

SMART METER — TEXAS —

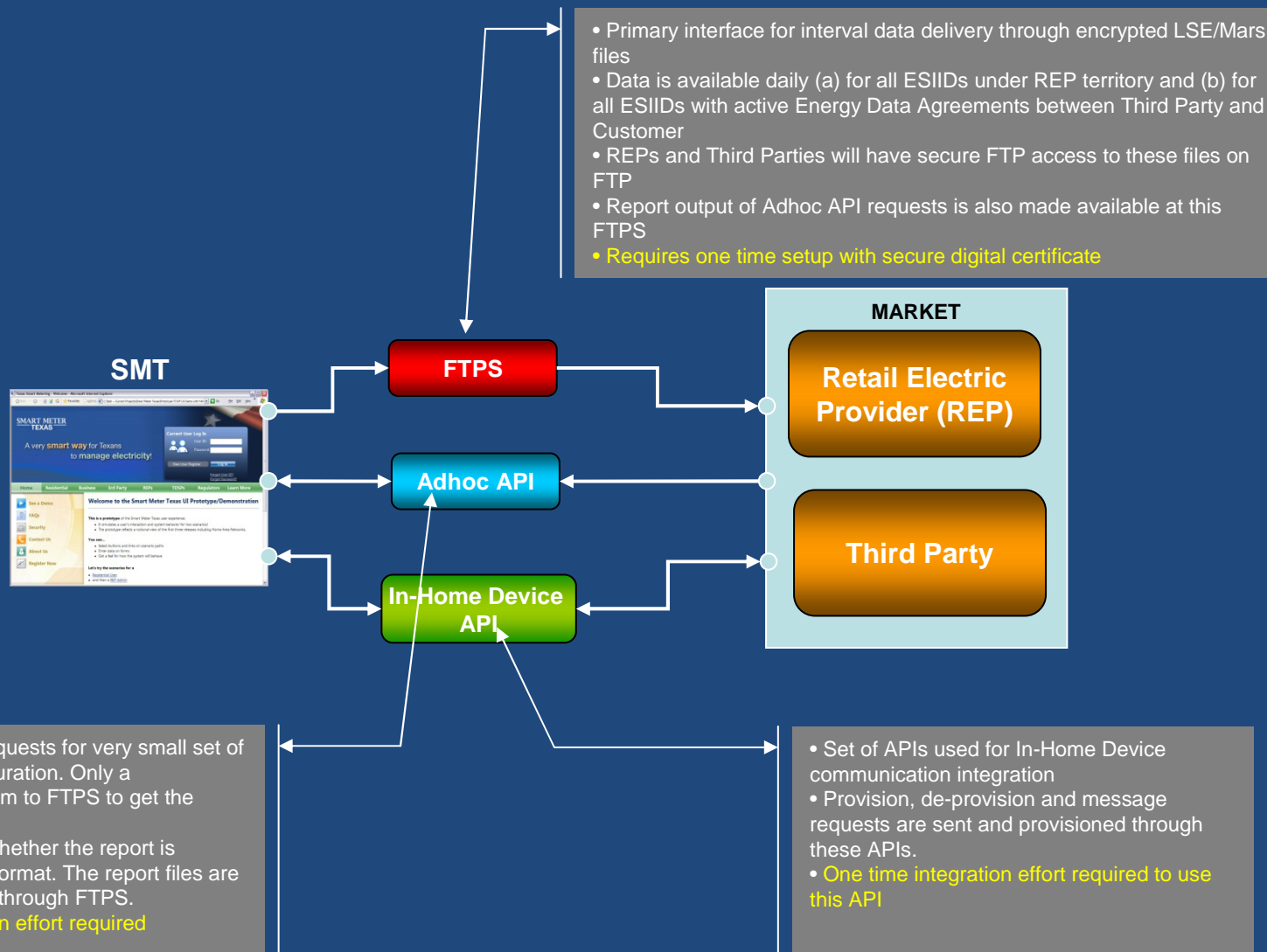
Smart Meter Texas
Third Party
Integration Prerequisites and Processes

Table of Contents



- Overview of the SMT Interfaces
- Integration Prerequisites
- Integration Process Flow
- Integration Technical Activities Flow
- Key Points to Remember
- FTPS Integration with Windows SSL based UI Client
- FTPS Integration with Open SSL based Unix Client
- FTPS Integration Troubleshooting FAQ

Overview of the SMT Interfaces



Integration Prerequisites



✓ SSL Public certificate

- REPs / Third Parties provide their FTPS client security certificate (self signed for testing & certificate issued by public trusted authority for production) to SMT
- Key point: One certificate per machine – the Common Name “CN” in the certificate should match with the host name of the server request initiated

✓ Public PGP Key

- REPs / Third Parties to generate PGP key pair & provide their Public PGP Key to SMT
- If the files are pulled externally, one certificate per REP / Third Party account is required

✓ External public IP address

- REPs / Third Parties to provide their public external IP address from where the request will be originating
- If the REP / Third Party planning to pull the files from multiple machines, provide all the public IP addresses info applicable

✓ REP / Third Party DUNS info

- REPs / Third Parties to identify the DUNS numbers associated with their entity to SMT

✓ Connectivity & procedure to download the files

- SMT Operations team to configure REP / Third Party account and provide the documentation addressing:
 - The SMT FTPS host name and IP address
 - REP / Third Party Login user name & password for connecting to the FTPs site
 - Sample instructions for connecting to the FTPS site via Core FTP client
- REP / Third Party to coordinate the initial setup, download of files with SMT

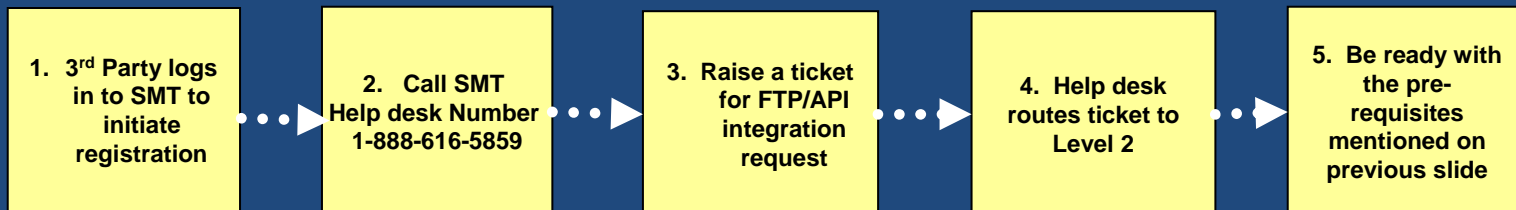
✓ Technical Skills Required

- Integration Specialist with knowledge of FTP, third party digital certificates (certification authority – CA) and integration technology used in the requester’s environment (e.g. SOAP UI, TIBCO, Datapower, TUXEDO, Websphere Commerce, Websphere Process Server, EDI, ESB etc.)

SMT Integration Process Flow

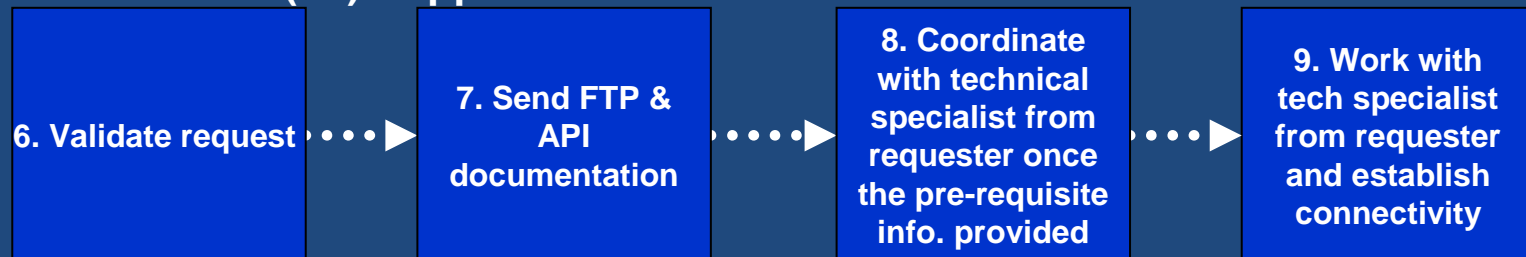


Request for Integration



SMT Level 2 Response

SMT Level 2 (L2) Support



3rd Party Integration to SMT Production

Production

1. Obtain FTPS
Client Security
Certificate
(from Verisign)

2. Provide Public
PGP Key
to SMT
(self signed)

3. Obtain
Credentials
And Addresses
For SMT
Production

4. Exercise
Production
Usage
Downloads

Key Points to Remember



- Adhoc API output is delivered via FTPS, so FTPS should have been configured first before requesting API reports.
- The adhoc API report output is available as a CSV or LSE file, which can be chosen at the time of requesting.
- The file is encrypted with PGP key provided by you.
- The files on FTP – both regular LSE files and Adhoc API outcome are stored for a maximum of 10 days on the FTP site. It is advisable to delete the files from FTP location as you download it, if you do not download the files will be deleted after 10 days.
- The intent of Adhoc API is to access a small subset of data only for the specific needs and not as a regular mechanism to get the interval data, hence there are specific limits on the size of the request (number of ESIIDs, duration of data required), please refer to the Adhoc API documentation for the specific limits on the requests.

SMART METER — TEXAS —

FTPS Integration with
Windows SSL based UI clients

Example FTPS Windows SSL Client Configuration (Core FTP Lite)



✓ Windows SSL client

- “Core FTP Lite” is a free Windows UI software available at www.coreftp.com
- Core FTP Pro and many other tools available with Windows SSL implementation
- Main criteria in selecting the tool is **FTP over SSL/TLS integration with client certificates.**

✓ “Core FTP Lite” prerequisites

- Download and install “Core FTP LE” client from <http://www.coreftp.com/download.html>
- Obtain the SSL certificates or generate self-signed certificates.
 - The Common Name “CN” in the certificate should match with the host name from where the FTP request originates.
 - Import the certificates in to the Windows. Detailed steps included in next slides.

Configuring core FTP for connecting to SMTxP Staging (Page 1 of 3)



➤ The following steps should help in configuring core-ftp client on a computer running Windows XP, with Internet Explorer 8, and Java installed. Java “keytool” command is used to create a self signed certificates, there are various other methods available if Java is not available. For other operating systems and browsers please adjust accordingly.

1.Download and install Core FTP Lite version from

<http://www.coreftp.com/download.html>

2.For testing purposes, create self signed client certificate. Use Verisign for Production. In a command window, run the following command on a machine that has java installed

- keytool -genkey -keypass "password" -storetype pkcs12 -storepass "password" -keystore "mystore.p12".
- For the prompt “what is your first and last name” enter your computer name. Sample MS-DOC command snapshot provided below for reference.

```
C:\>keytool -genkey -keypass "password" -storetype pkcs12 -storepass "password" -keystore "mystore.p12"
What is your first and last name?
[Unknown]: DESKTOP1
What is the name of your organizational unit?
[Unknown]: REP1
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]: DALLAS
What is the name of your State or Province?
[Unknown]: TX
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=DESKTOP1, OU=REP1, O=Unknown, L=DALLAS, ST=TX, C=US correct?
[no]: yes
```

Configuring core FTP for connecting to SMTxP Staging (Page 2 of 3)



3. Import the private certificate just created to your windows
 - a) Launch Internet Explorer
 - b) Go to Tools->Internet Options and click on *Content* tab, and click on *Certificates* button.
 - c) The Certificates window will open, in that window, select the *Personal Tab* and click on *Import* button.
 - d) The Certificate import wizard will launch, follow the instructions to import the “mystore.p12” file create the previous step.
 - e) When prompted for password, enter the password you provided when executing the keytool command.
4. Export the public certificate to publish to SMTxP
 - a) Once the certificate is imported, select the newly imported certificate in certificates windows and click on the *Export* button.
 - b) The certificates export wizard will launch, and follow the on screen instructions to export the public certificate. Ensure that “Do not export the private key” option is selected during the export process.
 - c) When selecting the Export file format in the wizard, choose the “Base-64 encoded X.509 (.CER) format.
 - d) Email the exported certificate to SMTxP contact person. Some e-mail systems block .cer files, it is recommended to zip the file before sending.

Note: Wait for SMT Contact person accept your certificate and to provide you with user name and password.

Configuring core FTP for connecting to SMTxP Staging (Page 3 of 3)



5. Configure Core-FTP

- a) Launch Core-FTP
- b) Go to *File -> Connect* and configure the Site Manager as shown below
- c) For *Host/IP/URL* field enter the information provided by SMT Contact person click on *Connect button*. When prompted to accept the certificate, click on “Always Accept” button.
- d) Now you can fetch files as you would with any other FTP client.

SMART METER — TEXAS —

FTPS integration with
OpenSSL based UNIX clients

Example FTPS OpenSSL Client Configuration (cURL)



✓ OpenSSL client

- “cURL” an open source command line tool available <http://curl.haxx.se/download.html>.
- Many tools available with OpenSSL implementation but the main criteria in selection is **FTP over SSL/TLS integration with client certificates.**

✓ “cURL” key points

- Simple and good tool to automate the FTP steps in cron / batch scripts in UNIX and Windows
- Supports varieties of Operating Systems.

✓ “cURL” prerequisites

- Download and install “cURL” client.
- “cURL” only support certificates in PEM format, you can convert certificates from different formats to PEM using OpenSSL commands:
 - Run the 'openssl' application to convert the certificate. If you cd to the openssl installation, you can do it like:#
 - `./apps/openssl pkcs12 -in [file you saved] -clcerts -out [PEMfile]`

OpenSSL (cURL) command line syntax



cURL command syntax to get list of file names in SMT FTP site intervaldata directory with Verisign certs in production environment

```
curl -I --ftp-method nocwd --ftp-ssl -u <user>:<password> --key <mykey>.pem --cert <myclient>.pem:<password>
```

cURL command syntax to get abc.asc file from SMT FTP site intervaldata directory with Verisign certs in production environment

```
curl -G -o abc.asc --ftp-method nocwd --ftp-ssl -u <user>:<password> --key <mykey>.pem --cert <myclient>.pem:password
```

cURL command syntax to delete abc.asc file from SMT FTP site intervaldata directory with Verisign certs in production environment

```
curl -Q "DELE intervaldata/abc.asc" --ftp-method nocwd --ftp-ssl -u <user>:<password> --key <mykey>.pem --cert <myclient>.pem:password
```

Example cURL script to pull the LSE files from SMT



- Sample KSH shell script to poll the list of files, retrieve & delete the LSE files in SMT Production FTP server
- Baseline script to help the integration & many tuning options available in curl documentation @ <http://curl.haxx.se/docs/manpage.html>

```
#!/bin/ksh

if [ $# -ne 2 ]; then
    echo "Usage: $0 <username:password> <intervaldata/adhocusage> "
    return 1
fi

# command to list the files from the server
INPUT_DATA_FILES=`curl -I --ftp-method nocwd --connect-timeout 45 --ftp-ssl -u $1 --key mykey.pem --cert myclient.pem:password "ftp://ftp.smartmetertexas.biz/$2/" 2>/dev/null | grep "asc" | tr "\n" " "`

if [ $? -eq 0 ]; then
    echo "files available in server = $INPUT_DATA_FILES"

    for i in `echo $INPUT_DATA_FILES`;
    do
        # Get the listed files in to local filesystem
        curl -G -o $i --ftp-method nocwd --connect-timeout 45 --ftp-ssl -u $1 --key mykey.pem --cert myclient.pem:password "ftp://ftp.smartmetertexas.biz/$2/$i"
        if [ $? -eq 0 ]; then
            echo "File [$i] received successfully from the server"
            # Delete the files on the SMT FTPS server
            curl -Q "DELE $2/$i" --ftp-method nocwd --connect-timeout 45 --ftp-ssl -u $1 --key mykey.pem --cert myclient.pem:password "ftp://ftp.smartmetertexas.biz"
            if [ $? -eq 0 ]; then
                echo "File [$i] deleted successfully from the server"
            else
                echo "File [$i] failed to delete from the server"
            fi
        else
            echo "Failed to receive the file [$i]"
        fi
    done
fi
```


FTPS Integration troubleshooting FAQ:



➤ Few initial debugging steps for REP to resolve the FTPS connectivity issues with SMT FTPS server.

1. Check if you can ping the SMT FTPS server, Example: "ping ftp.smartmetertexas.biz" from the machine where the FTPS client is running?

2. Check if you can "telnet [ftp.smartmetertexas.biz](ftp://ftp.smartmetertexas.biz) 21" from the machine where FTPS (Core FTP or cURL) client is running?

3. Check your public SSL key "Common Name" is same as the "hostname" of the server where FTPS client is running?

4. Applicable for Core FTP: Check if your Core FTP client "Advanced" options --> SSL/TLS --> "Managed Certificates" listed with the certificate with your hostname?

5. Applicable for cURL: Check the curl command execution with verbose option "-v" to debug the connection log trace.