CHASE™
Paymentech

NetConnect Batch Interface Specification

A Developer's Guide

Version 1.5
09.15.06

Preface

This edition of the Chase Paymentech Solutions NetConnect Batch Interface Specification contains information available at the time of publication and supersedes, in its entirety, all previously published documents.

4 Northeastern Blvd.
Salem, NH 03079
Tel (603) 896-6000
www.chasepaymentech.com

TABLE OF CONTENTS

Revision History

Date	Version	Description	Author
4/24/06	1.0	Document Creation	MG Chiasson
6/2/06	1.1	Section 2.4 ▪ Added a Zip option for AIX clients Section 3 ▪ Changed expected zipped and encrypted file names ▪ Added a note to inbound file naming ▪ Added note to outbound file naming Section 3.1.2 ▪ Added error code 6903	MG Chiasson
6/27/06	1.2	Section 3 ▪ Added detailed explanation of outbound file naming Section 3.1.2 ▪ Added error code 6903	MG Chiasson
8/1/06	1.3	Section 2.1.1 ▪ Added third bullet regarding authentication Section 2.1.2 ▪ Added section on availability of outbound files	MG Chiasson
8/23/06	1.4	Section 2.6.1 ▪ Added rule for password xml file name imbedded in ZIP which must be lower case – see third bullet	MG Chiasson
9/15/06	1.5	Section 3 ▪ Added last paragraph and bullets for format for date and time stamp which is added to the name of the Error Message File	MG Chiasson

1. INTRODUCTION

1.1 OVERVIEW

The Salem platform, sometimes referred to as the Stratus, is primarily targeted to Card-Not-Present and larger customers. There is a processing platform in Tampa, FL and Salem, NH.

NetConnect Batch is a communication method, which utilizes SFTP (Secure File Transfer Protocol) to enable any certified Salem merchant, aggregator or software vendor partner to send and receive batch files to the Salem processing platform over the Internet. Using a standard SFTP client and an Internet connection, NetConnect Batch users will have the ability to send batch authorization and settlement files to the Salem host servers for processing. In addition to sending and retrieving batch transaction processing files, NetConnect Batch users will have the ability to retrieve BIN Range, Account Updater, and DFR files from a secure NetConnect Batch directory at their convenience.

NetConnect Batch is designed to work with all versions of the Salem Batch Technical Specifications and can be used to transmit batch files for merchants using NetConnect for online authorizations through the Salem processing platform. It is important to note that processing features and functionality are dependent on the merchant's payment processing software.

The purpose of this documentation is to provide a developer with the necessary information on how to integrate NetConnect Batch as a communication method for batch files.

1.2 SUPPORTING DOCUMENTATION

The following documents are complementary and will aid in understanding other aspects of file submission.

- Current versions of the Chase Paymentech Batch Technical Specifications for the Salem platform
- NetConnect Interface Specification (online authorization processing over the Internet)
- Testing and Production Guidelines for NetConnect processing

1.3 FILE TYPES SUPPORTED

Chase Paymentech will make the following file types available through NetConnect Batch

- Batch transaction processing files using any version of the Salem Batch Technical Specifications
- Commercial Card BIN Range files
- PINLess Debit BIN Range files (signed license agreements required)
- PIN Debit BIN Range files
- MasterCard Account Updater files
- Visa Account Updater files
- RFR Redirect
- Delimited File Reports (DFR)

Continued on next page

1.4 SAMPLE PROCESS FLOW – FOR SUBMISSION PROCESSING

1. Merchant's software generates a batch file
2. Batch file is compressed and encrypted
3. Merchant's software initiates a secure connection to NetConnect Batch by:
    a. Initiating an SFTP session to the NetConnect Batch URL
        i. Merchant's Source IP is authenticated
    b. Entering user ID and password (also referred to as SFTP password) provided by Chase Paymentech
        i. The user ID and password are validated
4. The zipped and encrypted file is placed in the user's NetConnect Batch directory.
5. The batch file is processed by Chase Paymentech
    a. If the merchant receives a response file, it is zipped, encrypted, and placed in the designated directory.
    b. The merchant initiates a secure connection to NetConnect Batch and retrieves the response file from the designated directory.
    c. The merchant may delete the response file from the directory.

1.5 SAMPLE PROCESS FLOW – FOR RETRIEVAL OF NON-INITIATED FILES

Examples of non-initiated files are BIN Range files, Account Updater, etc.

1. Chase Paymentech places the zipped and encrypted file in the designated directory.
2. The merchant initiates a secure connection to NetConnect Batch and retrieves the file from the designated directory.
3. The merchant may delete the file from the directory.

1.6 CERTIFICATION

Merchants, submitters, and software vendors using NetConnect Batch must certify with Chase Paymentech. Please contact your Chase Paymentech Representative to schedule certification.

2. PROCESSING

This section describes the information necessary for establishing a connection and correctly negotiating with Chase Paymentech's NetConnect Batch.

2.1 ESTABLISHING A CONNECTION

NetConnect Batch is available 24 x 7, 365 days a year. To initiate a file transmission the following are required:

- An Internet connection that guarantees a static Source IP (not a dial up connection)
- A standard SFTP product
- The designated URLs provided by Chase Paymentech

The secondary URLs listed in this section will be available when the primary URLs are unavailable.

Continued on next page

2.1.1 NetConnect Batch URLs

Chase Paymentech maintains two NetConnect Batch interfaces:

1. Test system:
   Primary URL
   - netconnectbatchvar1.chasepaymentech.net

   Secondary URL
   - netconnectbatchvar2.chasepaymentech.net

2. Production system:
   Primary URL
   - netconnectbatch1.chasepaymentech.net

   Secondary URL
   - netconnectbatch2.chasepaymentech.net

Chase Paymentech exposes redundant endpoints to ensure high availability for NetConnect Batch. Developers should code to the fail over URL. The failover should be automatic and completely transparent to the end-user. Each file transmission should first use the Primary URL.

Notes:

- The NetConnect Batch test interface is monitored for availability and supported during business hours [8:00am EST – 5:00pm EST Monday – Friday, excluding major holidays].
- Caching IP Addresses of NetConnect Batch servers is strongly discouraged. For redundancy reasons, NetConnect Batch processing is divided amongst multiple data centers. Therefore, the DNS service should be used to determine the destination IP address for each connection. If IP addresses are required for merchant firewall rules purposes, these values can be obtained from your certification analyst.
- SSH [SFTP] utilizes a key fingerprint system for verifying the authenticity of the server when the client connects. A user will be prompted to enter yes only when connecting for the first time. Future attempts to login are all verified against the saved fingerprint key. The SSH client will alert you if the saved fingerprint differs from the received fingerprint on future login attempts. Based on this, it should be noted that Chase Paymentech utilizes two separate servers [and therefore two separate SSH fingerprint keys] for the NetConnect Batch process. If your client is authenticating the fingerprint keys, both sets must be registered in your known host file in order to prevent authentication errors when Chase Paymentech switches servers.

2.1.2 Availability of Outbound Files

NetConnect Batch will always write outbound files to the primary and secondary server regardless of which server received the inbound files. The files remain on each server for 30 days, unless they are deleted from each server manually by the user.

2.2 TRANSMISSION

Given the inherent risks associated with processing transactions over the Internet, NetConnect Batch requires both encrypted traffic to prevent interception of the payload, and authentication of the source request generation. The following sections define the process flow, certification, and transmission requirements for NetConnect Batch communication method.

All transmissions will be made to the NetConnect Batch Server using a valid SFTP tool. This will require a user ID and password, which is provided by Chase Paymentech.

Note: The SFTP user ID expires. See requirements in Section 2.6.

Once the session is successfully established, the user will be logged into their directory. The client can FTP 'put' the request files and FTP 'get' the response files.

Once NetConnect Batch detects the presence of a new request file, it is retrieved and deleted from the directory.

Output files are placed in the same directory. Once the zipped file is retrieved, it can be deleted by the user. Files are auto-deleted by the NetConnect Batch system on day 30 if not deleted by the user.

2.3 SFTP PRODUCTS

Establishing an SFTP session requires an SFTP product. Chase Paymentech does **not** either recommend or support any SFTP products. Some examples of open source options are:

- Open SSH --- http://www.openssh.org/
- PuTTY --- http://www.chiark.greenend.org.uk/~sgtatham/putty/

2.3.1 SFTP Commands

Once connected, in addition to the SFTP 'get' and 'put' commands to send and retrieve files, the following FTP commands are available for use:

- cp – Copies file into the same directory or into another directory specified by path
- ls – Displays directory listing of either path or current directory if path is not specified
- rm – Deletes file specified by path
- mkdir – Creates directory specified by path
- rmdir – Removes directory specified by path

Warning: Do not rename files. Renaming files can cause files to be reprocessed.

2.4 ZIP AND ENCRYPT FILE

All files must be zipped/compressed and encrypted using compression software prior to sending them via NetConnect Batch. This provides an extra measure of security to ensure that the request/response files cannot be compromised.

The software should zip and password protect the file. Chase Paymentech has tested using both PKZip and WinZip. The URL's for these products are:

- PKZip --- http://www.pkware.com/
- WinZip --- http://www.winzip.com/
- Infozip works for AIX clients ---- http://www.info-zip.org/

The outbound file is zipped and encrypted with a password. The same password that is assigned for the SFTP logon must be used for the zip process during the initial set up. After initial set up, the SFTP and zip passwords may be different. Refer to section 2.6 for more information.

2.5 CLIENT AUTHENTICATION

Connections to NetConnect Batch requires client authentication using a combination of the Salem Presenter ID (PID), user ID, and password. These data elements are provided to the customer during testing by the Chase Paymentech Merchant Certification Analyst. The NetConnect Batch system validates the source IP is registered to allow the SFTP connection to be established.

- When processing transactions to NetConnect Batch, the client server's Source IP(s) must be registered in the NetConnect Batch system. Any activity presented from an IP address that is not registered will result in an SFTP connection failure without any error.
- Source IP addresses are updated 4 times daily on the NetConnect Batch Server [5:05am EST, 11:05am EST, 5:05pm EST, 11:05pm EST]. IP entries must be made at least 1 hour prior to these windows to be included in the update.

2.6 NETCONNECT BATCH PASSWORD RESET

NetConnect Batch passwords must be reset at least every 90 days or they will expire. The zip password does not expire automatically. There are two ways to reset passwords.

2.6.1 Automated Password Reset

Prior to the expiration of the existing password, the user places a password file in their directory. The structure of the password file is:

- The name of the file must be: password_yymmddhhmi.zip, where yymmddhhmi is the creation date and time.
  - yy = year
  - mm = month
  - dd = day of month
  - hh = hour military (01-24)
  - mi = minute

- The file format is XML and the file layout for a password reset is:

```
<passwordRequest>
        <userID> TESTUSER </userID>
        <password>ab123456</password>
</passwordRequest>
```

- The password file imbedded within the ZIP must be lower case xml as opposed to uppercase.
  - Example of a good file name = password_yymmddhhmi.xml
  - Example of an invalid file name = password_yymmddhhmi.XML

- This file layout can be validated using the schema PasswordRequest001.xsd

- Password rules:
  - Exactly 8 characters in length
  - Valid Character types:
    - A-Z
    - a-z
    - 0-9
    - Dash and underscores allowed
    - Must contain at least two alphabetic characters and at least one numeric or special character

- Password changes via the XML file can only be made 7 days after the last password change. Passwords expire on day 90. Section 4.1.2 describes password format and errors.

- The new password cannot be the same as any previous password.

- The password should be usable within 15 minutes after the file is submitted.

- The zip password will not change.
    - Changing the password via the XML file process will **not** change the zip password.
    - The zip password will change **only if** the user ID password is changed manually by a Chase Paymentech Representative.

- A successful password change will not generate a response file.

- A response file is created when the password reset request fails.

2.6.2 Manual Password Reset

Manual Reset is available during normal business hours. [8:00am EST – 5:00pm EST, Monday - Friday, excluding major holidays].

- Manual reset service should only be used in the case where an automated password reset attempt has failed. To initiate a manual reset to the SFTP Password, contact your Chase Paymentech Representative.

If the password is reset through the manual reset process, the following rules apply:

- New Passwords are systemically generated (the customer cannot self define it).
- Manually resetting the password will reset the SFTP password **and** the zip password.
- Manual password changes can take up to 2 hours after the entry is completed.

3. FILE NAMING RULES

A specific file naming convention has been designed for the NetConnect Batch file transmission process. Using the correct file naming convention will allow the files to move quickly through all the security checks and automated processing interfaces.

- Inbound File Naming Rules (Files submitted to Chase Paymentech):

    - Prior to zipping the file:
        - File name = PID.fileID.extension
        - Maximum file name length = 31 bytes.
        - The PID is the Presenter ID assigned by Chase Paymentech for the submission files. It is always 6 bytes in length, numeric.
        - Valid Character types for fileID:
            - A-Z
            - a-z
            - 0-9
            - Dash and underscores allowed
        - There are 5 file extensions that are **not** allowed when naming the data file
            - .dat
            - .xml
            - .zip
            - .err
            - .dfr

- Every file name must be unique. It may never repeat itself or an error will be generated and the file will not process. Error Message 6782 (Batch file name already exists in the database) will be received.

NOTE: A file submitted without an extension in the file name will cause a file failure.

- Post Zipping:
  - The file name inside the zip file [i.e. PID.fileID.extension] must be the same as the zipped file name with the exception of the extension.
  - The encrypted file extension must be '.zip'.
  - Per zip convention, if the pre-zipped file name contains an extension, it is replaced by '.zip'.
    - For example:
      - Pre-zipped: 123456.1234567_ABCDEF.KLMNOP789
      - Post-zipped: 123456.1234567_ABCDEF.zip
  - Per zip convention, if the pre-zipped file name does not contain an extension, '.zip' is added.
    - For example:
      - Pre-zipped: 123456.AUTH1
      - Post-zipped: 123456.AUTH1.zip

- Outbound File Naming Rules (Files retrieved from Chase Paymentech):
  - The zipped and encrypted outbound file name = PID.fileID_resp.zip
  - The unzipped outbound file name will be PID.fileID_resp.extension. Each file type has its own naming rules. The NetConnect Batch process adjusts those default file names in two ways:
    - 'PID.' is prefixed to the beginning of the file name
    - '_resp' is added to the file name.

  - Examples of the expected file naming rules for zipped and encrypted files are:
    - Batch Processing Response File name:
      - PID.ymmdd.xxxxx.out_resp.zip
        - y = year
          - variable numeric 0-9
        - mm = month
          - variable numeric 0-9
        - dd = day
          - variable numeric 0-9
        - xxxxx
          - variable 0– 9 and a-z
        - out = constant, lower case

    - Commercial BIN file:
      - PID.actbinyymmdd_hhmmss_resp.zip
        - actbin is constant
        - yy = year
          - – numeric 0-9
        - mm = month
          - numeric 0-9
        - dd = day
          - numeric 0-9
        - hh = hour
          - numeric 0-9
        - mm =minute
          - numeric 0-9
        - ss = second
          - numeric 0-9

Continued on next page

- PINLess Debit BIN file:
  - PID.ymmdd.xxxxx.out.BIN_resp.zip
    - y = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - xxxxx = variable 0-9 and a-z and A-Z
    - out.BIN = constant
- PIN Debit BIN file:
  - PID.ymmdd.xxxxx.out.PBIN_resp.zip
    - y = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - xxxxx = variable 0-9, a-z or A-Z upper and lower case
    - out.BIN = constant

- MasterCard Account Updater file:
  - PID.nnnnnnnnnn.yymmdd.MAU_resp.zip
    - nnnnnnnnnn is variable numeric 0-9
    - yy = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - MAU is upper case and constant

- Visa Account Updater file:
  - PID.nnnnnnnnnn.yymmdd.VAU_resp.zip
    - nnnnnnnnnn = variable numeric 0-9
    - yy = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - VAU is upper case and constant

- RFR Redirect:
  - PID.ymmdd.xxxxx.out_resp.zip
    - y = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - xxxxx = variable 0-9, a-z or A-Z upper and lower case

Continued on next page

- Delimited File Report (DFR):
  - PID.nnnnnnnnnn.yymmdd.a.AAAA.dfr_resp.zip
    - nnnnnnnnnn is variable numeric 0-9
    - yy = year
      - numeric 0-9
    - mm = month
      - numeric 0-9
    - dd = day
      - numeric 0-9
    - a = variable a-z lower case
    - AAAA = variable upper case A-Z
    - dfr is constant and lower case

1.

NOTE: The outbound file name will not be the same as the inbound file name.

- **Error File Naming:**
  Error message files will have a date and time added to the file name to enable the user to easily detect when an error has occurred. This will also prevent a good file from being overwritten.
  The date and time formula is as follows:
  - JJJHHMMSS
    - JJJ = Julian day of the year
    - HH = Hour
    - MM = Min
    - SS = Sec
  - Example of inbound file name
    - `911111.2006091101.zip`
  - Example of outbound error file name
    - `911111.2006091101.zip_254171629_resp.zip`

3.1 PASSWORD FILES

Password update files must be formatted in XML as stated in section 2.6.

3.1.1 Error File Format

In the event of a file failure during an attempt to update a Password, an error message will be returned. The format of the message is listed below.

3.1.2 Error Reason Codes Table

Code	Definition	Status	Action
6801	Zip file needs to be encrypted	Error	Fix
6804	FTP passwords can only be changed every 7 days	Error	Resend
6805	The selected password is currently in use. Please select another	Error	Fix
6806	Input must be <file name>.xml	Error	Fix
6814	Password format is invalid. All passwords must be 8 characters in length and contain at least one numeric digit and one alpha character	Error	Fix
6903	SAX Exception – This will be sent back to the sender with exact schema violation	Error	Fix

3.2 REQUEST FILES

3.2.1 Error File Format

Error files are generated to detail processing failures. The format of the message is listed below.

Batch Sequence Number: [1234567]
User ID: [abcdef99]
File ID: [file name]

Error Message Number: 6815
Error Message Description: Presenter ID is not valid for this user.

The Batch Sequence Number is defined as the NetConnect Batch Internal Reference Number, which may be used in error escalation situations.

3.2.2 Request File Error Reason Codes Table

The following is a list of potential error messages a NetConnect Batch user may encounter and how to proceed toward resolution. Chase Paymentech Operations Center is available 24 x 7 and can be reached at (603) 896-8320.

Error Message Number	Error Message Definition	Status	Action
6782	Batch file name already exists in the database	Error	Fix
6785	User is currently set to inactive in the database	Error	Resend
6787	The sender has sent more then one file per zip	Error	Fix
6799	The name of the zip file and the payload file zipped inside do not match	Error	Fix
6801	Zip file needs to be encrypted	Error	Fix
6810	File name is too long	Error	Fix
6815	Presenter ID is not valid for this user	Error	Fix

END OF THE NETCONNECT BATCH

INTERFACE SPECIFICATION

Version 1.5

09/15/2006