secure trading
ONLINE PAYMENT EXPERTS

Card Store

Card Store Requests allow merchants to store a customer's card details in Secure Trading's systems without performing an initial authorisation payment. These details can then be used for future requests.

Version: 1.15 (a)
Published: 1 August 2017

Table of Contents

1 Introduction

This document outlines the process of performing Card Store Requests through the Secure Trading Payment Platform (STPP). It contains an overview of the Card Store process, a breakdown of how Card Store XML Requests and Responses are structured and detailed XML examples.

1.1 Overview

The Secure Trading Payment Platform (STPP) allows you to store a customer's card details in Secure Trading's systems for later use in future requests. This allows you to store details for a customer, without the need to take an initial payment from their card, or needing to store the data on your own server.

An example of where this would be useful is if a customer was registering an account on your online shop. You can use a Card Store Request to store their card details within STPP, so whenever the customer is logged-in and opts to make a payment, they will not have to re-enter their card details.

Once stored on Secure Trading's systems, you only need to refer to the Card Store transaction reference in a future request in order to use the customer's card details to process a payment.

Please note that although the customer's card details are stored, the security code (**CVV2**) is not. **You must never store the customer's security code on your system.**

Please note that Card Store Requests do not send any card details to your bank. Providing the submitted card details are valid, they are stored securely in Secure Trading's systems for future use.

1.2 Account Configuration

You will need to have Card Store enabled on your account in order to process these requests. In order to check if this is enabled, log in to MyST and navigate to the User Details page.

More information on the User Details page can be found in the **STPP MyST User Guide** (see section **6.3 Useful Documents** on **page 23**).

If Card Store is not available on your account or you require further assistance, please contact Secure Trading Support, in order to have this option enabled (see section **6.1 Secure Trading Support** on **page 23**).

Please note when checking that the Card Store option is available on your account, you should ensure it is enabled for all the payment types required.

1.3 Additional Notes

1.3.1 Maestro must use 3D Secure

All e-commerce Maestro transactions **must** be processed using 3D Secure.

The customer **must** be present for any subsequent transactions to input their 3D Secure Password. Without the user input, you **cannot process** a Maestro transaction.

You can reference a Card Store transaction for an initial 3D Query, but the customer **must be present** for the validation.

Please note that Card Store can be used for subsequent Mail Order Telephone Order (MOTO) transactions without requiring user input.

1.3.2 Supported Payment Types

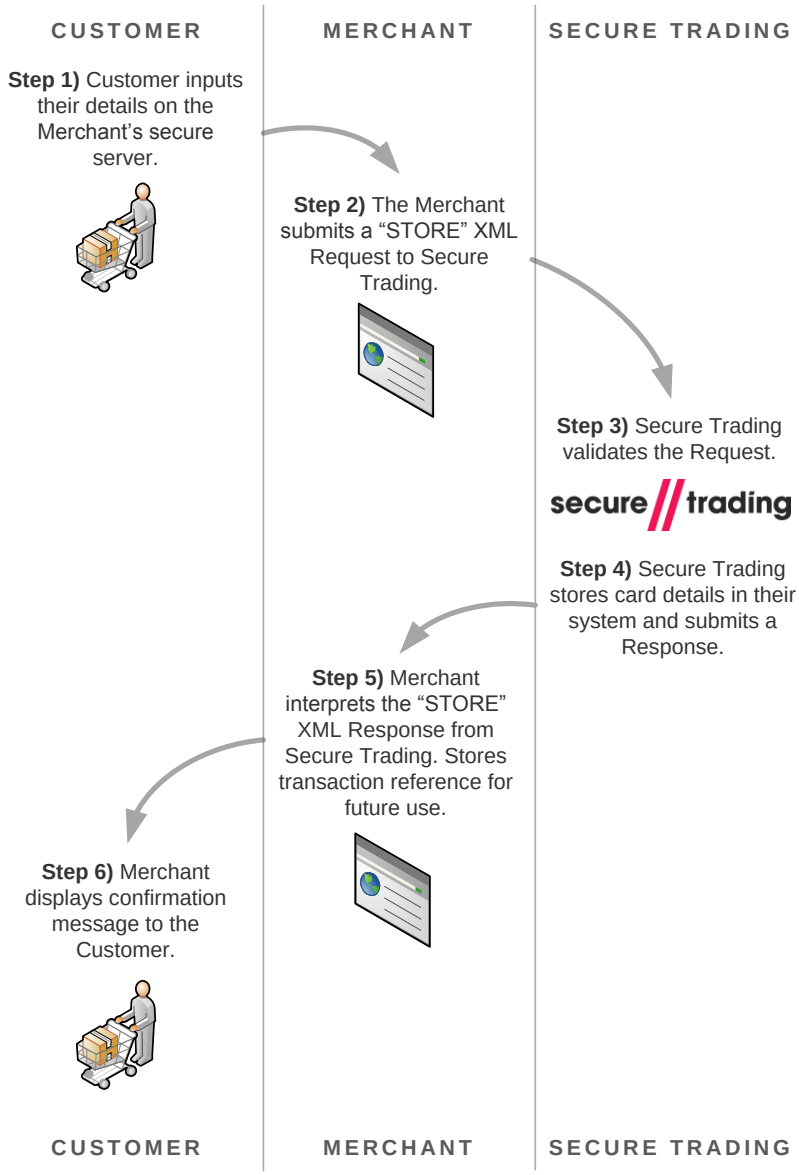
Card Store Requests can be performed for any card-based payment type supported by Secure Trading.

2 Process overview

This section of the document explains the process of submitting a Card Store Request through Secure Trading, including a data flow diagram and an explanation of each of the stages depicted.

2.1 Data Flow Diagram

The following diagram displays the overall process of submitting a Card Store Request to Secure Trading. Each step is explained in greater detail in section **2.2 Steps in detail**. There are a number of ways that Card Store can be implemented on your system, however the overall process always follows the basic overview outlined below:



2.2 Steps in detail

Step 1 – Customer inputs their details

The customer will need to submit their details to the merchant in order to perform the initial request.

Please note that it is not necessary to perform a payment before storing the customer's card details. Card Store Requests will not reserve or transfer any funds.

It is imperative that you ensure card details are received using a secure server.

Step 2 – Merchant submits a Card Store request to Secure Trading

Once the customer has submitted their card details, the merchant will submit a Card Store XML Request. This request will include the customer's card details that are to be stored. The fields that are included are described in greater detail in section 3 **STORE XML Request** on **page 7**.

Step 3 – Validation on the request

Secure Trading will perform validation on the request, such as ensuring the submitted expiry date has not already expired and that the merchant's account has been set up to manage Card Store Requests.

Step 4 – Secure Trading store the details

If the merchant is set up to perform Card Store Requests through their account, and the request submitted is valid, Secure Trading will process the request and store the customer's details. Secure Trading will then return a Card Store XML Response to the merchant.

Step 5 – The Merchant's system interprets the response

The merchant receives the Card Store XML Response from Secure Trading. Providing the XML Request sent to Secure Trading was valid and was processed successfully, the value returned in the `error` element will be 0.

For a successfully processed request, a transaction reference will be included within the XML Response. The merchant will need to store this transaction reference for use in future requests. The transaction reference will uniquely identify the Card Store Request within Secure Trading's systems.

Step 6 – Customer confirmation

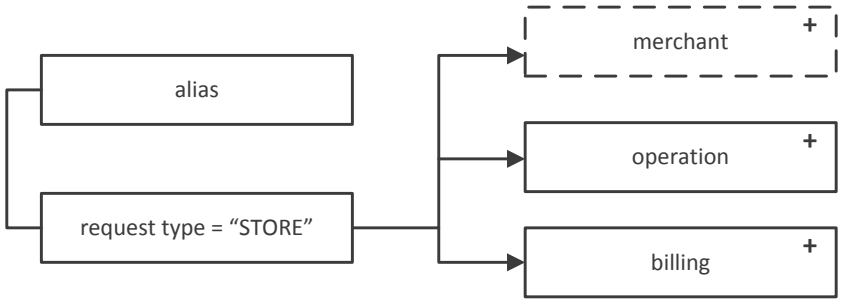
The merchant displays a confirmation message to the customer that the request has processed successfully.

3 STORE XML Request

This section of the document outlines all the fields that can be submitted within the Card Store Requests. An overview of the XML is provided, and each XML tag is detailed in the following sections.

Please note that although the customer's card details are stored, the security code (**CVV2**) is not. **You must never store the customer's security code on your system.**

3.1 XML Overview

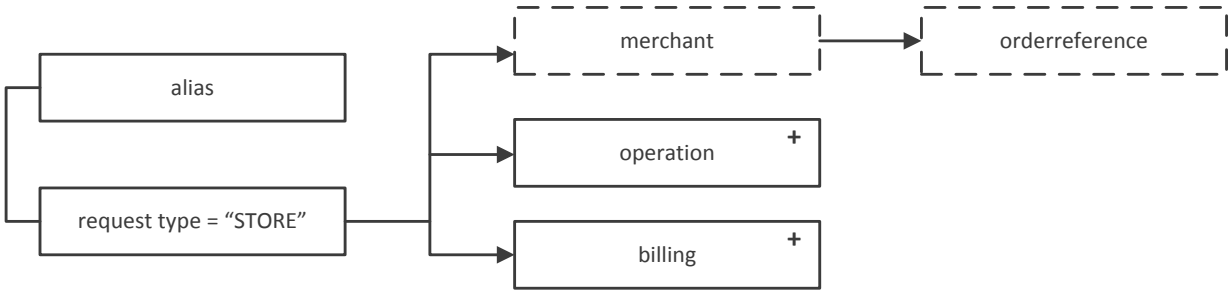


The STORE XML Request has two mandatory tags and one optional tag. Each tag is outlined in greater detail below.

Please note the name of the **`request type`** is "**`STORE`**".

3.2 <merchant>

The <**`merchant`**> tag is optional and allows you to store your own reference for the request.

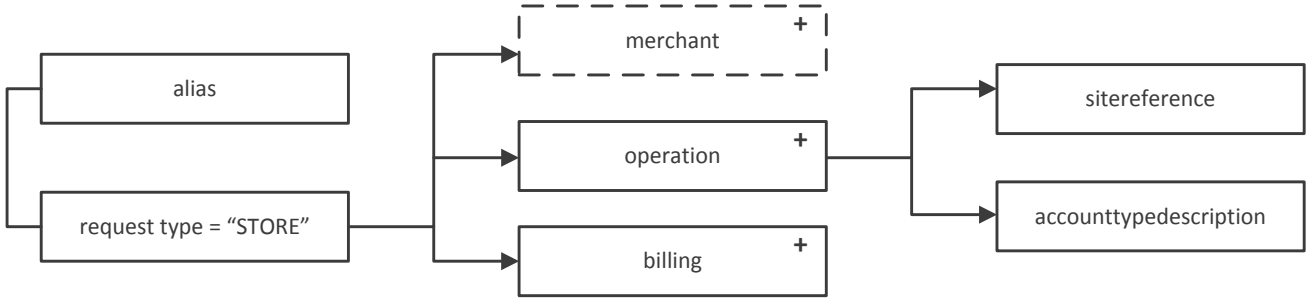


The following table describes the information that can be supplied within the <**`merchant`**> tag.

Tag	Type	Length	Required	Comment
`merchant`			N	
`orderreference`	an	255	N	Your optional unique reference for the request.

3.3 <operation>

The <**operation**> tag contains information relating to your account.

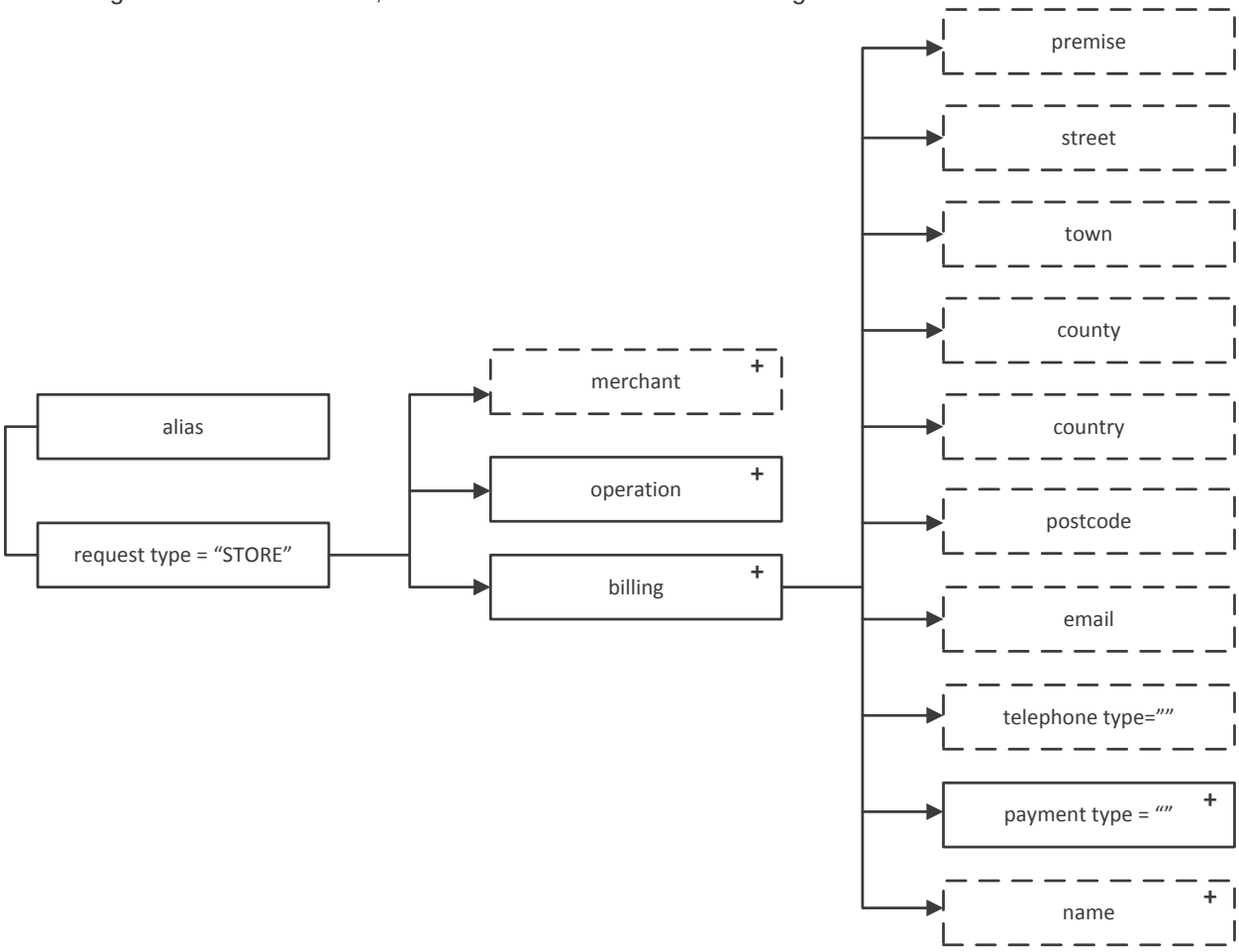


There are two mandatory elements within this tag, as described in the following table:

Tag	Type	Length	Required	Comment
operation				
sitereference	an	50	Y	The unique Secure Trading reference that identifies your site.
accounttype description	an	20	Y	The type of account being used for the request. For Card Store Requests, the value will be "CARDSTORE".

3.4 <billing>

The **<billing>** tag contains information relating to the customer. It also contains two child tags with further children, which are described in the following sections.



Although most of the elements within the **<billing>** tag are optional, they can all be stored within Secure Trading's systems for future use, and are described in the following table:

Tag		Type	Length	Required	Comment
billing				Y	
	premise	an	25	N	The house number or first line of the customer's billing address.
	street	an	127	N	The street entered for the customer's billing address
	town	an	127	N	The town entered for the customer's billing address.
	county	an	127	N	The county entered for the customer's billing address.
	country	an	2	N	The country for the customer's billing address. This will need to be in ISO2A format. For a list of country codes, please see http://webapp.securetrading.net/countrycodes.html.
	postcode	an	25	N	The postcode entered for the customer's billing address.
	email	an	255	N	The customer's e-mail address (for correspondence with the customer). Maximum length of 255 (maximum of 64 characters before the"@" symbol).

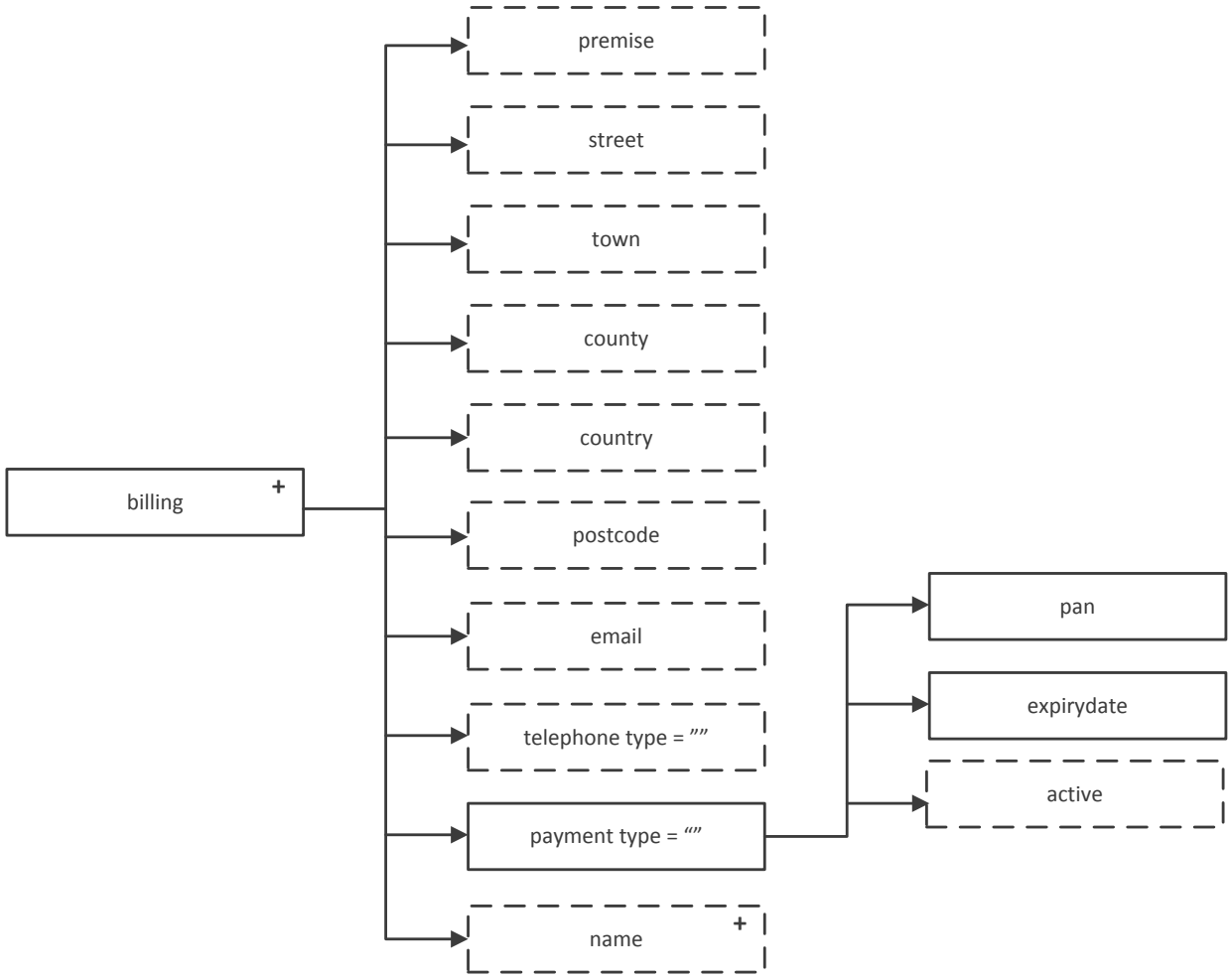
	telephone type = ""	an	1	N	The type of telephone number. The options available are:
					// H = Home
					// M = Mobile
					// W = Work

	telephone	n	20	N	The billing telephone number.
					Valid characters:
					// Numbers 0-9
					// Spaces
					// Special characters: + - ( )

Secure Trading recommends that you include the customer's **<premise>** and **<postcode>** information, as these fields are used in Address Verification System (AVS) checks. For more information, please refer to the **STPP AVS and CVV2** document (see section **6.3 Useful Documents** on **page 23**).

3.4.1 <payment>

The <**payment**> tag is the only mandatory child tag within the <**billing**> tag. It contains the customer's card details (excluding the CVV2 code).

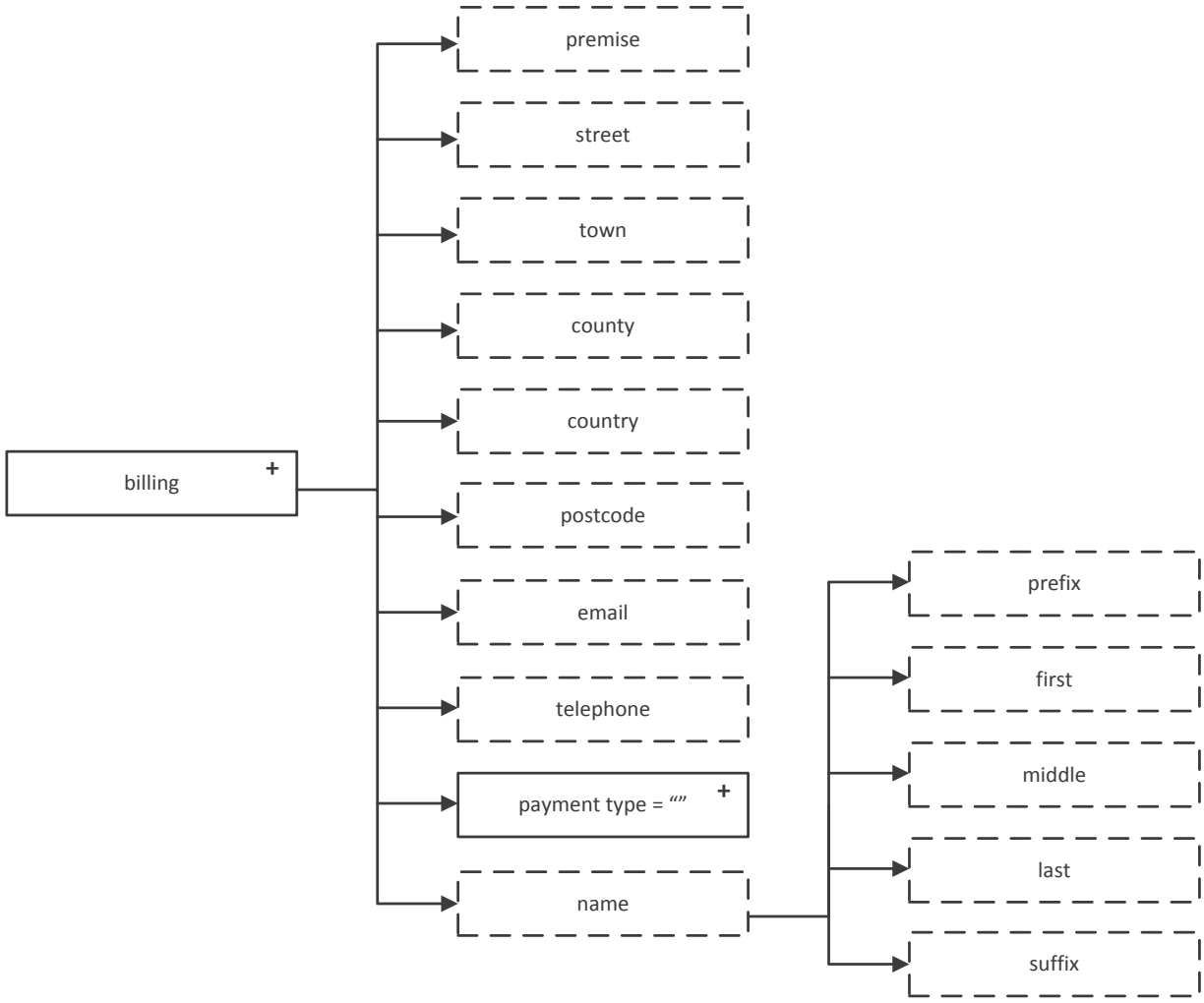


The elements included within this tag are described in the following table:

Tag	Type	Length	Required	Comment
billing			Y	
payment type = ""	an	20	Y	The customer's card type (e.g. "VISA").
pan	an	16-21	Y	This is the card number printed on the front of the customer's card.
expirydate	an	7	Y	The expiry date on the back of the card. This needs to be submitted in the format "MM/YYYY".
active	n	1	N	This flag indicates if the card details are enabled for future requests. It can be one of two values: // "0" for **No** // "1" for **Yes** If not included, the value defaults to "1". If the value is "0", the card details cannot be used in subsequent authorisations. You can update this field by submitting the **<active>** element in a TRANSACTIONUPDATE XML Request to Secure Trading (see section **5.2**).

3.4.2 <name>

Secure Trading recommends that you store the customer's name with their card details. The **<name>** tag is optional and used to store the customer's name.



The elements included within the <**name**> tag are outlined in the following table:

Tag	Type	Length	Required	Comment
billing			N	
name			N	
prefix	an	25	N	The prefix of the customer's billing name (e.g. Mr, Miss, Dr).
first	an	127	N	The customer's billing first name.
middle	an	127	N	The customer's billing middle name(s).
last	an	127	N	The customer's billing last name.
suffix	an	25	N	The suffix of the customer's billing name (e.g. Bsc).

3.5 XML Request Example

The following is an example of a STORE XML Request to be submitted to Secure Trading's systems:

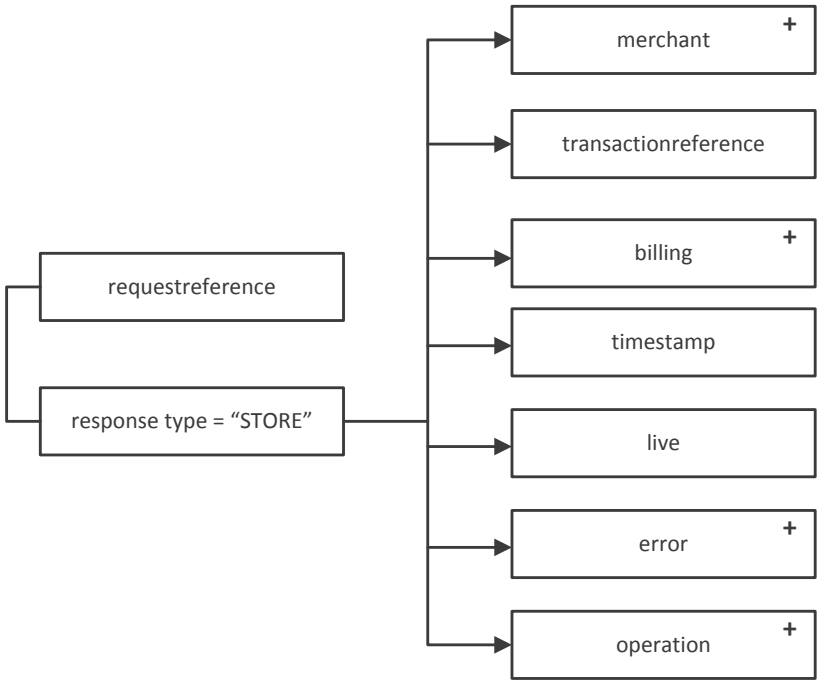
```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>test_site12345</alias>
  <request type="STORE">
    <merchant>
      <orderreference>EXAMPLE CARDSTORE</orderreference>
    </merchant>
    <operation>
      <sitereference>test_site12345</sitereference>
      <accounttypedescription>CARDSTORE</accounttypedescription>
    </operation>
    <billing>
      <town>Town</town>
      <street>Street</street>
      <county>County</county>
      <country>GB</country>
      <postcode>TE45 6ST</postcode>
      <premise>789</premise>
      <email>example@email.com</email>
      <telephone type="H">01248672050</telephone>
      <payment type="VISA">
        <pan>4111111111111111</pan>
        <expirydate>10/2031</expirydate>
      </payment>
      <name>
        <first>Joe</first>
        <last>Bloggs</last>
      </name>
    </billing>
  </request>
</requestblock>
```

4 STORE XML Response

This section covers the response to a successful STORE XML Request to Secure Trading. The XML Response outlined in this section will only be returned if the STORE XML Request was successful.

4.1 XML Overview

The structure of the XML Response for a Card Store Request is outlined in the following diagram. There are three elements and four child tags:



Please note that the name of type of the **`response type`** is “**`STORE`**”.

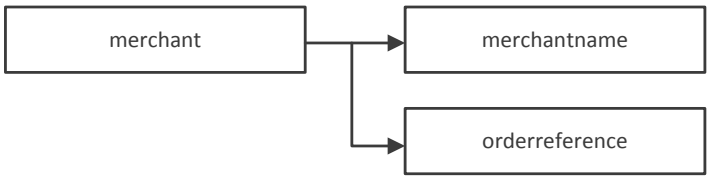
The following table describes the three elements included within the response:

Tag	Type	Length	Required	Comment
response type = "STORE"			Y	
transaction reference	an	25	Y	The unique Secure Trading reference for the transaction. It is important that you keep a record of this reference, as this is used to reference the stored card details submitted for future payment requests.
timestamp	an	19	Y	The timestamp relates to the time of the individual transaction. It will be in the format: "0000-00-00 00:00:00"
live	n	1	Y	This will indicate if the account is live or in test. A value of "1" indicates a live transaction. A value of "0" indicates a test transaction.

The **<transactionreference>** element returned in the STORE XML Response needs to be included in the **<parenttransactionreference>** element of a future request, in order to inherit the stored billing and payment details. Please refer to section 5.3 for further information on constructing AUTH XML Requests.

4.2 <merchant>

The <**merchant**> tag contains two elements.

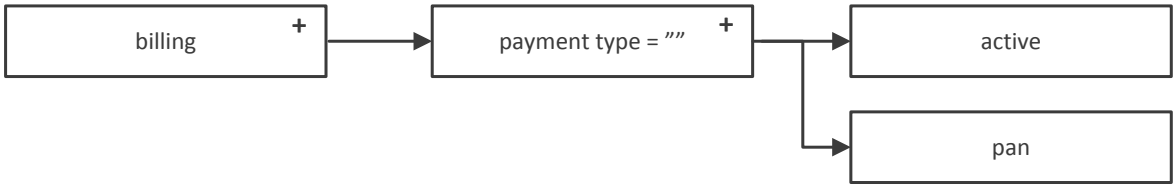


The following table describes the two elements returned within the <**merchant**> tag:

Tag	Type	Length	Required	Comment
merchant			Y	
merchantname	an	255	Y	The merchant name associated with your Secure Trading account.
orderreference	an	255	Y	Your unique reference for the request.

4.3 <billing>

The **<billing>** tag within the XML Response contains information on the customer's card details that have been stored.



The following table describes the elements included within the **<billing>** tag:

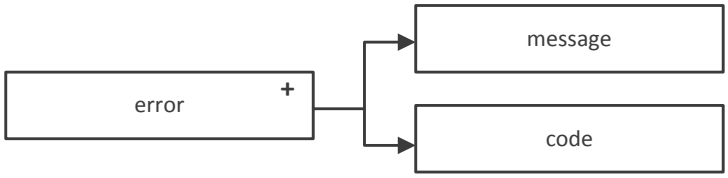
Tag	Type	Length	Required	Comment
billing			Y	
payment type = ""	an	20	Y	The customer's card type (e.g. "VISA").
active	n	1	Y	This flag indicates if the card details are enabled for future requests. It can be one of two values: // "0" for **No** // "1" for **Yes** You can update this field by submitting the **<active>** element in a TRANSACTIONUPDATE XML Request to Secure Trading (see section 5).
pan	n	16-21	Y	This will display the first four and last four digits of the card details submitted.
issuer country	an	2	N	The country for the customer's card issuer. This will be in ISO2A format. For a list of Country Codes, see http://webapp.securetrading.net/countrycodes.html
issuer	an	255	N	The customer's card issuer.

Please note that for any STORE XML Responses received, only the payment fields shown above are returned in the **<billing>** tag. However, all valid data submitted in the request is stored for later use.

All of the stored details for a Card Store Request (such as the billing address) can be viewed in MyST, or by performing a TRANSACTIONQUERY Request. For more information, please see the relevant documentation referenced in section **6.3 Useful Documents** on **page 23**.

4.4 <error>

The **<error>** tag contains information on whether or not the Card Store Request was successful.



The following table describes both elements returned in the <**error**> tag:

Tag	Type	Length	Required	Comment
error			Y	
message	an	255	Y	This text describes the error. For a successful request, the value of this string will be “Ok”.
code	n	5	Y	This code is used to help troubleshoot errors. For a successful request, this value will be “0”.

For a full list of the different error codes that can be received in XML Responses, please refer to http://webapp.securetrading.net/errorcodes.html

4.5 <operation>

The <**operation**> tag will return the type of account used to perform the request.

The following table details the element contained within the **<operation>** tag:

Tag	Type	Length	Required	Comment
operation			Y	
account type description	an	20	Y	The type of account being used for the request. For Card Store Requests, the value will be “CARDSTORE”.

4.6 XML Response Example

The following is an example of a STORE XML Response to be returned from Secure Trading's systems:

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X81946467</requestreference>
  <response type="STORE">
    <merchant>
      <merchantname>Example Merchant</merchantname>
      <orderreference>EXAMPLE CARDSTORE</orderreference>
      <operatorname>test_site12345</operatorname>
    </merchant>
    <transactionreference>12-52-1</transactionreference>
    <billing>
      <payment type="VISA">
        <active>1</active>
        <issuercountry>US</issuercountry>
        <pan>4111########1111</pan>
        <issuer>My Test Issuer</issuer>
      </payment>
    </billing>
    <timestamp>2010-06-25 14:26:47</timestamp>
    <live>1</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <operation>
      <accounttypedescription>CARDSTORE</accounttypedescription>
    </operation>
  </response>
</responseblock>
```

5 Managing stored card details

5.1 Querying Card Stores

You can submit a TRANSACTIONQUERY XML Request to view the details stored for a Card Store. Your system will be returned an XML Response, including the customer's name, billing address, the card issuer and expiry date.

The PAN returned is partially masked. We do not store the security code (CVV2) found on the back of the card due to PCI restrictions.

5.1.1 XML Request Example

The following is an example of a TRANSACTIONQUERY XML Request that can be used to view details of a Card Store. You will need to include the correct transaction reference (highlighted in **bold**) that was returned in the STORE XML Response. You will also need to ensure you include your site reference.

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>test_site12345</alias>
  <request type="TRANSACTIONQUERY">
    <filter>
     <sitereference>test_site12345</sitereference>
     <transactionreference>50-2-2</transactionreference>
    </filter>
  </request>
</requestblock>
```

For further information on transaction queries, please refer to the **Transaction Query** document
All Secure Trading documents can be found on our website.

5.2 Updating Card Stores

You can submit a TRANSACTIONUPDATE XML Request to update details stored for a Card Store. Following an update, the updated details will be used whenever the Card Store is referenced in the future.

An example of where this can be useful would be if a customer changed their address. You can update the customer's address details without needing to request the customer to input their card details again.

5.2.1 XML Request Example

The following is an example of a TRANSACTIONUPDATE XML Request that can be used to update the details associated with a Card Store. The XML Request consists of two main parts:

- The **<filter>** tag is used to specify which Card Store is to be updated. You will need to specify the unique transaction reference that you would like to update, in addition to the site reference the Card Store was processed with.
- The **<updates>** tag contains the fields you would like to update. These can include the customer's billing address, or the card's expiry date, but can **never** be the payment type or card number.

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>test_site12345</alias>
  <request type="TRANSACTIONUPDATE">
    <filter>
      <sitereference>test_site12345</sitereference>
      <transactionreference>51-2-5</transactionreference>
    </filter>
    <updates>
      <billing>
        <premise>12</premise>
        <street>Test Road</street>
        <town>Testville</town>
        <county>Testshire</county>
        <country>GB</country>
        <postcode>TE45 6ST</postcode>
        <payment>
          <active>1</active>
        </payment>
      </billing>
    </updates>
  </request>
</requestblock>
```

Please note that the card number field (**pan**) is not updatable. New card numbers should be sent to Secure Trading's systems by submitting a new Card Store Request.

When updating the <billing> address fields, we recommend that you re-submit the address in its entirety (country is required).

For more info on transaction updates (including a list of fields that can be updated), please refer to the **Transaction Update** document
All Secure Trading documents can be found on our website.

5.3 Using Card Stores

Following a successful Card Store, you can use stored details in future requests to STPP. These can be inherited by the following types of requests:

- ACCOUNTCHECK
- AUTH (also includes recurring payments)
- RISKDEC
- THREEDQUERY

All billing and payment details (except the security code) can be inherited when performing the request types listed above. This is achieved by including the **<parenttransactionreference>** element in the new request. This field must include the transaction reference associated with the Card Store, which is returned in the STORE XML Response.

5.3.1 XML Request Example

The following is an example of an AUTH XML Request that is using the previously-stored details from a Card Store.

You will need to exchange the site reference used for your own, and ensure the **<parenttransactionreference>** field (highlighted below in **bold**) includes the correct transaction reference associated with the Card Store you would like to use.

It is also recommended that you include the card's security code in the request (highlighted below in **bold**). This will allow the acquirer to perform CVV2 checks if they support it.

```
<?xml version='1.0' encoding='utf-8'?>
<requestblock version="3.67">
  <alias>test_site12345</alias>
  <request type="AUTH">
    <merchant>
      <orderreference>My Test Order</orderreference>
    </merchant>
    <billing>
      <amount currencycode="GBP">500</amount>
      <payment>
        <securitycode>123</securitycode>
      </payment>
    </billing>
    <operation>
      <sitereference>test_site12345</sitereference>
      <accounttypedescription>ECOM</accounttypedescription>
      <parenttransactionreference>1-2-3</parenttransactionreference>
    </operation>
  </request>
</requestblock>
```

For more info on performing authorisations, please refer to the **XML Specification**
All Secure Trading documents can be found on our website.

You must never store the customer's security code on your system.
If you are submitting the security code in an AUTH XML Request, you will need to prompt the customer to enter the card's security code.

6 Further Information and Support

This section provides useful information with regards to documentation and support for your Secure Trading solution.

6.1 Secure Trading Support

If you have any questions regarding integration or maintenance of the system, please contact our support team using one of the following methods.

Method	Details
Telephone	+44 (0) 1248 672 050
Fax	+44 (0) 1248 672 099
Email	support@securetrading.com
Website	http://www.securetrading.com/support/support.html

6.2 Secure Trading Sales

If you do not have an account with Secure Trading, please contact our Sales team and they will inform you of the benefits of a Secure Trading account.

Method	Details
Telephone	0800 028 9151
Telephone (Int'l)	+44 (0) 1248 672 070
Fax	+44 (0) 1248 672 079
Email	sales@securetrading.com
Website	http://www.securetrading.com

6.3 Useful Documents

The documents listed below should be read in conjunction with this document:

- STAPI Setup Guide – This document outlines how to install the STAPI java client for processing XML Requests and Responses through Secure Trading.
- STPP Web Services User Guide – This document describes how to process XML Requests and Responses through Secure Trading's Web Services solution.
- STPP XML Specification – This document describes how to perform AUTH, REFUND and ACCOUNTCHECK XML Requests through Secure Trading.
- STPP Transaction Update – This document describes how to perform TRANSACTIONUPDATE XML Requests through Secure Trading.
- STPP Transaction Query – This document describes how to perform TRANSACTIONQUERY XML Requests through Secure Trading.
- STPP AVS and CVV2 – This document explains how the Address Verification System and security code checks are used, and provides test details to test your implementation.

Any other document regarding STPP can be found on Secure Trading's website (http://www.securetrading.com). Alternatively, please contact our support team as outlined above.

6.4 Frequently Asked Questions

Please visit the FAQ section on our website (http://www.securetrading.com/support/faq).