

# Interoperable Interface Control Document ICD-01: File Transfer

*June 21, 2007*

*Version 2.03*

---

***Do Not Redistribute***

*This document contains confidential and proprietary information.  
The unauthorized use, release or distribution of, or reliance, on any information or materials  
contained in this document is strictly prohibited.*

---



Copyright © 2007 by North Texas Tollway Authority.  
All rights reserved.

# DOCUMENT STATUS SHEET

Date	Revision	Author	Pages Modified	Sections Modified	Description of Modifications
03/23/2007	0.01	ETC	N/A	N/A	Initial draft of document.
05/15/2007	2.00	ETC	N/A	N/A	Made As-Built.
06/08/2007	2.01	ETC			Updated document per TXDOT Review.
06/18/2007	2.02	ETC			Updated per IOP ICD discussion with the IOP Authorities & ETC Internal Review.
06/21/2007	2.03	ETC			Updated per NTTA Review.

# Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
1.1	PURPOSE.....	1
1.2	DEFINITIONS, ACRONYMS AND ABBREVIATIONS .....	1
1.3	REFERENCES .....	1
1.4	OVERVIEW .....	2
<b>2</b>	<b>Specification</b> .....	<b>4</b>
2.1	TYPE.....	4
2.2	SECURITY .....	4
2.3	FILE TRANSFER GUIDELINES.....	4
2.4	PROCESSING GUIDELINES .....	4
2.4.1	Sender:.....	5
2.4.2	IOPHub .....	5
2.4.3	Receiver:.....	6
2.4.4	Sender Processing.....	6
2.4.5	IOPHUB Processing.....	7
2.4.6	Receiver Processing .....	7
2.4.7	Audit Capability .....	7
2.4.8	Archive & Purge .....	7
2.5	FILE FORMAT .....	8
2.5.1	File Header Format .....	8
2.5.2	Data Record.....	9
2.5.3	ZIP File Format.....	9
2.5.4	Sample Data.....	9
2.6	FILE TRANSFER DEPICTION .....	10
2.7	AVAILABILITY .....	10

# 1 Introduction

## 1.1 Purpose

This Interoperability Interface Control Document (ICD) describes the general file structure used by interoperable authorities to construct files that are exchanged between authorized Service Providers and authorized Subscribers by means of the IOPHub system.

This interoperable ICD defines the format, content and physical transfer of the files transferred between authorized Service Providers or authorized Subscribers and authorized Service Providers via the IOPHub system.

## 1.2 Definitions, Acronyms and Abbreviations

A comprehensive glossary of terms is being maintained for the entire Interoperability project. The terms, acronyms and abbreviations used in this document will be contained in the Interoperable Project Glossary.

For easy reference, the following terms are provided.

**Table 1.2: Definitions, Acronyms, and Abbreviations**

<b>Term</b>	<b>Description</b>
Home Authority (HA)	An Authority that issues transponders to patrons, owns and manages accounts associated with those transponders, and posts transactions to those accounts.
Service Provider (SP)	An Authority that operates and maintains a customer service center that issues AVI transponders for electronic payment of AVI transactions, such as toll road fees and parking fees. For this document, the Service Provider shall be defined as an Authority that sends transponder transactions and toll variance transactions to the IOPHub system for reconciliation.
Subscriber	An Authority that utilizes a service provider to conduct customer service center operations. These types of Authorities do not maintain their own customer accounts, or operate a customer service center.
Tag Validation List (TVL)	A comprehensive list of transponders issued by each interoperable Authority, as specified in the ICDs.
Tag Validation List Update	A list of Tag Validation List (TVL) changes since the last TVL Update or TVL List, as specified in the this document.
Visited Authority (VA)	Any Authority, or its designated representative, that is not the customer's Home Authority.

## 1.3 References

The following items are referenced in this document:

- *Interoperable Business Requirements Document*
- *Interoperable ICD-02: Tag Validation List*

- Interoperable ICD-03: Financial Transactions File.
- IOPHub Data Security Guidelines
- IOPHub Project Glossary

## 1.4 Overview

The IOPHub uses a standard set of data exchange protocols that provide Interoperability between one or more Service Providers to communicate and exchange data.

The ICDs have been drafted to define the protocols used to exchange financial transactions, reconciliation data, and AVI tag status information. These ICDs describe the content and structure of the Tag Validation List file, Tag Validation List acknowledgement file, transaction file and reconciliation file and their associated data records, as well as the associated processing required. The document *Interoperable-ICD-02: Tag Validation List*, for example, describes the protocol employed between Service Providers to exchange Tag Validation List information.

The exchange of data (financial transactions and AVI tag statuses) is governed by the requirements as set forth in the *Interoperable Business Requirements Document*.

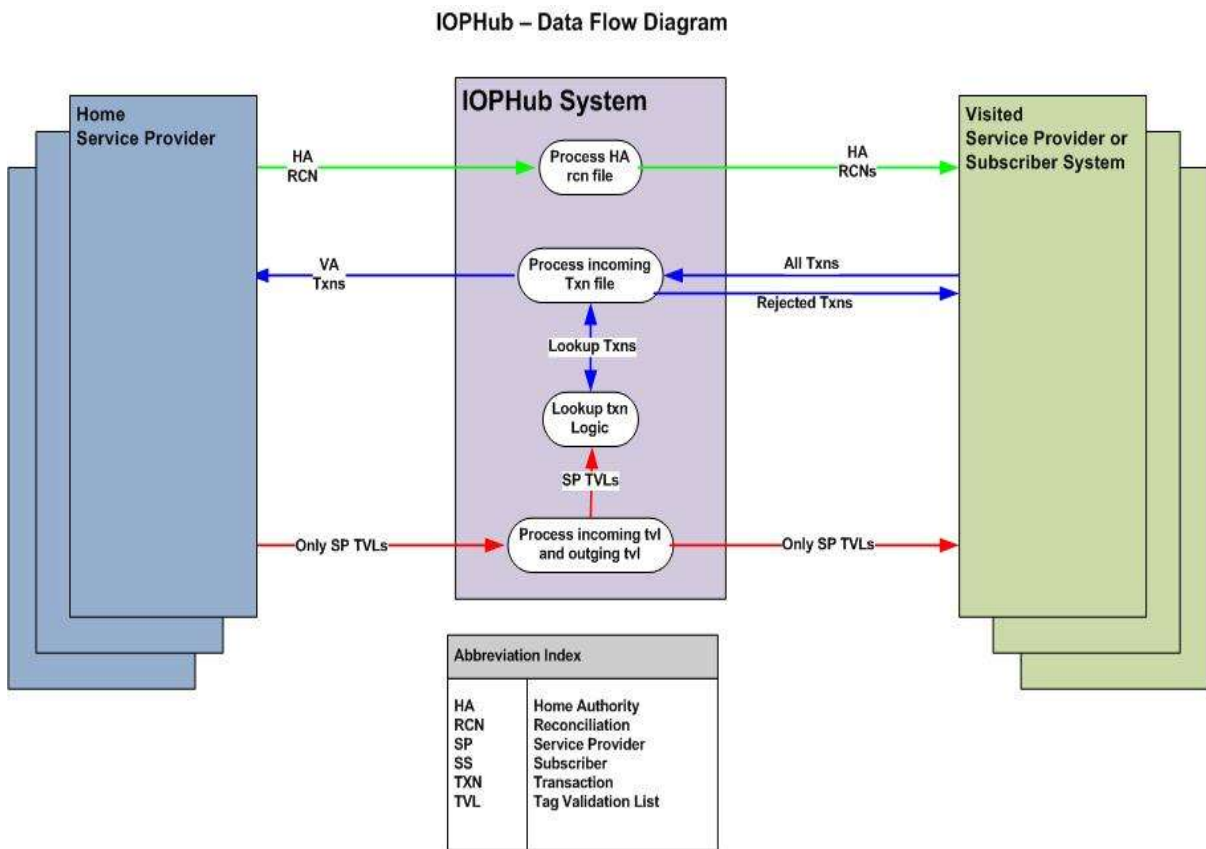


Figure 1. Interoperable Data Flow.

This ICD describes the format of the data files required to support the interoperable protocol between Service Providers to facilitate the physical exchange of data files. This ICD describes the format of the file header and the associated processing of the file required to ensure data files are consistently constructed, transferred and received.

Since data flows between Service Providers via the IOPHub, the interface between Service Providers is important to define. As data is prepared to be sent from the sender's side, additional items are added to the file to support the interoperable protocols. In this instance, a file header is created. The details of the file header are described in this document.

When the IOPHub receives the file in the appropriate Service Provider incoming FTP folder, the file is validated prior to processing. Once the file is validated, the file is processed by the IOPHub and then distributed to the appropriate Service Providers' outgoing FTP folder for pickup. The receiving Service Provider picks up the file and also validates the file header prior to using the file.

The following sections describe the general file structure format and location of the file header required. The content of the data records contained in the file is detailed in the documents *Interoperable-ICD-02: Tag Validation List* and *Interoperable-ICD-03: Financial Transaction File*.

## 2 Specification

---

### 2.1 Type

---

This specification defines the general structure of ASCII data files transmitted between Service Providers. This specification does not address the content of the files beyond the file header.

### 2.2 Security

---

The data files will be written with no special security considerations. The contents of the files are viewable in a standard text editor. The files contain no security-sensitive information.

The IOPHub shall utilize a firewall scheme that will prevent unauthorized access by authorized or unauthorized users. Captive accounts or similar accounts shall be used to prevent unauthorized users from accessing other areas of the IOPHub and Service Provider computer systems.

Each Service Provider shall utilize a firewall scheme that will prevent access by unauthorized users. Captive accounts or similar accounts shall be used to prevent an unauthorized user from accessing other areas of the Service Providers' computer systems.

The IOPHub Data Security Guidelines document should be reviewed and implemented where appropriate.

### 2.3 File Transfer Guidelines

---

All data files transmitted (pushed) to the IOPHub FTP or picked up (pulled) from the IOPHub FTP by Service Providers will be packaged in a .zip file. The .zip file will be named the same name as the file contained within the .zip file. The '.ZIP' (all capital letters) file extension will be used for all .zip files. The .ZIP file name will also have a '\$' character added to the beginning of the file name prior to sending the file. After the file is delivered to the appropriate FTP folder and validated by the sender, the file name will be changed to the original file name.ZIP without the leading '\$'.

Only one, comma-delimited ASCII data file will be included in each .ZIP file. The file will be unzipped prior to processing.

### 2.4 Processing Guidelines

---

Files will be exchanged between Service Providers and other Service Providers or Subscribers on a regular basis as specified in the Interoperability Business Requirements. Files will be sent on a "push" basis to the IOPHub system for distribution. That is, each Service Provider or Subscriber that has a file ready for transmittal will transmit that file to the other Service Providers or Subscribers via the IOPHub FTP.

The general steps taken in creating, transmitting and receiving a file are as follows:

#### **2.4.1 Sender:**

---

Sender can be Authority, Service Provider, Subscriber or future entities.

1. Sender generates data file contents
2. Sender constructs file header and append data file contents
3. Sender generates checksum and place in file header
4. Sender generates file size and place in file header
5. Sender generates record count and place in record header
6. Sender zips file using PKZIP and place '\$' as leading character of .ZIP file name
7. Sender transmits (push) zipped file to appropriate IOPHub Sender's FTP incoming folder
8. Sender verifies file size of zipped file at destination folder
9. If file verified correctly, Sender renames .ZIP file by removing '\$' from beginning of file-name.ZIP to make file available for pickup by the IOPHub or
10. If file did not verify correctly, Sender removes file

#### **2.4.2 IOPHub**

---

1. Check Sender's FTP incoming folders at IOPHub for new files
2. Verify file name does **not** have '\$' prefix; verify the file name has .ZIP extension
3. Unzip file if no errors
4. Verify file checksum, file size and record count contained in the contents of the file header and record header
5. Verify file record integrity
6. Process file by parsing and validating each record field
7. Mark the file as "Processed" in Sender's FTP incoming folder at IOPHub.
8. Generate data file contents for Receiver
9. Construct file header and append to data file contents
10. Generate checksum and place in file header
11. Generate file size and place in file header
12. Generate record count and place in record header
13. Zip file using PKZIP
14. Place file to appropriate Receiver FTP outgoing folder at IOPHub

### 2.4.3 Receiver:

---

Receiver can be Authority, Service Provider, Subscriber or future entities.

1. Receiver checks Receiver's FTP outgoing folders at IOPHub for new files
2. Receiver verifies file name does **not** have '\$' prefix; verify the file name has .ZIP extension
3. Receiver pulls ZIP file from IOPHub to the Receiver site; verify the ZIP file size at Receiver site matches with the ZIP file size at IOPHub
4. The file in Receiver's FTP outgoing folder at IOPHub will be marked as "Deleted" by IOPHub
5. Receiver unzips file at the Receiver site if no errors
6. Receiver verifies file checksum, file size and record count contained in the contents of the file header and record header
7. Receiver verifies file record integrity
8. Receiver processes file

Sections 2.4.4, 2.4.5 and 2.4.6 provide the details of these general steps.

### 2.4.4 Sender Processing

---

When a data file is available for transmission to IOPHub, the Sender must construct a file header containing the file size and checksum value. The format of the file header is described in Section 2.5.1. The name of the file is determined based upon the contents of the file.

Once the file header is constructed, the data file contents are appended and the entire file is zipped in a .ZIP file. The name of the file will be the same name as the original file with the addition of '\$' character as the leading character of the file name and a file extension of .ZIP (all capital letters).

The file is then transmitted to the Sender's FTP incoming folder at the IOPHub. The '\$' character prevents the IOPHub from prematurely processing the file. The receiver is obliged to ignore any file beginning with the '\$' character.

Upon completion of the transmission, the sender verifies the file size at the incoming FTP folder of the IOPHub.

If the file size is incorrect, the sender shall remove the data file ('\$' prefixed named file.ZIP) from the FTP folder. In accordance with the Business Requirements document, an attempt to retransmit the file will be made by the sender. It is the sender's responsibility to repeat this failure processing before halting further file transfer attempts to the IOPHub. After failed attempts, the sender should notify IOPHub Support. Each sender can decide the number of attempts and the duration criteria for resending / repackaging files.

If the file size is verified by the sender at the IOPHub FTP folder, the sender shall rename the file by removing the '\$' prefix character. At this point, the sender has delivered the file and made it available for processing at the IOPHub.

### **2.4.5 IOPHUB Processing**

---

The IOPHub shall check for incoming files at the Sender's FTP incoming folders. Upon detection of a new ZIP file that is **not** preceded by a '\$', the IOPHub shall unzip the file if no errors. The IOPHub then shall verify the contents of the file. The file header shall contain both the file size and a checksum value. The record header shall contain the record count.

If either the file size or checksum value is invalid, the entire data file shall be disregarded. The IOPHub will mark the file as an error status file, notify the appropriate personnel, or take other such similar action.

If the file size and checksum are verified, the file is picked up from the Sender's FTP incoming folder and processed by the IOPHub.

The IOPHub will then mark the file as "Processed" in the Sender's FTP incoming folder.

The IOPHub will generate data file contents for the Receiver, construct file header, generate checksum and file size to place in the file header and generate record count to place in the record header. The IOPHub will zip the file and place the ZIP file to the appropriate Receiver FTP outgoing folder at IOPHub.

### **2.4.6 Receiver Processing**

---

The Receiver shall check for outgoing files at their outgoing FTP folders at the IOPHub. Upon detection of a new ZIP file without '\$' prefix, the Receiver shall pull the ZIP file from IOPHub to the Receiver site. The file in the Receiver's FTP outgoing folder at the IOPHub will be marked as "Deleted" by IOPHub. (**Note:** The file is deleted logically only; the actual file can still be retrieved for review.)

The Receiver shall verify the ZIP file size is correct and unzip the file if no errors.

The Receiver then shall verify the contents of the file. The file header shall contain both the file size and a checksum value. The record header shall contain the record count. If file size, record count, checksum value or file format is invalid, then the entire data file shall be disregarded. The Receiver may choose to rename the file, move the file to an unprocessed holding area and notify the appropriate personnel within 24 hours.

If the file size, checksum and record count are verified, the file is processed by the Receiver.

### **2.4.7 Audit Capability**

---

All files are archived on IOPHub Server and they can be viewed or downloaded via the IOPHub User Interface. The User Interface allows the viewing of various file activities with option to organize the file activities by Service Provider or Subscriber.

### **2.4.8 Archive & Purge**

---

Currently there is no purge processing. All the files exist on IOPHub Server.

## 2.5 File Format

The format of an exchanged data file is depicted in Figure 2. The first element in the file is a file header. The format and content of the file header is detailed in Section 2.5.1. Typically the file header is followed by a record header, and an arbitrary number of data records. The format of the record header is dependent upon the file category of data contained within the file. The formats of the various record headers are described in the appropriate ICDs.

Each file must contain only one file header at the beginning of the file. The file header must contain the checksum and the file size only. A file that does not contain this minimum element is considered invalid.

Each record in a file consists of ASCII characters terminated by a Carriage Return (ASCII hex 0x0D) and Line Feed (ASCII hex 0x0A). The size of the file header is fixed in length. The sizes of the record header and data records are variable and are specified in the appropriate ICDs.

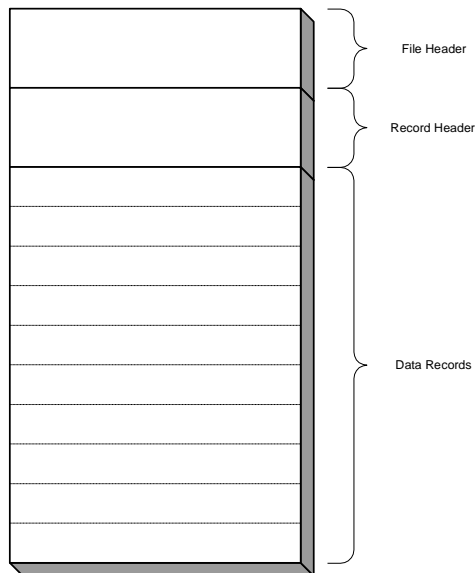


Figure 2. Interoperable File Structure.

### 2.5.1 File Header Format

The file header is a fixed length ASCII record with comma-delimited fields, terminated by a Carriage Return & Line Feed. Although the fields are fixed in length, they are still separated by commas. This is to allow processing by either of two means: (1) specifying absolute file offset position and field length; or (2) parsing the record, breaking on the comma-delimiter. This format was developed to afford implementers maximum flexibility in processing the record type at their system.

File Header Format					
Description	Type	Max. Length	Delimiter	Red's	Comment
File Checksum	Character	8	,	Y	A 32-bit checksum computed for the contents of the file, beginning at the character immediately following the header record and associated CR/LF. This value is displayed as an 8-digit ASCII hex number.
File Size	Numeric	12	CR&LF	Y	The size of the file, in bytes.

The CRC32 standard algorithm is used to compute the checksum value. The checksum is a 32-bit value and is displayed as 8 fixed characters in ASCII hex number. The file size is a base-10 ASCII number. The field is fixed length, although it may be zero-padded.

Note: The checksum field will not be required initially. A value of FFFFFFFF will be used as default. Currently, CTRMA uses checksum in file exchanges with IOPHub, HCTRA and NTTA use default checksum value with IOPHub and TTA uses checksum with TTA P2P IOPHub.

## 2.5.2 Data Record

The Data record portion of the file may contain one or more records.

All file types may contain data records from one or more Service Providers, Subscribers or Authorities.

The Transaction file and RCN file may contain one or more types of data records from one or more Service Providers, Subscribers or Authorities.

## 2.5.3 ZIP File Format

Each file sent or received in by the IOPHub FTP must be zipped using PKZIP.

Each ZIP file shall contain only one data file.

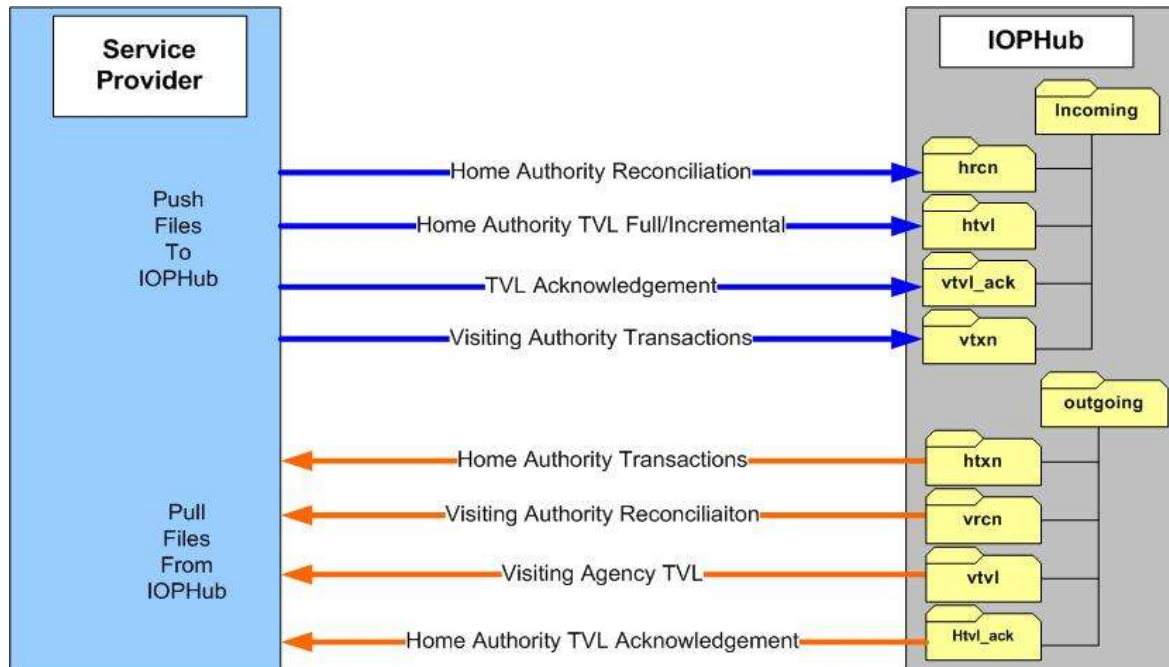
## 2.5.4 Sample Data

A sample File Header is shown below. It contains a checksum value of '13579BDF' (324,508,639 in base-10) and a file size of 53,724 bytes. For illustration purposes, the file size is zero-padded and the Carriage Return & Line Feed is represented as a "¶".

```
13579BDF,000000053724¶
```

## 2.6 File Transfer Depiction

The diagram below provides a visual image of how Service Providers will transmit files (Push) to the IOPHub and how they will receive (Pull) files from the IOPHub.



Legend	
File Transfer Diagram	
Abbreviation	Description
TVL	Tag Validation List
TXN	Transaction
RCN	Reconciliation
TVL_ACK	Acknowledgment of TVL

- All files from Interoperable Authorized Entities will be sent as a data file zipped in a .ZIP file.
- All files shall be validated by size and record count
- Attribute 4 of the TVL file denotes Home Agency.
- TVL files will contain a Home/Orig Agency ID to denote where the tag/transaction originated.
- 

## 2.7 Availability

IOPHub shall be available 24 hours a day, 7 days a week for the file exchanges. Exceptions will be for scheduled maintenance activities. All Service Providers and Subscribers should be notified of extended downtime periods.