EPX Certification - Credentials

Public - Security Level 0

October 2021

REVISION HISTORY

Date	Version	Author(s)	Comments
5/9/16	2.0	C. Meaney	Reformatting
10/17/16	2.1	C. Meaney	Add Browser Post and EPXPay Semi-Integration to Certifications chapter.
10/20/2021	2.2	M. Billips	Bring up to date, add EPI & Magtek SDK

CONFIDENTIALITY STATEMENT

Contents

List of Tables

EPX Certification Credentials Overview

To certify with EPX, you will be working with the Integration team who will assist you with any issues or questions you might have throughout the integration process. To complete the certification, you are required to submit samples of the requests and successful responses for each type of transaction (TRAN_TYPE) in the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted for certification on a text file and sent via email to the integration team to validate. Once this information is received by the Integration team, it is validated and an Integration specialist will provide feedback if any issues are identified or present your certification letter.

NOTE:

- For EMV integrations, an additional L3 certification process is required with the EPX EMV team and the card brands.
- Only dummy data should be used when integrating and certifying to EPX.

Certifications

Server Post Certification

To complete the Server Post certification, you are required to submit samples of the request POST(s) and successful responses received for each transaction type (TRAN_TYPE) form the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted on a text file and sent via email to the EPX Integration team for review and approval.

EPI (EPX Payment Interface) Certification

To complete the EPI certification, you are required to submit samples of the request POST(s) and successful responses received for each transaction type (endpoint) from the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted on a text file and sent via email to the EPX Integration team for review and approval.

PayPage Certification

To complete the PayPage certification, you are required to submit a sample of the successful KeyExchange and PayPage request POSTs and responses for each transaction type (TRAN_CODE) from the UAP / Test environment that will be supported in the production environment. EPX will also need to validate the custom CSS and JavaScript files along with any associated images used to customize the PayPage. This information should be sent via email to the EPX Integration team for review and approval.

Browser Post Certification

To complete the Browser Post certification, you are required to submit a sample of the successful KeyExchange and Browser Post requests and responses for each transaction type (TRAN_CODE) from the UAP / Test environment that will be supported in the production environment. EPX must also review and certify the custom code that is used for the client side Payment Form. This information should be sent via email to the EPX Integration team for review and approval.

XML Batch File Certification

To complete the XML Batch File certification, you are required to submit a sample of the successful request and response XML files from the UAP / Test environment containing each transaction type (TRAN_TYPE) that will be supported in the production environment. The request and response XML files should be sent via email to the EPX Integration team for review and approval.

EPXPay Semi-Integration Certification

To complete the EPXPay Semi-Integration certification, you are required to submit samples of the request POST to the EPXPay SI device and successful response for each transaction type (TRAN_TYPE) from the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted on a text file and sent via email to EPX Integration team for review and approval. EPX will also need an image* of the actual receipt displaying the required EMV tags and values. (*A sample of the receipt is required only when the actual POS application receipt is in use.)

Magtek SDK (iOS) Certification

To complete the Magtek SDK certification, you are required to submit samples of the request POST(s) and successful responses received for each transaction type form the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted on a text file and sent via email to the EPX Integration team for review and approval.

PayTrans Certification

To complete the PayTrans certification, you are required to submit samples of the request POST(s) and successful responses received for each transaction type (TRAN_TYPE) form the UAP / Test environment that will be supported in the production environment. The requests and responses should be submitted on a text file and sent via email to the EPX Integration team for review and approval.

Address Verification and Interchange Qualification

The Address Verification System (AVS) is a system used to verify the identity of the person claiming to own the credit card. The system will check the billing address and/or the zip code of the credit card provided by the user with the address and/or zip code on file at the credit card company. As described below, in some cases sending AVS will allow the transaction to achieve a better interchange rate when processed.

- Retail (Card Present) transactions where the credit/debit card is present and a chip read or card swipe is performed do not require AVS information to be submitted. The track data and EMV data being supplied alone is sufficient for qualifying for the best possible interchange rate.
- Retail (Card Not Present or Chip / MSR Unreadable) transactions where the credit/debit card information is key entered, it is recommended to include AVS information (ADDRESS and/or ZIP_CODE) to help the transaction qualify for a better interchange rate.
- Card Not Present Ecommerce or MOTO transactions require the AVS information (ADDRESS and/or ZIP_CODE) to be sent in order help qualify for the best possible interchange rate. The attempt to check AVS is sufficient and the AVS response received does not change the interchange qualification of the transaction. It is also recommended to include CVV2 for security purposes.

Setting Max Connection Timeout

When communicating with EPX it is recommended that 35 seconds be set as the merchant timeout value once the connection is established to account for any "out of the norm" issuer behavior. The EPX internal processes are similarly configured to timeout around 33 seconds.

BRIC Lifetime

The EPX BRIC (GUID/Token) received with the response of a financial transaction, such as an authorization, by default have a lifespan of 13 months from creation. For Recurring and Card on File / MIT business models, EPX has introduced the COF_PERIOD API tag that will allow a maximum BRIC lifetime of 24 months and the lifespan will reset to the specified amount of months each time the financial BRIC is used to process a transaction. Please refer to the Card on *File_Recurring_Installment* Transaction Specs and *EPX BRIC Reference* manual for more information.

For those merchants who need the BRIC availability to exceed the 24 month limitation, the BRIC Storage transaction is available and will create BRICs that will be accessible indefinitely. For more information about the usage of BRIC Storage, refer to the *BRIC Storage* Transaction Specs and *EPX BRIC Reference* manual.

Accessing the Certification Environment

This chapter contains information on accessing the certification environment for processing transactions. The following sections contain information on the four part key which defines the merchant's profile, a list of certification URLs that are currently available, testing the ACH and credit card values, the amount response code triggers, and the process for certification.

The EPX integration team will release the 4 part key (CUST_NBR , MERCH_NBR , DBA_NBR , TERMINAL_NBR) and the URL endpoints when the client is ready to begin their implementation.

CAUTION!

DO NOT use real customer data for testing. EPX DOES NOT accept liability for any data submitted to the test environment. The Certification environment merchant accounts are used by all in certification, so any data submitted can potentially be viewed by other merchants in certification. Be sure to use only fictitious account holder data when performing any certification transactions!

Four-Part Key

In the production environment, the four-part key defines the merchant profile down to the terminal level. For certification purposes, *Table 1* below contains a sample of what a 4 part key consists of. The integration team will release the Test / UAP credentials once the integrated client is ready to begin their implementation.

Table 1: Four-part key example

CUST_NBR	MERCH_NBR	DBA_NBR	TERMINAL_NBR
1234	1234567	1	1

Certification URLs

The integration team will release the Test / UAP URL endpoints once the API for implementation is determined. The URLs include the following services:

- Server Post API
- EPI API (EPX Payment Interface)
- PayPage API
- Browser Post API
- XML Batch File API
- EPXPay Semi-Integration

- Magtek SDK (iOS)
- PayTrans API
- webSuite Reporting Portal

Using DNS

When connecting to EPX, it is required to use the DNS rather than the IP address. Redundancy on the EPX side allows for an easy change of Internet Service Providers (ISPs) when there is an issue. EPX uses a short time-to-live (TTL) on the DNS values so that within seconds we can change the IP behind the DNS entry when it is necessary.

In some cases, the merchant will have a firewall in their environment that is blocking outbound access to EPX. In this scenario, the merchant must contact EPX to get the range of IPs so that the EPX smart DNS can work effectively and so that the merchant is not restricted to only one EPX IP address outbound. To obtain the IP address ranges EPX utilizes, send your request to EPX Integration.

Testing Values

Below are values that can be used in the UAP / Test environment to simulate various accounts using credit card, credit card track data, and ACH information. These account numbers will generate approval responses.

ACH

Table 2 contains the test account and routing numbers used when testing the ACH processes.

Table 2: ACH test details

Account Number	Routing Number
1234567890	031100092

Credit Card

Table 3 contains the list of test numbers used with specific card types, and lengths of the test numbers used.

Table 3: Credit card test details

Card Association	Card Number	Length
MasterCard	5000000000000009	16
Visa	4000000000000002	16
Amex	340000000000009	15
Diners	38520000023237	14
Discover	6011499300000005	16
JCB	3530111333300000	16

PIN-Less

Table 4 contains the list of test numbers used with specific card types, and lengths of the test numbers used.

Table 4: PIN-less card test details

Card Association	Card Number	Length
MasterCard	5179080000000006	16
Visa	4000520000000009	16

Track Data

Table 5 contains the list of test card types, numbers, and Track 1 and 2 Data.

NOTE: The Code column indicates the Card Type value that will be returned in the Authorization Response.

Credit Card

Table 5: Credit card track details

Card Type	Code	Card Number	Track 1 and 2 Data		Network
Master Card	M	5000000000000009	1	%B5000000000000009^TEST/MC ^25121010000000000000000?	Master Card
			2	;5000000000000009=251210100000000?	
Visa	V	4000000000000002	1	%B4000000000000002^CARD/VISA ^25121010000000000000?	Visa
			2	;4000000000000002=25121010000000000000?	
Amex	S	340000000000009	1	%B340000000000009^TEST/AMX ^25121010000000000000000?	Amex
			2	;340000000000009=251210100000000?	
Discover	R	6011499300000005	1	%B6011499300000005^TEST/DISCOVER ^25121011000112164301?	Discover
			2	;6011499300000005=25121011000112164301?	