LDC's MDM/R ORG ID through the AS2 gateway hosted by the LDC.

Example: LDC with Separate AMI Operator

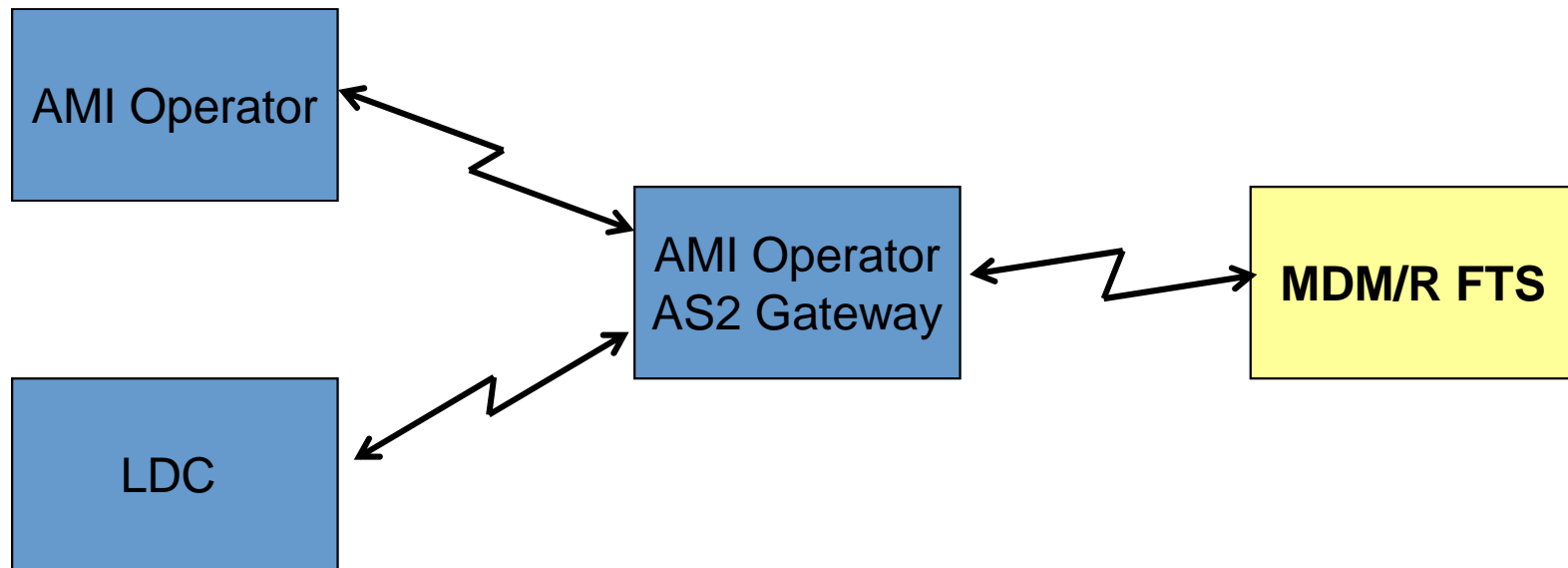


The LDC identifies a separate organization as their defined AMI Operator. The LDC uses their own AS2 gateway and MDM/R ORG ID. The defined AMI Operator uses their own gateway and their own MDM/R ORG ID.

Sharing an AS2 Gateway

- If either the LDC or their AMI Operator do not wish to host their own AS2 gateway, they could with appropriate arrangements, send files to the MDM/R FTS through a single AS2 gateway hosted by either one of them.
 - Files sent to the MDM/R through an AS2 gateway must use the MDM/R ORG ID of the organization that is hosting the gateway. (i.e. If the LDC is sending files through the AMI Operator's gateway, then the files must use the AMI Operator's ORG ID.)
 - The host of the host of the AS2 gateway may also wish to enforce restrictions by filtering the files from the secondary agent before they are sent to the gateway.

Example: LDC and Separate AMI Operator Sharing the same AS2 Gateway



When two organizations share one AS2 Gateway, the MDM/R ORG ID of the organization hosting the Gateway must be used. In this example:

- The LDC would have to use the AMI Operator's ORG ID.
- Network access would be provided by the AMI Operator.
- All files received at the gateway from the MDM/R could be sent to both the AMI Operator and the LDC.

How to Accommodate a Secondary AMI Operator

– Sending Files to the MDM/R



- Although the MDM/R cannot define a second AMI Operator for an SDP, a secondary agent could share an AS2 gateway hosted by either the LDC or the primary defined AMI Operator.
 - Files sent to the MDM/R through an AS2 gateway must use the MDM/R ORG ID of the organization that is hosting the gateway. (i.e. If either the primary defined or the secondary agent is sending files through the LDC's gateway, then the files must use the LDC's ORG ID.)
 - The host of the gateway can either pass all files through or they could enforce restrictions by filtering the files from the secondary agent before they are sent to the gateway.

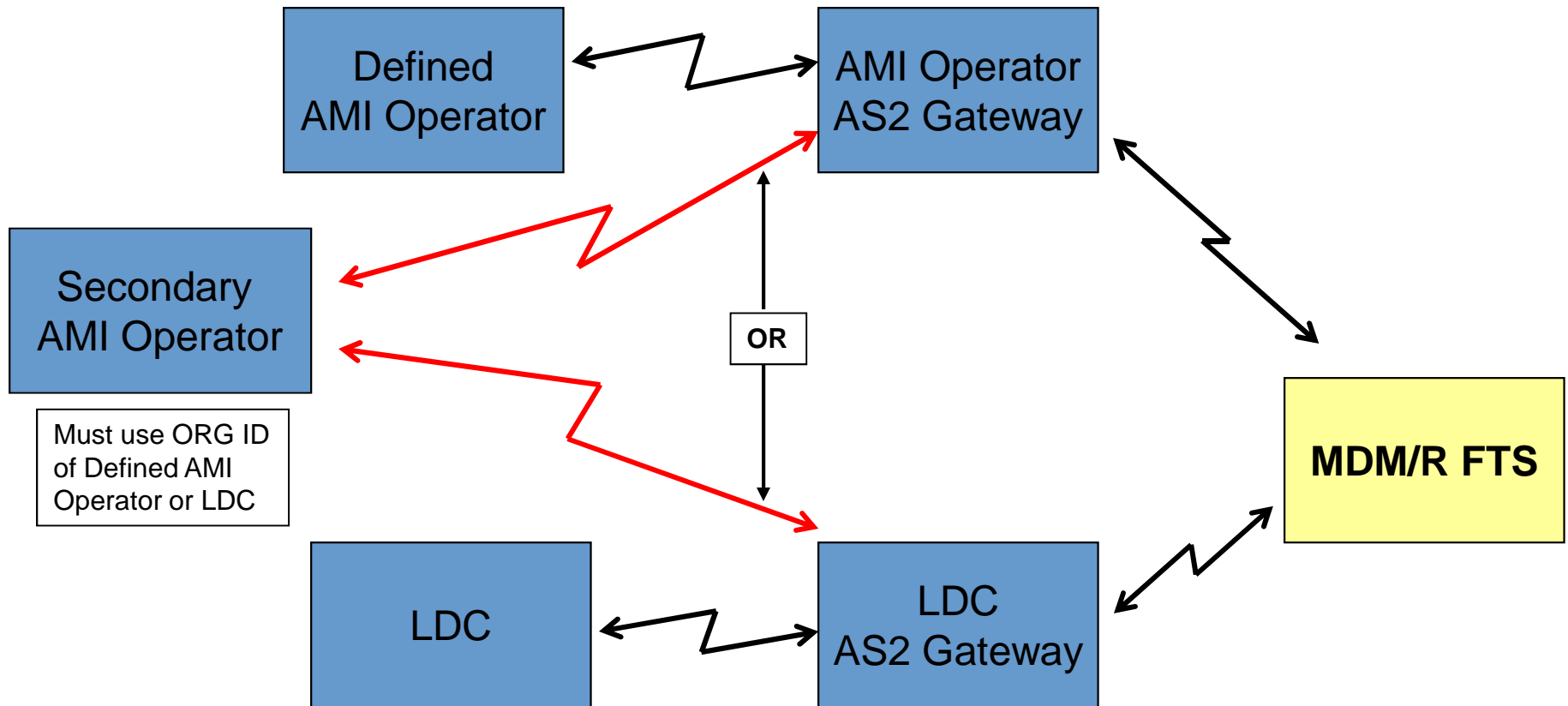
How to Accommodate a Secondary AMI Operator

– Receiving Files from the MDM/R



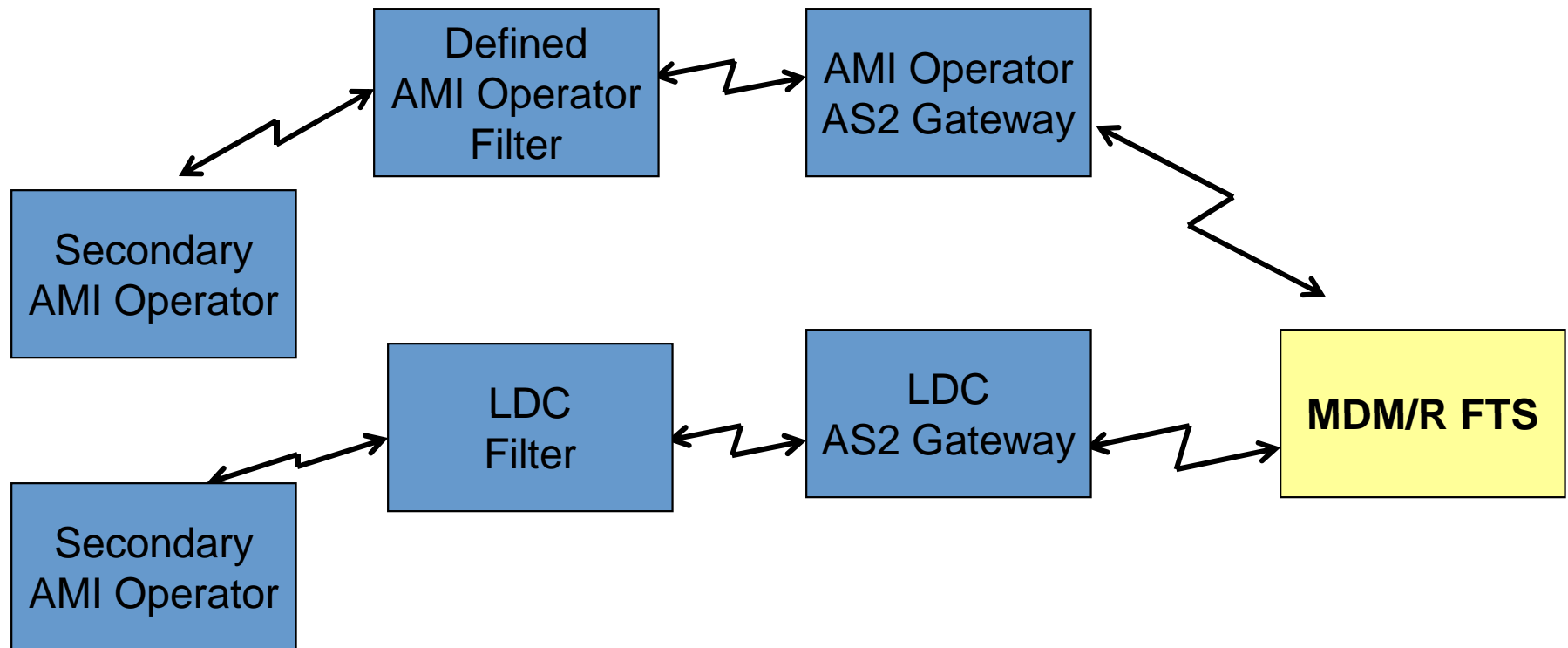
- The secondary AMI Operator could receive copies of all reports that are received at the AS2 gateway of the host organization. This would include all reports sent to the host's MDM/R ORG ID.
 - The host organization could restrict the reports received by the secondary organization by filtering the reports before they are forwarded on;
- or
- The secondary agent can receive its own authorized list of reports through its own AS2 gateway using its own MDM/R ORG ID.

Example: Secondary AMI Operator - Full Privileges



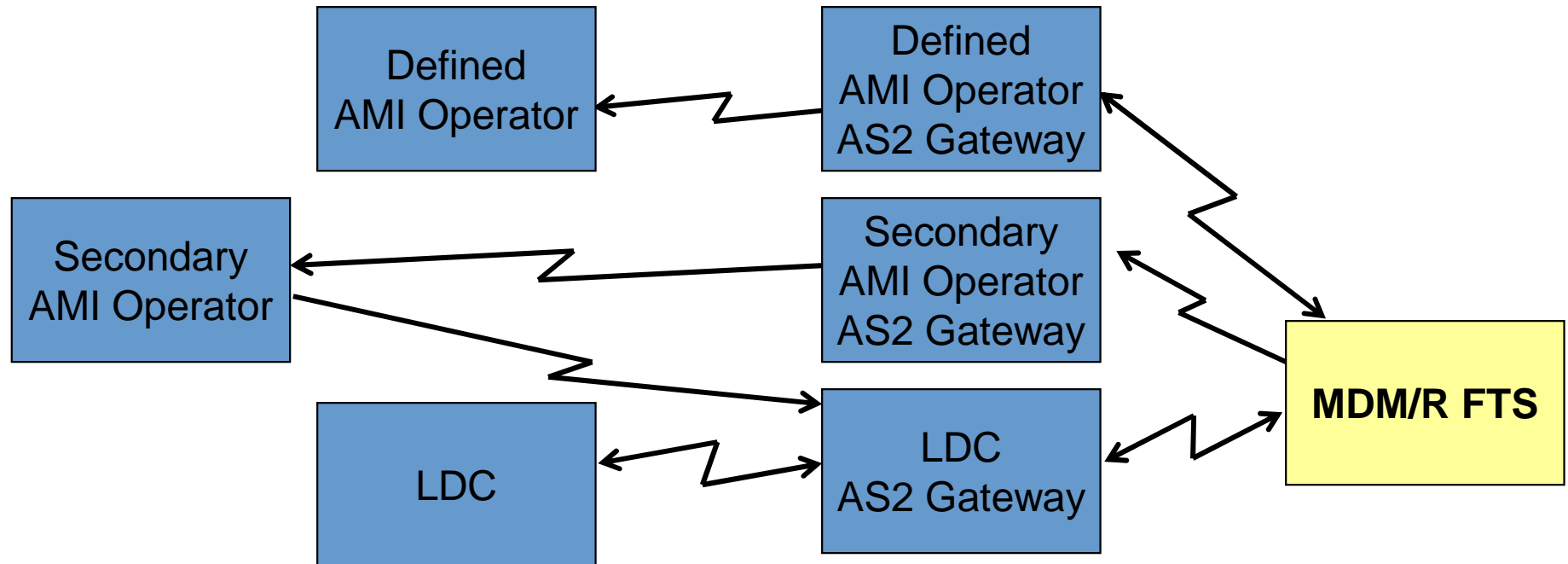
The LDC or Defined AMI Operator will pass all files that they receive from the Secondary AMI Operator through their AS2 gateway to the MDM/R FTS. All reports received at the gateway will be passed to the Secondary Operator.

Example: Restricted Privileges for Secondary Agents



The Defined AMI Operator and the LDC could add logic to their systems to impose restrictions on what files could be sent from or received by the Secondary Agents.

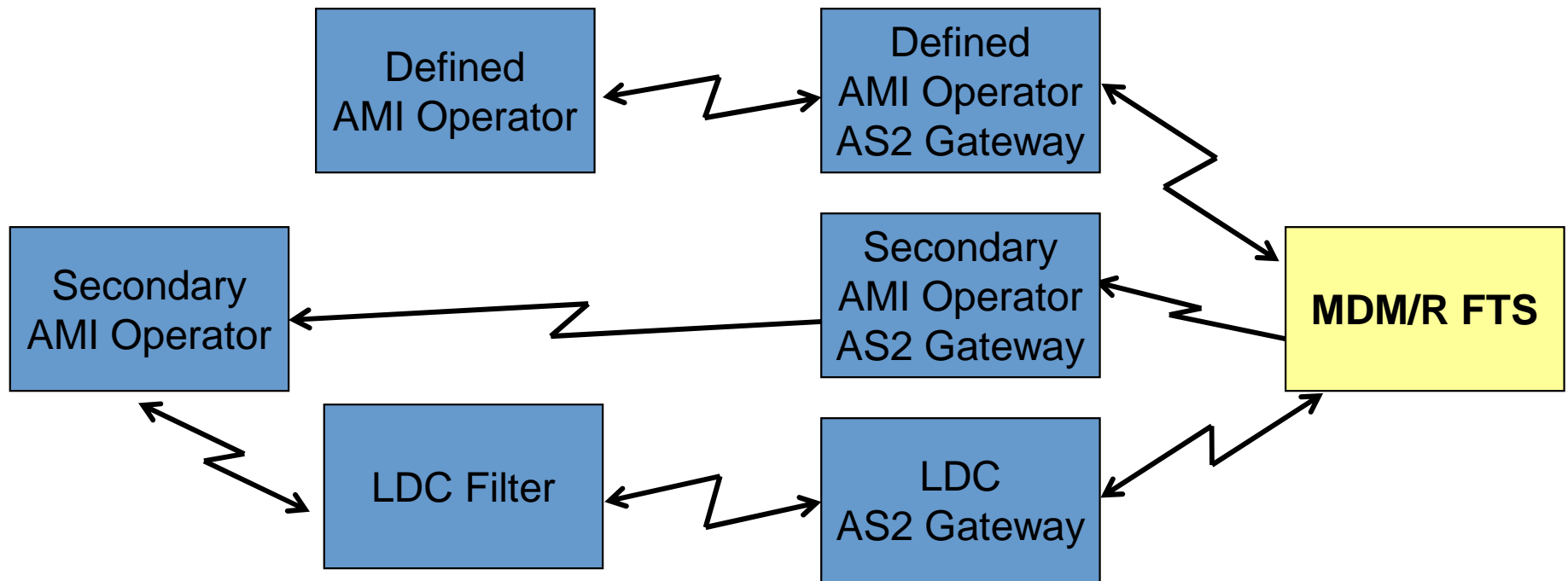
Example: Full Privileges for the Secondary Agent with Separate AS2 Gateway for Receiving Reports



The Secondary AMI Operator will submit meter read data directly through the LDC's AS2 Gateway using the MDM/R ORG ID of the LDC.

But they will receive their own approved set of reports through their own AS2 gateway using their own MDM/R ORG ID.

Example: Restricted Privileges for the Secondary Agent with Separate AS2 Gateway for Receiving Reports



The Secondary AMI Operator will submit meter read data to the LDC using the LDC's MDM/R ORG ID and the LDC will restrict which files get sent onto the MDM/R.

The Secondary AMI Operator will receive their own approved set of reports using their own MDM/R ORG ID through their own AS2 gateway.

How to accommodate a Secondary Billing Agent

- A secondary billing agent could be accommodated in a similar way to a secondary AMI Operator with one exception:
 - Only the defined Billing Agent (either the LDC or a separate Billing Agent) can submit Billing Quantity Requests and receive Billing Quantity Responses.

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example

- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned

- Q&A

Web Services Information Available



- Provides all interval consumption data and daily billing quantity data contained in the MDM/R:
 - To an authorized external application server provided by an LDC, AMI Operator, Billing Agent or other Customer Contracted Agent
 - For a specified timeframe of up to 90 days at a time (i.e.: to retrieve data for a period greater than 90 days will require multiple requests)
 - Date and Time of all data expressed in EST
 - For one Universal SDP ID at a time.

Web Services Information Available



- The MDM/R has the capability to provide 4 types of daily data:
 - Hourly Interval Consumption data
 - Time of Use Consumption data
 - Total Consumption data
 - Hourly Interval and Time of Use Consumption data

- Type of data available is dependant on how the SDP is framed
 - If SDP is framed as Time of Use, then all 4 types of data are available via Web Services
 - If SDP is not framed as Time of Use, then only Hourly Interval and Total Consumption data is available

Web Services Information Available

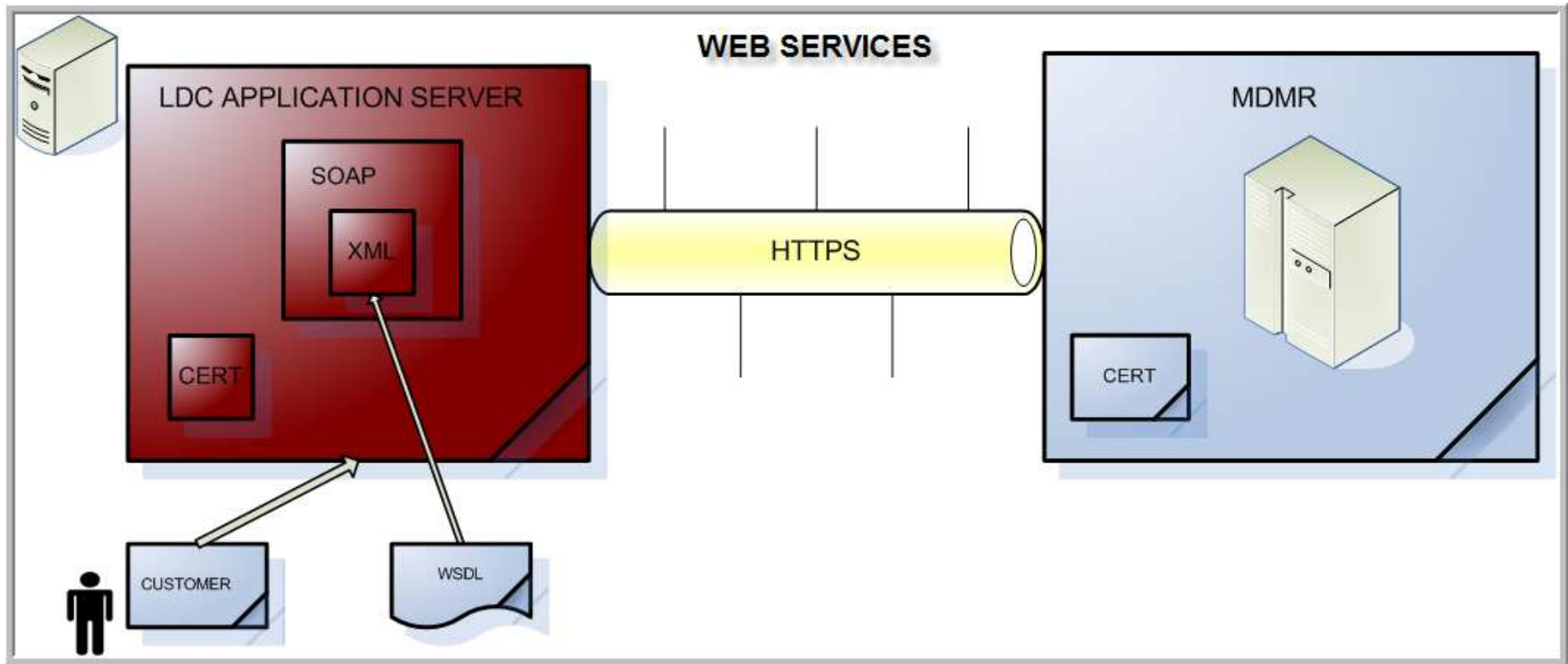


- Prior versions of data are available, if requested
- Data quality indicators are provided
 - Validation status and failure reason
 - Change method
 - For Interval Data only, other validation flags are available
 - Reverse Rotation
 - No Data
 - Power Off
 - Partial Data

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned
- Q&A

Web Services High Level Architecture Diagram



Web Services Technical Requirements



- Synchronous request / response interface to the MDM/R
- SOAP (Simple Object Access Protocol) over HTTPS
- Exchanges XML-based messages using the same infrastructure implemented for FTS including digital certificates
- NOT file based, AS2 software not required

Web Services Technical Requirements



- IESO will supply the Web Services Description Language (.WSDL) file
 - This will include the components necessary to facilitate the transport of the Web Services messages across the interface to and from the MDM/R
 - It includes, amongst other things, the format of the XML file
- The LDC and/or their agents need to load this file into their systems

Web Services

Technical Requirements – Digital Certificates



- Similar to FTS, MDM/R web services will utilize digital certificates
 - The same digital certificate for FTS can be used for web services (if you already have FTS connectivity)
 - Alternatively, you can create and exchange new certificates to be used solely by your web services application

- Self-signed certificates are recommended
 - However, a commercial certificate (e.g.: Verisign, Thawte) is also acceptable

Web Services

Technical Requirements – Connectivity Testing



- Connectivity test involves the validation of digital certificate only. No other communication or firewall configuration required
- The certificate can be tested by LDC by loading their keypair file to a web browser (Internet Explorer, Firefox) and trying to connect to the MDM/R Web Services URL

Web Services

Technical Requirements – Connectivity Testing



- From your server, load your keypair file (.p12) to the internet web browser
- After loading your keypair file, restart the web browser (close and open browser window).
- In the web browser's URL field, type in the inbound DNS name of the environment you wish to test
 - The inbound DNS names of the different MDM/R environments are provided in the MDM/R FTS and Web Services Configuration Template.

Web Services

Technical Requirements – Connectivity Testing

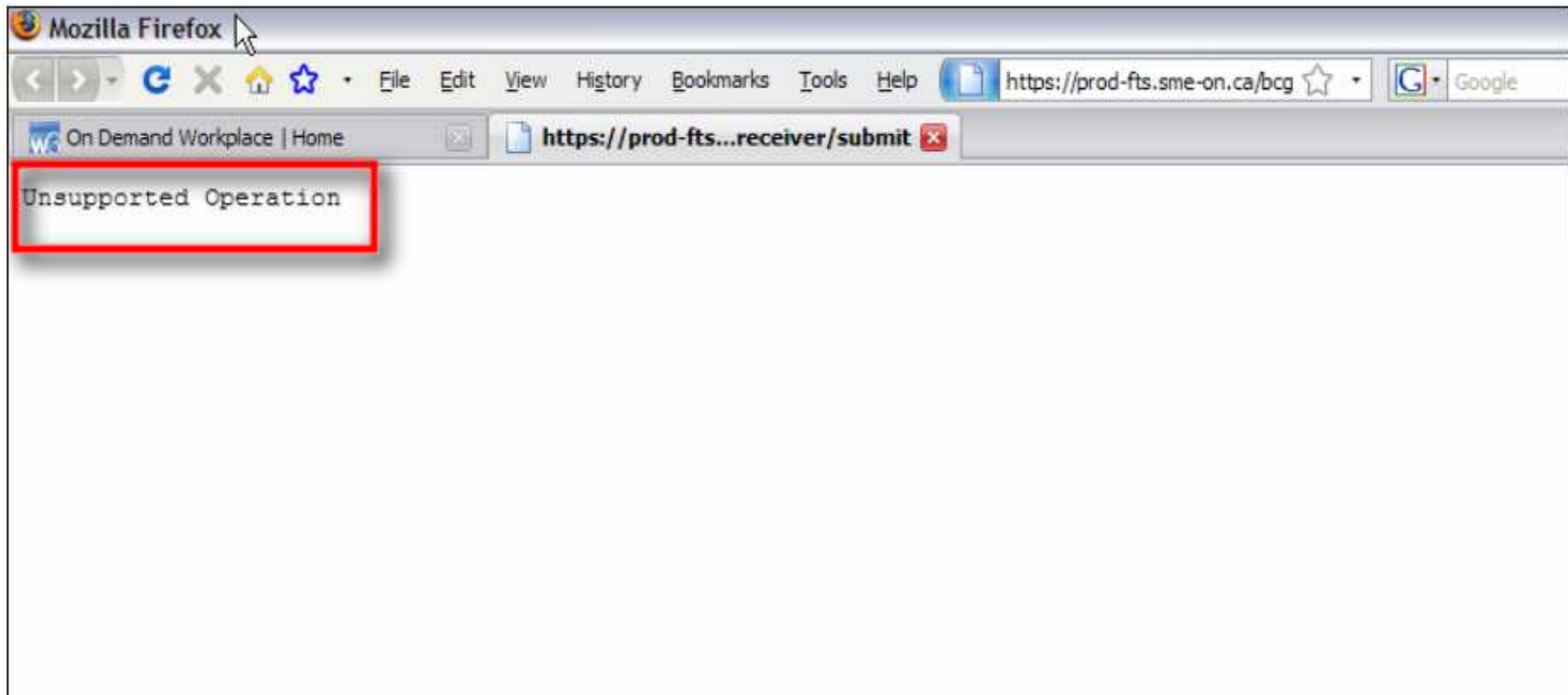


- For each request to each environment, you should expect to receive an “Unsupported Operation” response. This indicates that your firewall is opened for communication with the MDM/R and that the SSL connection is successful.

Web Services Technical Requirements – Connectivity Testing



- This message is good:



Web Services

Technical Requirements – Connectivity Testing



- In the event you receive a “Forbidden” response, please verify your firewall and SSL settings.



Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example
- Web Services
 - Information available
 - Technical requirements
 - **Lessons Learned**
- Q&A

Lessons Learned

Digital Certificates



- While commercial certificates are acceptable, you need to be sure that the provider allows the embedding of Organization IDs into the Public Certificate filename format and/or Subject: Common Name (CN) Field
 - Refer to the *MDM/R File Transfer Services and Web Services Configuration Workbook* for further details
- If using a commercial certificate there is a requirement to also provide the root certificate for the issuing organization

Lessons Learned

EST versus Prevailing Local Time



- LDCs using the MDM/R's Web Services to support their own web presentment of consumption data must make any necessary adjustments from EST to prevailing local time
- This adjustment is necessary if the desired presentation of the data to the customer is in prevailing local time

Topics

- File Transfer Services
 - Brief overview of MDM/R FTS
 - File naming
 - AS2 file name preservation issue
 - What is needed?
 - When is it needed?
 - How is it implemented?
 - Who is responsible for what?
 - Lessons Learned
 - Secondary Agents Example

- Web Services
 - Information available
 - Technical requirements
 - Lessons Learned

- Q&A

End of Slides

Thank you!

