Real-Time XML API

Document Version:	1.2.20
Issue Date:	March 2 2020

Table of Contents

Introduction 3
Test Account Information 3
XML Interface 4
Creating an XML request 5
The Request Structure 5
Adding Order Detail 6
Adding Custom Descriptors 6
Adding Item Detail 7
Adding Item Options 8
Adding Coupon Detail 9
Adding Fraud Checking Detail 10
Adding Level 2 Card Data Detail 11
Creating an Order using Track 2 (Magnetic Stripe) Data 12
Creating an Order using the payment details of a previous Order 12
Adding Split-Funding Instructions 13
Adding Split-Funding Refund Instructions (Credit Requests Only) 14
Adding Stored Credential Information 15
Adding Custom Merchant Data 16
Adding Airline Ticket Detail 17
The Response Structure 18
Payment Types 19
Payment Type – Credit Card 19
Payment Type – Visa Debit Card (Hybrid cards) 19
Payment Type – Interac Online 19
Request Types (AKA. Card Actions) 20
Sale 20
PreAuth 20
PostAuth 20
Credit (Refund) 21
Forced PostAuth 21
Extended PostAuth 21
Pure Credit 22
Void 22
Request Elements 23
Common Request Elements 23
Sale Elements 24
PreAuth Elements 26
PostAuth Elements 27
Credit (Refund) Elements 28
Forced PostAuth Elements 29
Extended PostAuth Elements 30
Pure Credit Elements 31
Void Elements 31
Additional Authorization Elements 32
Airline Ticket Elements 34
Detailed Element List – Credit Card Payment 35
Detailed Element List – Item Elements 37
Detailed Element List – Option Elements 37
Result Elements 38
Result Elements – Payment Type: All 38
Result Elements – Payment Type: Credit Card & Visa Debit Card 40
Appendix A – Validation of fields containing credit card data 42
Appendix B – Sample of PSiGate Welcome kit 43
Appendix C – List of Test Credit Card Numbers 44
Appendix D – Connection Troubleshooting Guide 45
Appendix E – Simulating AVS and Card ID responses 46

Introduction

PSiGate specializes in the integration and deployment of e-commerce payment service solutions. PSiGate's payment solutions enable automated and secure authorization and fulfillment of credit card transactions. PSiGate communicates directly with major Canadian and U.S. credit card financial institutions and supports businesses that wish to deploy an online storefront.

This document provides merchants and their affiliates with the tools to integrate PSiGate's ***XML Messenger Interface*** so that PSiGate may process their transaction requests.

Note: PSiGate's ***XML Messenger Interface*** supports only credit card payment processing

Test Account Information

PSiGate's testing environment supports a shared test account that you are welcome to use while you develop and test your interface.

IMPORTANT:

- *Do **NOT** use real credit card numbers within the test environment.*
- *When you are ready to go live, refer to the Welcome kit the merchant should have received when their gateway account (store) was configured to get the Realtime XML production URL you will need to process live transactions.*

Send test transactions to: https://realtimestaging.psigate.com/xml

To process a transaction through the test account, pass the following control element values within your transaction requests:

StoreID: `teststore`
Passphrase: `psigate1234`

To review your test transactions, log into https://staging.psigate.com/MerchantTools/Login/login with the following account information:

CID: `1000001`
User: `teststore`
Pass: `Testpass1234`

If you require an unshared test account, send an e-mail to support@psigate.com and we shall do our best to supply the test account within one week of your request.

XML Interface

The XML Interface transfers data securely from a merchant's host server to PSiGate's transaction server.

Development/Production Network Requirements:

- Ability to communicate across the standard HTTPS port 443
- Ability to process transactions using encryption protocol TLS 1.1 or better

Creating an XML request

The Request Structure

The ***XML Messenger Interface*** receives transaction requests sent by the Merchant. The transaction requests are then forwarded to PSiGate's payment engine for real-time processing. An *Order* element encloses each XML transaction request, meaning that the request must begin with <Order> and end with </Order>. Each transaction request consists of transaction elements that define the request. The minimum number of transaction elements needed to successfully transmit an order depends on the type of transaction request.

Note: The ampersand symbol ("&") is not a valid character and will cause an error if inputted within any element of the XML request. Please encode any special characters you wish to transmit to the XML Messenger Interface.

The following is an example of a basic **Sale** transaction request:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
        <StoreID>teststore</StoreID>
        <Passphrase>psigate1234</Passphrase>
        <Subtotal>10.00</Subtotal>
        <PaymentType>CC</PaymentType>
        <CardAction>0</CardAction>
        <CardNumber>4111111111111111</CardNumber>
        <CardExpMonth>02</CardExpMonth>
        <CardExpYear>08</CardExpYear>
        <CardIDNumber>3422</CardIDNumber>
</Order>
```

This request processes a **Sale** transaction in the "**teststore"** account for ten dollars and applies the charge to the credit card number "4111111111111111" whose expiration date is "02/08". The value of the *SubTotal* element is the dollar amount to charge the card. The value of the *PaymentType* element, which is set to "CC" (credit card) in the above example, establishes the payment context. The value of the *CardAction* element, which is set to "0" (**Sale** transaction) in the above example, determines the type of transaction request. The values of the *CardNumber*, *CardExpMonth* and *CardExpYear* elements set the credit card details. The value of the *CardIDNumber* element tells the payment engine to verify that "3422" is the security code printed on the card. For a list of the elements required for each transaction type, please refer to the ***XML Interface - Request Elements*** table.

Adding Order Detail

Add more order detail to a request by including additional *Request Elements*. For a complete list of recognized *Request Elements*, refer to the ***XML Interface Detailed Element Listing – General Request Elements*** table.

The following is an example of a Sale transaction with additional order detail:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Bname>John Smith</Bname>
	<Bcompany>PSiGate</Bcompany>
	<Baddress1>123 Main St.</Baddress1>
	<Baddress2>Apt 6</Baddress2>
	<Bcity>Toronto</Bcity>
	<Bprovince>Ontario</Bprovince>
	<Bpostalcode>L5N2B3</Bpostalcode>
	<Bcountry>Canada</Bcountry>
	<Phone>416-555-2092</Phone>
	<Fax>416-555-2091</Fax>
	<Email>someone@somewhere.com</Email>
	<Comments>No comments today</Comments>
	<Tax1>5.00</Tax1>
	<ShippingTotal>5.00</ShippingTotal>
	<Subtotal>10.00</Subtotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<CardNumber>4111111111111111</CardNumber>
	<CardExpMonth>02</CardExpMonth>
	<CardExpYear>08</CardExpYear>
	<CardIDNumber>3422</CardIDNumber>
</Order>
```

This request includes additional billing information, payment information and comments which allows merchants to capture more information about their customers' purchases.

Adding Custom Descriptors

The descriptor on the cardholder statement may be customized to help identify transactions with recognizable details, order numbers, or customer references. For clarity, include a portion of the merchant name.

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Subtotal>10.00</Subtotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<CardNumber>4111111111111111</CardNumber>
	<CardExpMonth>02</CardExpMonth>
	<CardExpYear>08</CardExpYear>
	<CardIDNumber>3422</CardIDNumber>
	<MerchantName>The Store Name</MerchantName>
</Order>
```

This request includes a *MerchantName* value that replaces the default descriptor in the merchant profile.

Adding Item Detail

Add item details within your transaction requests by including *Item* elements. The *Item* elements will display in your online reports and email receipts. We list the predefined sub elements of the *Item* elements in the ***XML Interface Detailed Element Listing – Item Elements*** table***.***

Note: If your transaction request includes item detail, we will calculate the *Subtotal* value from *ItemPrice* and *ItemQty* values.

Note: If you include the *Subtotal* element within a transaction request, the derived item detail *Subtotal* amount will supersede the amount given in the *Subtotal* element.

The following is an example of a Sale transaction with **item detail**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Bname>John Smith</Bname>
	<Bcompany>PSiGate</Bcompany>
	<Baddress1>123 Main St.</Baddress1>
	<Baddress2>Apt 6</Baddress2>
	<Bcity>Toronto</Bcity>
	<Bprovince>Ontario</Bprovince>
	<Bpostalcode>L5N2B3</Bpostalcode>
	<Bcountry>Canada</Bcountry>
	<Phone>416-555-2092</Phone>
	<Fax>416-555-2091</Fax>
	<Email>someone@somewhere.com</Email>
	<Comments>No comments today</Comments>
	<Item>
		<ItemID>PSI-BOOK</ItemID>
		<ItemDescription>XML Interface Doc</ItemDescription>
		<ItemQty>2</ItemQty>
		<ItemPrice>10.00</ItemPrice>
	</Item>
	<Tax1>5.00</Tax1>
	<ShippingTotal>5.00</ShippingTotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<CardNumber>4111111111111111</CardNumber>
	<CardExpMonth>02</CardExpMonth>
	<CardExpYear>08</CardExpYear>
	<CardIDNumber>3422</CardIDNumber>
</Order>
```

This request adds a single item identified as “PSI-BOOK” to the order. The *Subtotal* value automatically becomes a *Subtotal* amount of $20.00, derived from the multiplication of the *ItemQty* which is “2” and the *ItemPrice* which is “$10.00”.

Adding Item Options

Additionally, you may require customized item descriptors.

You may add item options such as colour, size or weight to describe an item's details.

The following is an example of a Sale transaction with **item detail and item options**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Bname>John Smith</Bname>
	<Bcompany>PSiGate</Bcompany>
	<Baddress1>123 Main St.</Baddress1>
	<Baddress2>Apt 6</Baddress2>
	<Bcity>Toronto</Bcity>
	<Bprovince>Ontario</Bprovince>
	<Bpostalcode>L5N2B3</Bpostalcode>
	<Bcountry>Canada</Bcountry>
	<Phone>416-555-2092</Phone>
	<Fax>416-555-2091</Fax>
	<Email>someone@somewhere.com</Email>
	<Comments>No comments today</Comments>
	<Item>
		<ItemID>PSI-BOOK</ItemID>
		<ItemDescription>XML Interface Doc</ItemDescription>
		<ItemQty>2</ItemQty>
		<ItemPrice>10.00</ItemPrice>
		<Option>
			<Type>Electronic</Type>
			<url>http://www.psigate.com/docs/</url>
			<file>XML.doc</file>
		</Option>
	</Item>
	<Tax1>5.00</Tax1>
	<ShippingTotal>5.00</ShippingTotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<CardNumber>4111111111111111</CardNumber>
	<CardExpMonth>02</CardExpMonth>
	<CardExpYear>08</CardExpYear>
	<CardIDNumber>3422</CardIDNumber>
</Order>
```

The *Option* sub elements, "*Type*", "*url*" and "*file*" are **not** predefined. PSiGate will recognize the inputted string of an *Option* sub element as the option name and the inputted string that is enclosed by the *Option* sub element as the option value. For example, if <Colour>Red</Colour> was included as an *Option* sub element, the option name would be "Colour" and its value would be "Red".

Adding Coupon Detail

Coupons may be applied by including an additional item that has a negative *ItemPrice* dollar value. The coupon value is then subtracted from the total dollar value of all items prior to processing a card authorization.

The following is an example of a basic Sale transaction request with **item and coupon details**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<CardNumber>4111111111111111</CardNumber>
	<CardExpMonth>02</CardExpMonth>
	<CardExpYear>08</CardExpYear>
	<Item>
		<ItemID>PSI-BOOK</ItemID>
		<ItemDescription>XML Interface Doc</ItemDescription>
		<ItemQty>2</ItemQty>
		<ItemPrice>10.00</ItemPrice>
	</Item>
	<Item>
		<ItemID>COUPON</ItemID>
		<ItemDescription>10% discount</ItemDescription>
		<ItemQty>1</ItemQty>
		<ItemPrice>-2.00</ItemPrice>
	</Item>
</Order>
```

This request includes a negative dollar amount for one of the items. The payment engine allows negative dollar amounts for individual items as long as the entire order is for a positive dollar amount.

Note: If the coupon is a percentage of the order total, you must calculate the coupon amount and send the amount as a negative value to apply to the order total.

Adding Fraud Checking Detail

To fully utilize this payment engine's fraud checking capabilities, you must include credit card verification data (CVV2, CVC2, etc.); address verification data and the customer's IP address. For a complete list of Fraud checking responses, refer ***to Result Elements – Payment Type: Credit Card***.

The following is an example of a Sale transaction with additional fraud-checking detail:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
        <StoreID>teststore</StoreID>
        <Passphrase>psigate1234</Passphrase>
        <Baddress1>123 Main St.</Baddress1>
        <Bcity>Toronto</Bcity>
        <Bprovince>Ontario</Bprovince>
        <Bpostalcode>L5N2B3</Bpostalcode>
        <Bcountry>Canada</Bcountry>
        <CustomerIP>192.0.10.55</CustomerIP>
        <CardIDNumber>3422</CardIDNumber>
        <Subtotal>10.00</Subtotal>
        <PaymentType>CC</PaymentType>
        <CardAction>0</CardAction>
        <CardNumber>4111111111111111</CardNumber>
        <CardExpMonth>02</CardExpMonth>
        <CardExpYear>08</CardExpYear>
</Order>
```

This request sends the customer's IP address and security number (3 or 4 digit number found on the front/back of the credit card) to PSiGate's payment engine for verification.

The *CardIDNumber* element verifies that the customer has correctly inputted the card's security number; the *Baddress1* and *Bpostalcode* elements verify that the inputted street number and postal code match that on record with the issuing bank; the *CustomerIP* element verifies that the inputted city, province and postal code match their machine's city, state/province and country. The payment engine returns its Card verification response within the *CardIDResult* response element, the Address verification response within the *AVSResult* response element and the GeoIP response within the *IPResult*, *IPCity, IPRegion* and *IPCountry* response elements. PSiGate compares the IP location responses to the inputted *Bcity*, *Bprovince* and *Bcountry*.

Adding Level 2 Card Data Detail

Visa and Mastercard created a specialized type of credit card used primarily by government agencies and businesses. Businesses that accept these cards enable their government or corporate clients to include special purchase information (level 2 card data) that will help the government agency or corporation reconcile the transaction. In exchange for enabling Level 2 Card data acceptance, merchants receive their funds quicker, pay lower fees, and have a greater chance of winning government contracts where purchasing cards are the required form of payment.

The following is an example of a basic Sale transaction request with additional **Level 2 card data**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
        <StoreID>teststore</StoreID>
        <Passphrase>psigate1234</Passphrase>
        <Subtotal>10.00</Subtotal>
        <PaymentType>CC</PaymentType>
        <CardAction>0</CardAction>
        <CardNumber>4111111111111111</CardNumber>
        <CardExpMonth>02</CardExpMonth>
        <CardExpYear>08</CardExpYear>
        <CardLevel2ComCardType>B</CardLevel2ComCardType>
        <CardLevel2PO>Order 18</CardLevel2PO>
        <CardLevel2Tax>15.00</CardLevel2Tax>
</Order>
```

This request informs the card-issuing bank that the Credit Card type is “business”, the purchase order information is “Order 18” and the total sales tax applied to the order is fifteen dollars. The card-issuing bank may display this information on your customer’s credit card statement.

Note: Some card-issuing banks require Card Level 2 data.

Creating an Order using Track 2 (Magnetic Stripe) Data

There are up to three tracks on magnetic cards known as tracks 1, 2, and 3. Track 3 is virtually unused by the major worldwide networks, and often isn't even physically present on the card by virtue of a narrower magnetic stripe. Point-of-sale card readers almost always read track 1, or track 2, and sometimes both, in case one track is unreadable. The minimum cardholder account information needed to complete a transaction is present on both tracks. The Track 2 format was developed by the banking industry (ABA) and was written with a 5-bit scheme (4 data bits + 1 parity), which allows for sixteen possible characters, which are the numbers 0-9, plus the six characters : ; < = > ? .

We are able to process credit card requests if the TrackII field is passed instead of the CardNumber, CardExpMonth and CardExpYear fields.

The following is an example of a basic **Sale** transaction request with additional **Track 2 data**:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Subtotal>10.00</Subtotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<TrackII>;4005550000000019=99011200XXXX00000000?*</TrackII>
</Order>
```

This request uses the Track2 data retrieved from swiping a customer's credit card through a point-of-sale reader to get an authorization for the customer's purchase.

Creating an Order using the payment details of a previous Order

Merchants that need to reprocess their customers card, may do so by referencing the OrderID of a previously authorized order belonging to the customer they need to recharge.

We can process credit card requests if the OrderID of a previous order is submitted within the request. Please note that when you do this, do not also send us payment details as that will produce an error.

The following is an example of a basic **Sale** transaction request that uses the payment details of a previous order:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Subtotal>10.00</Subtotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>
	<PreOrderID>20190301145115O1568</PreOrderID>
</Order>
```

Adding Split-Funding Instructions

Split Funding allows merchants to distribute transaction funds across multiple stores without the cardholder receiving multiple billing line items.

For example: Multiple vendors, or convenience fees, taxes, and reserve amounts. (*A single transaction of $100, with $5 being deposited to a convenience fee account, and the remaining $95 deposited to a merchant account.*)

Prerequisites:

- All stores must be active.
- All stores must share the same Client ID.
- Split Funding is enabled (contact Merchant Services).
- The full total must equal the sum of the split amounts.

To create a transaction request with Split Funding that divides a subtotal of $100.00 (store01 receives $95.00, and store02 receives $5.00), use the following sample code:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
    <StoreID>store01</StoreID>
    <Passphrase>psigate1234</Passphrase>
    <Subtotal>100.00</Subtotal>
    <PaymentType>CC</PaymentType>
    <CardAction>0</CardAction>
    <SplitFunded>
        <SplitPart>
            <StoreID>store01</StoreID>
            <SplitAmount>95.00</SplitAmount>
        </SplitPart>
        <SplitPart>
            <StoreID>store02</StoreID>
            <SplitAmount>5.00</SplitAmount>
        </SplitPart>
    </SplitFunded>
</Order>
```

Adding Split-Funding Refund Instructions (Credit Requests Only)

Return funds to the cardholder from all stores involved in a Split Funding transaction.

For example: Cardholder disputes or transaction amount corrections. (*A refund of $5 from a convenience fee account and $95 from the merchant account returns $100 to the cardholder.*)

Prerequisites:

- All stores must be active.
- All stores must share the same Client ID.
- Split Funding is enabled (contact Merchant Services).
- The full total of the refund request must equal the sum total of the split amounts.
- The full total of the refund cannot exceed the full total of the original order.
- The split amount for each store cannot exceed the original split amount for that store.
- Refunds may only occur once.

To create a refund after Split Funding that returns a subtotal of $100.00 (store01 refunds $95.00, and store02 refunds $5.00), use the following sample code:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
    <StoreID>store01</StoreID>
    <Passphrase>psigate1234</Passphrase>
    <Subtotal>100.00</Subtotal>
    <PaymentType>CC</PaymentType>
    <CardAction>3</CardAction>
    <OrderID>20171201093710059 85</OrderID>
    <SplitFunded>
        <SplitPart>
            <StoreID>store01</StoreID>
            <SplitAmount>95.00</SplitAmount>
        </SplitPart>
        <SplitPart>
            <StoreID>store02</StoreID>
            <SplitAmount>5.00</SplitAmount>
        </SplitPart>
    </SplitFunded>
</Order>
```

Note: The full total will be refunded from the store assigned to the StoreID value if there is no SplitFunded element.

Adding Stored Credential Information

Visa and Mastercard introduced a new framework for merchant or cardholder-initiated transactions that include stored credentials. PSiGate merchants are required to comply with all Card Brand Rules and Regulations including this mandate which became effective on April 30, 2018.

The framework defines the rules and requirements for initial storage and subsequent use of payment credentials. Merchants are required to establish a consent agreement with the cardholder prior to storing credentials for future use. Stored credentials are defined as information that is stored by a merchant, a merchant's agent, a Payment Facilitator or a Staged Digital Wallet Operator to process future purchases for a cardholder.

In addition to disclosing to cardholders how their credentials will be used, obtaining cardholder's consent to store their credentials, and notifying cardholders when any changes are made to the terms of use, merchants are required to inform issuers when payment credentials are stored on file, the type of agreement the merchant has with the cardholder and whether the transaction was an initial purchase or subsequent purchase.

To indicate the type of agreement, you must include the "Recurring" element within your transaction requests, where a value of:

- "Y" indicates a Recurring payment, which is one of many transactions processed at predetermined intervals that do not exceed one year between transactions, and represents an agreement between the cardholder and merchant to purchase goods or services over an undefined period.
- "I" indicates an Installment payment, which is part of a series of transactions processed at predetermined intervals that do not exceed one year between transactions, has a defined end date and represents an agreement between the cardholder and merchant to purchase a single good or service.
- "C" indicates a Credentials on file payment, which is a transaction initiated by a merchant using payment credentials the cardholder previously permitted the merchant to store.
- "T" indicates a Cardholder-initiated recurring payment, which is a transaction initiated by a cardholder to purchase a good or service from a merchant. For example, the cardholder orders a magazine subscription from the merchant website.

The following is an example of a basic **Sale** transaction request with additional **Stored Credential** information:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
       <StoreID>teststore</StoreID>
       <Passphrase>psigate1234</Passphrase>
       <Subtotal>10.00</Subtotal>
       <PaymentType>CC</PaymentType>
       <CardAction>0</CardAction>
       <CardNumber>4111111111111111</CardNumber>
       <CardExpMonth>02</CardExpMonth>
       <CardExpYear>08</CardExpYear>
       <CardIDNumber>3422</CardIDNumber>
       <Recurring>Y</Recurring>
       <Iteration>1</Iteration>
</Order>
```

For merchants to comply with the Stored Credential Transaction Framework, merchants may need to complete some development work. Merchants that do not store customer payment credentials are not required to include Stored Credential information within their Pre-authorization or Sale requests.

For more information on the Stored Credential Transaction Framework, please review information made available by Visa on the subject at: https://usa.visa.com/dam/VCOM/global/support-legal/documents/stored-credentialtransaction-framework-vbs-10-may-17.pdf.

Adding Custom Merchant Data

The following is an example of a basic **Sale** transaction request with customized data that the merchant wishes returned within the ThanksURL or NoThanksURL response.

Sample Post:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
    <StoreID>store01</StoreID>
    <Passphrase>psigate1234</Passphrase>
    <Subtotal>100.00</Subtotal>
    <PaymentType>CC</PaymentType>
    <CardAction>0</CardAction>
    <OrderID>Smith0123</OrderID>
    <UserID>jsmith</UserID>
    <Comments>I am stored and displayed</Comments>
    <Description>I can be displayed only</Description>
    <CustomerRefNo>Monday Evening Muay Thai Classes</CustomerRefNo>
</Order>
```

There are several variables that a merchant can use to customize the way they view or find records in the reports.

The *OrderID*, *UserID, Comments, Description or CustomerRefNo* variables are the primary way to do this.

XML Tag	Returned	Reported in MT	Stored	Email	# of Chars.
OrderID (CC)	Yes	Yes	Yes	Yes	100
OrderID (DB)	Yes	Yes	Yes	Yes	20
UserID	No	Yes	Yes	Yes	64
Comments	No	Yes	Yes	Yes	300
Description	No	No	No	No	64
CustomerRefNo	Yes	No	No	No	25

If you do not pass an *OrderID*, PSiGate will automatically generate one for you. This is the primary way PSiGate identifies orders.

Adding Airline Ticket Detail

Government agencies and businesses may include airline ticket details to maintain data on travel purchased with company credit cards.

The following is an example including the airline ticket details:

```
<?xml version="1.0" encoding="UTF-8"?>
<Order>
	<StoreID>teststore</StoreID>
	<Passphrase>psigate1234</Passphrase>
	<Subtotal>10.00</Subtotal>
	<PaymentType>CC</PaymentType>
	<CardAction>0</CardAction>

	<AirlineTicket>
		<TicketNum>NRJ0123456789</TicketNum>
		<PassengerName>John Smith</PassengerName>
		<DepartureDate>20190530</DepartureDate>
		<AirportCode>YYZ</AirportCode>
		<TicketCarrierCode>014</TicketCarrierCode>
		<TicketCarrierName>NORTHJET</TicketCarrierName>
		<TransType>TKT</TransType>
		<DocumentType>01</DocumentType>
		<IssuingCity>TORONTO</IssuingCity>
		<IssuingDate>20190316</IssuingDate>
		<PurchaseAmt>65</PurchaseAmt>
		<NumberInParty>1</NumberInParty>
		<ConjunctionInd>N</ConjunctionInd>
		<ElectronicInd>Y</ElectronicInd>
		<AirlineTrip>
			<CarrierCode>NJ</CarrierCode>
			<ServiceClass>B</ServiceClass>
			<DepartureDate>20190530</DepartureDate>
			<DepartureCity>YYZ</DepartureCity>
			<ArrivalCity>YTZ</ArrivalCity>
			<FlightNum>88</FlightNum>
			<FareBasis>M</FareBasis>
		</AirlineTrip>
	</AirlineTicket>
</Order>
```

The Response Structure

PSiGate's payment engine will return a formatted XML response to any server that sends a transaction request to the ***XML Messenger Interface***. A *Result* element will envelop the response.

The following is an example of a formatted XML response:

```
<?xml version="1.0" encoding="UTF-8"?>
<Result>
        <TransTime>Mon Nov 08 20:21:06 PST 2004</TransTime>
        <OrderID>20041108202106051 47</OrderID>
        <Approved>APPROVED</Approved>
        <ReturnCode>Y:TEST:TESTTRANS:M:X:YYY</ReturnCode>
        <ErrMsg></ErrMsg>
        <TaxTotal>5.00</TaxTotal>
        <ShipTotal>15.00</ShipTotal>
        <SubTotal>55.00</SubTotal>
        <FullTotal>75.00</FullTotal>
        <PaymentType>CC</PaymentType>
        <CardNumber>411111...1111</CardNumber>
        <CardExpMonth>05</CardExpMonth>
        <CardExpYear>07</CardExpYear>
        <TransRefNumber>1bd0082c392b7c5b</TransRefNumber>
        <CardIDResult>M</CardIDResult>
        <AVSResult>X</AVSResult>
        <CardAuthNumber>TEST</CardAuthNumber>
        <CardRefNumber>TESTTRANS</CardRefNumber>
        <CardType>VISA</CardType>
        <IPResult>YYY</IPResult>
        <IPCountry>CA</IPCountry>
        <IPRegion>Ontario</IPRegion>
        <IPCity>Toronto</IPCity>
</Result>
```

The bolded elements are common to all payment types. The italicized values are specific to the credit card payment type. Please refer to the Result Elements – Payment Type Credit Card table for more details regarding the credit card payment type return values. The Approved sub element indicates the success of the transaction request. If the Approved sub element returned any value other than "APPROVED", the transaction request was unsuccessful. Please refer to the Result Elements – Common Elements table for more details regarding other possible return values for the Approved sub element.

Payment Types

Payment Type – Credit Card

Credit Cards issued by credit card providers allow card holders to pay for goods and services based on the card holder's promise to pay back the card issuer.

All API requests within this document support this payment type.

Payment Type – Visa Debit Card (Hybrid cards)

Visa Debit is a payment option which allows card holders to safely pay for goods and services directly from their bank account. Unlike a normal debit card, these hybrid cards are accepted more frequently when you shop online or around the world because it uses the VISA network.

Card holders who use their Visa Debit card online are protected with Visa Layers of Security including Zero Liability and the Visa E-Promise.

To accept your customers' Visa Debit cards, you must send an email to merchant.services@psigate.com to request that Visa Debit acceptance is enabled on your store.

Please note the following differences in the way Visa Debit card transactions are handled versus credit card transactions.

- Visa Debit card transactions cannot be pre-authorized since there is never a situation in which funds are not captured. Since funds are not reserved, PSiGate will convert any *PreAuth* requests involving Visa Debit cards to *Sale* requests prior to the request being processed by our gateway.
- You may not void Visa Debit card orders. You may only credit (refund) orders involving Visa Debit cards.
- To distinguish Visa Debit card transactions from credit card transactions, look for "VISADEBIT" to be returned within the *DebitType* element.

Payment Type – Interac Online

The Interac Online service is a payment option that allows clients to securely pay for goods and services directly from their bank account through the internet. Interac Online purchase requests cannot be processed through the Realtime XML API since the client's browser is required to redirect to their online bank account. Interac Online Refund requests, on the other hand, may be processed through the Realtime XML API. To do this, submit a Credit Request with the PaymentType element equal to "DB" instead of "CC".

Request Types (AKA. Card Actions)

Sale

Sale transactions (*CardAction* = 0) authorize and capture funds in a single transaction. Merchants perform *Sale* transactions when services or products are immediately delivered such as with software download or service membership.

PreAuth

PreAuth transactions (*CardAction* = 1) authorize and reserve funds, but do not capture funds unless you issue a PostAuth transaction request that corresponds with the PreAuth. Merchants perform PreAuth transactions when services or products are not immediately delivered such as with most physical goods. Card issuers will reserve the authorized amount for at least five days.

Verify Account Request

If a PreAuth request is submitted with a total dollar amount of zero dollars ($0.00), it will be considered to be a Verify Account request. Verify Account requests will not reserve an authorized amount, but will verify that the account is in good standing and return the AVS, CVV and GeoIP responses as in the case of a regular PreAuth request.

PostAuth

PostAuth transactions (*CardAction* = 2) capture funds that were reserved by previous PreAuth transactions. Merchants perform PostAuth transactions when they initiate the delivery of the associated service or product. In the case of physical goods, you may only issue PostAuth transactions once the product has been shipped or prepared for shipment.

PostAuth - PSiGate will capture the full amount of the associated PreAuth transaction when you issue a PostAuth transaction with no *SubTotal* value.

Partial PostAuth - PSiGate will capture an amount less than the full amount of the associated PreAuth transaction when you issue a PostAuth transaction with a *SubTotal* value less than the amount indicated within the *SubTotal* of the PreAuth transaction.

Note: PSiGate's reporting tool includes PostAuth functionality; however you may also decide to program PostAuth functionality into your own reporting tool. If you do include PostAuth functionality, you will need to enable the PostAuth real-time restriction within your "CC Fraud Settings" panel of your online ***Merchant Tools***.

Credit (Refund)

Credit transactions (*CardAction* = 3) debit the merchant's account and credit the account of their client. Merchants perform Credit transactions to refund their customers. You can issue multiple Credit transaction requests so long as the sum of those transactions does not exceed the amount of the approved Sale or PostAuth transaction. If the total amount of credits equals the amount of approved Sale or PostAuth transaction, the order will be cancelled. Merchants may now refund clients whose accounts were originally debited via the Interac Online purchase request offered through PSiGate's Realtime HTML API.

Forced PostAuth

Forced PostAuth transactions (*CardAction* = 4) capture funds based on an authorization number that was previously obtained from PSiGate or from outside of PSiGate. Example: Merchant authorizes a transaction through the authorization center of their merchant-issuing bank. Merchant performs a Forced PostAuth transaction to settle the already authorized transaction.

***Warning*:** The financial institution will reverse a Forced PostAuth transaction if its amount does not equal the amount that was previously authorized.

Extended PostAuth

Extended PostAuth transactions (*CardAction* = 6) capture funds that were previously authorized by PreAuth transactions whose reservation of those funds has expired.

Note: If you use an Extended PostAuth transaction request to capture funds, the transaction will be considered a non-qualified order by your merchant account provider which could cause the discount rate charged to you to be nominally higher. To determine your qualified and non-qualified discount rate, please contact your merchant account provider.

Note: When capturing funds for sold physical goods, VISA/MC regulations state that merchants should only capture funds once the product has been shipped or is in the process of being shipped.

Note: PSiGate's reporting tool includes this functionality by way of a Forced Confirm Selected Orders button within the Confirm Orders screen. You may also decide to program this functionality into your own reporting tool. If you do, you will need to enable the PostAuth real-time restriction within your "CC Fraud Settings" panel of your online ***Merchant Tools***.

Pure Credit

Pure Credit transactions (*CardAction* = 8) debit the merchant's account and credit the account of the cardholder. Unlike, Credit transaction requests, Pure Credit transaction requests do not reference a pre-existing order. Merchants must request special permission to issue Pure Credit transaction requests within a store. Those merchants who are granted Pure Credit permissions can refund their customers up to an agreed upon refund limit.

Void

Void transactions (*CardAction* = 9) cancel the effect of a previous transaction. Merchants perform Void transaction requests to reverse a PostAuth, Sale or Credit transaction and to prevent a transaction record from displaying on a customer's credit card statement. Example: A Sale followed by a Credit would appear as two separate transactions on a cardholder's statement. A Sale followed by a Void would result in neither transaction appearing on the cardholder's statement. The limitation of a Void transaction is that you cannot void a transaction that has already been settled.

Note: Transactions are settled at midnight by default.

Request Elements

Common Request Elements

All requests require the following elements:

Element	Example	Description
StoreID	`Teststore`	PSiGate provides the *StoreID* within the ***PSiGate Welcome kit***. **Note:** *StoreID* is unique and case sensitive.
Passphrase	`Testpass`	PSiGate provides the *Passphrase* within the ***PSiGate Welcome kit***. **Note:** *Passphrase* is case sensitive.
PaymentType	`CC`	Indicates the chosen payment method. **CC** – Credit Card **Note:** Currently, only the credit card payment method is available real-time.
CardAction	`0, 1, 2, 3, 4, 6, 9`	Indicates the type of transaction requested. 0 – **Sale** 1 – **PreAuth** 2 – **PostAuth** 3 – **Credit** 4 – **Forced PostAuth** 6 **– Extended PostAuth** 9 – **Void** Information on these transaction types is found within the ***PaymentType –Credit Card*** table.

Note: All elements and values are case sensitive.

Sale Elements

Element	Example	Required?	Description
CardAction	`0`	Yes	The CardAction indicates the type of transaction requested. **0** for **Sale** transactions.
Subtotal	`30.00`	Yes*	The Subtotal is the dollar amount that the merchant is requesting to be authorized and captured by the issuer. If items are added to the Sale request, the calculated item total will override this Subtotal value. The *Subtotal* or calculated item total must: • Be greater than 0 • Contain a maximum of two decimal places • Contain no commas.
Subtotal	`49.00`	Yes	Amount to be authorized. **Note:** Must be greater than zero, contain a maximum of two decimal places and contain no commas.
PreOrderID	`2019030114511501568`	100/AN	Include a PreOrderID variable if you need to recharge a customer. Give it a value of the OrderID of an order whose payment details you would like to use for a PreAuth or Sale request. **Note:** If you use this field, do not also include the CardNumber, CardExpMonth, CardExpYear as that will result in an error.
CardNumber	`4111111111111111`	Yes	Valid Mod10 Number.
CardExpMonth	`07`	Yes	2-digit Card Expiration Month. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardExpYear	`24`	Yes	2-digit Card Expiration Year. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardIDNumber	`999`	Yes	3 to 4-digit security code on the front or back of a credit card.

SplitFunded	`<SplitPart>`
	`  <StoreID>primary</StoreID>`
	`  <SplitAmount>80.00</SplitAmount>`
	`</SplitPart>`
	`<SplitPart>`
	`  <StoreID>secondary</StoreID>`
	`  <SplitAmount>20.00</SplitAmount>`
	`</SplitPart>`
		No	Contains two or more SplitPart elements.
			
			StoreIDs must have permission to send SplitFunding Instructions.
			
			SplitAmounts may contain up to two decimal places.
			
			The sum of all SplitAmounts must equal the SubTotal value and cannot include a zero-dollar value for any SplitAmount.

Element	Example	Required?	Description
SplitPart	<StoreID>primary</StoreID> <SplitAmount>80.00</SplitAmount>	No	These elements contain split-funding instructions (StoreID and Amount) which PSiGate uses to fund the primary store and all secondary stores.
Recurring	Y	No	This element identifies the type of agreement the merchant has with the cardholder. Set this element to “Y” if the transaction is part of a recurring payment schedule. Set this element to “I” if the transaction is one payment installment of a payment schedule. Set this element to “C” if the transaction uses credentials on file. Set this element to "T" if the transaction is cardholder initiated. If you set this element to “N” or choose not to include it, the transaction will not be considered a recurring transaction. **Note:** Due to compliance regulations, submit either ‘Recurring’ value OR 3DS values within your authorization request. Recurring transactions are not capable of undergoing 3DS authentication.
Iteration	1	No	This element identifies whether the stored card credentials included within the transaction request is the first (initial) use or a subsequent use of the card credentials. Set to “1” for initial payments that involve stored credentials. Set to “2” for subsequent payments that involve stored credentials.
CoFSchedule	U	No	This element is specifically for merchants whose processor is FirstData and transaction is Visa. Set to ‘U’ if CoF (Credential on File) transaction is an unscheduled one.
MerchantName	The Store Name	No	Soft descriptor displayed on the cardholder statement.

PreAuth Elements

Element	Example	Required?	Description
CardAction	1	Yes	**1** for **PreAuth** transactions.
Subtotal	49.00	Yes	Amount to authorize **Note:** Must be greater than zero, contain a maximum of two decimal places and contain no commas.
PreOrderID	2019030114511501568	100/AN	Include a PreOrderID variable if you need to recharge a customer. Give it a value of the OrderID of an order whose payment details you would like to use for a PreAuth or Sale request. **Note:** If you use this field, do not also include the CardNumber, CardExpMonth, CardExpYear as that will result in an error.
CardNumber	4111111111111111	Yes	Valid Mod10 Number.
CardExpMonth	07	Yes	2-digit Card Expiration Month. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardExpYear	24	Yes	2-digit Card Expiration Year. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardIDNumber	999	Yes	3 to 4-digit security code on the front or back of a credit card.
Recurring	Y	No	This element identifies the type of agreement the merchant has with the cardholder. Set this element to “Y” if the transaction is part of a recurring payment schedule. Set this element to “I” if the transaction is one payment installment of a payment schedule. Set this element to “C” if the transaction uses credentials on file. Set this element to "T" if the transaction is cardholder initiated. If you set this element to “N” or choose not to include it, the transaction will not be considered a recurring transaction. **Note:** Due to compliance regulations, submit either ‘Recurring’ value OR 3DS values within your authorization request. Recurring transactions are not capable of undergoing 3DS authentication.

Element	Example	Required?	Description
Iteration	1	No	This element identifies whether the stored card credentials included within the transaction request is the first (initial) use or a subsequent use of the card credentials. Set to "1" for initial payments that involve stored credentials. Set to "2" for subsequent payments that involve stored credentials.

PostAuth Elements

This action allows merchants to confirm a PreAuth less than or equal to 5 days old.

Element	Example	Required?	Description
CardAction	2		**2** for **PostAuth** transactions.
OrderID	20040919113333292 9		The *OrderID* of the pre-authorized order to be confirmed.
Subtotal	1.00		Amount to confirm for settlement. You are not required to submit the *Subtotal* within a **PostAuth** transaction request. If you provide a *Subtotal*, PSiGate will confirm the order for the submitted amount. If you do not provide a *Subtotal*, PSiGate will confirm the order for the amount referenced in the **PreAuth** transaction. **Note:** Must be equal to or less than the amount of the original transaction, contain a maximum of two decimal places, contain no commas and be greater than or equal to zero. If you provide a zero-dollar amount, the *Subtotal* will become the amount of the original transaction.
SplitFunded	<SplitPart> <StoreID>primary</StoreID> <SplitAmount>80.00</SplitAmount> </SplitPart> <SplitPart> <StoreID>secondary</StoreID> <SplitAmount>20.00</SplitAmount> </SplitPart>		Contains two or more SplitPart elements. StoreIDs must have permission to send Split Funding Instructions. SplitAmounts may contain up to two decimal places. The sum of all SplitAmounts must equal the SubTotal value and cannot include a zero-dollar value for any SplitAmount.
SplitPart	<StoreID>primary</StoreID> <SplitAmount>80.00</SplitAmount>		These elements contain split-funding instructions (StoreID and Amount) which PSiGate uses to fund the primary store and all secondary stores.

Note: Do not include Credit Card information within PostAuth transaction requests. Also, see Appendix A for the list of non-credit card fields that will return an error if their values include data that could be a card number.

Credit (Refund) Elements

Element	Example		Description
PaymentType	CC or DB		See ***Request Elements*** table Set to "CC" if the order referenced was processed using a credit card. Set to "DB" if the order referenced was processed via Interac Online through the Realtime HTML API.
CardAction	3		**3** for **Credit** transactions
OrderID	20040919133332929		The *OrderID* of the order you wish to credit.
Subtotal	1.00		The amount credited to your customer's card. **Note:** You must submit a *SubTotal* amount greater than zero, contains a maximum of two decimal places, does not include commas and is equal to or less than the balance remaining on the order. If at the end of the transaction, the balance remaining is zero, the order has been cancelled.
SplitFunded	<SplitPart> <StoreID>primary</StoreID> <SplitAmount>80.00</SplitAmount> </SplitPart> <SplitPart> <StoreID>secondary</StoreID> <SplitAmount>20.00</SplitAmount> </SplitPart>		Contains two or more SplitPart elements. StoreIDs must have permission to send SplitFunding Instructions. SplitAmounts may contain up to two decimal places. The sum of all SplitAmounts values must equal the SubTotal value and cannot include a zero dollar value for any SplitAmount.
SplitPart	<StoreID>primary</StoreID> <SplitAmount>80.00</SplitAmount>		These elements contain split-funding instructions (StoreID and Amount) which PSiGate uses to fund the primary store and all secondary stores.

Note: A Credit transaction request does not need credit card information. Also, see Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Forced PostAuth Elements

Element	Example	Description
StoreID	`Teststore`	PSiGate provides the StoreID within the ***PSiGate Welcome kit***. **Note:** *StoreID* is unique and case sensitive.
Passphrase	`Testpass`	PSiGate provides the *Passphrase* within the ***PSiGate Welcome kit***. **Note:** *Passphrase* is case sensitive.
PaymentType	`CC`	See ***Request Elements*** table
Subtotal	`10.00`	The authorized amount. **Note:** Must be greater than zero, contain a maximum of two decimal places and contain no commas.
CardAction	`4`	**4** for **Forced PostAuth** transactions
CardNumber	`4111111111111111`	Valid Mod10 Number
CardExpMonth	`08`	Two-digit Card Expiration Month. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardExpYear	`06`	Two-digit Card Expiration Year. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardIDNumber	`111, 9999`	3-4 digit numeric security code on the front or back of a credit card
CardAuthNumber	`102145`	You may input within this element the authorization number given by your customer's financial institution during a voice authorization or a previous PreAuth or Sale performed through PSiGate. **Note:** Match the value given by your customer's financial institution otherwise PSiGate will reject the settlement request.

SplitFunded	`<SplitPart>`
	`<StoreID>primary</StoreID>`
	`<SplitAmount>80.00</SplitAmount>`
	`</SplitPart>`
	`<SplitPart>`
	`<StoreID>secondary</StoreID>`
	`<SplitAmount>20.00</SplitAmount>`
	`</SplitPart>`
		Contains two or more SplitPart elements.
		
		StoreIDs must have permission to send SplitFunding Instructions.
		
		SplitAmounts may contain up to two decimal places.
		
		The sum of all SplitAmounts must equal the SubTotal value and cannot include a zero dollar value for any SplitAmount.

SplitPart	`<StoreID>primary</StoreID>` `<SplitAmount>80.00</SplitAmount>`	These elements contain split-funding instructions (StoreID and Amount) which PSiGate uses to fund the primary store and all secondary stores.

Note: See Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Extended PostAuth Elements

This action allows merchants to confirm a PreAuth less than or equal to 15 days old.

Element	Example	Description
StoreID	`Teststore`	PSiGate provides the StoreID within the ***PSiGate Welcome kit***. **Note:** *StoreID* is unique and case sensitive.
Passphrase	`Testpass`	PSiGate provides the *Passphrase* within the ***PSiGate Welcome kit***. **Note:** *Passphrase* is case sensitive.
PaymentType	`CC`	See ***Request Elements*** table
Subtotal	`10.00`	The authorized amount. **Note:** Must be greater than zero, contain a maximum of two decimal places and contain no commas.
CardAction	`6`	**6** for **Extended PostAuth** transactions
OrderID	`200409191133332929`	The *OrderID* of the order you wish to confirm.

SplitFunded	`<SplitPart>`
	`  <StoreID>primary</StoreID>`
	`  <SplitAmount>80.00</SplitAmount>`
	`</SplitPart>`
	`<SplitPart>`
	`  <StoreID>secondary</StoreID>`
	`  <SplitAmount>20.00</SplitAmount>`
	`</SplitPart>`
		Contains two or more SplitPart elements.
		
		StoreIDs must have permission to send SplitFunding Instructions.
		
		SplitAmounts may contain up to two decimal places.
		
		The sum of all SplitAmounts must equal the SubTotal value and cannot include a zero-dollar value for any SplitAmount.

SplitPart	`<StoreID>primary</StoreID>` `<SplitAmount>80.00</SplitAmount>`	These elements contain split-funding instructions (StoreID and Amount) which PSiGate uses to fund the primary store and all secondary stores.

Note: See Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Pure Credit Elements

Merchants must request permission to support this request type through their store(s).

Element	Example	Description
StoreID	`teststore`	PSiGate provides the StoreID within the ***PSiGate Welcome kit***. **Note:** *StoreID* is unique and case sensitive.
Passphrase	`Testpass`	PSiGate provides the Passphrase within the ***PSiGate Welcome kit***. **Note:** *Passphrase* is case sensitive.
PaymentType	`CC`	See ***Request Elements*** table
CardAction	`8`	**8** for **Pure Credit** transactions
CardNumber	`4111111111111111`	Valid Mod10 Number
CardExpMonth	`08`	Two-digit Card Expiration Month. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
CardExpYear	`06`	Two-digit Card Expiration Year. **Note:** PSiGate shall recognize only the first two digits if more than two digits are given.
Subtotal	`1.00`	The amount credited to your customer's card. **Note:** You must submit a *SubTotal* amount greater than zero, contains a maximum of two decimal places, does not include commas and is equal to or less than the balance remaining on the order. If at the end of the transaction, the balance remaining is zero, the order has been cancelled.

Void Elements

Element	Example	Description
StoreID	`teststore`	PSiGate provides the StoreID within the ***PSiGate Welcome kit***. **Note:** *StoreID* is unique and case sensitive.
Passphrase	`Testpass`	PSiGate provides the *Passphrase* within the ***PSiGate Welcome kit***. **Note:** *Passphrase* is case sensitive.
PaymentType	`CC`	See ***Request Elements*** table
CardAction	`9`	**9** for **Void** transactions
OrderID	`200409191133332929`	The *OrderID* references the **Sale**, **PostAuth** or **Credit** you wish to void.
TransRefNumber	`07abef21992`	Transaction requests return a unique *TransRefNumber* to reference the requests. **Void** transactions cancel the referred request.

Note: See Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Additional Authorization Elements

Element	Example	Length / Validation	Description
TestResult	A, D, R, F	1/A	You may set the *TestResult* element to simulate bank responses. PSiGate will return a simulated transaction result once the transaction request passes fulfillment and fraud checks. A – Simulates an approved response. D – Simulates a declined response. R – Randomly simulates an approved or declined response. F – Simulates a fraud response.
Userid	jsmith	64/AN	You may use the *Userid* to track your users or some other purpose. PSiGate's transaction server does not use the *Userid*. **Note:** You may sort based on the *Userid* within the Reports
Bname	John Smith	100/AN	Billing Name
Bcompany	PSiGate	100/AN	Billing Company
Baddress1	123 Main St	100/AN	Billing Address1
Baddress2	Suite 987	100/AN	Billing Address2
Bcity	Toronto	100/AN	Billing City
Bprovince	ON	100/AN	Billing Province/State/Region Please use ISO 3166-2 Province and State codes. Use FIPS 10-4 Region codes for outside Canada and US. Use of these codes will increase IP fraud checking accuracy.
Bpostalcode	L5N5V2,90120	100/AN	Billing Postal/Zip code
Bcountry	CA	50/AN	Billing Country Please use ISO 3166 Country Codes. Use of these codes will increase IP fraud checking accuracy.
Sname	John Smith	100/AN	Shipping Name
Scompany	Psigate	100/AN	Shipping Company
Saddress1	123 Main St	100/AN	Shipping Address1
Saddress2	Suite 987	100/AN	Shipping Address2
Scity	Toronto	100/AN	Shipping City
Sprovince	ON	100/AN	Shipping Province/State/Region
Spostalcode	L5N5V2,90120	100/AN	Shipping Postal/Zip code
Scountry	CA	50/AN	Shipping Country
Phone	+49(176)2105-2449	50/AN	Billing Phone
Fax	905-555-5555	50/AN	Billing Fax
Email	jsmith@domain.com	100/Email	Email address to receive E-mail receipt.
Comments	None today	300/AN	Comments regarding a transaction
Tax1	1.00	N	Component of *TaxTotal* amount. PSiGate calculates the sum of all of the *Tax1* through to *Tax5* element values and submits the sum within the *TaxTotal* element.

Element	Example	Length / Validation	Description
Tax2	2.00	N	Component of *TaxTotal* amount.
Tax3	3.00	N	Component of *TaxTotal* amount.
Tax4	4.00	N	Component of *TaxTotal* amount.
Tax5	5.00	N	Component of *TaxTotal* amount.
ShippingTotal	15.00	N	Total shipping dollar amount
CustomerIP	xxx.xxx.xxx.xxx	15/AN	Customer's IP address. IP fraud checking through PSiGate's online Merchant Tools relies on this variable's value.

Note: See Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Airline Ticket Elements

Element	Example	Length / Validation	Description
TicketNumber	NRJ0123456789	13/AN	Airline ticket number. Contains a three character International Air Transport Association (IATA) carrier code followed by a ten character ticket identifier.
PassengerName	John Smith	20/AN	Airline passenger name. If unavailable, include cardholder name.
DepartureDate	20190530	6/N	Flight departure date with format YYYYMMDD.
AirportCode	YYZ	3/AN	International Air Transport Association (IATA) airport or city code for original flight departure.
TicketCarrierCode	NRJ	3/AN	Ticket issuer International Air Transport Association (IATA) carrier code.
TicketCarrierName	NORTHJET	25/AN	Airline carrier name that generated the airline travel tickets.
TransType	TKT	3/AN	Transaction type. TKT = Ticket Purchase REF = Refund EXC = Exchange Ticket MSC = Miscellaneous
DocumentType	01	2/AN	Document type. 01 = Passenger Ticket 02 = Additional Collection 03 = Excess Baggage
IssuingCity	TORONTO	18/AN	Municipality where transaction occurred.
IssuingDate	20190316	8/N	Ticket issuing date with format YYYYMMDD.
PurchaseAmt	65	N	Total ticket purchase amount.
NumberInParty	1	3/N	Total number of individuals traveling.
ConjunctionInd	N	1/A	Indicates whether the itinerary contains more than four segments of travel.
ElectronicInd	Y	1/A	Indicates whether an electronic ticket was issued.
CarrierCode	NJ	2/AN	International Air Transport Association (IATA) airline carrier that provided the transportation for this trip segment.
ServiceClass	B	1/AN	International Air Transport Association (IATA) code that corresponds to the fare class.
DepartureDate	20190530	8/N	Departure date for this trip segment with format YYYYMMDD.
DepartureCity	YYZ	3/AN	Departure city or airport for this trip segment.
ArrivalCity	YTZ	3/AN	Arrival city or airport for this trip segment.
FlightNum	88	4/AN	Carrier assigned flight number for this trip segment.
FareBasis	M	15/AN	Fare basis code that corresponds to the specific fare level which the passenger is entitled for this segment.

Detailed Element List – Credit Card Payment

Element	Example	Length / Validation	Description
PaymentType	CC	25/AN	The *PaymentType* element denotes the payment method. **CC** – Credit Card **Note:** Currently, only the credit card payment method is available real-time. PSiGate will add payment methods such as E-cheque and ACH in the near future.
CardAction	0, 1, 2, 3, 4, 6, 9	1/N	Indicates the type of transaction request you wish to perform. 0 – **Sale** 1 – **PreAuth** 2 – **PostAuth** 3 – **Credit** 4 – **Forced PostAuth** 6 – **Extended PostAuth** 9 – Void You may find information about these transaction types within the ***PaymentType –Credit Card*** table.
PreOrderID	2019030114511501568	100/AN	Include a PreOrderID variable if you need to recharge a customer. Give it a value of the OrderID of an order whose payment details you would like to use for a PreAuth or Sale request. **Note:** If you use this field, do not also include the CardNumber, CardExpMonth, CardExpYear as that will result in an error.
CardNumber	4111111111111111	N	Credit Card Number **Note:** Any spaces or dashes inputted will be removed prior to processing.
CardExpMonth	05	2/N	Credit Card Expiry Month
CardExpYear	09	2/N	Credit Card Expiry Year
CardAuthNumber	182819	N	The *CardAuthNumber* stores the authorization number given by a financial institution during a voice authorization or a previous PreAuth or Sale performed through PSiGate. **Note:** Your financial institution will reject our nightly settlement requests if this value does not match the value returned by your financial institution.
TransRefNumber	0124ae4	18/AN	Each transaction request returns a unique *TransRefNumber*. The *TransRefNumber* references transaction requests. **Void** transactions cancel the referred request.

Element	Example	Length / Validation	Description
CardIDCode	0,1,2,9	1/Numeric	Passes the status for Visa CVV2, MasterCard CVC2, and Amex CID. If unknown leave blank. 0 = Bypassed 1 = Value present 2 = Value illegible 9 = Card has no CVV2 value
CardIDNumber	111, 9999	3-4 Digit Numeric	Passes Visa CVV2, MasterCard CVC2, and Amex CID numbers
CardXid	alViWlRyYkRJN3E1d0FSS3pYWTA= or: c4e59ceb-a382-4d6a-bc87-385d591fa09d	28/AN 36/AN	Passes Visa Secure 3D and Mastercard UCAF fields. **Note:** The length of the value returned by *CardXID* is 28 characters encoded in Base64. In 3DS Version 2, passes 36 characters Directory Server Transaction ID for MasterCard;
CardECI	7	N	Passes ECI
CardCavv	BwACA4ZXiAAAAAA5dFeIAAAAAAA=	28/AN	Passes Visa Secure 3D and Mastercard UCAF fields. **Note:** The length of the value returned by *CardCavv* is 28 characters.
Card3DSVersion	1, 2	1/Numeric	3DS program Version 1 = 3DS Secure Version 1.0 2 =. EMV 3-D Secure
CardLevel2ComCardType	B, C, P	1/A	Passes the commercial card type. If unknown, leave blank. B = Business C = Corporate P = Purchasing
CardLevel2PO	Order 18	25/AN	Purchase order information displayed on the customer's credit card statement if it supports Purchase Level 2 data.
CardLevel2Tax	15.00	N	Tax amount displayed on the customer's credit card statement if it supports Purchase Level 2 data.

Detailed Element List – Item Elements

Item Element	Example	Length / Validation	Description
ItemID	PSI-BOOK	50/AN	Merchant reference to the item. Typically, a product or item code.
ItemDescription	PSiGate User Manual	200/AN	Description of the product, item or service.
ItemQty	1	N	Quantity of the purchased item.
ItemPrice	10.00	N	The Unit Cost of the Item The dollar amount may contain a maximum of two decimal places and contain no commas.
Option	Please see ***Option Elements***	Please see Option Elements	Please see ***Option Elements***

Note: PSiGate calculates the individual item totals (*ItemQty* multiplied by *ItemPrice*) and the item subtotal (sum of item totals) if you add items to an order.
The calculated item subtotal will replace the value given in the *SubTotal* element.
Each item's total can be less than zero, but the item subtotal must be greater than or equal to zero.
Also, see Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Detailed Element List – Option Elements

Option Element	Example	Length / Validation	Description
<UserDefined>	<Type>HardCover</Type>	50/AN	Additional Item Information.
Option elements allow the creation of additional item descriptions that you might require. Options are defined within an Item context. See ***Adding Item Options***			

Note: See Appendix A for the list of non-credit card fields that will return an error if their values include data that could be deemed as cardholder data.

Result Elements

Result Elements – Payment Type: All

Result Element	Example	Length / Validation	Description
TransTime	Mon Nov 08 20:21:06 PST 2004	50/AN	Time stamp of the transaction request.
OrderID	Order1	100/AN	*OrderID* of the transaction. Either an echo of the user's input or a system generated value.
Approved	APPROVED	50/AN	There are three possible values: APPROVED - The transaction request was approved. DECLINED - The transaction request was accepted as a valid request and was declined by the card issuing bank. **Note:** Check the Return Code and ErrMsg for details. ERROR - The transaction request encountered an error. **Note**: Check the Return Code and ErrMsg for details.
ReturnCode	Y:123221:431319003178:M:N:YY Y	50/AN	Summary of result codes returned from the transaction request. The first character indicates whether the transaction was approved or declined. A "Y" signifies the transaction request was approved. Any other value indicates the transaction request was declined. PSiGate returns the *ReturnCode* in any one of the following formats: N:ERROR – An error occurred and the request was not completed. See *ErrMsg* for details. N:FRAUD – The transaction request activated a fraud condition. See *ErrMsg* for details. N:BANK ERROR CODE/DECLINE MSG – The transaction request was declined by the issuer. Y:CardAuthNumber:CardRefNumber: CardIDResult:AVSResult:IPResult – The transaction request was approved by the issuer.
ErrMsg	PSI-3000:TESTFRAUD.	150/AN	Error Message detail. Populated if the *ReturnCode* is "N:ERROR" or "N:FRAUD". The format is *ERRORCODE:ERRORTEXT*. Where ERRORCODE is the system assigned error code and ERRORTEXT is a text summary that describes the ERRORCODE.
TaxTotal	5.00	N	Calculated Tax Total. Sum of the five tax elements.

Result Element	Example	Length / Validation	Description
ShipTotal	15.00	N	The echo of the submitted *ShippingTotal* value
SubTotal	55.00	N	Either an echo of the submitted *SubTotal* value or the calculated item subtotal if you pass item information. In some cases, such as when processing a **Void** transaction, the returned *SubTotal* will equal the value of the referenced transaction.
FullTotal	75.00	N	The sum of the *TaxTotal*, *ShipTotal*, and *SubTotal* elements.
PaymentType	CC	25/AN	The *PaymentType* element denotes the payment method. **CC** – Credit Card **Note:** Currently, only the credit card payment method is available in real-time.

Result Elements – Payment Type: Credit Card & Visa Debit Card

Result Element – Credit Card	Example	Length / Validation	Description
CardNumber	……1111	25/AN	Abbreviated card number used within a transaction.
TransRefNumber	0124ae4	18/AN	Each transaction request generates and returns a unique *TransRefNumber* when the transaction request contains the minimum required elements as outlined in ***Request Elements*** and the values are valid.
CardIDResult	M	25/AN	M – Match N – No match P – Not processed S – Not passed U – Issuer does not support CardID verification Blank – Not passed or not processed. *See Appendix E – Simulating AVS and Card ID responses*
AVSResult	X	25/AN	X- Exact match, 9-digit zip Y- Exact match, 5-digit zip A – Address match W – 9-digit zip match only Z – 5-digit zip match only N – No address or zip match U – Address unavailable R – Card Issuer system unavailable E – Not a MOTO order S – Service not supported Blank – Not processed **Note**: For AVS to function, you must enter the numeric street address into *Baddress1* and the zip/postal code into *Bpostalcode.* *See Appendix E – Simulating AVS and Card ID responses*
CardAuthNumber	123456	N	Card authorization number from the financial institution that issued the card.
CardRefNumber	177e541278a	AN/25	Transaction reference number assigned by the bank processor. **Note:** PSiGate only uses the *CardRefNumber* element for reference during the reconciliation process.
CardType	VISA	AN/10	Credit card type
DebitType	VISADEBIT	AN/9	Only returned for transactions where the card number is a visa debit card.

Result Element – Credit Card	Example	Length / Validation	Description
IPResult	YYY	AN/3	The IP fraud result. First Character – Country match Second Character – Region match Third Character – City match Y - Match N - No match
IPCountry	CA	AN/2	Country of the submitted IP address. UN – IP address unknown or unable to determine
IPRegion	Mississauga	AN/50	Region, state or province of the submitted IP address. UN – IP address unknown or unable to determine
IPCity	Toronto	AN/50	City of the submitted IP address. UN – IP address unknown or unable to determine

Appendix A – Validation of fields containing credit card data

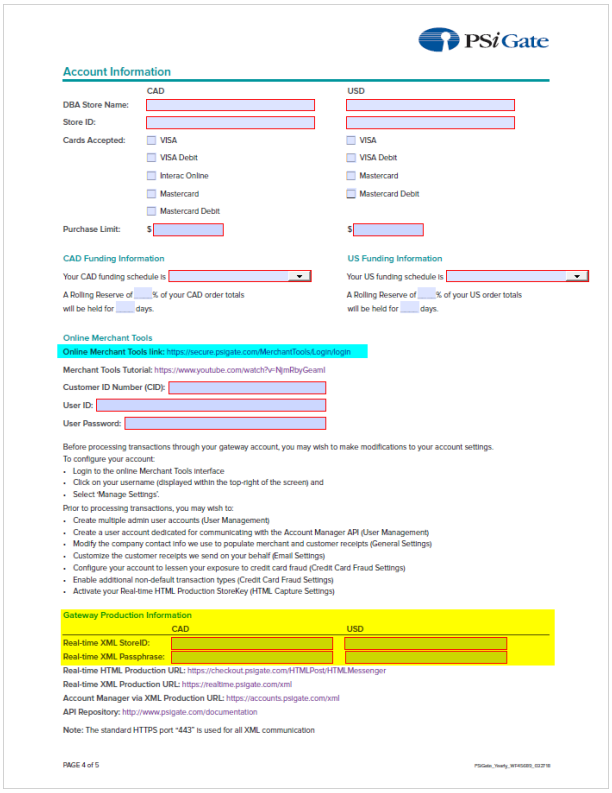
In an effort to provide merchants with a more secure processing platform and reduce credit card fraud, PSiGate has added field validation rules that are in compliance with PCI DSS v3.1. These rules aim to ensure that credit card data is always secure throughout the payment transaction process. Therefore as of code release 2.1.2 of our payment engine, PSiGate will no longer allow merchants to pass data that could be interpreted as cardholder data within any field other than *CardNumber*. Merchants may be required to update their systems in order to prevent cardholder data from being sent to PSiGate within any of the non-credit card fields listed below:

OrderID	Bpostalcode	Phone
UserID	Sname	Fax
Bname	Scompany	Email
Bcompany	Saddress1	Comments
Baddress1	Saddress2	Items
Baddress2	Scity	ItemID
Bcity	Sprovince	ItemDescription
Bprovince	Scountry	ESDFile
Bcountry	Spostalcode	Options (Option Name, Option Value)

Note: If one of the fields above is passed to PSiGate containing credit card data, PSiGate will return the response “PSI-0127:One or more non-credit card data fields contain a credit card number.” within the ErrMsg response field.

Appendix B – Sample of PSiGate Welcome kit

Displayed below is a sample of the Welcome kit PSiGate sends merchants when their gateway account is configured. The production information that you need to configure your XML API requests are highlighted in yellow. If your Welcome kit does not contain this information, then it is likely that the store which is specified within the Welcome kitl was not configured to accept transaction requests from outside of the virtual terminal provided to all merchants within the online Merchant Tools.



PSiGate

Account Information

	CAD	USD
DBA Store Name:		
Store ID:		
Cards Accepted:	VISA	VISA
	VISA Debit	VISA Debit
	Interac Online	Mastercard
	Mastercard	Mastercard Debit
	Mastercard Debit	
Purchase Limit:	$	$

CAD Funding Information

Your CAD funding schedule is

A Rolling Reserve of ___% of your CAD order totals will be held for ___ days.

US Funding Information

Your US funding schedule is

A Rolling Reserve of ___% of your US order totals will be held for ___ days.

Online Merchant Tools

Online Merchant Tools link: https://secure.psigate.com/MerchantTools/Login/login

Merchant Tools Tutorial: https://www.youtube.com/watch?v=NjmRbyGeaml

Customer ID Number (CID):

User ID:

User Password:

Before processing transactions through your gateway account, you may wish to make modifications to your account settings.
To configure your account:

- Login to the online Merchant Tools interface
- Click on your username (displayed within the top-right of the screen) and
- Select 'Manage Settings'.

Prior to processing transactions, you may wish to:

- Create multiple admin user accounts (User Management)
- Create a user account dedicated for communicating with the Account Manager API (User Management)
- Modify the company contact info we use to populate merchant and customer receipts (General Settings)
- Customize the customer receipts we send on your behalf (Email Settings)
- Configure your account to lessen your exposure to credit card fraud (Credit Card Fraud Settings)
- Enable additional non-default transaction types (Credit Card Fraud Settings)
- Activate your Real-time HTML Production StoreKey (HTML Capture Settings)

Gateway Production Information

	CAD	USD
Real-time XML StoreID:		
Real-time XML Passphrase:		

Real-time HTML Production URL: https://checkout.psigate.com/HTMLPost/HTMLMessenger

Real-time XML Production URL: https://realtime.psigate.com/xml

Account Manager via XML Production URL: https://accounts.psigate.com/xml

API Repository: http://www.psigate.com/documentation

Note: The standard HTTPS port "443" is used for all XML communication

PAGE 4 of 5

Appendix C – List of Test Credit Card Numbers

If you need to use credit card numbers to test transaction in our dev environment please use the test card numbers below. Please keep in mind that the appropriate response for a test card number submitted within a live transaction is a response indicating that the card does not belong to a valid institution because although these numbers fit the credit card algorithm, they have not been issued by a credit card issuer.

VISA test numbers
4111111111111111
4012000033330026
4111111111111112
4012000033330036
4005550000000019
4387751111111111
4387752222222227
4005519255555555
4116110000000018

MC test numbers
5454545454545454
5424180279791732
5191230005263745
5442982222222220
5405070000000011
5529040000000015

MC 2BIN test numbers
2221011111222226
2221000000111111
2720999999111113
2222400041240011
2223000048400011

Discover (MC test numbers)
6011000991300009

AMEX test numbers
371449635398431

VISA Debit test numbers
*4005*550000000001 + TestResult = "A"

Appendix D – Connection Troubleshooting Guide

If you cannot connect to PSiGate via XML, it could be that:

1. PSiGate's service was down
2. The Action URL is incorrect (Not https://realtimestaging.psigate.com/xml or your production URL if you have gone live.
3. The DNS did not resolve the name correctly.
   The test environment communicates via:
   - https://realtimestaging.psigate.com/xml (IP 216.220.59.210 across port 443)
   - https://staging.psigate.com/Messenger/XMLMessenger (IP 216.220.59.210 across ports 7989, 17989 or 27989)
4. The port within your Action URL does not support the same encryption protocols that your server supports. Try a different, yet acceptable, port number.
5. Your firewall has blocked PSiGate's IP address.
6. Your applications timeout setting is set too low. Try setting it to 30 seconds.

If you have tried all of the above, please ask your host to perform a traceroute and notify us of the result if the trace shows that the connection was dropped after it reached PSiGate.

If you would like us to check our logs for your transaction requests, ask your host provider to run four telnet tests (details below), report to us the results of each and supply us with their server's Source IP or Subnet and the timestamp of the last transaction attempt.

From the command window,

- Input "telnet secure.psigate.com"
- Input "telnet secure.psigate.com 7989"
- Input "telnet secure.psigate.com 17989"
- Input "telnet secure.psigate.com 27989"

Results include:
PASS if the DOS screen goes blank.
FAIL if you see a "Trying to connect…" message.

Send an email to support@psigate.com with the results of all four tests.

Appendix E – Simulating AVS and Card ID responses

To generate simulated AVS responses, set the dollar part of the total amount (after SubTotal, tax and shipping values are summed) as follows:

AVS Response Code	AVS Response Code Description	FullTotal value that generates the simulated AVS code
X	AVS Match (MasterCard)	1.xx
Y	AVS Match (VISA, MC, AMEX) or Address match only (Discover)	2.xx
A	Address match only (VISA, MC, AMEX)	3.xx
W	Zip/Postal code match only (MC) or AVS information unavailable (Discover)	4.xx
Z	Zip/Postal code match only	5.xx
N	No match	6.xx
U	AVS information unavailable	7.xx
S	AVS not supported	8.xx
R	Retry	9.xx
E	Error	10.xx
D	AVS Match (International VISA)	11.xx
M	AVS Match (International VISA)	12.xx
B	Address match only (VISA)	13.xx
P	Zip/Postal code match only (VISA)	14.xx
C	AVS Not Verified (VISA)	15.xx
I	AVS Not Verified (International VISA)	16.xx
G	AVS Not Verified (International VISA)	17.xx
“”	(Empty String)	18.xx
F	AVS Match (UK VISA)	Not yet supported
T	Zip/Postal code match only (Discover)	Not yet supported

To generate simulated CardID responses, set the cents part of the total amount (after SubTotal, tax and shipping values are summed) as follows:

Card ID Code	Card ID Code Description	FullTotal value that generates the simulated Card ID
M	Match	x.01
N	No Match	x.02
P	Not processed	x.03
S	Should have been present	x.04
U	Issuer unable to process	x.05
“ ”	N/A	x.06
Y	Match (AMEX only)	N/A