



Secure XML API Integration Guide
(with FraudGuard add in)

Document Control

This is a control document

DESCRIPTION	Secure XML API Integration Guide (with FraudGuard add in)		
CREATION DATE	02/04/2007	CREATED BY	SecurePay
VERSION	1.5	DATE UPDATED	03/02/2011

Version 1.5 Changes

- New FraudGuard sub-element added < IpCountryCardCountryFail>
- Examples updated
- Appendix updated

Version 1.4 Changes

- Description updated for some elements

Version 1.3 Changes

- New FraudGuard element and sub-elements added
- Existing ThirdPartyResponse element and sub-elements now deprecated

Table of Contents

1 Introduction.....	4	9.2	Response Messages	35	
1.1	About this Guide	4	9.3	Echo URLs.....	35
1.2	Intended Audience	4	9.4	Sample XML Messages.....	35
			9.4.1	Echo	35
2 System Overview.....	5	10 XML Over HTTP.....	37		
3 Secure XML Payments.....	7	10.1	Request.....	37	
3.1	Payment.....	7	10.2	Response	37
3.2	Echo	7			
3.3	Authentication, Communication & Encryption	7			
4 Message Formats and Contents	8	Appendix A: Transaction Types	39		
4.1	XML Header	8	Appendix B: Transaction Sources	40	
4.2	Element Definitions.....	8	Appendix C: Card Types.....	41	
4.2.1	Element Codes	8	Appendix D: Location of CVW	42	
4.2.2	Element Types and Constraints	8	Appendix E: Timestamp String Format	43	
4.3	Sample XML Request and Response...9		Appendix F: SecurePay Status Codes	44	
4.3.1	Request	9	Appendix G: XML Request DTD	45	
4.3.2	Response	10	Appendix H: XML Response DTD	46	
5 Common XML Message Elements	12	Appendix I: Currency Codes List.....	48		
5.1	Request Messages.....	12	Appendix J: EBCDIC Character Set.....	49	
5.1.1	MessageInfo Element	12	Appendix H: ISO 3166 Country Codes	50	
5.1.2	MerchantInfo Element	12			
5.1.3	RequestType Element	13			
5.2	Response Messages.....	13			
5.2.1	MessageInfo Element	13			
5.2.2	MerchantInfo Element	14			
5.2.3	RequestType Element	14			
5.2.4	Status Element	15			
6 Payment Message Elements.....	16				
6.1	Request Messages.....	16			
6.1.1	Payment Element	16			
6.2	Response Messages.....	21			
6.2.1	Payment Element	21			
7 Payment URLs.....	29				
8 Sample XML Messages	30				
8.1	Antifraud Payment.....	30			
8.1.1	Request	30			
8.1.2	Response	30			
8.1.3	Antifraud Only Request	32			
9 Echo Message Elements	35				
9.1	Request Messages.....	35			

1 Introduction

1.1 About this Guide

This guide provides technical information about integrating and configuring Secure XML within your environment.

Secure XML uses an Application Programming Interface as well as platform independent XML interface allowing developers to build their own products to utilise Secure XML functionality.

Secure XML uses XML request and response messages which can be run on any platform and in any programming language. These messages are transport is via HTTP over SSL.

This guide covers the process of configuring Secure XML within an environment in order to integrate the XML API.

1.2 Intended Audience

This document is intended for developers, integrating SecurePay's Secure XML interface into their own applications or websites.

It is recommended that someone with web site, XML or application programming experience reads this guide and implements the Secure XML

2 System Overview

SecurePay's Payment Gateway provides merchants with the ability to process credit card and direct entry payments in a secure environment.

SecurePay partners with the following major banks and financial institutions in the provision of the SecurePay Payment Gateway:

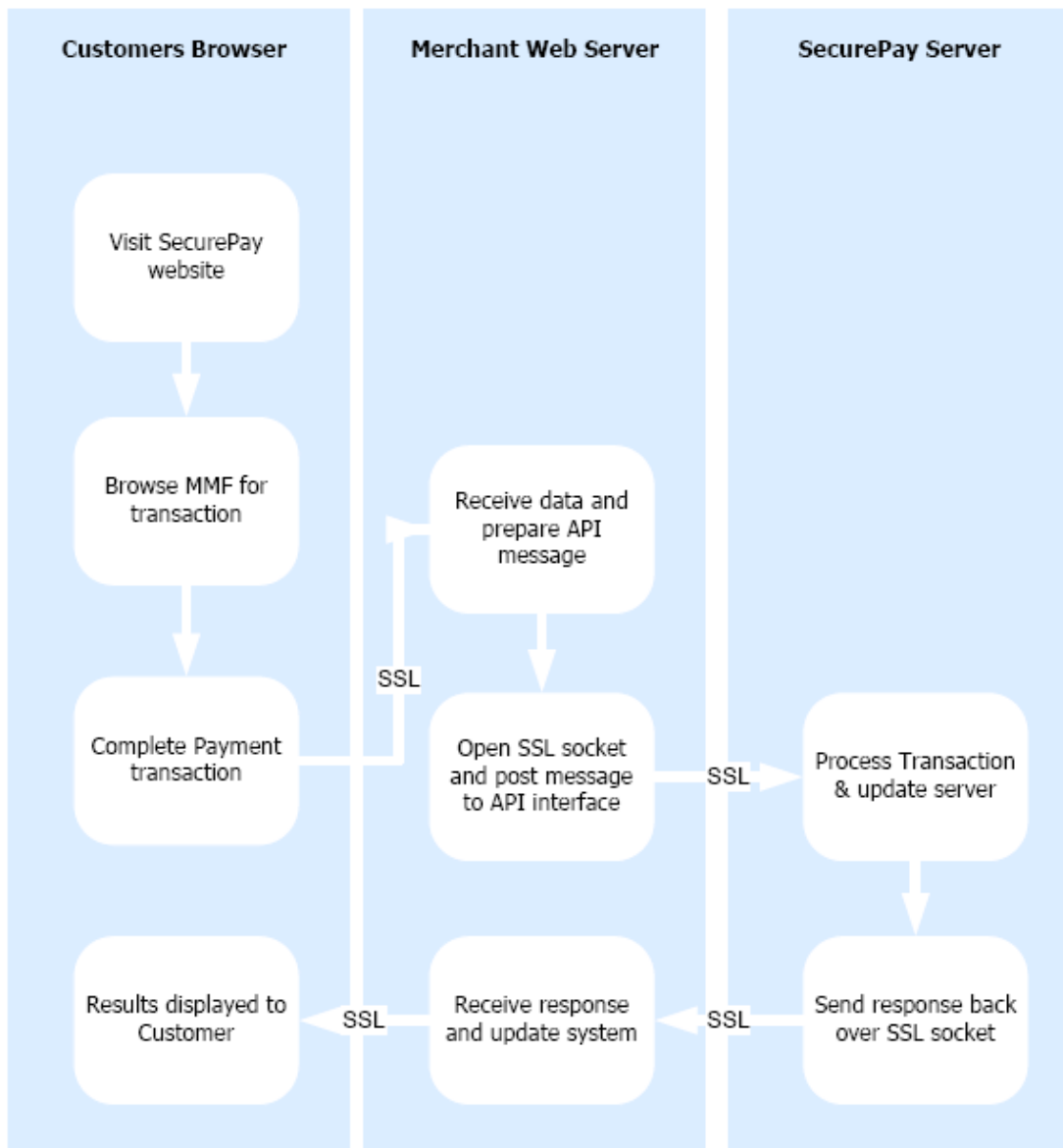
- ANZ
- American Express
- BankWest
- Commonwealth Bank
- Diners Club
- National Australia Bank
- St George (including Bank of SA)
- Westpac (including Challenge Bank and Bank of Melbourne)

Direct entry payments are not processed in real time; they are stored in SecurePay's database and processed daily at 4.30pm EST.

SecurePay XML supports four payment transaction types:

- Payments
- Refunds
- Preauthorise
- Preauthorise Complete

Secure XML utilises a XML request and response messages, and can be run on any platform and in any programming language. The message transport is done via HTTP protocol using SSL.



3 Secure XML Payments

Secure XML allows easy, platform independent way to processing financial transactions.

3.1 Payment

The Payment requests are used to pass financial credit card transaction messages to SecurePay's Payment Server, which will authorise the transaction with the merchant's bank and customer's card issuer, and produce a response based on the banks' authorisation of the transaction.

The Payment request can be used to send following credit card transaction types:

- Credit Card Payment
- Credit Card Refund
- Credit Card Reversal (Void)
- Credit Card Preauthorise
- Credit Card Preauthorise Complete (Advice)

SecurePay's Payment Server is also capable of processing direct entry transactions. Direct entry transactions are not processed real time. SecurePay Payment Server stores direct entry transaction in a database and processes them daily at 4.30pm Melbourne time.

The Payment request can be used to send following direct entry transaction types:

- Direct Debit
- Direct Credit

In case of antifraud transactions SecurePay first performs antifraud verification. If the verification fails the transaction is not sent to the bank for processing.

There are two antifraud transaction types:

- Antifraud payment – the payment is processed by the bank if the antifraud verification is successful.
- Antifraud only request – regardless of the antifraud verification outcome the transaction is not processed by the bank. This transaction type is used only to perform the antifraud verification

3.2 Echo

The Echo message is used to verify that the SecurePay Payment Server port can be accessed. The Echo message does not validate any data, but merely sends a request message to SecurePay, and receives a response message if the SecurePay Server port is open.

3.3 Authentication, Communication & Encryption

To ensure security, each merchant is issued with password. This password requires authentication before a request can be processed. This makes sure that unauthorised users will be unable to use the interface.

The password can be changed by the merchant via SecurePay's Merchant Management facility.

The Secure XML interface uses HTTP protocol and SSL for communication with SecurePay's Payment servers.

Merchants using Secure XML will automatically use SecurePay's security certificate to encrypt requests and decrypt responses from SecurePay.

4 Message Formats and Contents

4.1 XML Header

The XML document will begin with an XML declaration that contains the following data:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Markup	Usage	Explanation
<?	required	Begins a processing instruction.
xml	required	Declares this to be an XML instruction.
Version=""	required	Identifies the version of XML specification in use.
Encoding=""	required	Indicates which international character set is used.
?>	required	Terminates the processing instruction.

The XML document must contain a following top level (root) element:

```
<SecurePayMessage>
```

4.2 Element Definitions

4.2.1 Element Codes

The XML elements located in the Element matrices in sections below have the following definitions used to indicate whether the elements are present in the request and response messages:

Code	Condition
P	Present, the element is required in the message and must be present.
O	Optional, the element is not required in the message but may be present.
X	Not present, the element should not be present.

4.2.2 Element Types and Constraints

The value format descriptions in sections below use keys from the following table:

Type	Constraint	Description
String	A	<ul style="list-style-type: none"> Alphabetic characters Value in the element is valid if it only contains characters in the specified set (alphabetic)
	N	<ul style="list-style-type: none"> Numeric characters Value in the element is valid if it only contains characters in the specified set (numeric)
	S	<ul style="list-style-type: none"> Special characters Will be followed with a list of allowed characters Value in the element is valid if it only contains characters in the specified set (special characters)
	LEN	<ul style="list-style-type: none"> Number of characters in the string Value in the element is valid if the length of the value is equal to the defined length
	MINLEN	<ul style="list-style-type: none"> Minimum number of characters in the string Value in the element is valid if the length of the value is greater than or equal to the defined minimum length
	MAXLEN	<ul style="list-style-type: none"> Maximum number of characters in the string Value in the element is valid if the length of the value is less than or equal to the defined maximum length

Type	Constraint	Description
Integer	DIGNO	<ul style="list-style-type: none"> Number of digits in the integer value Value in the element is valid if the number of digits in the value is less than or equal to the defined digits number
	MINVAL	<ul style="list-style-type: none"> Minimum numerical value Value in the element is valid if it is numerically greater than or equal to the defined minimum value
	MAXVAL	<ul style="list-style-type: none"> Maximum numerical value Value in the element is valid if it is numerically less than or equal to the defined maximum value

4.3 Sample XML Request and Response

4.3.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>
    <messageTimestamp>20152303111359163000+660</messageTimestamp>
    <timeoutValue>60</timeoutValue>
    <apiVersion>xml-4.2</apiVersion>
  </MessageInfo>
  <MerchantInfo>
    <merchantID>ABC0001</merchantID>
    <password>changeit</password>
  </MerchantInfo>
  <RequestType>Payment</RequestType>
  <Payment>
    <TxnList count="1">
      <Txn ID="1">
        <txnType>21</txnType>
        <txnSource>23</txnSource>
        <amount>100</amount>
        <currency>AUD</currency>
        <purchaseOrderNo>test</purchaseOrderNo>
        <CreditCardInfo>
          <cardNumber>4444333322221111</cardNumber>
          <expiryDate>09/15</expiryDate>
          <cvv>000</cvv>
        </CreditCardInfo>
        <BuyerInfo>
          <firstName>John</firstName>
          <lastName>Smith</lastName>
          <zipCode>000</zipCode>
          <town>Melbourne</town>
          <billingCountry>GBR</billingCountry>
          <deliveryCountry>NZL</deliveryCountry>
          <emailAddress>test@hotmail.com</emailAddress>
          <ip>203.89.255.137</ip>
        </BuyerInfo>
      </Txn>
    </TxnList>
  </Payment>
</SecurePayMessage>
```

4.3.2 Response

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>
    <messageTimestamp>20152303111359163000+660</messageTimestamp>
    <apiVersion>xml-4.2</apiVersion>
  </MessageInfo>
  <MerchantInfo>
    <merchantID>ABC0001</merchantID>
  </MerchantInfo>
  <RequestType>Payment</RequestType>
  <Status>
    <statusCode>000</statusCode>
    <statusDescription>Normal</statusDescription>
  </Status>
  <Payment>
    <TxnList count="1">
      <Txn ID="1">
        <txnType>21</txnType>
        <txnSource>0</txnSource>
        <amount>100</amount>
        <currency>AUD</currency>
        <purchaseOrderNo>test</purchaseOrderNo>
        <approved>Yes</approved>
        <responseCode>00</responseCode>
        <responseText>Approved</responseText>
        <settlementDate>20040318</settlementDate>
        <txnID>009844</txnID>
        <CreditCardInfo>
          <pan>444433...111</pan>
          <expiryDate>09/15</expiryDate>
          <cardType>6</cardType>
          <cardDescription>Visa</cardDescription>
        </CreditCardInfo>
        <antiFraudResponseCode>000</antiFraudResponseCode>
        <antiFraudResponseText>Antifraud check passed</antiFraudResponseText>
        <FraudGuard>
          <score>85</score>
          <infoIpCountry>AUD</infoIpCountry>
          <infoCardCountry>NZL</infoCardCountry>
          <ipCountryFail>yes</ipCountryFail>
          <minAmountFail>yes</minAmountFail>
          <maxAmountFail>yes</maxAmountFail>
          <openProxyFail>5</openProxyFail>
          <IpCountryCardCountryFail>5</IpCountryCardCountryFail>
          <ipCardFail>5</ipCardFail>
          <ipRiskCountryFail>5</ipRiskCountryFail>
          <ipBillingFail>5</ipBillingFail>
          <ipDeliveryFail>5</ipDeliveryFail>
          <billingDeliveryFail>5</billingDeliveryFail>
          <freeEmailFail>5</freeEmailFail>
          <tooManySameBank>5</tooManySameBank>
          <tooManyDeclined>5</tooManyDeclined>
          <tooManySameIp>5</tooManySameIp>
          <tooManySameCard>5</tooManySameCard>
          <lowHighAmount>5</lowHighAmount>
          <tooManySameEmail>5</tooManySameEmail>
        </FraudGuard>
      </Txn ID="1">
    </TxnList count="1">
  </Payment>
</SecurePayMessage>
```

```
</FraudGuard>
<ThirdPartyResponse>
  <returnCode>0</returnCode>
  <result1>1</result1>
  <result2>1</result2>
  <additionalInfo1 />
  <additionalInfo2 />
  <PSPResult>1</PSPResult>
  <PSPScore>100</PSPScore>
  <MerchantResult>1</MerchantResult>
  <MerchantScore>100</MerchantScore>
  <ProxyIp />
  <FreeE-MailDomain />
  <IPCountry>AUS</IPCountry>
  <BINCountry>NZL</BINCountry>
  <Geo-RegionMatch>1</Geo-RegionMatch>
  <Geo-CountryMatch>1</Geo-CountryMatch>
</ThirdPartyResponse>
</Txn>
</TxnList>
</Payment>
</SecurePayMessage>
```

5 Common XML Message Elements

5.1 Request Messages

Requests are the messages sent to SecurePay. Following sections describe elements common to all requests.

5.1.1 MessageInfo Element

Description:	Identifies the message.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Sub-elements:	Yes, see table below

<MessageInfo> sub-elements:

Element	Comments
<messageID>	<p>Description: Unique identifier for the XML message.</p> <p>Format type: String</p> <p>Format constraints: AN, MINLEN = 0, MAXLEN = 30</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "8af793f9af34bea0cf40f5fb5c630c"</p> <p>Sub-elements: No</p>
<messageTimestamp>	<p>Description: Time of the request.</p> <p>Format type: String, see Appendix E: Timestamp String Format</p> <p>Format constraints: NS ('+', '-'), LEN = 24</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "20041803161306527000+660"</p> <p>Sub-elements: No</p>
<timeoutValue>	<p>Description: Timeout value used, in seconds.</p> <p>Format type: Integer</p> <p>Format constraints: DIGNO = 3, MINVAL = 1</p> <p>Validated by SecurePay: Yes</p> <p>Value: Recommended "60"</p> <p>Sub-elements: No</p>
<apiVersion>	<p>Description: Version of the product used.</p> <p>Format type: String</p> <p>Format constraints: ANS ('-', '.'), MINLEN = 1, MAXLEN = 13</p> <p>Validated by SecurePay: Yes</p> <p>Value: Always "xml-4.2"</p> <p>Sub-elements: No</p>

5.1.2 MerchantInfo Element

Description:	Identifies the merchant.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Sub-elements:	Yes, see table below

<MerchantInfo> sub-elements:

Element	Comments
<merchantID>	<p>Description: Merchant ID. 5 or 7-character merchant ID supplied by SecurePay.</p> <p>Format type: String</p> <p>Format constraints: AN, LEN = 7</p> <p>Validated by SecurePay: Yes</p> <p>Value: 5-character merchant ID for Direct Entry transactions, eg: "ABCOO" 7-character merchant ID for Credit Card transactions, eg: "ABC0001"</p> <p>Sub-elements: No</p>
<password>	<p>Description: Payment password. Password used for authentication of the merchant's request message, supplied by SecurePay.</p> <p>Note: The password can be changed via SecurePay's Merchant Management facility.</p> <p>Format type: String</p> <p>Format constraints: ANS (All characters are allowed), MINLEN = 6, MAXLEN = 20</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "password_01"</p> <p>Sub-elements: No</p>

5.1.3 RequestType Element

Description:	Defines the type of the request being processed.
Format type:	String
Format constraints:	A, MINLEN = 1, MAXLEN = 20
Validated by SecurePay:	Yes
Value:	One of the following: <ul style="list-style-type: none"> • "Payment" • "Echo"
Sub-elements:	No

5.2 Response Messages

Responses are the messages sent from SecurePay to the merchant in a response to a request message. Following sections describe elements common to all responses.

5.2.1 MessageInfo Element

Description:	Identifies the message.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<MessageInfo> sub-elements:

Element	Comments
---------	----------

<messageID>	<p>Description: Unique identifier for the XML message. Returned unchanged from the request.</p> <p>Format type: String</p> <p>Format constraints: AN, MINLEN = 0, MAXLEN = 30</p> <p>Value: Eg: "8af793f9af34bea0cf40f5fb5c630c"</p> <p>Sub-elements: No</p>
<messageTimestamp>	<p>Description: Time of the response.</p> <p>Format type: String, see Appendix E: Timestamp String Format</p> <p>Format constraints: NS ('+', '-'), LEN = 24</p> <p>Value: Eg: "20041803161306527000+660"</p> <p>Sub-elements: No</p>
<apiVersion>	<p>Description: Version of the product used. Returned unchanged from the request.</p> <p>Format type: String</p> <p>Format constraints: ANS ('-', '.'), MINLEN = 1, MAXLEN = 13</p> <p>Value: Eg: "xml-4.2"</p> <p>Sub-elements: No</p>

5.2.2 MerchantInfo Element

Description:	Identifies the merchant.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<MerchantInfo> sub-elements:

Element	Comments
<merchantID>	<p>Description: Merchant ID. 5 or 7-character merchant ID supplied by SecurePay. Returned unchanged from the request.</p> <p>Format type: String</p> <p>Format constraints: AN, LEN = 7</p> <p>Value: 5-character merchant ID for Direct Entry transactions, eg: "ABCOO" 7-character merchant ID for Credit Card transactions, eg: "ABC0001"</p> <p>Sub-elements: No</p>

5.2.3 RequestType Element

Description:	Defines the type of the request being processed. Returned unchanged from the request.
Format type:	String
Format constraints:	A, MINLEN = 1, MAXLEN = 20
Value:	One of the following: <ul style="list-style-type: none"> • "Payment" • "Echo"
Sub-elements:	No

5.2.4 Status Element

Description:	Status of the processing of merchant's request.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<Status> sub-elements:

Element	Comments
<statusCode>	<p>Description: Status code.</p> <p>Format type: String, see Appendix F: SecurePay Status Codes</p> <p>Format constraints: N, LEN = 3</p> <p>Value: Eg: "000"</p> <p>Sub-elements: No</p>
<statusDescription>	<p>Description: Status description.</p> <p>Format type: String, see Appendix F: SecurePay Status Codes</p> <p>Format constraints: ANS (All characters are allowed), MINLEN = 0</p> <p>Value: Eg: "Normal"</p> <p>Sub-elements: No</p>

6 Payment Message Elements

6.1 Request Messages

Following sections describe elements used in Payment requests.

The following <RequestType> element value must be used for all Payment messages:

<RequestType>Payment</RequestType>

6.1.1 Payment Element

Description:	Contains information about financial transactions to be processed.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Sub-elements:	Yes, see table below

<Payment> sub-elements:

Element	Comments
<TxnList>	See TxnList Element

6.1.1.1 TxnList Element

Description:	Contains list of transactions to be processed.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Attributes:	Yes, see table below
Sub-elements:	Yes, see table below

<TxnList> sub-elements:

Element	Comments
<TxnList.count>	<p>Description: Transaction count is an attribute of <TxnList> element and specifies number of <Txn> elements.</p> <p>Note: Currently only single transactions per request are supported. Payments submitted with more than one <Txn> element will be rejected with Status code "517".</p> <p>Format type: Integer</p> <p>Format constraints: DIGNO = 1, MINVAL = 1, MAXVAL = 1</p> <p>Validated by SecurePay: Yes</p> <p>Value: Currently always "1"</p> <p>Sub-elements: No</p>
<Txn>	See Txn Element

6.1.1.1.1 Txn Element

Description:	Contains information about a financial transaction.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Attributes:	Yes, see table below
Sub-elements:	Yes, see table below

<Txn> sub-elements:

Not all of the <Txn> sub-elements are required for different types of payments. Please refer to section Transaction Type-Required Element Map for information what elements are required for various payment types.

Element	Comments
<Txn.ID>	<p>Description: Transaction ID is an attribute of <Txn> element and specifies transaction ID. All transactions should be numbered sequentially starting at "1".</p> <p>Note: Currently only single transactions per request are supported. Payments submitted with more than one <Txn> element will be rejected with Status code "517".</p> <p>Format type: Integer</p> <p>Format constraints: DIGNO = 1, MINVAL = 1, MAXVAL = 1</p> <p>Validated by SecurePay: Yes</p> <p>Value: Currently always "1"</p> <p>Sub-elements: No</p>
<txnType>	<p>Description: Transaction type specifies the type of transaction being processed.</p> <p>Format type: Integer, see Appendix A: Transaction Types</p> <p>Format constraints: DIGNO = 2, MINVAL = 0, MAXVAL = 99</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "0"</p> <p>Sub-elements: No</p>
<txnSource>	<p>Description: Transaction source specifies the source of transaction being processed. For Secure XML the source must always have a value "23".</p> <p>Format type: Integer, see Appendix B: Transaction Sources</p> <p>Format constraints: DIGNO = 2, MINVAL = 0, MAXVAL = 99</p> <p>Validated by SecurePay: Yes</p> <p>Value: Always "23"</p> <p>Sub-elements: No</p>
<amount>	<p>Description: Transaction amount in cents.</p> <p>Format type: Integer</p> <p>Format constraints: MINVAL = 1</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "123" for \$1.23</p> <p>Sub-elements: No</p>

Element	Comments
<currency>	<p>Description: Transaction currency.</p> <p>Note: Only applicable to Credit Card payments. Currency only needs to be set for payment and preauthorisation. Refund, Reversal and Complete transactions are processed in a currency used for the original payment or preauthorisation. If not set for payment or preauthorisation, a default currency is used. Default currency is "AUD" - Australian Dollars.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "AUD" for Australian Dollars</p> <p>Sub-elements: No</p>
<purchaseOrderNo>	<p>Description: Unique merchant transaction identifier, typically an invoice number.</p> <p>Note: Must be the same as <purchaseOrderNo> element of the original transaction when performing a refund, reversal or advice.</p> <p>Format type: String</p> <p>Format constraints: For Credit Card payments ANS (All characters allowed except spaces and "" single quote), For Direct Entry payments EBCDIC (see Appendix J), MINLEN = 1, MAXLEN = 60 For Direct Entry payments it is recommended that the purchase order number does not exceed 18 characters in length.</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "order_#000235"</p> <p>Sub-elements: No</p>
<CreditCardInfo>	See CreditCardInfo Element
<BuyerInfo>	See BuyerInfo Element

6.1.1.1.2 CreditCardInfo Element

Description:	Contains credit card information.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Sub-elements:	Yes, see table below

<CreditCardInfo> sub-elements:

Element	Comments
<cardNumber>	<p>Description: Credit card number.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 13, MAXLEN = 16</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "4242424242424242"</p> <p>Sub-elements: No</p>

Element	Comments
<cvv>	<p>Description: Card verification value. The CVV value assists the bank with detecting fraudulent transactions based on automatically generated card numbers, as the CVV number is printed on the physical card and cannot be generated in conjunction with a card number. If passed, the bank may check the supplied value against the value recorded against the card. See Appendix D: Location of CVV</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 3, MAXLEN = 4</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "123"</p> <p>Sub-elements: No</p>
<expiryDate>	<p>Description: Credit card expiry date.</p> <p>Format type: String</p> <p>Format constraints: NS ('/'), LEN = 5</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "05/06" for May 2006</p> <p>Sub-elements: No</p>

6.1.1.1.3 BuyerInfo Element

Description:	Contains buyer information.
Format type:	(No value)
Format constraints:	(No value)
Validated by SecurePay:	Yes
Value:	(No value)
Sub-elements:	Yes, see table below

<BuyerInfo> sub-elements:

Element	Comments
<ip>	<p>Description: IP address from which the transaction originated.</p> <p>Format type: String</p> <p>Format constraints: NS (Must contain three periods), MAXLEN = 15</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "203.89.101.20"</p> <p>Sub-elements: No</p>
<firstName>	<p>Description: Buyer's first name.</p> <p>Format type: String</p> <p>Format constraints: ANS (All characters allowed), MINLEN = 0, MAXLEN = 40</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "John"</p> <p>Sub-elements: No</p>
<lastName>	<p>Description: Buyer's last name.</p> <p>Format type: String</p> <p>Format constraints: ANS (All characters allowed), MINLEN = 0, MAXLEN = 40</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "Smith"</p> <p>Sub-elements: No</p>

Element	Comments
<zipcode>	Description: Buyer's zip code. Format type: String Format constraints: ANS (All characters allowed), MINLEN = 0, MAXLEN = 30 Validated by SecurePay: Yes Value: Eg: "3000" Sub-elements: No
<town>	Description: The billing or delivery town of the buyer. Format type: String Format constraints: ANS (All characters allowed), MINLEN = 0, MAXLEN = 60 Validated by SecurePay: Yes Value: Eg: "Melbourne" Sub-elements: No
<billingCountry>	Description: Billing country. Can contain the 3 digit numeric ISO code or the 2 or 3 alpha character ISO code. See Appendix H: ISO 3166 Country Codes Format type: String Format constraints: N, LEN = 3 or A, MINLEN = 2, MAXLEN = 3 Validated by SecurePay: Yes Value: Eg: "AU" Sub-elements: No
<deliveryCountry>	Description: Delivery country. Can contain the 3 digit numeric ISO code or the 2 or 3 alpha character ISO code. See Appendix H: ISO 3166 Country Codes Format type: String Format constraints: N, LEN = 3 or A, MINLEN = 2, MAXLEN = 3 Validated by SecurePay: Yes Value: Eg: "AU" Sub-elements: No
<emailAddress>	Description: Email address of the buyer. Format type: String Format constraints: ANS, MAXLEN = 100 Validated by SecurePay: Yes Value: Eg: "johnsmith@somedomain.com" Sub-elements: No

6.1.1.1.4 Transaction Type-Required Element Map

The table below shows which elements are required for each transaction type. Elements are mandatory, optional or not required.

TXN TYPE	Antifraud payment	Antifraud Request Only

ELEMENT	21	22
<txnType>	M	M
<txnSource>	M	M
<amount>	M	M
<currency>	O	O
<purchaseOrderNo>	M	M
<cardNumber>	M	M
<cvv>	O	O
<expiryDate>	M	M
<ip>	M	M
<firstName>	O	O
<lastName>	O	O
<zipcode>	O	O
<town>	O	O
<billingCountry>	O	O
<deliveryCountry>	O	O
<emailAddress>	O	O
M – Mandatory O – Optional X – Not required (ignored)		

6.2 Response Messages

Following sections describe elements used in Payment requests. The following elements will only be returned if Status received in the response is “000 – Normal”.

6.2.1 Payment Element

Description:	Contains information about financial transactions processed.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<Payment> sub-elements:

Element	Comments
<TxnList>	See TxnList Element

6.2.1.1 TxnList Element

Description:	Contains list of transactions processed.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Attributes:	Yes, see table below
Sub-elements:	Yes, see table below

<TxnList> sub-elements:

Element	Comments
---------	----------

<TxnList.count>	<p>Description: Transaction count is an attribute of <TxnList> element and specifies number of <Txn> elements. Returned unchanged from the request.</p> <p>Note: Currently only single transactions per request are supported. Payments submitted with more than one <Txn> element will be rejected with Status code "517".</p> <p>Format type: Integer</p> <p>Format constraints: DIGNO = 1, MINVAL = 1, MAXVAL = 1</p> <p>Value: Currently always "1"</p> <p>Sub-elements: No</p>
<Txn>	See Txn Element

6.2.1.1.1 Txn Element

Description:	Contains information about a financial transaction.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Attributes:	Yes, see table below
Sub-elements:	Yes, see table below

<Txn> sub-elements:

Element	Comments
<Txn.ID>	<p>Description: Transaction ID is an attribute of <Txn> element and specifies transaction ID. All transactions returned should be numbered sequentially starting at "1" just as they were in the request message. Returned unchanged from the request.</p> <p>Note: Currently only single transactions per request are supported. Payments submitted with more than one <Txn> element will be rejected with Status code "577".</p> <p>Format type: Integer</p> <p>Format constraints: DIGNO = 1, MINVAL = 1, MAXVAL = 1</p> <p>Value: Currently always "1"</p> <p>Sub-elements: No</p>
<txnType>	<p>Description: Transaction type specifies the type of transaction being processed. Returned unchanged from the request.</p> <p>Format type: Integer, see Appendix A: Transaction Types</p> <p>Format constraints: DIGNO = 2, MINVAL = 0, MAXVAL = 99</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "0"</p> <p>Sub-elements: No</p>
<txnSource>	<p>Description: Transaction source specifies the source of transaction being processed. For Secure XML the source must always have a value "23". Returned unchanged from the request.</p> <p>Format type: Integer, see Appendix B: Transaction Sources</p> <p>Format constraints: DIGNO = 2, MINVAL = 0, MAXVAL = 99</p> <p>Validated by SecurePay: Yes</p> <p>Value: Always "23"</p> <p>Sub-elements: No</p>

Element	Comments
<amount>	<p>Description: Transaction amount in cents. Returned unchanged from the request.</p> <p>Format type: Integer</p> <p>Format constraints: MINVAL = 1</p> <p>Value: Eg: "123" for \$1.23</p> <p>Sub-elements: No</p>
<currency>	<p>Description: Transaction currency. Returned unchanged from the request. If not set in the request, a default value of "AUD" is returned.</p> <p>Note: Only applicable to Credit Card payments.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Validated by SecurePay: Yes</p> <p>Value: Eg: "AUD" for Australian Dollars</p> <p>Sub-elements: No</p>
<purchaseOrderNo>	<p>Description: Unique merchant transaction identifier, typically an invoice number. For refunds, reversals and advice transactions the purchase order number returned in response is the bank transaction ID of the original transaction. For payments and preauthorise transactions this value is returned unchanged from the request.</p> <p>Format type: String</p> <p>Format constraints: For Credit Card payments ANS (All characters allowed except spaces and "" single quote), For Direct Entry payments EBCDIC (see Appendix J: EBCDIC Character Set), MINLEN = 1, MAXLEN = 60</p> <p>Value: Eg: "order_#000235"</p> <p>Sub-elements: No</p>
<approved>	<p>Description: Indicates whether the transaction processed has been approved or not. It will be returned only for transaction type 21 and only if the antifraud verification passed.</p> <p>Format type: String</p> <p>Format constraints: A, MINLEN = 2, MAXLEN = 3</p> <p>Value: Always "Yes" or "No"</p> <p>Sub-elements: No</p>
<responseCode>	<p>Description: Response code of the transaction. Either a 2-digit bank response or a 3-digit SecurePay/Gateway response. Element <responseText> provides more information in a textual format. Refer to SecurePay Payment Response Codes documents for details of codes returned. This document can be downloaded from the SecurePay website.</p> <p>Format type: String</p> <p>Format constraints: AN, MINLEN = 2, MAXLEN = 3</p> <p>Value: Eg: "00"</p> <p>Sub-elements: No</p>
<responseText>	<p>Description: Textual description of the response code received.</p> <p>Format type: String</p> <p>Format constraints: ANS (All characters allowed), MINLEN = 0</p> <p>Value: Eg: "Approved"</p> <p>Sub-elements: No</p>

Element	Comments
<settlementDate>	<p>Description: Bank settlement date when the funds will be settled into the merchant's account. This will be the current date mostly, however after the bank's daily cut-off time, or on non-banking days, the settlement date will be the next business day.</p> <p>Will not be returned if the bank did not receive the transaction. (A settlement date may be returned for declined transactions.)</p> <p>It will be returned only for transaction type 21 and only if the antifraud verification passed.</p> <p>Format type: String</p> <p>Format constraints: N, LEN = 8</p> <p>Value: Eg: "20040326" for 26th March 2004</p> <p>Sub-elements: No</p>
<txnID>	<p>Description: Bank transaction ID.</p> <p>Will not be returned if the transaction has not been processed or in some cases if it was not received by the bank.</p> <p>It will be returned only for transaction type 21 and only if the antifraud verification passed.</p> <p>Format type: String</p> <p>Format constraints: AN, MINLEN = 6, MAXLEN = 16</p> <p>Value: Eg: "TX123456"</p> <p>Sub-elements: No</p>
<CreditCardInfo>	See CreditCardInfo Element
<antiFraudResponseCode>	<p>Description: Result of the antifraud verification check.</p> <p>It will be returned for transaction type 21 and 22. Refer to SecurePay Payment Response Codes documents for details of codes returned. This document may be downloaded from the SecurePay website</p> <p>Format type: String</p> <p>Format constraints: AN, LEN = 3</p> <p>Value: Eg: "000"</p> <p>Sub-elements: No</p>
<antiFraudResponseText>	<p>Description: Textual description of the antifraud response code received.</p> <p>It will be returned for transaction type 21 and 22.</p> <p>Format type: String</p> <p>Format constraints: ANS (All characters allowed), MINLEN = 0</p> <p>Value: Eg: "Antifraud check passed"</p> <p>Sub-elements: No</p>
<FraudGuard>	See FraudGuard Element
<ThirdPartyResponse>	See ThirdPartyResponse Element

6.2.1.1.2 CreditCardInfo Element

Description:	Contains credit card information.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<CreditCardInfo> sub-elements:

Element	Comments
---------	----------

Element	Comments
<pan>	<p>Description: Truncated credit card number. Contains first 6 digits of the card number, followed by “...” and then last 3 digits of the card number. Will not be returned for transactions with invalid credit card number.</p> <p>Format type: String</p> <p>Format constraints: N, LEN = 12</p> <p>Value: Eg: “424242...242”</p> <p>Sub-elements: No</p>
<expiryDate>	<p>Description: Credit card expiry date. Returned unchanged from the request.</p> <p>Format type: String</p> <p>Format constraints: NS ('/'), LEN = 5</p> <p>Value: Eg: “05/06” for May 2006</p> <p>Sub-elements: No</p>
<cardType>	<p>Description: Card type used. Will not be returned for transactions with invalid credit card number.</p> <p>Format type: Integer, see Appendix C: Card Types</p> <p>Format constraints: DIGNO = 1</p> <p>Value: Eg: “6” for Visa cards</p> <p>Sub-elements: No</p>
<cardDescription>	<p>Description: Card description. Will not be returned for transactions with invalid credit card number.</p> <p>Format type: String, see Appendix C: Card Types</p> <p>Format constraints: A, MINLEN = 0, MAXLEN = 20</p> <p>Value: Eg: “Visa”</p> <p>Sub-elements: No</p>

6.2.1.1.3 FraudGuard Element

Description:	Contains FraudGuard check information.
Format type:	(No value)
Format constraints:	(No value)
Value:	(No value)
Sub-elements:	Yes, see table below

<FraudGuard> sub-elements:

Element	Comments
<score>	<p>Description: Total of checks performed by FraudGuard. A score greater than or equal to 100 will be declined.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: “50”</p> <p>Sub-elements: No</p>
<infoIpCountry>	<p>Description: ISO 3166 three letter country code of IP address submitted in request element <IP>.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Value: Eg: “AUS”</p> <p>Sub-elements: No</p>

Element	Comments
<infoCardCountry>	<p>Description: ISO 3166 three letter country code of issuing bank location for credit card number submitted in request element <cardNumber>.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Value: Eg: "AUS"</p> <p>Sub-elements: No</p>
<ipCountryFail>	<p>Description: Country returned in <infoIpCountry> is blocked in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Value: Eg: "YES"</p> <p>Sub-elements: No</p>
<minAmountFail>	<p>Description: Amount submitted in request element <amount> is less than the minimum amount set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Value: Eg: "YES"</p> <p>Sub-elements: No</p>
<maxAmountFail>	<p>Description: Amount submitted in request element <amount> is more than the maximum amount set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: A, LEN = 3</p> <p>Value: Eg: "YES"</p> <p>Sub-elements: No</p>
<openProxyFail>	<p>Description: IP address submitted in request element <IP> is from a known open proxy. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "15"</p> <p>Sub-elements: No</p>
<IpCountryCardCountryFail>	<p>Description: Values for response elements <infoIpCountry> and <infoCardCountry> do not match. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "15"</p> <p>Sub-elements: No</p>
<ipCardFail>	<p>Description: Values for response elements <infoIpCountry> and <infoCardCountry> do not match. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "20"</p> <p>Sub-elements: No</p>

Element	Comments
<ipRiskCountryFail>	<p>Description: IP address submitted in request element <IP> is from a high risk country. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "25"</p> <p>Sub-elements: No</p>
<ipBillingFail>	<p>Description: Response element <infolpCountry> and billing county submitted in request element <billingCountry> do not match. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "30"</p> <p>Sub-elements: No</p>
<ipDeliveryFail>	<p>Description: Response element <infolpCountry> and delivery county submitted in request element <deliveryCountry> do not match. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "35"</p> <p>Sub-elements: No</p>
<billingDeliveryFail>	<p>Description: Values for request elements <billingCountry> and <deliveryCountry> do not match. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "40"</p> <p>Sub-elements: No</p>
<freeEmailFail>	<p>Description: Email address submitted in request element <emailAddress> is from a free domain. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "45"</p> <p>Sub-elements: No</p>
<tooManySameBank>	<p>Description: Too many transactions from same issuing bank within specified time frame. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "10"</p> <p>Sub-elements: No</p>

Element	Comments
<tooManyDeclined>	<p>Description: Too many declined transactions from the same IP Address within specified time frame. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "15"</p> <p>Sub-elements: No</p>
<tooManySameIp>	<p>Description: Too many transactions from the same IP Address within specified time frame. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "20"</p> <p>Sub-elements: No</p>
<tooManySameCard>	<p>Description: Too many transactions from the same full card number within specified time frame. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "25"</p> <p>Sub-elements: No</p>
<lowHighAmount>	<p>Description: Low Amount followed by a high amount from the same card number within specified time frame. Value returned is the score set in the FraudGuard. Element only returned if the FraudGuard rule is triggered. settings</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "30"</p> <p>Sub-elements: No</p>
<tooManySameEmail>	<p>Description: Too many declined transactions with same customer email within specified time frame. Value returned is the score set in the FraudGuard settings. Element only returned if the FraudGuard rule is triggered.</p> <p>Format type: String</p> <p>Format constraints: N, MINLEN = 1, MAXLEN = 3</p> <p>Value: Eg: "40"</p> <p>Sub-elements: No</p>

6.2.1.1.4 ThirdPartyResponse Element

Description: Contains third party antifraud response. This is now a deprecated element

Format type: (No value)

Format constraints: (No value)

Value: (No value)

Sub-elements: Yes, all sub-elements are deprecated

7 Payment URLs

The Payment messages must be sent to the following URLs.

For credit card transactions:

Non-SSL Test URL: <http://test.securepay.com.au/antifraud/payment>

SSL Test URL: <https://test.securepay.com.au/antifraud/payment>

SSL Live URL: <https://www.securepay.com.au/antifraud/payment>

8 Sample XML Messages

8.1 Antifraud Payment

8.1.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>
    <messageTimestamp>20152303111359163000+660</messageTimestamp>
    <timeoutValue>60</timeoutValue>
    <apiVersion>xml-4.2</apiVersion>
  </MessageInfo>
  <MerchantInfo>
    <merchantID>ABC0001</merchantID>
    <password>changeit</password>
  </MerchantInfo>
  <RequestType>Payment</RequestType>
  <Payment>
    <TxnList count="1">
      <Txn ID="1">
        <txnType>21</txnType>
        <txnSource>23</txnSource>
        <amount>100</amount>
        <currency>AUD</currency>
        <purchaseOrderNo>test</purchaseOrderNo>
        <CreditCardInfo>
          <cardNumber>4444333322221111</cardNumber>
          <expiryDate>09/15</expiryDate>
          <cvv>000</cvv>
        </CreditCardInfo>
        <BuyerInfo>
          <firstName>John</firstName>
          <lastName>Smith</lastName>
          <zipCode>000</zipCode>
          <town>Melbourne</town>
          <billingCountry>GBR</billingCountry>
          <deliveryCountry>NZL</deliveryCountry>
          <emailAddress>test@hotmail.com</emailAddress>
          <ip>203.89.255.137</ip>
        </BuyerInfo>
      </Txn>
    </TxnList>
  </Payment>
</SecurePayMessage>
```

8.1.2 Response

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>
    <messageTimestamp>20152303111359163000+660</messageTimestamp>
    <apiVersion>xml-4.2</apiVersion>
```

```
</MessageInfo>
<MerchantInfo>
  <merchantID>ABC0001</merchantID>
</MerchantInfo>
<RequestType>Payment</RequestType>
<Status>
  <statusCode>000</statusCode>
  <statusDescription>Normal</statusDescription>
</Status>
<Payment>
  <TxnList count="1">
    <Txn ID="1">
      <txnType>21</txnType>
      <txnSource>0</txnSource>
      <amount>100</amount>
      <currency>AUD</currency>
      <purchaseOrderNo>test</purchaseOrderNo>
      <approved>Yes</approved>
      <responseCode>00</responseCode>
      <responseText>Approved</responseText>
      <settlementDate>20040318</settlementDate>
      <txnID>009844</txnID>
      <CreditCardInfo>
        <pan>444433...111</pan>
        <expiryDate>09/15</expiryDate>
        <cardType>6</cardType>
        <cardDescription>Visa</cardDescription>
      </CreditCardInfo>
      <antiFraudResponseCode>000</antiFraudResponseCode>
      <antiFraudResponseText>Antifraud check passed</antiFraudResponseText>
      <FraudGuard>
        <score>85</score>
        <infoIpCountry>AUD</infoIpCountry>
        <infoCardCountry>NZL</infoCardCountry>
        <ipCountryFail>yes</ipCountryFail>
        <minAmountFail>yes</minAmountFail>
        <maxAmountFail>yes</maxAmountFail>
        <openProxyFail>5</openProxyFail>
        <IpCountryCardCountryFail>5</IpCountryCardCountryFail>
        <ipCardFail>5</ipCardFail>
        <ipRiskCountryFail>5</ipRiskCountryFail>
        <ipBillingFail>5</ipBillingFail>
        <ipDeliveryFail>5</ipDeliveryFail>
        <billingDeliveryFail>5</billingDeliveryFail>
        <freeEmailFail>5</freeEmailFail>
        <tooManySameBank>5</tooManySameBank>
        <tooManyDeclined>5</tooManyDeclined>
        <tooManySameIp>5</tooManySameIp>
        <tooManySameCard>5</tooManySameCard>
        <lowHighAmount>5</lowHighAmount>
        <tooManySameEmail>5</tooManySameEmail>
      </FraudGuard>
      <ThirdPartyResponse>
        <returnCode>0</returnCode>
        <result1>1</result1>
        <result2>1</result2>
        <additionalInfo1 />
        <additionalInfo2 />
    </Txn ID="1">
  </TxnList count="1">
</Payment>
```

```
<PSPResult>1</PSPResult>
<PSPScore>100</PSPScore>
<MerchantResult>1</MerchantResult>
<MerchantScore>100</MerchantScore>
<ProxyIp />
<FreeE-MailDomain />
<IPCountry>AUS</IPCountry>
<BINCountry>NZL</BINCountry>
<Geo-RegionMatch>1</Geo-RegionMatch>
<Geo-CountryMatch>1</Geo-CountryMatch>
</ThirdPartyResponse>
</Txn>
</TxnList>
</Payment>
</SecurePayMessage>
```

8.1.3 Antifraud Only Request

8.1.3.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>
    <messageTimestamp>20152303111359163000+660</messageTimestamp>
    <timeoutValue>60</timeoutValue>
    <apiVersion>xml-4.2</apiVersion>
  </MessageInfo>
  <MerchantInfo>
    <merchantID>ABC0001</merchantID>
    <password>changeit</password>
  </MerchantInfo>
  <RequestType>Payment</RequestType>
  <Payment>
    <TxnList count="1">
      <Txn ID="1">
        <txnType>22</txnType>
        <txnSource>23</txnSource>
        <amount>100</amount>
        <currency>AUD</currency>
        <purchaseOrderNo>test</purchaseOrderNo>
        <CreditCardInfo>
          <cardNumber>4444333322221111</cardNumber>
          <expiryDate>09/15</expiryDate>
          <cvv>000</cvv>
        </CreditCardInfo>
        <BuyerInfo>
          <firstName>John</firstName>
          <lastName>Smith</lastName>
          <zipCode>000</zipCode>
          <town>Melbourne</town>
          <billingCountry>GBR</billingCountry>
          <deliveryCountry>NZL</deliveryCountry>
          <emailAddress>test@hotmail.com</emailAddress>
          <ip>203.89.255.137</ip>
        </BuyerInfo>
      </Txn>
    </TxnList>
  </Payment>
</SecurePayMessage>
```

```
</TxnList>  
</Payment>  
</SecurePayMessage>
```

8.1.3.2 Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<SecurePayMessage>  
  <MessageInfo>  
    <messageID>8af793f9af34bea0cf40f5fb5c630c</messageID>  
    <messageTimestamp>20152303111359163000+660</messageTimestamp>  
    <apiVersion>xml-4.2</apiVersion>  
  </MessageInfo>  
  <MerchantInfo>  
    <merchantID>ABC0001</merchantID>  
  </MerchantInfo>  
  <RequestType>Payment</RequestType>  
  <Status>  
    <statusCode>000</statusCode>  
    <statusDescription>Normal</statusDescription>  
  </Status>  
  <Payment>  
    <TxnList count="1">  
      <Txn ID="1">  
        <txnType>22</txnType>  
        <txnSource>0</txnSource>  
        <amount>100</amount>  
        <currency>AUD</currency>  
        <purchaseOrderNo>test</purchaseOrderNo>  
        <approved>Yes</approved>  
        <responseCode />  
        <responseText />  
        <settlementDate />  
        <txnID />  
        <CreditCardInfo>  
          <pan>444433...111</pan>  
          <expiryDate>09/15</expiryDate>  
          <cardType>6</cardType>  
          <cardDescription>Visa</cardDescription>  
        </CreditCardInfo>  
        <antiFraudResponseCode>000</antiFraudResponseCode>  
        <antiFraudResponseText>Antifraud check passed</antiFraudResponseText>  
        <FraudGuard>  
          <score>85</score>  
          <infoIpCountry>AUD</infoIpCountry>  
          <infoCardCountry>NZL</infoCardCountry>  
          <ipCountryFail>yes</ipCountryFail>  
          <minAmountFail>yes</minAmountFail>  
          <maxAmountFail>yes</maxAmountFail>  
          <openProxyFail>5</openProxyFail>  
          <IpCountryCardCountryFail>5</IpCountryCardCountryFail>  
          <ipCardFail>5</ipCardFail>  
          <ipRiskCountryFail>5</ipRiskCountryFail>  
          <ipBillingFail>5</ipBillingFail>  
          <ipDeliveryFail>5</ipDeliveryFail>  
          <billingDeliveryFail>5</billingDeliveryFail>  
          <freeEmailFail>5</freeEmailFail>  
          <tooManySameBank>5</tooManySameBank>  
          <tooManyDeclined>5</tooManyDeclined>
```

```
<tooManySameIp>5</tooManySameIp>
<tooManySameCard>5</tooManySameCard>
<lowHighAmount>5</lowHighAmount>
<tooManySameEmail>5</tooManySameEmail>
</FraudGuard>
<ThirdPartyResponse>
  <returnCode>0</returnCode>
  <result1>1</result1>
  <result2>1</result2>
  <additionalInfo1 />
  <additionalInfo2 />
  <PSPResult>1</PSPResult>
  <PSPScore>100</PSPScore>
  <MerchantResult>1</MerchantResult>
  <MerchantScore>100</MerchantScore>
  <ProxyIp />
  <FreeE-MailDomain />
  <IPCountry>AUS</IPCountry>
  <BINCountry>NZL</BINCountry>
  <Geo-RegionMatch>1</Geo-RegionMatch>
  <Geo-CountryMatch>1</Geo-CountryMatch>
</ThirdPartyResponse>
</Txn>
</TxnList>
</Payment>
</SecurePayMessage>
```

9 Echo Message Elements

9.1 Request Messages

Echo requests do not have any additional elements.

The following <RequestType> element value must be used for all Echo messages:

```
<RequestType>Echo</RequestType>
```

SecurePay recommends that the Echo messages should not be sent more often than every 5 minutes and only if there were no real transactions processed in the last 5 minutes.

9.2 Response Messages

Echo responses do not return any additional elements. The <Status> element will return a response code "000" if the service is available.

9.3 Echo URLs

Echo requests can be sent to any of the Payment URLs to verify if the service is available. The Status Code returned in the Echo response will be "000" if the service is up.

9.4 Sample XML Messages

9.4.1 Echo

9.4.1.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
    <messageID>8af793f9af34bea0cf40f5fb79f383</messageID>
    <messageTimestamp>20152403095953349000+660</messageTimestamp>
    <timeoutValue>60</timeoutValue>
    <apiVersion>xml-4.2</apiVersion>
  </MessageInfo>
  <MerchantInfo>
    <merchantID>ABC0001</merchantID>
    <password>changeit</password>
  </MerchantInfo>
  <RequestType>Echo</RequestType>
</SecurePayMessage>
```

9.4.1.2 Response

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurePayMessage>
  <MessageInfo>
```

```
<messageID>8af793f9af34bea0cf40f5fb79f383</messageID>
<messageTimestamp>20152403095956732000+660</messageTimestamp>
<apiVersion>xml-4.2</apiVersion>
</MessageInfo>
<RequestType>Echo</RequestType>
<Status>
  <statusCode>000</statusCode>
  <statusDescription>Normal</statusDescription>
</Status>
</SecurePayMessage>
```

10 XML Over HTTP

The structure of the HTTP request and response messages will conform to the HTTP 1.1 network protocol.

Below are examples of the expected HTTP exchange.

The HTTP communication between the client and SecurePay Payment Server must be done via SSL socket so that the sensitive information included in the request and response messages is encrypted.

10.1 Request

```
POST /antifraud/payment HTTP/1.1
host: www.securepay.com.au
content-type: text/xml
content-length: 947
```

```
<?xml version="1.0" encoding="UTF-
8" ?><SecurePayMessage><MessageInfo><messageID>8af793f9af34bea0cf40f5fb5c630c</m
essageID><messageTimestamp>20152303111359163000+660</messageTimestamp><timeoutV
alue>60</timeoutValue><apiVersion>xml-
4.2</apiVersion></MessageInfo><MerchantInfo><merchantID>ABC0001</merchantID><pa
ssword>changeit</password></MerchantInfo><RequestType>Payment</RequestType><Pay
ment><TxnList count="1"><Txn
ID="1"><txnType>21</txnType><txnSource>23</txnSource><amount>100</amount><curre
ncy>AUD</currency><purchaseOrderNo>test</purchaseOrderNo><CreditCardInfo><cardN
umber>4444333322221111</cardNumber><expiryDate>09/15</expiryDate><cvv>000</cvv>
</CreditCardInfo><BuyerInfo><firstName>John</firstName><lastName>Smith</lastNam
e><zipCode>000</zipCode><town>Melbourne</town><billingCountry>GBR</billingCount
ry><deliveryCountry>NZL</deliveryCountry><emailAddress>test@hotmail.com</emailA
ddress><ip>203.89.255.137</ip></BuyerInfo></Txn></TxnList></Payment></SecurePay
Message>
```

10.2 Response

The initial HTTP server response (100 continue) is to indicate that the request has been received and should be ignored. The 200 response should follow with the XML response message. If content length is 0 and no XML response is included then the request could not be understood and no response was produced.

```
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Mon, 23 Mar 2015 06:19:48 GMT
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 23 Mar 2015 06:20:01 GMT
Content-Type: text/xml; charset=ISO-8859-1
Content-Length: 1002
```

```
<?xml version="1.0" encoding="UTF-
8" ?><SecurePayMessage><MessageInfo><messageID>8af793f9af34bea0cf40f5fb5c630c</m
essageID><messageTimestamp>20152303111359163000+660</messageTimestamp><apiVersi
on>xml-
4.2</apiVersion></MessageInfo><MerchantInfo><merchantID>ABC0001</merchantID></M
```

```
erchantInfo><RequestType>Payment</RequestType><Status><statusCode>000</statusCode><statusDescription>Normal</statusDescription></Status><Payment><TxnList
count="1"><Txn
ID="1"><txnType>21</txnType><txnSource>0</txnSource><amount>100</amount><current
cy>AUD</currency><purchaseOrderNo>test</purchaseOrderNo><approved>Yes</approved
><responseCode>00</responseCode><responseText>Approved</responseText><settleme
ntDate>20040318</settlementDate><txnID>009844</txnID><CreditCardInfo><pan>444433
...111</pan><expiryDate>09/15</expiryDate><cardType>6</cardType><cardDescription>
Visa</cardDescription></CreditCardInfo><antiFraudResponseCode>000</antiFraudRes
ponseCode><antiFraudResponseText>Antifraud check
passed</antiFraudResponseText><FraudGuard><score>80</score><infoIpCountry>AUD</
infoIpCountry><infoCardCountry>NZL</infoCardCountry><ipCountryFail>yes</ipCount
ryFail><minAmountFail>yes</minAmountFail><maxAmountFail>yes</maxAmountFail><ope
nProxyFail>5</openProxyFail><IpCountryCardCountryFail>5</IpCountryCardCountryFa
il><ipCardFail>5</ipCardFail><ipRiskCountryFail>5</ipRiskCountryFail><ipBilling
Fail>5</ipBillingFail><ipDeliveryFail>5</ipDeliveryFail><billingDeliveryFail>5<
/billingDeliveryFail><freeEmailFail>5</freeEmailFail><tooManySameBank>5</tooMan
ySameBank><tooManyDeclined>5</tooManyDeclined><tooManySameIp>5</tooManySameIp><
tooManySameCard>5</tooManySameCard><lowHighAmount>5</lowHighAmount><tooManySame
Email>5</tooManySameEmail></FraudGuard><ThirdPartyResponse><returnCode>0</retur
nCode><result1>1</result1><result2>1</result2><additionalInfo1
/><additionalInfo2
/><PSPResult>1</PSPResult><PSPScore>100</PSPScore><MerchantResult>1</MerchantRe
sult><MerchantScore>100</MerchantScore><ProxyIp
/><FreeE-MailDomain
/><IPCountry>AUS</IPCountry><BINCountry>NZL</BINCountry><Geo-
RegionMatch>1</Geo-RegionMatch><Geo-CountryMatch>1</Geo-
CountryMatch></ThirdPartyResponse></Txn></TxnList></Payment></SecurePayMessage>
```

Appendix A: Transaction Types

Transaction type codes define the type of financial transaction processed by SecurePay.

Codes with **shaded background** are permitted in Antifraud Payment transactions processed using Secure XML. All other codes are provided for completeness.

Code	Description
0	Standard Payment
1	Mobile Payment
2	Batch Payment
3	Periodic Payment
4	Refund
5	Error Reversal (Void)
6	Client Reversal (Void)
10	Preauthorise
11	Preauth Complete (Advice)
14	Recurring Payment
15	Direct Entry Debit
17	Direct Entry Credit
19	Card-Present Payment
20	IVR Payment
21	Antifraud payment
22	Antifraud (only) request

Appendix B: Transaction Sources

Transaction source codes track the origin of financial transaction processed by SecurePay.

Codes with **shaded background** are permitted in Payment transactions processed using Secure XML. All other codes are provided for completeness.

Code	Description
0	Unknown
1	SecureLink
2	Merchant Login
3	SATM
4	SecureBill Portal
5	SecureBill Link
6	Reserved
7	SecurePOS
8	API (SecureJava)
9	Call Centre Payment Switch
10	Batch Server
11	IVR1
12	IVR2
13	SecureMobile
14	Reconciliation Engine
15	Reserved
16	Helpdesk Login
18	eSec Client
19	Periodic Server
20	Reserved
21	Reserved
22	Reserved
23	XML
24	DirectOne Interface
25	Antifraud Server
90	Reserved

Appendix C: Card Types

SecurePay uses numeric codes to refer to credit card types in our system.

Code	Description
0	Unknown
1	JCB
2	American Express (Amex)
3	Diners Club
4	Bankcard
5	MasterCard
6	Visa

Appendix D: Location of CVV

The Card Verification Value is an anti-fraud measure used by some banks to prevent payments from generated card numbers. The CVV number is printed on the physical card, and is randomly assigned, therefore cannot be auto-generated.

The CVV number can be found in the following places:

Card Type	Location
Visa	Signature strip on back of card. Last digits of card number are re-printed in reverse italics, followed by 3-digit CVV.
MasterCard	Signature strip on back of card. Last digits of card number are re-printed in reverse italics, followed by 3-digit CVV.
Bankcard	Signature strip on back of card. Last digits of card number are re-printed in reverse italics, followed by 3-digit CVV.
Amex	4 digit CVV above card number on front of card.
Diners Club	Signature strip on back of card. Last digits of card number are re-printed in reverse italics, followed by 3-digit CVV.
JCB	Not used

Appendix E: Timestamp String Format

The format of the Timestamp or Log Time strings returned by SecurePay xmlapi is:

YYYYDDMMHHNNSSKKK000s000

where:

- YYYY is a 4-digit year
- DD is a 2-digit zero-padded day of month
- MM is a 2-digit zero-padded month of year (January = 01)
- HH is a 2-digit zero-padded hour of day in 24-hour clock format (midnight =0)
- NN is a 2-digit zero-padded minute of hour
- SS is a 2-digit zero-padded second of minute
- KKK is a 3-digit zero-padded millisecond of second
- 000 is a Static 0 characters, as SecurePay does not store nanoseconds
- s000 is a Time zone offset, where s is "+" or "-", and 000 = minutes, from GMT.

E.g. June 24, 2010 5:12:16.789 PM, Australian EST is:

20102406171216789000+600

Appendix F: SecurePay Status Codes

Status Code	Response Text	Description
000	Normal	Message processed correctly (check transaction response for details).
504	Invalid Merchant ID	If Merchant ID does not follow the format XXXDDDD, where X is a letter and D is a digit, or Merchant ID is not found in SecurePay's database.
505	Invalid URL	The URL passed to either Echo, Query, or Payment object is invalid.
510	Unable To Connect To Server	Produced by SecurePay Client API when unable to establish connection to SecurePay Payment Gateway
511	Server Connection Aborted During Transaction	Produced by SecurePay Client API when connection to SecurePay Payment Gateway is lost after the payment transaction has been sent
512	Transaction timed out By Client	Produced by SecurePay Client API when no response to payment transaction has been received from SecurePay Payment Gateway within predefined time period (default 80 seconds)
513	General Database Error	Unable to read information from the database.
514	Error loading properties file	Payment Gateway encountered an error while loading configuration information for this transaction
515	Fatal Unknown Error	Transaction could not be processed by the Payment Gateway due to unknown reasons
516	Request type unavailable	SecurePay system doesn't support the requested transaction type
517	Message Format Error	SecurePay Payment Gateway couldn't correctly interpret the transaction message sent
524	Response not received	The client could not receive a response from the server.
545	System maintenance in progress	The system maintenance is in progress and the system is currently unable to process transactions
550	Invalid password	The merchant has attempted to process a request with an invalid password.
575	Not implemented	This functionality has not yet been implemented
577	Too Many Records for Processing	The maximum number of allowed events in a single message has been exceeded.
580	Process method has not been called	The process() method on either Echo, Payment or Query object has not been called
595	Merchant Disabled	SecurePay has disabled the merchant and the requests from this merchant will not be processed.

Appendix G: XML Request DTD

```
<!ELEMENT SecurePayMessage (MessageInfo, MerchantInfo, RequestType
    Payment?)>

<!-- define elements for SecurePayMessage -->
<!ELEMENT MessageInfo (messageID, messageTimestamp, timeoutValue, apiVersion)>
<!ELEMENT MerchantInfo (merchantID, password)>
<!ELEMENT RequestType (#PCDATA)>
<!ELEMENT Payment (TxnList)>

<!-- define elements for MessageInfo -->
<!ELEMENT messageID (#PCDATA)>
<!ELEMENT messageTimestamp (#PCDATA)>
<!ELEMENT timeoutValue (#PCDATA)>
<!ELEMENT apiVersion (#PCDATA)>

<!-- define elements for MerchantInfo -->
<!ELEMENT merchantID (#PCDATA)>
<!ELEMENT password (#PCDATA)>

<!-- define elements for Payment -->
<!ELEMENT TxnList (Txn)>
<!ATTLIST TxnList
    count CDATA #REQUIRED>

<!-- define elements for TxnList -->
<!ELEMENT Txn (txnType, txnSource, amount, currency?, purchaseOrderNo,
    CreditCardInfo, BuyerInfo)>
<!ATTLIST Txn
    ID CDATA #REQUIRED>

<!-- define elements for Txn -->
<!ELEMENT txnType (#PCDATA)>
<!ELEMENT txnSource (#PCDATA)>
<!ELEMENT amount (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT purchaseOrderNo (#PCDATA)>
<!ELEMENT CreditCardInfo (cardNumber, cvv?, expiryDate)>
<!ELEMENT BuyerInfo (firstName?, lastName?, zipCode?, town?, billingCountry?,
    deliveryCountry?, emailAddress?, ip)>

<!-- define elements for CreditCardInfo -->
<!ELEMENT cardNumber (#PCDATA)>
<!ELEMENT cvv (#PCDATA)>
<!ELEMENT expiryDate (#PCDATA)>

<!-- define elements for BuyerInfo -->
<!ELEMENT firstName (#PCDATA)>
<!ELEMENT lastName (#PCDATA)>
<!ELEMENT zipCode (#PCDATA)>
<!ELEMENT town (#PCDATA)>
<!ELEMENT billingCountry (#PCDATA)>
<!ELEMENT deliveryCountry (#PCDATA)>
<!ELEMENT emailAddress (#PCDATA)>
<!ELEMENT ip (#PCDATA)>
```

Appendix H: XML Response DTD

```
<!ELEMENT SecurePayMessage (MessageInfo, MerchantInfo, RequestType,
    Status, Payment)>

<!-- define elements for SecurePayMessage -->
<!ELEMENT MessageInfo (messageID, messageTimestamp, apiVersion)>
<!ELEMENT MerchantInfo (merchantID)>
<!ELEMENT RequestType (#PCDATA)>
<!ELEMENT Status (statusCode, statusDescription)>
<!ELEMENT Payment (TxnList)>

<!-- define elements for MessageInfo -->
<!ELEMENT messageID (#PCDATA)>
<!ELEMENT messageTimestamp (#PCDATA)>
<!ELEMENT apiVersion (#PCDATA)>

<!-- define elements for MerchantInfo -->
<!ELEMENT merchantID (#PCDATA)>

<!-- define elements for Status -->
<!ELEMENT statusCode (#PCDATA)>
<!ELEMENT statusDescription (#PCDATA)>

<!-- define elements for Payment -->
<!ELEMENT TxnList (Txn*)>
<!ATTLIST TxnList
    count CDATA #REQUIRED>

<!-- define elements for TxnList -->
<!ELEMENT Txn (txnType, txnSource, amount, currency, purchaseOrderNo,
approved, responseCode, responseText, settlementDate, txnID,
CreditCardInfo, antiFraudResponseCode, antiFraduResponseText, FraudGuard,
ThirdPartyResponse)>
<!ATTLIST Txn
    ID CDATA #REQUIRED>

<!-- define elements for Txn -->
<!ELEMENT txnType (#PCDATA)>
<!ELEMENT txnSource (#PCDATA)>
<!ELEMENT amount (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT purchaseOrderNo (#PCDATA)>
<!ELEMENT approved (#PCDATA)>
<!ELEMENT responseCode (#PCDATA)>
<!ELEMENT responseText (#PCDATA)>
<!ELEMENT settlementDate (#PCDATA)>
<!ELEMENT txnID (#PCDATA)>
<!ELEMENT CreditCardInfo (pan, expiryDate, cardType?, cardDescription?)>
<!ELEMENT antiFraudResponseCode (#PCDATA)>
<!ELEMENT antiFraudResponseText (#PCDATA)>
<!ELEMENT FraudGuard (score, infoIpCountry, infoCardCountry, ipCountryFail,
minAmountFail, maxAmountFail, openProxyFail, IpCountryCardCountryFail,
ipCardFail, ipRiskCountryFail, ipBillingFail, ipDeliveryFail,
billingDeliveryFail, freeEmailFail, tooManySameBank, tooManyDeclined,
tooManySameIp, tooManySameCard, lowHighAmount, tooManySameEmail)>
```

```
<!ELEMENT ThirdPartyResponse (returnCode, result1, result2, additionalInfo1,
additionalInfo2, PSPResult, PSPScore, MerchantResult, MerchantScore, ProxyIp,
FreeE-MailDomain, IPCountry, BINCountry, Geo-RegionMatch, Geo-CountryMatch)>
```

```
<!-- define elements for CreditCardInfo -->
```

```
<!ELEMENT pan (#PCDATA)>
<!ELEMENT expiryDate (#PCDATA)>
<!ELEMENT cardType (#PCDATA)>
<!ELEMENT cardDescription (#PCDATA)>
```

```
<!-- define elements for FraudGuard -->
```

```
<!ELEMENT score (#PCDATA)>
<!ELEMENT infoIpCountry (#PCDATA)>
<!ELEMENT infoCardCountry (#PCDATA)>
<!ELEMENT ipCountryFail (#PCDATA)>
<!ELEMENT minAmountFail (#PCDATA)>
<!ELEMENT maxAmountFail (#PCDATA)>
<!ELEMENT openProxyFail (#PCDATA)>
<!ELEMENT IpCountryCardCountryFail (#PCDATA)>
<!ELEMENT ipCardFail (#PCDATA)>
<!ELEMENT ipRiskCountryFail (#PCDATA)>
<!ELEMENT ipBillingFail (#PCDATA)>
<!ELEMENT ipDeliveryFail (#PCDATA)>
<!ELEMENT billingDeliveryFail (#PCDATA)>
<!ELEMENT freeEmailFail (#PCDATA)>
<!ELEMENT tooManySameBank (#PCDATA)>
<!ELEMENT tooManyDeclined (#PCDATA)>
<!ELEMENT tooManySameIp (#PCDATA)>
<!ELEMENT tooManySameCard (#PCDATA)>
<!ELEMENT lowHighAmount (#PCDATA)>
<!ELEMENT tooManySameEmail (#PCDATA)>
```

```
<!-- define elements for ThirdPartyResponse -->
```

```
<!ELEMENT returnCode (#PCDATA)>
<!ELEMENT result1 (#PCDATA)>
<!ELEMENT result2 (#PCDATA)>
<!ELEMENT additionalInfo1 (#PCDATA)>
<!ELEMENT additionalInfo2 (#PCDATA)>
<!ELEMENT PSPResult (#PCDATA)>
<!ELEMENT PSPScore (#PCDATA)>
<!ELEMENT MerchantResult (#PCDATA)>
<!ELEMENT MerchantScore (#PCDATA)>
<!ELEMENT ProxyIp (#PCDATA)>
<!ELEMENT FreeE-MailDomain (#PCDATA)>
<!ELEMENT IPCountry (#PCDATA)>
<!ELEMENT BINCountry (#PCDATA)>
<!ELEMENT Geo-RegionMatch (#PCDATA)>
<!ELEMENT Geo-CountryMatch (#PCDATA)>
```

Appendix I: Currency Codes List

You must meet certain requirements with your bank and SecurePay before using SecurePay's multi-currency features. Please ask SecurePay if we support multi-currency payments through your bank, and if so, what currency types are available. You may also need to open multi-currency accounts with your bank for each currency you propose to transact in. Contact SecurePay Support or your SecurePay Account Manager for full details.

Code	Description	Minor Units	Example*	
			Amount	Pass As
AUD	Australian Dollar	2	\$20	2000
CAD	Canadian Dollar	2	\$20	2000
CHF	Swiss Franc	2	20	2000
DEM	German Deutschmark	2	20	2000
EUR	Euro	2	€20	2000
FRF	French Franc	2	20	2000
GBP	English Pound	2	£20	2000
GRD	Greek Drachma	0	20	20
HKD	Hong Kong Dollar	2	\$20	2000
ITL	Italian Lira	0	L20	20
JPY	Japanese Yen	0	¥20	20
NZD	New Zealand Dollar	2	\$20	2000
SGD	Singapore Dollar	2	\$20	2000
USD	US Dollar	2	\$20	2000

* To pass a multicurrency payment to SecurePay, set `<currency>` field with the value from the Code column, and set `<amount>` field with the amount to be charged, ensuring you set the correct number of Minor Units for the selected currency, as shown in the examples.

E.g. For US Dollars, \$4,125.90 is set using:

```
<amount>412590</amount>
<currency>USD</currency>
```

or for Japanese Yen, ¥67,925 is set using:

```
<amount>67925</amount>
<currency>JPY</currency>
```

Appendix J: EBCDIC Character Set

Description	Characters allowed
Numeric	0 - 9
Alphabetic	a - z, A - Z
Oblique slash	/
Hyphen	-
Ampersand	&
Period	.
Asterisk	*
Apostrophe	'
Blank space	

Appendix H: ISO 3166 Country Codes

Country	Alpha 2 code	Alpha 3 code
AFGHANISTAN	AF	AFG
ALAND ISLANDS	AX	ALA
ALBANIA	AL	ALB
ALGERIA	DZ	DZA
AMERICAN SAMOA	AS	ASM
ANDORRA	AD	AND
ANGOLA	AO	AGO
ANGUILLA	AI	AIA
ANTARCTICA	AQ	ATA
ANTIGUA AND BARBUDA	AG	ATG
ARGENTINA	AR	ARG
ARMENIA	AM	ARM
ARUBA	AW	ABW
AUSTRALIA	AU	AUS
AUSTRIA	AT	AUT
AZERBAIJAN	AZ	AZE
BAHAMAS	BS	BHS
BAHRAIN	BH	BHR
BANGLADESH	BD	BGD
BARBADOS	BB	BRB
BELARUS	BY	BLR
BELGIUM	BE	BEL
BELIZE	BZ	BLZ
BENIN	BJ	BEN
BERMUDA	BM	BMU
BHUTAN	BT	BTN

Country	Alpha 2 code	Alpha 3 code
BOLIVIA, PLURINATIONAL STATE OF	BO	BOL
BONAIRE, SAINT EUSTATIUS AND SABA	BQ	BES
BOSNIA AND HERZEGOVINA	BA	BIH
BOTSWANA	BW	BWA
BOUVET ISLAND	BV	BVT
BRAZIL	BR	BRA
BRITISH INDIAN OCEAN TERRITORY	IO	IOT
BRUNEI DARUSSALAM	BN	BRN
BULGARIA	BG	BGR
BURKINA FASO	BF	BFA
BURUNDI	BI	BDI
CAMBODIA	KH	KHM
CAMEROON	CM	CMR
CANADA	CA	CAN
CAPE VERDE	CV	CPV
CAYMAN ISLANDS	KY	CYM
CENTRAL AFRICAN REPUBLIC	CF	CAF
CHAD	TD	TCD
CHILE	CL	CHL
CHINA	CN	CHN
CHRISTMAS ISLAND	CX	CXR
COCOS (KEELING) ISLANDS	CC	CCK
COLOMBIA	CO	COL
COMOROS	KM	COM
CONGO	CG	COG
CONGO, THE DEMOCRATIC REPUBLIC OF THE	CD	COD
COOK ISLANDS	CK	COK
COSTA RICA	CR	CRI

Country	Alpha 2 code	Alpha 3 code
COTE D'IVOIRE	CI	CIV
CROATIA	HR	HRV
CUBA	CU	CUB
CURACAO	CW	CUW
CYPRUS	CY	CYP
CZECH REPUBLIC	CZ	CZE
DENMARK	DK	DNK
DJIBOUTI	DJ	DJI
DOMINICA	DM	DMA
DOMINICAN REPUBLIC	DO	DOM
ECUADOR	EC	ECU
EGYPT	EG	EGY
EL SALVADOR	SV	SLV
EQUATORIAL GUINEA	GQ	GNQ
ERITREA	ER	ERI
ESTONIA	EE	EST
ETHIOPIA	ET	ETH
FALKLAND ISLANDS (MALVINAS)	FK	FLK
FAROE ISLANDS	FO	FRO
FIJI	FJ	FJI
FINLAND	FI	FIN
FRANCE	FR	FRA
FRENCH GUIANA	GF	GUF
FRENCH POLYNESIA	PF	PYF
FRENCH SOUTHERN TERRITORIES	TF	ATF
GABON	GA	GAB
GAMBIA	GM	GMB
GEORGIA	GE	GEO

Country	Alpha 2 code	Alpha 3 code
GERMANY	DE	DEU
GHANA	GH	GHA
GIBRALTAR	GI	GIB
GREECE	GR	GRC
GREENLAND	GL	GRL
GRENADA	GD	GRD
GUADELOUPE	GP	GLP
GUAM	GU	GUM
GUATEMALA	GT	GTM
GUERNSEY	GG	GGY
GUINEA	GN	GIN
GUINEA-BISSAU	GW	GNB
GUYANA	GY	GUY
HAITI	HT	HTI
HEARD ISLAND AND MCDONALD ISLANDS	HM	HMD
HOLY SEE (VATICAN CITY STATE)	VA	VAT
HONDURAS	HN	HND
HONG KONG	HK	HKG
HUNGARY	HU	HUN
ICELAND	IS	ISL
INDIA	IN	IND
INDONESIA	ID	IDN
IRAN (ISLAMIC REPUBLIC OF)	IR	IRN
IRAQ	IQ	IRQ
IRELAND	IE	IRL
ISLE OF MAN	IM	IMM
ISRAEL	IL	ISR
ITALY	IT	ITA

Country	Alpha 2 code	Alpha 3 code
JAMAICA	JM	JAM
JAPAN	JP	JPN
JERSEY	JE	JEY
JORDAN	JO	JOR
KAZAKHSTAN	KZ	KAZ
KENYA	KE	KEN
KIRIBATI	KI	KIR
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	KP	PRK
KOREA, REPUBLIC OF	KR	KOR
KUWAIT	KW	KWT
KYRGYZSTAN	KG	KGZ
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA	LAO
LATVIA	LV	LVA
LEBANON	LB	LBN
LESOTHO	LS	LSO
LIBERIA	LR	LBR
LIBYAN ARAB JAMAHIRIYA	LY	LBY
LIECHTENSTEIN	LI	LIE
LITHUANIA	LT	LTU
LUXEMBOURG	LU	LUX
MACAO	MO	MAC
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	MK	MKD
MADAGASCAR	MG	MDG
MALAWI	MW	MWI
MALAYSIA	MY	MYS
MALDIVES	MV	MDV
MALI	ML	MLI

Country	Alpha 2 code	Alpha 3 code
MALTA	MT	MLT
MARSHALL ISLANDS	MH	MHL
MARTINIQUE	MQ	MTQ
MAURITANIA	MR	MRT
MAURITIUS	MU	MUS
MAYOTTE	YT	MYT
MEXICO	MX	MEX
MICRONESIA, FEDERATED STATES OF	FM	FSM
MOLDOVA, REPUBLIC OF	MD	MDA
MONACO	MC	MCO
MONGOLIA	MN	MNG
MONTENEGRO	ME	MNE
MONTSERRAT	MS	MSR
MOROCCO	MA	MAR
MOZAMBIQUE	MZ	MOZ
MYANMAR	MM	MMR
NAMIBIA	NA	NAM
NAURU	NR	NRU
NEPAL	NP	NPL
NETHERLANDS	NL	NLD
NEW CALEDONIA	NC	NCL
NEW ZEALAND	NZ	NZL
NICARAGUA	NI	NIC
NIGER	NE	NER
NIGERIA	NG	NGA
NIUE	NU	NIU
NORFOLK ISLAND	NF	NFK
NORTHERN MARIANA ISLANDS	MP	MNP

Country	Alpha 2 code	Alpha 3 code
NORWAY	NO	NOR
OMAN	OM	OMN
PAKISTAN	PK	PAK
PALAU	PW	PLW
PALESTINIAN TERRITORY, OCCUPIED	PS	PSE
PANAMA	PA	PAN
PAPUA NEW GUINEA	PG	PNG
PARAGUAY	PY	PRY
PERU	PE	PER
PHILIPPINES	PH	PHL
PITCAIRN	PN	PCN
POLAND	PL	POL
PORTUGAL	PT	PRT
PUERTO RICO	PR	PRI
QATAR	QA	QAT
REUNION	RE	REU
ROMANIA	RO	ROU
RUSSIAN FEDERATION	RU	RUS
RWANDA	RW	RWA
SAINT BARTHELEMY	BL	BLM
SAINT HELENA, ASCENSION AND TRISTAN DA CUNHA	SH	SHN
SAINT KITTS AND NEVIS	KN	KNA
SAINT LUCIA	LC	LCA
SAINT MARTIN (FRENCH PART)	MT	MAF
SAINT PIERRE AND MIQUELON	PM	SPM
SAINT VINCENT AND THE GRENADINES	VC	VCT
SAMOA	WS	WSM

Country	Alpha 2 code	Alpha 3 code
SAN MARINO	SM	SMR
SAO TOME AND PRINCIPE	ST	STP
SAUDI ARABIA	SA	SAU
SENEGAL	SN	SEN
SERBIA	RS	SRB
SEYCHELLES	SC	SYC
SIERRA LEONE	SL	SLE
SINGAPORE	SG	SGP
SINT MAARTEN (DUTCH PART)	SX	SXM
SLOVAKIA	SK	SVK
SLOVENIA	SI	SVN
SOLOMON ISLANDS	SB	SLB
SOMALIA	SO	SOM
SOUTH AFRICA	ZA	ZAF
SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS	GS	SGS
SPAIN	ES	ESP
SRI LANKA	LK	LKA
SUDAN	SD	SDN
SURINAME	SR	SUR
SVALBARD AND JAN MAYEN	SJ	SJM
SWAZILAND	SZ	SWZ
SWEDEN	SE	SWE
SWITZERLAND	CH	CHE
SYRIAN ARAB REPUBLIC	SY	SYR
TAIWAN, PROVINCE OF CHINA	TW	TWN
TAJIKISTAN	TJ	TJK
TANZANIA, UNITED REPUBLIC OF	TZ	TZA

Country	Alpha 2 code	Alpha 3 code
THAILAND	TH	THA
TIMOR-LESTE	TL	TLS
TOGO	TG	TGO
TOKELAU	TK	TKL
TONGA	TO	TON
TRINIDAD AND TOBAGO	TT	TTO
TUNISIA	TN	TUN
TURKEY	TR	TUR
TURKMENISTAN	TM	TKM
TURKS AND CAICOS ISLANDS	TC	TCA
TUVALU	TV	TUV
UGANDA	UG	UGA
UKRAINE	UA	UKR
UNITED ARAB EMIRATES	AE	ARE
UNITED KINGDOM	GB	GBR
UNITED STATES	US	USA
UNITED STATES MINOR OUTLYING ISLANDS	UM	UMI
URUGUAY	UY	URY
UZBEKISTAN	UZ	UZB
VANUATU	VU	VUT
VATICAN CITY STATE (HOLY SEE)	VA	VAT
VENEZUELA, BOLIVARIAN REPUBLIC OF	VE	VEN
VIET NAM	VN	VNM
VIRGIN ISLANDS (BRITISH)	VG	VGB
VIRGIN ISLANDS (U.S.)	VI	VIR
WALLIS AND FUTUNA	WF	WLF
WESTERN SAHARA	EH	ESH
YEMEN	YE	YEM

Country	Alpha 2 code	Alpha 3 code
YUGOSLAVIA	YU	YUG
ZAMBIA	ZM	ZMB
ZIMBABWE	ZW	ZWE