element
payment services™

Express Interface Certification Details

Instructions

Please review and complete the Express Certification Details in the following pages and return to Element Payment Services. The simple step-by-step instructions are outlined below.

1. Please read this entire document thoroughly as this provides important information regarding your integration to the Element Payment Services Express platform.

2. In order to best assist you with your Certification, complete the sections "Certification Test Account Details" and "Software Information".

3. Read and acknowledge the "Important Notifications" section.

4. E-mail this completed document to certification@elementps.com

Certification Test Account Details

Please fill in the details of your Element Express Certification below:

Company/Vendor Name	
Date Submitted (yyyymmdd)	
Application ID (assigned by Element)	
Application Name (e.g. "ABC Software Name")	
Application Version (must be in x.x.x format, e.g."1.1.1")	
Terminal ID(s) (0001 is default assigned by Element for testing; allow this Element-assigned value to be entered by merchant.)	Submit on All requests to EPS
Reference Number (<=16 digits, enter sample used by application)	
Ticket Number (<=6 digits, enter sample used by application)	
Special Notes	* Ensure the TransactionAmount is ALWAYS in a #.## format (e.g. 0.25, 1.50, 3456.25). It should NEVER include commas or the dollar sign. * Ensure appropriate receipts (Retail, E-commerce, etc.) are generated based on provided requirements. * Note that some special characters (e.g. &, <, >, `, ") may not be allowed, depending on the implementation. It is recommended that these characters be replaced (e.g. and for &) or left out entirely.
Software Vendor Compliance Plans (select one if solution is resellable; not applicable to Check/ACH processing)	□ Application is in scope for PA-DSS and will become PA-DSS compliant □ Application using Hosted Payments or other solution for PCI compliance
Integration Interface	□ XML Post □ SOAP Web Service
Software Application Type	□ Distributed Application □ Software-as-a-Service Application (SaaS)
Software Integration Type	□ Hosted Payments □ Direct Integration
Test AccountID (assigned by Element)	
Hardware Certified (if applicable)	

Software Information

Please select the appropriate information regarding functionality supported by your payment application/integration.

Transaction Support

□ Address Verification (AVS)[1] □ Commercial Card Level II □ Commercial Card Level III[2] □ DuplicateCheckDisableFlag

□ DuplicateOverrideFlag □ Card Verification Code (CVV2) □ RecurringFlag □ Partial Approval Support[3]

1: Not including Address and/or Zip Code on keyed transactions may affect interchange.
2: Enhanced Data and Line-Item Detail
3. Required for face-to-face POS Applications. Highly recommended for all other applications.

Hosted Payments Support (select only if utilizing a Hosted Payments integration)

□ Embedded Flag (True) □ AutoReturn Flag (True)

Terminal/Device Support (select for card-present integration; can be Direct or Hosted Payments)

□ Non-Encrypted Reader[1] □ Encrypted Reader □ Encrypted Terminal/PINPad □ Encrypted Keypad Only

□ Encrypted Reader/Keypad □ Stand-alone PINPad (e.g. 1000SE)[1]

1: Not supported with Hosted Payments.

Direct Integration Card Present Support (select for direct card-present integration)

□ Track1Data[1] □ Track2Data[1] □ MagneprintData □ EncryptedTrack1Data

□ EncryptedTrack2Data □ EncryptedCardData

1: Requires PA-DSS (Payment Application) or PCI-DSS (Service Provider) security assessment.

Check/ACH Support (select if implementing Check/ACH processing)

□ Face-to-Face □ Web-E-commerce □ Telephone □ Mail

Certification Test Cards

Use only the following physical test cards or test card numbers during your certification testing on the Test platform.

Note: NEVER use these cards on the Production (live) platform. Using them in Production will prevent your batch from settling, and you will be required to re-key those transactions.

Type	Card Number	Expiration Month	Expiration Year
Visa/Debit	4003000123456781	12	2015
Visa2 (keyed)	4003002345678903	12	2015
MasterCard/Debit	5499990123456781	12	2015
MasterCard2 (keyed)	5499992345678903	12	2015
American Express	373953191351005	9	2015
Discover	6011000990191250	12	2015
Discover2	6011000990191243	12	2015
Discover3	36018634567895	12	2016

Element Express Integration Support

Data Security Policy

When storing, processing, or transmitting sensitive cardholder data, all merchant and vendor interface applications must be compliant with the Payment Card Industry Data Security Standard ("PCI DSS"), the Payment Application Data Security Standard ("PA DSS"), and Visa's Payment Application Best Practices ("PABP") as applicable (collectively the PCI DSS, PA DSS, and PABP shall be known as the "Security Standards"). The PCI DSS and PA DSS are set forth at pcisecuritystandards.org; the PABP is set forth at usa.visa.com. The Security Standards help to ensure that merchants and payment applications do not store prohibited data elements such as full magnetic stripe, CVV2, and PIN data. Please visit the following Visa Web site for additional information (including lists of certified assessors and network scan vendors): http://www.visa.com/cisp

**Suggested Configuration Settings

The Suggested Terminal Settings document (provided by Element) displays several payment scenarios, along with the suggested payment application configuration settings for each. These recommendations should be used as you develop and test your Express-integrated payment application.

**Response Codes and Descriptions

The Response Codes and Descriptions document (provided by Element) provides response codes and their descriptions returned from the Express platform.

**Please email certification@elementps.com to request these documents.

Important Notifications

Acknowledge you have read and understand each notification by selecting the “Accept” checkbox and initialing each section in the table at the bottom of these notifications.

PCI DSS and PA DSS Compliance Notification

All proprietary software should be Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS) compliant. Please visit www.visa.com/cisp to determine application and security requirements.

Visa Operating Regulations

The Visa Operating Regulations are available on the Visa web site at http://usa.visa.com/merchants/operations/op_regulations.html and should be downloaded and reviewed where applicable. The purpose of this document is to provide merchants information on processing transactions, while minimizing risk of loss from fraud and chargebacks.

Transaction Receipt and Web Site Requirements

For card-present certifications, please review the appropriate credit and/or debit card transaction receipt requirements provided by your certification contact. For card-not-present certifications, please review the direct marketing/e-commerce receipts and web page requirements outlined in the card-not-present certification script(s) provided by your certification contact.

Check Processing Compliance Language and Receipt Requirements

When processing checks, the merchant is responsible for handling certain front-end compliance aspects, which include displaying or conveying the appropriate legal language to the customer that meets the NACHA and Fair Credit Reporting Act requirements. It is the merchant's responsibility to ensure they have the most current language. Generally, if there are changes to the authorization consent, merchants will receive a notification of change from their provider.

Please contact your check processing provider representative for full integration documentation and processes related to any front-end compliance verbiage or receipt requirements.

Sale vs Authorization/Completion Notification

When processing card-present and card-not-present transactions, the Sale method should only be used when providing goods or services immediately to the cardholder. Otherwise, if goods or services are not provided immediately, or if an order does not ship immediately, the Authorization method should be used to hold funds, with the Completion being used to charge the card once goods and services are provided or the order has been shipped. For Visa and MasterCard partial completions (where the final amount transaction amount is less than the authorized amount), a partial reversal should also be processed before the completion.

Void Notification

When integrating to the Element Express payment platform, it is requested that the software application support the Void transaction method (CreditCardVoid) for all transaction types, including Voids of Refunds (CreditCardReturn, CreditCardCredit).

Track Data Capture/”Order of Operations” Notification

When processing swiped credit card transactions, the recommended “order of operations” is as follows: Track2 only should be submitted initially; if Track2 cannot be read, then Track1 only should be submitted; if neither track field can be read, the card number should be manually-keyed.

To prevent potential processing issues, only one of the track fields should be submitted per credit card transaction. Do not send both Track2 AND Track1 in the same transaction request.

When processing swiped PIN-secured debit card transactions, the submission of Track2 only is required. It is not possible to manually key the card number during a PIN-secured debit card transaction. If Track2 cannot be read, the software application should request a different form of payment.

Duplicate Checking Notification (Credit, Debit)

By default, all transaction requests submitted through the Express platform will process through duplicate logic. For example, credit card transactions submitted using the same card number (and type) for the same amount and within the same batch will be declined as a duplicate transaction. If the transaction request is valid and should be processed/forced, your software application should handle this scenario by submitting or resubmitting the request and including one of the duplicate flags (DuplicateOverrideFlag, DuplicateCheckDisableFlag) available in the Express interface specification. This is only available on a per-transaction basis; this is not available on a per-account basis. It is recommended that duplicates are handled by using the DuplicateOverrideFlag on necessary transactions, as the DuplicateCheckDisableFlag will bypass ALL duplicate checking on the account, thus increasing merchant risk.

Duplicate Checking Notification (Checks)

Duplicate checking features are determined by the merchant account profile present at the check processing provider. By default, duplicate checking may be turned on at the check processor profile level. Because of this, ACH transactions initiated by the same merchant, on the same account/routing number, for the same amount, and within the same batch may be removed from the ACH batch when processed. These rejected ACH transactions will have a status indicating the processing rejection. It is possible to turn off this duplicate logic by contacting your check processor.

System Reversal Requirements Notification

The reversal methods attempt to reverse a transaction based on specified parameters passed. If a communication error occurs after the Sale, Credit, or Force request has been sent, it is possible that a transaction has been approved, but the merchant may or may not receive a reply. During these types of scenarios, a reversal should be submitted until a “success” or a “not found” response is received. At that time, the original transaction can be resubmitted.

System Reversal Scenarios

1. If a timeout response (RC 1001, 1002) is received from Express, a system reversal should be submitted (until a Not Found or Successful response is returned), and the transaction can then be re-attempted.
2. If no response is received from Express (after 65 seconds), a system reversal should be submitted (until a Not Found or Successful response is returned), and the transaction can then be re-attempted.

NOTE: When submitting reversals, it is recommended that the card number be submitted (and NOT the track data). Reversal programmatic coding can be tested by sending a transaction request, receiving an approval, and then separately sending the reversal request to void the prior transaction. This will verify the reversal request is sent properly. Once the reversal programmatic coding is verified, the reversal logic itself should be verified to ensure that reversals are kicked off at the appropriate times. It should also be noted that system reversals should only be used in the case where no response is received, or where a timeout response is returned. If you wish to reverse a transaction that successfully approved and responded, the full reversal and/or void method may be used.

Full Reversal Requirements Notification

In the event that a cardholder wishes to cancel an Authorization or Sale transaction on the same day, a Full Reversal should be attempted to remove the hold on cardholder funds and remove the transaction from the batch. If the Full Reversal is successful, then no additional action is necessary. If the Full Reversal is unsuccessful, then a Void should be attempted to remove the transaction from the batch.

IP Address Caching Notification

Caching of IP addresses of Element Express is prohibited. For load-balancing and redundancy reasons, Express transaction processing is divided among several data centers. Therefore, the DNS service should be used to determine the destination IP address of Express servers for each transaction. Requests should point to the appropriate URL only (not the IP address).

Implementing SSL Communication

All communication with the Element Express platform is performed via HTTPS. To ensure continuous platform availability via HTTPS, please ensure the software application being certified supports all current SSL Certificate Authorities, and please ensure that operating system, server, and software Certificate Authority updates (for Windows, Linux, AIX, etc.) are regularly performed.

Software Implementation Notification

To create a smooth software implementation as clients sign up with Element Payment Services, it is recommended that the software application being certified allow merchant(s) to key their Express AccountID, AccountToken, AcceptorID, and TerminalID credentials DIRECTLY into the POS or Web software application installed at that merchant location. If you wish to make other arrangements during your client implementation(s), please contact your certification coordinator.

Accepting Live Transactions Notification

After certification is complete, and once live merchant credentials (AccountID, AccountToken, and AcceptorID) have been issued, switching an application from Test mode to Production mode is simply a matter of pointing the application to the Element Express live Production URL and exchanging the Test server credentials for live Production credentials. The ApplicationID, ApplicationName, and ApplicationVersion, however, are bound to the application, and should not change between test and live modes. When an account is ready for live transaction processing, the Production URL is accessible by removing the word "test" or "cert" from the URL used during testing and certification.

Validation Code Comparison Logic to Mitigate Fraud Risk (applicable to Hosted Payments only)

URL Spoofing is the process by which a return parameter in the redirect URL query string can be modified so that an initially-declined transaction appears successful, thus allowing the merchant to potentially fulfill a fraudulent order. Important: URL Spoofing does NOT put cardholder data at risk.

Software vendors and merchants can now take advantage of a security enhancement that will mitigate the risk associated with this type of URL spoofing. The Hosted Payments interface will now automatically return an additional Validation Code.

- The Validation Code will be returned as a response parameter to the TransactionSetup request method.
- The Validation Code will be returned during the redirect to the ReturnURL as an additional appended name/value pair once the Hosted Payments transaction has completed.

This Validation Code should be captured as part of the response initiated by the TransactionSetup request, and it should be compared to the Validation Code that is returned from the appended values in the ReturnURL when redirecting back to the application after a successful Hosted Payments transaction. If the Validation Code values from both responses match, then it can be confirmed that the response data was returned directly from Element. If the Validation Code values from both responses do not match, then this indicates that the response data is not accurate and the merchant should not proceed with providing a product or service to the user. For your benefit, it is strongly recommended that you take advantage of this Hosted Payments security enhancement by implementing this comparison functionality.

Browser Support via Hosted Payments

It is recommended that only the Internet Explorer (PC) or Firefox (PC or Mac) browser be used within any application processing transactions via the Hosted Payments solution.

Notification Acknowledgment

Notification Acknowledgement	Accept	Initials
PCI DSS and PA DSS Compliance Notification (Credit, Debit)	□	
Visa Operating Regulations (Credit, Debit)	□	
Transaction Receipt and Web Site Requirements	□	
Check Processing Compliance Language and Receipt Requirements (Checks)	□	
Sales vs Authorization/Completion Notification (Credit, Debit)	□	
Void Notification (Credit, Checks)	□	
Track Data Capture/"Order of Operations" Notification (Credit, Debit)	□	
Duplicate Checking Notification (Credit, Debit)	□	
Duplicate Checking Notification (Checks)	□	
System Reversal Requirements Notification (All)	□	
Full Reversal Requirements Notification (Credit, Debit)	□	
IP Address Caching Notification (All)	□	
Implementing SSL Communication (All)	□	
Software Implementation Notification (All)	□	
Accepting Live Transactions Notification (All)	□	
Validation Code Comparison Logic to Mitigate Fraud Risk (Hosted Payments)	□	
Browser Support via Hosted Payments (Hosted Payments)	□	

INTEGRATION NOTES (FOR ELEMENT USE ONLY)

Integration & Receipt Notes	
Methods Certifying:	