



# Data Exchange Guide

April 25

2016

The document acts as a guide for Merchants integrated with the CSC platform and should be used as a reference document for understanding the usage and process for exchange of data towards reconciliation and reporting.

User Guide

## Table of Contents

Introduction .....	3
Summary .....	3
Data Security .....	4
Encryption Process and Flow .....	4
Public and Private Keys .....	4
Public Key Authentication .....	5
Definitions .....	6
Data Exchange Format & Frequency .....	7
ANNEXURE I - IP White Listing Form .....	8
ANNEXURE II – Data Delivery File .....	9
ANNEXURE III – Acknowledgement Return File .....	10

## Introduction

CSC e-Governance Services India Limited is a Special Purpose Vehicle (CSC SPV) incorporated under the Companies Act, 1956 by the Department of Electronics and Information Technology (DeitY), Government of India, to monitor the implementation of the Common Service Center Scheme. CSC SPV is connecting local population with the Government departments, banks, and insurance companies and with various service providers in private sector using IT-Enabled network of citizen service points.

## Summary

As we are growing in terms of number of services and customers with quality of service provided, CSC SPV is planning to redesign the process of data exchange with its service providers to streamline the process of sharing daily MIS. For better and effective integration of services, there should be a standardized format for the Merchant's Delivery file and Acknowledgement file shared by CSC SPV. This implementation will establish an automated data exchange mechanism between CSC SPV and Merchant for better delivery of services and integration.

This document for transactional data exchange covers **Delivery File data exchange format, Acknowledgement Return File data exchange format and IP White Listing Form**. Merchant should ensure field names of delivery file and acknowledgement return file for facilitating smoother data exchanges. Merchant needs to provide Server Path with Protocol, Server IP and Port to secure an efficient data exchange implementation. This implementation will minimize the chances in mismatch of transactional data and would help to further automate the process.

To be considered valid, the data exchange format must be confirmed and signed by merchant.

## Data Security

Data Security is a big challenge in today's cyber world. With the Internet continually growing, the threat to data travelling over the network increases exponentially. In the current business environment of increased security regulations as well as heightened security threats by hackers, secure file transfer has become extremely important and necessary.

In lieu of above, CSC e-Governance Services India Limited allows the option to use encryption in data exchange implementation as per Encryption Standards.

To ensure end to end data encryption the data is exchanged through SFTP (Secure File Transfer Protocol). SFTP is based on Secure Shell and automatically applies multiple layers of protection to the data in transit from eavesdropping attacks.

SFTP securely transfer data—usernames, passwords, and file contents and enables bidirectional secure data transfer using one port.

## Encryption Process and Flow

SFTP is a network protocol that facilitates file transfer, access and management over a reliable data stream. It is a secure binary, packet based protocol in which the client and server communicate with each other in the form of packets.

When a client attempts to establish a connection via SFTP there are two layers that come into play, these are the Transport & Authentication layers. The Transport Layer handles initial key exchange, server authentication, determines what encryption algorithm to use, decides whether to employ compression & performs integrity verification. The Authentication Layer handles client authentication and employs a number of methods to accomplish this including password and public-key cryptography.

## Public and Private Keys

Authentication and encryption use digital codes called "keys" - a public and a private key. The public key is used to encrypt messages, and the corresponding private key is used to decrypt them. It is important to note, however, that despite their symbiotic association, it is virtually impossible to infer the private key if you know the public key.

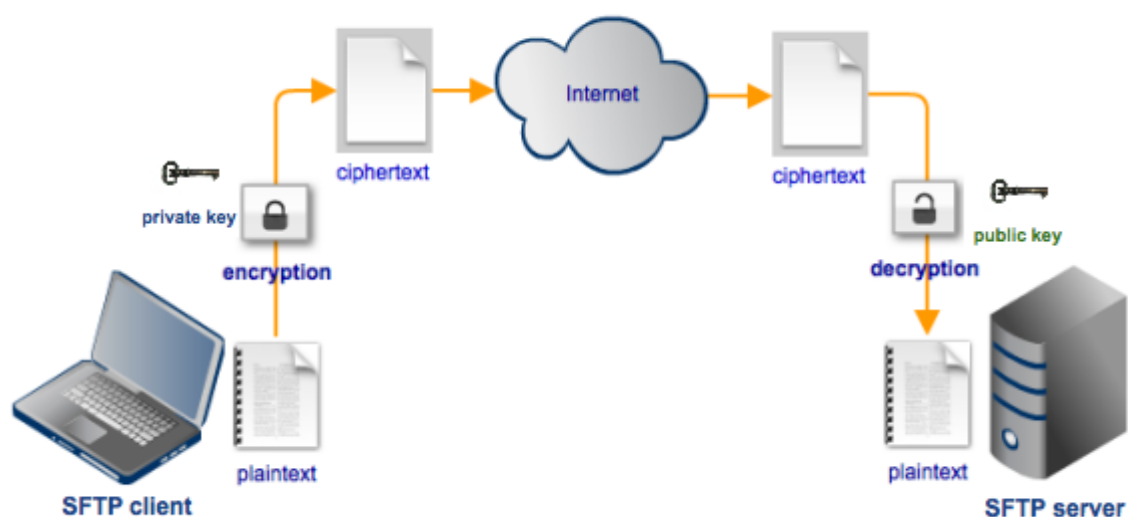
The public key has two major functions: validation and data encryption. As its name suggests, the public key is openly published to any party requesting one of these two functions.

The private key on the other hand, is necessary for decrypting the data encrypted by the associated party. Unlike the public key, this key is closely guarded.

## Public Key Authentication

Public-key authentication consists of public-private key pair. The public key is installed on the server and the private key resides with the user. Messages are encrypted using the recipient's public key and can only be decrypted with the associated private key. Note that it is near impossible to derive the private key using the corresponding public key therefore the security of the public key authentication mechanism depends largely on the safe keeping of the private key by the user; if it is lost the user account can be compromised.

The encryption used in data exchange mechanism is as shown in the figure below:



**Figure 1. Public Key Authentication**

As described in Figure 1, the same process will be carried out in our data exchange process through SFTP. As stated in the figure, Merchant will encrypt the Data Delivery Files with the public key of CSC and in return CSC will decrypt the files using its private key.

For acknowledgement Return File, CSC would encrypt the Data File with the Merchant's public key and in turn Merchant would decrypt the same file with the help of its private key.

## Definitions

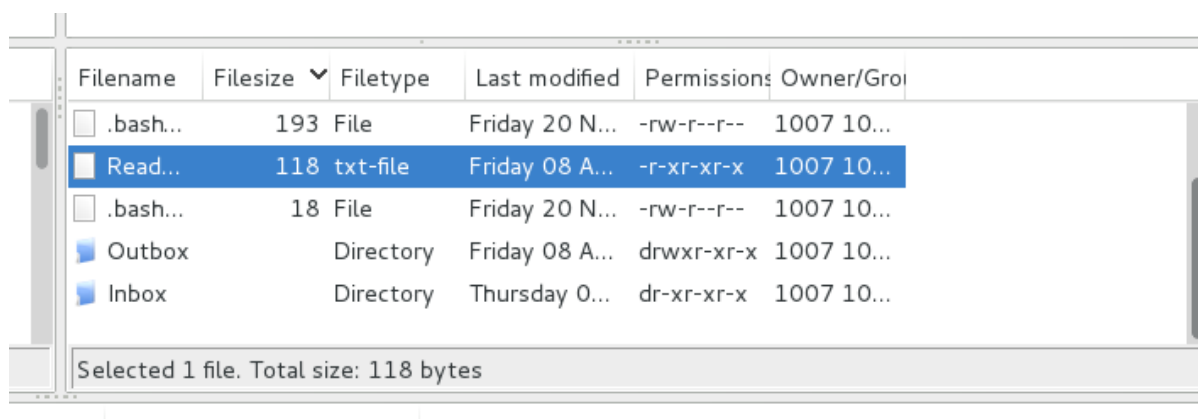
<b>CSC SPV</b>	CSC e-Governance Services India Limited
<b>Merchant</b>	A Government Body/Organization/Company/Agency/Person which has agreement with CSC SPV to deal and provide various goods and services to Indian citizens using CSC SPV IT-enabled access points across India
<b>Delivery File</b>	Transaction report provided by Merchant with standard file name as per specifications
<b>Acknowledgement Return File</b>	Transaction report acknowledged by CSC SPV with standard file name as per specifications
<b>Merchant ID/Code</b>	Unique Merchant ID/Code assigned by CSC SPV platform
<b>Merchant Transaction ID</b>	Unique Transaction ID generated on Merchant platform (common for both Delivery File and Acknowledgement Return File)
<b>CSC Transaction ID</b>	Unique Transaction ID generated on CSC SPV platform (Common for both files)
<b>Product ID</b>	ID of the product assigned by Merchant platform
<b>Merchant Transaction Date &amp; Time</b>	Transaction Date and Time generated on Merchant platform
<b>Amount</b>	Transaction Amount (Common for both files)
<b>CSC User ID/ VLE ID</b>	Unique ID of Village Level Entrepreneur generated by CSC SPV
<b>Merchant Transaction Status</b>	Processing Status of transaction on Merchant platform (S-Success, F-Fail, R-Reject)
<b>Merchant Receipt Number</b>	Receipt No. of Merchant for Transaction
<b>Description</b>	Details of Product, Type of transaction-Sale, Reversal etc.
<b>VLE</b>	Village Level Entrepreneur
<b>Reconciliation Status</b>	Reconciliation Processing Status by CSC SPV (S-Success, F-Fail, R-Reject)
<b>Reason (Optional)</b>	Reason in case of failure and reject case. For success append NA
<b>Additional Information 1</b>	Additional data provided by Merchant (separated by ;)
<b>Additional Information 2</b>	Additional data provided by Merchant (separated by ;)

## Data Exchange Format & Frequency

For standardization, the data exchange between CSC SPV and Merchant should adhere to a common and uniform format to enable seamless exchange of data and facilitate automated reconciliation of the transaction data.

The frequency of data exchange should be highlighted by the Merchant in Annexure I. Merchant should also indicate about the encryption enablement.

The SFTP folder would be organized as shown in Figure 2, SFTP Server Snapshot.



Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro
.bash...	193	File	Friday 20 N...	-rw-r--r--	1007 10...
Read...	118	txt-file	Friday 08 A...	-r-xr-xr-x	1007 10...
.bash...	18	File	Friday 20 N...	-rw-r--r--	1007 10...
Outbox		Directory	Friday 08 A...	drwxr-xr-x	1007 10...
Inbox		Directory	Thursday 0...	dr-xr-xr-x	1007 10...

Selected 1 file. Total size: 118 bytes

**Figure 2, SFTP Server Snapshot**

1. The **inbox directory** would be the location where the **acknowledgement** return file would be stored. Merchant will have only read access in the folder. This will enable the Merchant to download Acknowledgement Files as on when needed.
2. The **outbox directory** would be the default location to upload the **delivery** files. Merchant will have read/write access in the folder.
3. The **readme.txt** file will contain the details of the Merchant i.e Merchant ID, Merchant Name and Creation Date of account.

## ANNEXURE I - IP White Listing Form

This form has to be filled by the Merchant for white listing the IP of Merchant on the CSC SPV Server.

Please fill out the form and send a signed and scanned copy to [services@cscegovindia.com](mailto:services@cscegovindia.com) / [tech@csc.gov.in](mailto:tech@csc.gov.in)

<b>CONTACT DETAILS</b>	
<b>Merchant Name</b>	
<b>Contact Person</b>	
<b>Designation</b>	
<b>Mobile Number</b>	
<b>E-mail</b>	
<b>Landline Number</b>	
<b>DATA SPECIFICATIONS</b>	
<b>Frequency</b>	<input type="checkbox"/> Hourly <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly
<b>Encryption</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Keys</b>	<i>To be generated on CSC bridge Portal</i>
<b>SERVER DETAILS</b>	
<b>IP Address</b>	
<b>Port</b>	
<b>File Path on Server</b>	
<b>Username</b>	<i>To be shared separately</i>
<b>Password</b>	<i>To be shared separately</i>

(Signature and Seal)



## ANNEXURE II – Data Delivery File

The delivery file has to be shared by the Merchant in below mentioned specified format where the data should be pipe delimited (|). The delivery file should have to be pushed to the outbox directory of the CSC SPV SFTP location.

**File Name:** ZZZZZ\_YYYYMMDD\_SNO\_D.dat

<b>ZZZZZ</b>	Merchant ID/Code
<b>YYYYMMDD</b>	File generation year, month and date
<b>SNO</b>	Running serial number, three digit
<b>D</b>	Indicator for file type (D – for delivery files)

### Parameter List

S. No.	Parameter Name	TYPE	Parameter Description
1.	Merchant ID/Code	VARCHAR (5)	Unique code assigned by CSC SPV to the Merchant.
2.	Merchant Transaction ID	VARCHAR (64)	Unique Transaction ID generated on Merchant platform for each transaction
3.	CSC Transaction ID	VARCHAR (24)	Unique Transaction No. generated on CSC SPV platform assigned to each merchant transaction
4.	Product ID	VARCHAR (12)	ID of the product assigned by Merchant platform
5.	Merchant Transaction Date & Time	DATETIME	YYYY-MM-DD HH:MM:SS Transaction date from Merchant platform
6.	Date Format	VARCHAR (20)	Specify the date format whether YYYY-MM-DD HH:MM:SS or any other format
7.	Amount	DOUBLE (8,2)	Transaction Amount
8.	CSC User ID	VARCHAR (50)	Name/Receipt No/Other Detail for particular consumer
9.	Merchant Transaction Status	CHAR(1)	Processing status (S-Success, F- Fail ,R-Reject)
10.	Merchant Receipt Number	VARCHAR (50)	Request ID of Merchant for Transaction
11.	Additional Information 1	VARCHAR (50)	Additional data provided by Merchant (separated by ‘;’)
12.	Additional Information 2	VARCHAR (50)	Additional data provided by Merchant (separated by ‘;’)

### Delivery file data format

S.No.1|S.No.2|S.No.3|.....|S.No.12

#### Note:

- The serial numbers in sample data Format refers to the S. No. in the Parameter List table.
- It is mandatory to store the file with the name as specified in the format.

## ANNEXURE III – Acknowledgement Return File

The acknowledgement return file will be shared by CSC SPV with the Merchant, in a pipe delimited text file. This file will be uploaded by CSC SPV and can be seen and downloaded from the inbox directory of the SFTP location.

**File Name:** ZZZZZ\_YYYYMMDD\_SNO\_R.dat

**Server Directory Path:** /home/ZZZZZ/inbox

<b>ZZZZZ</b>	Merchant ID/Code
<b>YYYYMMDD</b>	File generation year, month and date
<b>SNO</b>	Running serial number, three digit
<b>R</b>	Indicator for File type (R – for return files)

### Request Parameters

S.NO.	Parameter Name	TYPE	Parameter Description
1.	Merchant Transaction ID	VARCHAR (64)	Transaction ID generated on Merchant platform with YYYY-MM-DD HH:MM:SS
2.	Product ID	VARCHAR (12)	ID of the product assigned by Merchant platform
3.	Amount	DOUBLE (8,2)	Transaction Amount
4.	CSC User ID	VARCHAR (11)	Name/Receipt No/Other Detail for particular consumer
5.	CSC Transaction ID	VARCHAR (24)	Unique Transaction No. generated on CSC SPV platform assigned to each merchant transaction
6.	CSC Transaction Date & Time	DATETIME	YYYY-MM-DD HH:MM:SS Transaction date from CSC SPV platform
7.	Reconciliation Status	CHAR (1)	Processing status by CSC SPV (S-Success, F- Fail ,R-Reject)
8.	Reason(Optional)	VARCHAR (50)	Reason in case of failure and reject case, for success append NA

### Acknowledgement file data format

ZZZZZ| S.No.1|S.No.2|.....|S.No.8

#### Note:

- The serial numbers in sample data Format refers to the S. No. in the above table.
- It is mandatory to store the file with the name as specified in the format.