Smart Meter Texas
M1 Application Programming Interface and FTPS

Prepared for

Texas Competitive Electric Market

October 28, 2014

Document History

Revision Number	Revision Date	Revision By	Summary of Changes	Changes marked
1.0	12/15/2009	IBM	Initial Verion	No
1.1	01/15/2010	IBM	Added Section 6	No
1.2	01/27/2010	IBM	Updated the folder structure for the FTP site	No
1.3	03/20/2012	IBM	Updated limitations for adhoc usage report requests	No
1.4	05/08/2012	IBM	Updated limitations for Adhoc usage report requests	No
2.0	10/27/3014	IBM	Updated for Release 4.3	No

Table of Contents

1 Introduction

This document provides the information of the Smart Meter Texas (SMT) application programming interfaces (APIs) that went into production in January, 2010 (Phase M1).

This API enables:

- Meter usage data (Interval reads, register reads and monthly billed usage data)
- Master data (non-usage data including meter attributes, premise info and REP of record)

In the first release, Transmission and Distribution Service Providers (TDSPs) and Retail Electric Providers (REPs) will be the primary users of this interface functionality. Today, Third-Party Service Providers (Third-Party) will be able to access the Meter Usage Data API once they setup a system account with SMT.

The interfaces described in this document are defined based on Service Oriented Architecture (SOA) principles. The interfaces have been specified in the Web Service Description Language (WSDL). Web Services between REPs, Third-Parties and SMT will be secured using mutual authentication implemented with Secure Socket Layer (SSL).

2 Related Information

2.1 Glossary of Terms

Term	Definition
API	Application Programming Interface that allows one program to talk to another
DUNS	Number assigned to a REP by Dunn and Bradstreet. REPS can establish multiple businesses within their parent company using multiple DUNS
ESB	Enterprise Server Bus
ETL	Extract Transform and Load
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL
ESIID	Electric Service Identifier, a unique identifier for the point of delivery
MQ	Message Queue
REP	Retail Electric Provider
ROR	REP of Record
SMT	Smart Meter Texas
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer is a set of cryptographic protocols that provide security and data integrity for communications over networks such as the Internet
TDSP	Transmission and Distribution Service Provider
XML	Extensible Markup Language
WPS	WebSphere Process Server
WSDL	Web Service Description Language - XML-based language for describing Web services

Table 1: Glossary of Terms.

3 AMI System Overview

The Integration System Context, Figure 1, represents the solution as a single object and identifies the logical interfaces between the SMT Web Portal and Data Repository and external entities during the M1 Phase. It shows the information and control flows that cross the system boundary. The Integration System Context is focused on Meter master data & usage data end-to-end functionality.

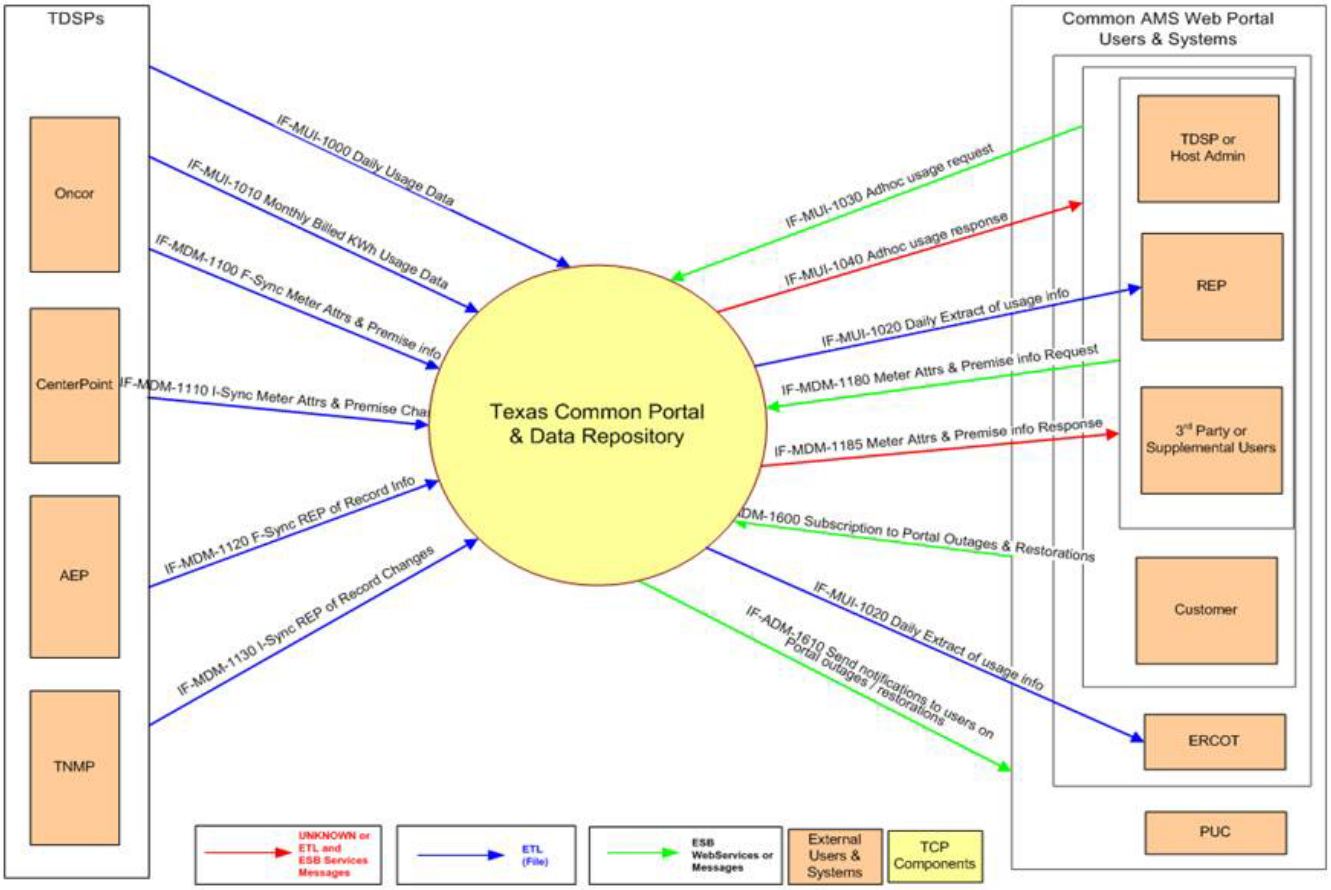

Figure 1: System Context Diagram.

3.1 Interface Overview

Based on the review of the AMIT requirements, approximately 13 different logical interfaces were in scope for the Common AMS Web Portal Release 1 to provide the M1 functionality addressing the following subject areas

- Meter usage data (Interval reads, register reads and monthly billed usage data)
- Master data (non-usage data including meter attributes, premise info and REP of record)

The following table lists the logical interfaces identified for Release 1 addressing M1 functionality and discusses high-level characteristics of each interface. It also indicates if data related to each interface must be migrated into the portal when the portal transitions to production. The exposition here is at high-level and the next section of this document covers each of these listed interfaces in detail.

Interface Number	Interface Description	Source	Destination	Interface Type (File, DB, Messaging, RPC, etc.)	Real time / Batch
IF-MUI-1000	Send meter usage data with 15 minutes interval and daily register read	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MUI-1010	Send meter monthly billed usage data	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MUI-1020	Send daily extract of usage info since the last extract for all usage data of the REP of Record's ESIIDs	Smart Meter Texas Portal	REPs	File	Batch
IF-MUI-1030	Send ad-hoc queries/request to get meter usage data with specific date range, usage data interval and one or multiple ESIIDs	Third-Parties REPs TDSPs Customers	Smart Meter Texas Portal	Web service	Real-time
IF-MUI-1040	Meter usage data response to ad-hoc queries for specific date range, usage data interval and one or multiple ESIIDs	Smart Meter Texas Portal	Third-Parties REPs TDSPs Customers	Web service / File	Real-time /Batch
IF-MDM-1100	Full Sync of Meter attributes (Non-Usage Data)	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MDM-1110	Incremental Sync of meter attributes (Non-Usage Data) changes	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MDM-1120	Full Sync of REP of Record	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MDM-1130	Incremental Sync of REP of Record changes to update data repository with the relationship (new, switch or move out)	TDSPs	Smart Meter Texas Portal	File	Batch
IF-MDM-1140	Full Sync of Premise Info	TDSPs	Smart Meter Texas Portal	Web service / File	Real-time / Batch
IF-MDM-1150	Incremental Sync of Premise Info	TDSPs	Smart Meter Texas Portal	Web service / File	Real-time / Batch

Table 2: Logical interfaces for Build 2 - M1 functionality.

3.2 Interface Security

TDSPs, REPs and Third-Parties who communicate with SMT web service interfaces must support mutual authentication over SSL. To support authentication, two kinds of security tokens will be used for authentication: Username or SAML tokens. Token data is used to map the sender of a request to a system account.

When a Username token is sent, the User Name element identifies the system account. If a SAML token is passed, the NameId element identifies the system account. The SMT security infrastructure will validate the request sender by verifying the WS-Security signature using the signer certificate from the SMT certificate store. If the digital signature is valid and the user can be authenticated, the web service request is passed to the Enterprise Service Bus (ESB). Otherwise, a SOAP fault is issued.

Instructions for the set up of accounts and security credentials will be made available through the REP and Third-Party specific SMT Account onboarding processes.

4 SMT Ad-hoc Meter Usage System Overview

Figure 2 presents the High level system view diagram for SMT Adhoc Meter Usage Interface.

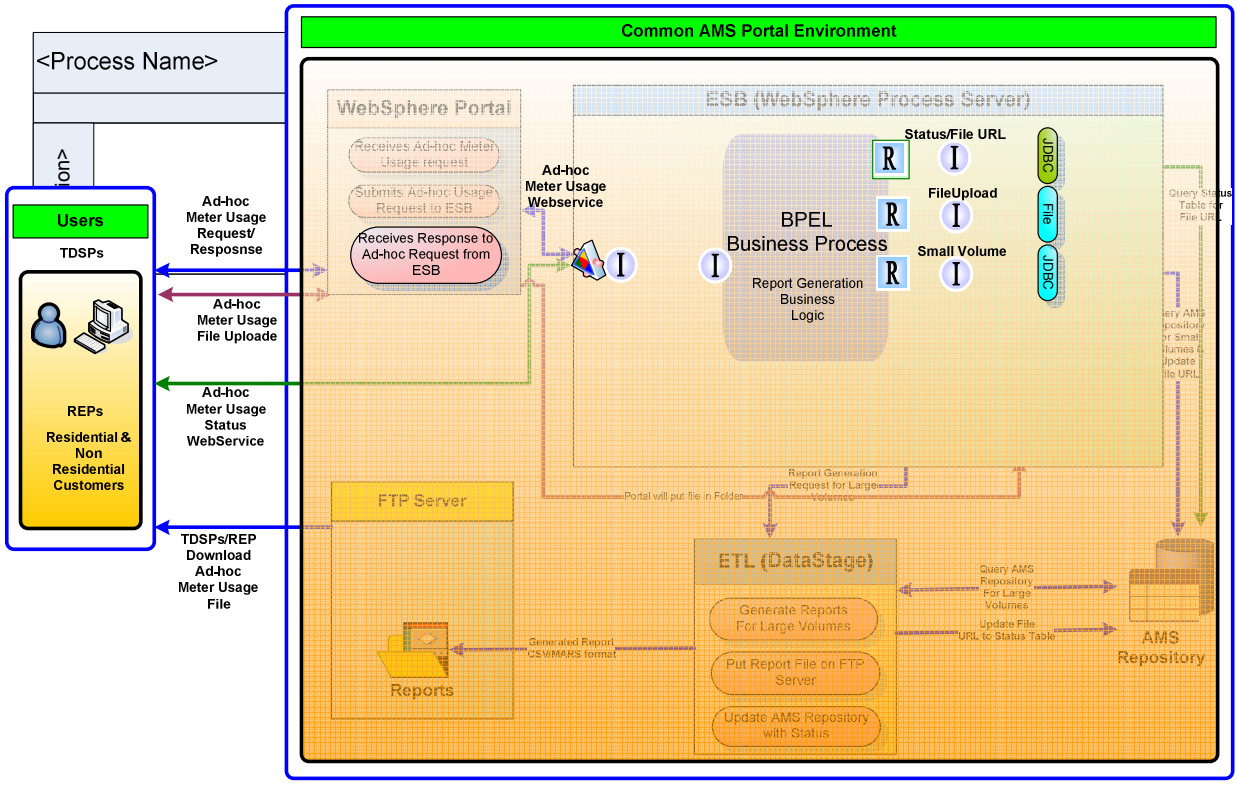

Figure 2: High Level System View

This interface facilitates SMT Portal & Data Repository users to request & receive interval & register reads via machine to machine interface.

4.1 Interface Overview

1) An authorized user initiates an ad hoc request in the web portal or invokes an ad hoc Meter Usage Web service directly to retrieve usage info (interval read, register read or monthly billed usage data) for a given UserID, ESIIDs, supplied date, reportFormat (CSV or MARS) and reportType (Daily Register read or 15 minutes interval read or Both) parameters to see the latest or all the updates that has occurred to the data.
2) For the users logged in to portal UI, portal will build the request based on the user inputs, XSD and WSDL provided. Portal will invoke ad hoc MeterUsage web service hosted on the ESB and pass request object in a SOAP envelope. For External users (TDSPs, REPs and Third-Parties) directly invoking the Web service, the SMT Datapower will do the security validations and then invoke ESB hosted Web service by passing the request object in a SOAP envelope.

3) ESB will map the incoming request object received from portal or external users to ASBO (Application Specific Business Object). Mapping is based on XSLT transformation. ASBO will contain all fields of request and common fields required for all AMS service that are going to take part in BPEL.

4) The BPEL deployed on the ESB contains the business logic to invoke appropriate service based on predefined criteria

5) For small volumes,
   a) One input ESIID and up to 40 days of usage data: ESB fetches data from the SMT data repository and writes the output to a CSV file in shared folder. ESB then responds to the synchronous Web service request and returns the file url in SOAP response message to the portal or external user.

6) For Medium volumes,

   a) One input ESIID and usage data greater than 40 days but less than 13 months and ReportType selected as CSV or MARS: ESB sets the priority based on input parameters and submits a message to a MQ queue to initiate an asynchronous request for the ETL components to fetch the data. The MQ message will have input parameters, message priority, correlationId generated by BPEL process and desired output file name.

7) For large volumes

   a) More than one ESIID and ReportType selected as CSV or MARS: ESB sets the priority based on input parameters and submits a message to a MQ queue to initiate an asynchronous request for the ETL components to fetch the data. The MQ message will have input parameters, message priority; correlationId generated by BPEL process and desired output file name.

   b) User uploaded ESIID/MeterId File and ReportType selected as CSV or MARS: Portal will call the ESB web service with the fileUrl ESB will read the file from the shared folder, parse the file content and validate the ESIID or MeterId in the file. ESB then sets the priority based on input parameters and submits a message to a MQ queue to initiate an asynchronous request for the ETL components to fetch the data. The MQ message will have input parameters, message priority; correlationId generated by BPEL process and desired output file name.

   Note: The File upload functionality is not supported for External users calling ESB Web service directly.

   Table 3 shows the ad hoc Meter Usage Message Volumes classification.

Message Volumes	Criteria	Invocation	Estimated Response Time
Small	1 ESIID and Usage data less than equal to 40 Days	Real-time Synchronous	Less than 3-5 minutes for 95% of the requests
Medium	1 ESIID and Usage date greater than 40 but less than equal to 13 Months	Batch & Asynchronous	2-3 hours for 95% of the requests
Large	More than 1 ESIID and Usage Data up to 4 years	Batch & Asynchronous	24 hours for 95% of the requests

Table 3: Ad-hoc Meter Usage Message Volumes

8) Limitations on the number of ESIIDs per adhoc usage request

Number of ESIIDs	Number of days	Number of requests per day	Max Estimated Response Time All
1	365	20	24 hours
10	20	20	24 hours
50	4	20	24 hours

Number of ESIIDs	Number of days	Number of requests per day	Max Estimated Response Time All
100	2	10	24 hours
200	1	10	24 hours

Table 4: Ad-hoc Meter Usage Message Limitations

§ *How to Read the Table*

– A REP would be able to raise one of the set of requests per day –

– 20 requests containing maximum 1 ESIIDs for the 365 days of data OR

– 20 requests containing maximum 10 ESIIDs for the 20 days of data OR

– 20 requests containing maximum 50 ESIIDs for the 5 days of data OR

– 10 requests containing maximum 100 ESIIDs for 2 days of data OR

– 10 requests containing maximum 200 ESIIDs for 1 day's data.

§ *Notes:*

– The intended use of ad-hoc API is for specific requests with a set of ESIIDs and for a defined period of time. The LSE usage files are sent daily to the REPs and the ad-hoc API is not advised to be used as a bulk backfill mechanism.

– The maximum number of ESIIDs per request = 200. This is a hard parameter

– Exceeding the parameters in the table (see table 3) may result in request being removed from queue. Notification will not be provided if this occurs.

– If a REP needs to make a large request for historical data that exceeds the above guidelines, it needs to submit a change request with AMIT at http://www.puc.state.tx.us/industry/projects/electric/34610/34610.aspx. The Operations Work Group can determine if and how to address the request.

9) For Medium and Large volumes scenarios # 6 (a), 7 (a) and 7 (b), ESB returns the SOAP response to the portal with the correlationId, statusCode and statusMessage. ETL processes the data and updates the Status table with userID, userType, correlationId, fileUrl, creationDate

10) ESB will host the Status web service to the give status response back to portal or External User.

a) An authorized user initiates an ad-hoc status request in the web portal to retrieve status of MeterUsage request by calling ESB webservice(Status)

b) The user request for status with UserID and correlationId(s).

c) ESB will validate the UserID, correlationID association before fetching the status.

d) If the validation is successful, ESB will fetch the data from the database for a given UserID & correlationId(s)

e) ESB will give response back to portal or external user with correlationId(s) and corresponding file name(s).

11) Compressed and encrypted output usage data file(s) and error report files (if any) are made available in the user specific directories for the requester to pull.

a) Output data file(s) remains for 10 calendar days on FTPS site and will be deleted thereafter.

Table 5 shows the set of ad hoc Meter usage interface requests, acknowledgements and responses.

Interface Message Description	Response	Invocation Type
Ad hoc Meter Usage Small Volume Request	Ad hoc Meter Usage Response	Synchronous
Ad hoc Meter Usage Medium Volume Request	Ad hoc Meter Usage Request Acknowledgement	Asynchronous
Ad hoc Meter Usage Large Volume Request	Ad hoc Meter Usage Request Acknowledgement	Asynchronous
Ad hoc Meter Usage Large Volume Request With file upload	Ad hoc Meter Usage Request Acknowledgement	Asynchronous
Ad hoc Meter Usage Status	Ad hoc Meter Usage Status Response	Synchronous

Table 5: Ad-hoc Meter Usage Request invocation pattern

5 SMT Ad-hoc Meter Usage Interface Definition

5.1 Schema Definitions

All Ad hoc Meter Usage requests use the following schema definition:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:met="http://schemas.esb.ams.com/meterusagesource">
```

5.2 Security Header Information

5.2.1 Sample Header Message

SMT messages use a common Security header. An example request header appears below.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:met="http://schemas.esb.ams.com/meterusagesource">
<soapenv:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
<wsse:UsernameToken>
<wsse:Username>Ambit</wsse:Username>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
```

5.2.2 Request Rule

Following are the steps performed by DataPower for security validations:

- Mutual Authentication between REP and SMT Datapower using 2-Way SSL.
- Validate the request Schema and populate SOAP Fault with appropriate Faultcode and Fault String.
- Get the entity name from the SSL Certificate.
- Validate the Signature by getting the entity's certificate from SMT Certificate Store.
- Get the UserName from UserName token of SOAP WS-Security header, User Type (TDSP, REP) from SOAP body and validate the user against LDAP against entity's System Account.
- Strip Security header.
- Send message to SMT ESB.

5.2.3 Response Rule

No Policy.

5.2.4 Error Rule

Create SOAP Fault based on Datapower error codes and custom error codes.

5.3 Schema and Sample Messages

5.3.1 SOAP Request Schema

Table 6 shows the Request Schema elements.

Element	Mandatory	Type	Description
UserId	Y	string(100)	UserId of the requester
UserType	Y	string(10)	UserType of the requester (e.g REP,TDSP,RES,NON, THRD and REG)
reportTypeArray	Y	Array	Report Type (Daily and/or Interval)
reportFormat	N	string(4)	Report Format (CSV or MARS)
ESIIDArray	Y	Array	Array of ESIID

Table 6: Ad-hoc Meter Usage Request Schema elements

SOAP request schema example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:met="http://schemas.esb.ams.com/meterusagesource">
  <soapenv:Header/>
  <soapenv:Body>
    <met:processMeterUsage>
      <MeterUsageReqList>
        <userId>JONBREZON</userId>
        <userType>THRD</userType>
        <reportTypeArray>
          <!--Zero or more repetitions:-->
          <reportTypeArray>
            <reportType>INTERVAL</reportType>
            <startDate>07/01/2009</startDate>
            <endDate>08/09/2009</endDate>
          </reportTypeArray>
          <reportTypeArray>
            <reportType>DAILY</reportType>
            <startDate>07/01/2009</startDate>
```

```
            <endDate>08/09/2009</endDate>
          </reportTypeArray>
        </reportTypeArray>
        <!--Optional :-->
        <reportFormat>CSV</reportFormat>
        <ESIIDArray>
          <!--1 or more repetitions:-->
          <ESIID>10089010229000600000000</ESIID>
        </ESIIDArray>
      </MeterUsageReqList>
    </met:processMeterUsage>
  </soapenv:Body>
</soapenv:Envelope>
```

5.3.2 SOAP Request Schema with File Upload

Table 7 shows the Request Schema elements with File Upload.

Element	Mandatory	Type	Description
UserId	Y	string	UserId of the requester
UserType	Y	string	UserType of the requester (e.g. REP,TDSP,RES,NON, THRD and REG)
reportTypeArray	Y	Array	Report Type (Daily and/or Interval)
reportFormat	N	string	Report Format (CSV or MARS)
FileUrl	Y	String	Url of user uploaded file

Table 7: Ad-hoc Meter Usage with uploaded file Request Schema elements

SOAP request schema example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:met="http://schemas.esb.ams.com/meterusagesource">
  <soapenv:Header/>
  <soapenv:Body>
    <met:processMeterUsageFile>
      <MeterUsageFileReq>
        <userId>JONBREZON</userId>
        <userType>THRD</userType>
        <reportTypeArray>
          <!--Zero or more repetitions:-->
          <reportTypeArray>
            <reportType>INTERVAL</reportType>
            <startDate>06/29/2009</startDate>
            <endDate>06/29/2009</endDate>
```

```
          </reportTypeArray>
        </reportTypeArray>
        <!--Optional:-->
        <reportFormat>CSV</reportFormat>
     <fileUrl> /data/AdhocMeterUsage/ESB/INPUT/DailyMeterUsage6e05214d0b4d5e700c96fd0f.CSV </fileUrl>
      </MeterUsageFileReq>
    </met:processMeterUsageFile>
  </soapenv:Body>
</soapenv:Envelope>
```

5.3.3 SOAP Response Schema

Table 8 shows the Response Schema elements.

Element	Mandatory	Type	Description
CorrelationId	Y	string(100)	UserId of the requester
statusCode	N	string(10)	UserType of the requester
statusMessage	N	Array	Report Type (Daily and/or Interval)

Table 8: Ad-hoc Meter Usage Response Schema elements

SOAP response schema example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <soapenv:Header/>
  <soapenv:Body>
    <me:processMeterUsageResponse xmlns:me="http://schemas.esb.ams.com/meterusagesource">
      <MeterUsageResponse xsi:nil="true"/>
      <MeterUsageSOAPResponse>
        <correlationId>f84da12ccbafc7dd16603909</correlationId>
        <statusCode>0</statusCode>
        <statusMessage>Data record completed successfully</statusMessage>
      </MeterUsageSOAPResponse>
    </me:processMeterUsageResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

5.3.4 Report File Naming Convention

IntervalMeterUsage<CorrelationID>.lse/.csv<OptionalDUNSNumber>

DailyMeterUsage<CorrelationID>.csv<OptionalDUNSNumber>

Table 9 shows the Ad hoc Meter Usage File Naming Convention.

Element	Explanation	Format
ReportName	IntervalMeterUsage/ DailyMeterUsage	Alpha(20)
CorrelationID	CorrelationID for specified request	Alphanumeric (32)
.lse / .csv DUNSNumber	Extension depending on file format CSV or MARS (lse) Optional DUNS Number	Alpha (3) Numeric(13)

Table 9: Ad-hoc Meter Usage Report File Naming Convention

5.3.5 Report File Format

Interval Meter Usage Report:

Suggested format:

Comma delimited file, with first line being field names.

Fields:

ESI ID (Varchar 64)

Time Stamp Start (date time stamp)

Time Stamp End (date time stamp)

Metered KWH (decimal)

File name format:

File Name will be generated by ESB with following pattern.

IntervalMeterUsage<CorrelationID>.lse/.csv.<OptionalDUNSNumber>

Ex: IntervalMeterUsage f84da12ccbafc7dd16603909.csv. 957877905

Ex:

File Format:

ESI ID, Time Stamp Start, Time Start End, Metered KWH, Status

Ex:

12345678909876543, 2009-05-22T12:00:00, 2009-05-22T12:15:00, 1.5

Daily Meter Usage Report:

Suggested format:

Comma delimited file, with first line being field names.

Fields:

ESI ID (Varchar 64)

Time Stamp (date time stamp)

Metered KWH (decimal)

File name format:

File Name will be generated by ESB with following pattern.

DailyMeterUsage<CorrelationID>.csv.<OptionalDUNSNumber>

Ex: DailyMeterUsage f84da12ccbafc7dd16603909.csv. 957877905

File Format:

ESI ID, Time Stamp Start, Time Start End, Metered KWH, Status

Ex:

12345678909876543, 2009-05-22, 2000,

5.3.6 SOAP Status Request

Table 10 shows the Status Request Schema elements.

Element	Explanation	Format
UserId	UserId of the requester	String
CorrelationID	CorrelationID for specified request	String

Table 10: Ad-hoc Meter Usage Status Request Schema elements

SOAP request schema example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:met="http://schemas.esb.ams.com/meterusagesource">
<soap:Header/>
 <soap:Body>
 <met:meterUsageStatus>
 <statusRequest>
  <userId> JONBREZON </userId>
  <correlationId> f84da12ccbafc7dd16603909</correlationId>
  </statusRequest>
  </met:meterUsageStatus>
  </soap:Body>
  </soap:Envelope>
```

5.3.7 SOAP Status Response

Table 11 shows the Status response Schema elements.

Element	Explanation	Format
correlationId	ESB generated correlationId	String
fileUrl	File url of the generated report	String
status	Report generation status	String

Table 11: Ad-hoc Meter Usage Status Response Schema elements

SOAP request schema example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:met="http://schemas.esb.ams.com/meterusagesource">
 <soap:Header/>
 <soap:Body>
 <met:meterUsageStatus>
 <BO_MeterUsageStatusResList>
 <UsageStatusResponse>
 <correlationId> f84da12ccbafc7dd16603909</correlationId>
 <fileUrl />
 <status>sucess</status>
 </UsageStatusResponse>
 </BO_MeterUsageStatusResList>
 </met:meterUsageStatus>
 </soap:Body>
 </soap:Envelope>
```

5.3.8 Sample SOAP Fault Message

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <soapenv:Header/>
  <soapenv:Body>
    <soapenv:Fault xmlns:m="http://AMSLib">
      <faultcode>m:SOAPFault</faultcode>
      <faultstring>1010</faultstring>
      <detail encodingStyle="">
        <me:SOAPFault_element xmlns:me="http://schemas.esb.ams.com/meterusagesource">
          <faultcode>1010</faultcode>
          <faultstring>Data cannot be loaded because a mandatory data element is missing</faultstring>
```

```
        <faulttime>12/01/2009 03:53:02 EST</faulttime>
        <faultdetails>
          <errorcode>userId</errorcode>
          <errormessage>CWLBN1009E: The value '' with length 0 must have at least length 1</errormessage>
          <applicationname>Ad-HocMeterUsage</applicationname>
          <modulename>BIM_MeterUsage</modulename>
          <srcsystem>Poratl</srcsystem>
          <tgtsystem>Oracle/ETL</tgtsystem>
        </faultdetails>
      </me:SOAPFault_element>
    </detail>
  </soapenv:Fault>
 </soapenv:Body>
</soapenv:Envelope>
```

6 SMT FTPS Interface Overview

Figure 3 depicts the components and processing related to the SMT secured File Transfer Protocol (FTPS) interface for REPs and Third-Parties.

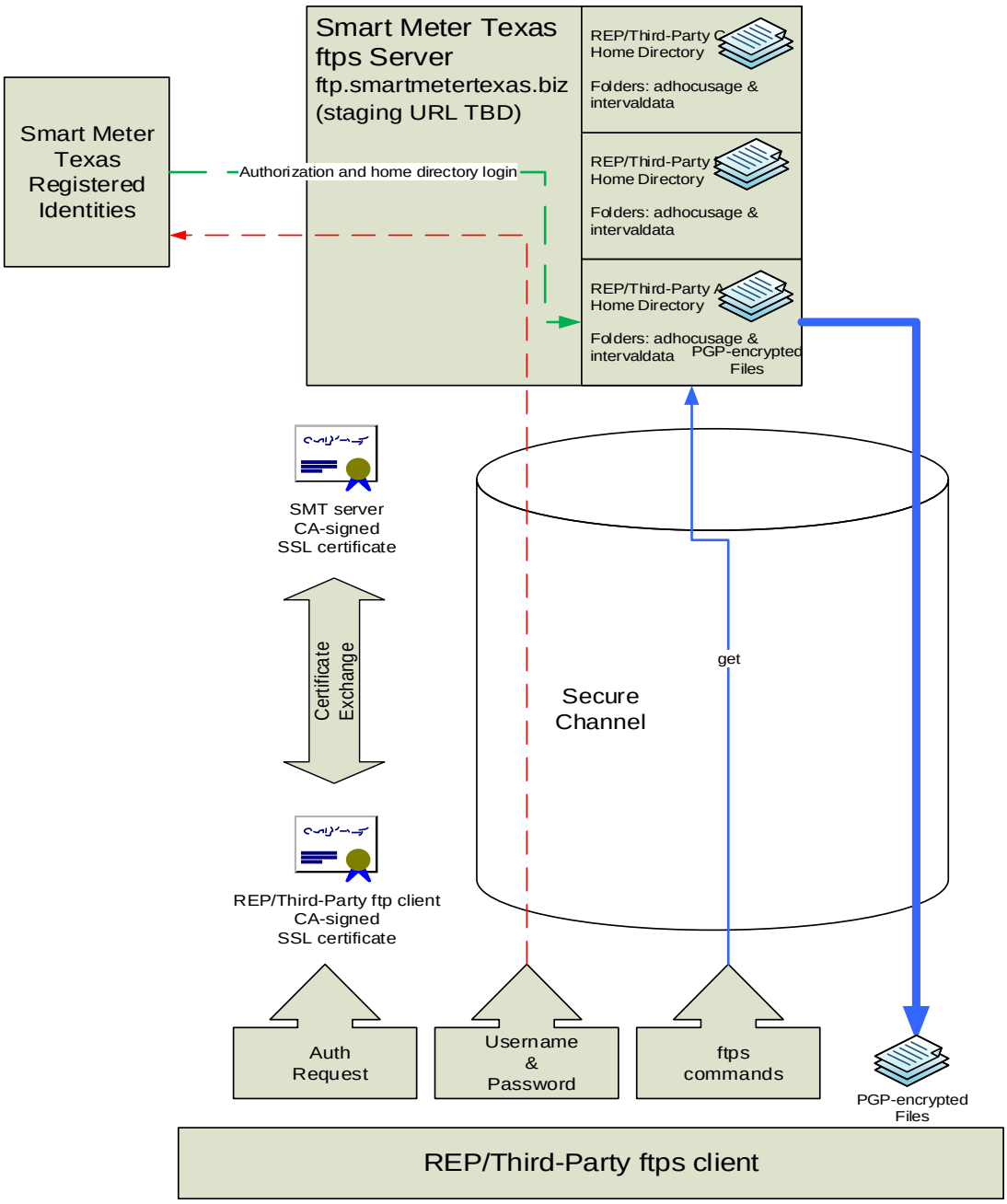

Figure 3: SMT FTPS Components

As depicted, REPs and Third-Parties need several pre-requisites to pull usage data from the Portal:

- Registered and active portal account, including an ftps username and password
- PGP encryption key pair (public key to Smart Meter Texas Portal)
- An ftps "client" software (commercial and free versions available
- CA-signed SSL certificate
- Outbound access to port 21

The completion of portal signup results in the establishment of an account, which includes a valid username and password. The registration also results in the creation of a home directory, from which the requester accesses their usage files. It should be noted that the FTPS account will be created by a Smart Meter Texas Portal administrator and is verbally conveyed to the administrator of the REP or Third-Party. This account is distinct from the Portal logon account username and password.

At the time of sign-up, the REP or Third-Party must generate a set of PGP encryption keys and provide the public key to Smart Meter Texas Portal. The Portal hosting team will use that public key to encrypt the usage files so that they can only be decrypted using the secret private key.

The REP or Third-Party must obtain a FTPS (FTP over SSL) client software to interact with the FTPS interface. This FTPS software, not to be confused with sftp software, is needed to request the usage files. These ftps client software packages are available commercially and in free forms.

Finally, the REP or Third-Party must obtain an SSL certificate signed by a recognized Certificate Authority, such as Verisign. These certificates facilitate the mutual authentication of the FTPS client computer and the Smart Meter Texas Portal ftps host computer, and set up a secure channel between those devices encrypted via SSL.

6.1 FTPS Server folder structure

FTP server contains two folders on each REP FTPS Sites # 1 for posting the Daily LSE files received from the TDSPs and # 2 for posting the usage response files generated for the Ad Hoc usage requests received from the REP users via SMT Portal or API call.

1. Folder Name – "intervaldata" → Contains the LSE files SMT received from the TDSPs .
    - Example file: 957877905IntervalData20100122123001980.lse.002.799530915
2. Folder Name – "adhocusage" → Contains the SMT generated CSV/LSE files for the adhoc usage requests
    - Example files:

      IntervalMeterUsagecfd024ab76ee195c3c326fe9.CSV.8286294561000
      IntervalMeterUsagecfd024ab76ee195c3c326fe9.lse.8286294561000
      DailyMeterUsage00122c501ff160ca73ad74a7.CSV.799530915

6.2 Connecting to FTPS server

The FTPS interaction follows a basic sequence depicted in the graphic and described in the text below.

1) The REP or Third-Party's FTP client contacts the Smart Meter Texas Portal FTPS server (ftp.smartmetertexas.biz) and requests mutual authentication. This results in the exchange of SSL certificates and the establishment of a secure encrypted channel between the FTPS client device and the Smart Meter Texas Portal FTPS server device. It is important to note that the REP or Third-Party's firewalls must be open to outbound traffic on port 21.
2) The REP or Third-Party provides FTPS username as password via the FTPS client software.
3) The Smart Meter Texas Portal FTPS server validates that username and password against the Identity database, and establishes user access to the REP or Third-Party's home directory. It should be understood that a REP or Third-Party can only access their own directory and have NO visibility to others' home directories or data.
4) Following successful validation of FTPS username and password credentials, the REP or Third-Party may request download of usage files & delete the same using standard FTPS commands. The specific commands should be referenced within the documentation for the chosen ftps client software package. The Smart Meter Texas Portal FTPS server delivers the usage files to the REP in an encrypted form that can only be decrypted using the REP or Third-Party's private PGP key, through an encrypted tunnel.
5) The Smart Meter Texas Portal FTPS server retains the files on the FTPS server for 10 calendar days and will be deleted thereafter.