



## IPP Integration Guide

### integrated Hosted Payment Page V 2.7

IP Payments Pty Ltd  
Level 3, 441 Kent Street  
Sydney  
NSW 2000  
Australia  
(ABN 86 095 635 680)

T +61 2 9255 9500  
F +61 2 8248 1276  
[www.ippayments.com](http://www.ippayments.com)

No part of this document may be reproduced or copied, except as permitted under the Copyright Act 1968 (Commonwealth), by any means or process whether electronic, photocopying or otherwise, without the prior written consent of IP Payments Pty Ltd.

## Table of Contents

<b>1</b>	<b>ABOUT THIS DOCUMENT .....</b>	<b>3</b>
1.1	DOCUMENT HISTORY .....	3
1.2	DEFINITIONS .....	3
<b>2</b>	<b>PURPOSE OF THIS DOCUMENT .....</b>	<b>5</b>
<b>3</b>	<b>INTRODUCTION .....</b>	<b>5</b>
<b>4</b>	<b>SOLUTION OVERVIEW .....</b>	<b>7</b>
4.1	IHPP PROCESS .....	7
4.1.1	<i>iHPP Process Overview.....</i>	7
4.1.2	<i>Session Initiation.....</i>	8
4.1.3	<i>Payment Page and Transaction Processing .....</i>	13
4.1.4	<i>Query a Transaction.....</i>	16
4.2	PAYMENT PAGE DESIGN .....	18
4.2.1	<i>Standard Payment Page .....</i>	18
4.2.2	<i>Modified Payment Page.....</i>	18
4.3	PAYMENT PAGE FUNCTIONALITY .....	27
4.3.1	<i>DL Naming Convention .....</i>	27
4.3.2	<i>Functionality Options.....</i>	27
4.3.3	<i>Form Validation and Error Messages.....</i>	29
4.3.4	<i>Tokenisation.....</i>	30
4.4	ACCOUNT HIERARCHY .....	31
4.5	SURCHARGING .....	32
4.5.1	<i>Dynamic Display of Surcharge .....</i>	32
<b>5</b>	<b>ENVIRONMENTS.....</b>	<b>33</b>
5.1	TEST ENVIRONMENT (DEMO) .....	33
5.2	PRODUCTION ENVIRONMENT (PROD) .....	33
<b>6</b>	<b>APPENDIX.....</b>	<b>34</b>
6.1	PRE-REQUISITES .....	34
6.2	REFERENCE DOCUMENTS .....	34
6.3	STANDARD IHPP DESIGN AND EXAMPLES .....	35
6.4	BANK RESPONSE CODES .....	36
6.5	IP PAYMENTS DECLINED RESPONSES CODES.....	37

# 1 About this document

## 1.1 Document history

Version	Date Modified	Author	Summary of Changes
V1.0	01/05/2014	Anne Kehoe	Document created.
V1.1	12/05/2014	Anne Kehoe	Tokenisation added.
V1.2	19/05/2014	Anne Kehoe	Content update.
V1.3	04/07/2014	Anne Kehoe	Updated the Payment Page Design section.
V1.4	18/07/2014	Anne Kehoe	Update to session initiation response field names.
V1.5	26/09/2014	Vickie Oyston	Included Prod details and changed Custref to mandatory.
V1.6	09/10/2014	Anne Kehoe	Content update.
V1.7	17/11/2014	Anne Kehoe	Added surcharge.
V1.8	11/12/2014	Anthony Fulton	Updated SessionId to Alphanumeric. AccountNumber optional
V1.9	02/02/2015	Celine Wang	Updated content for new features.
V2.0	04/02/2015	Anne Kehoe	Updated content for new features.
V2.1	06/02/2015	Celine Wang	Updated content for new features.
V2.2	12/02/2015	Anne Kehoe	Updated content for new features.
V2.3	05/03/2015	Celine Wang	Updated to Functionality type.
V2.4	19/03/2015	Celine Wang	Updated template structure, Result values and cancel button details.
V2.5	1/06/2015	Celine Wang	Added reference to external content.
V2.6	23/07/2015	Celine Wang	Updated content for new features.
V2.7	09/09/2015	Celine Wang	Added ReCaptcha

## 1.2 Definitions

The following terms and abbreviations are used in this document:

Term	Description
IPP	IP Payments, a premium payments solutions provider uniquely skilled in providing high-quality, efficient and customised solutions to corporate organisations in all industry sectors.
Merchant	For the purposes of this document your company will be referred to as the 'merchant'. A person or company involved in wholesale trade, supplying goods or services to a business or consumer market.
Acquiring Bank	An acquiring bank (or acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant.
CR	A change request is an issue, defect or new requirement which is raised by a business person and/or representative of a local affiliate which is not described or described in a different way in the latest version of the SDS document (+ amendments).
CC	Creditcard.
Security Code (CVV2/CSC2/CCV)	The Security Code is a 3 or 4 digit code on the back of the cardholder's card. This is used to verify the customer is in possession of the card.
PAN	Primary Account Number (Credit Card Number).

PCI-DSS	Payment Card Industry Data Security Standard. PCI-DSS is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
Access Portal	Access Portal is the platform used by IPP to implement our hosted payment applications – HPP and iHPP.
HPP	The Hosted Payment Page is a standalone payment page which is not integrated into an application.
iHPP	The integrated Hosted Payment Page is integrated into the merchant's website dynamically accepting transaction data prior to the customer entering their card details. Notification of the transaction result is sent back to the merchant in real-time.
iFrame	Inline Frame, a HTML tag used to embed another document within an existing HTML document. Specifically used in this document to describe how to embed the IPP payment page in the merchants website.
DL	Direct Link, this is the value used to specify which iHPP template is to be used. Required where more than one iHPP exists for a particular client account.
HTML	Hypertext Markup Language
POST	A method for sending HTML form data over the Internet. Post data is encoded within the message body.
GET	A method for sending HTML form data over the Internet. Get data is encoded by a browser into the URL.
CSS	Cascading Style Sheets is a style sheet language used for describing the presentation of a web page.
SST	Secure Session Token
URL	Uniform Resource Locator
WSDL	Web Services Description Language
PRM	Payment Relationship Manager, IPP's transaction reporting tool used for user administration, viewing transaction history, refunding and downloading reports among other functionality.
CSV	CSV meaning Comma Separated Values is a report format which can be downloaded from our reporting tool, PRM.
API	Application Programming Interface, a merchant can use IPP's API to gain access to the features and data of our services and applications.
SOAP	Simple Object Access Protocol, a protocol specification for exchanging structured information in the implementation of web services.
XML	eXtensible Markup Language defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.
SIPP	Statement of Invoice Presentment and Payment
TCP/IP	Transmission Control Protocol/Internet Protocol
Tokenisation	Storage of the customer's card data against a unique reference called a token in IPP's secure PCI-DSS compliant system for future use in recurring payments or adhoc payments using a stored payment method. This removes the need for the merchant to store card data minimising their PCI DSS scope. If you require tokenisation of bank account details, please contact IPP.  This is an additional service and must be enabled on your account.
Token	The unique reference that the customers card data is stored against in IPP's secure PCI-DSS compliant system.

MOD10 Check	A simple algorithm used to validate a credit card number.
APCA ID	An ID provided by APCA (Australian Payments Clearing Association) required for the processing of bank account payments.

## 2 Purpose of this document

The purpose of this document is to describe the requirements and functionality of the integrated Hosted Payment Page (iHPP) solution that will be implemented for you by IP Payments Pty Ltd ("IPP").

This document also outlines what is involved for you, the merchant, to integrate into the IPP iHPP using an iFrame implementation.

If this document does not meet your needs, please contact us to discuss your requirements and the bespoke solutions we can offer.

## 3 Introduction

IP Payments is a premium payments solutions provider, uniquely skilled in providing high-quality, efficient, reliable and customised solutions to corporate organisations in all industry sectors. We develop and manage web based billing, payment and reconciliation services for some of the most recognised brand names in the world.

This document outlines the integration of the iHPP. If you would like further information on other IPP products or wish to discuss your businesses requirements in more detail, please don't hesitate to contact us.

### Access Portal

IPP have developed a flexible and innovative platform called Access Portal for delivering our hosted payments applications.

### Hosted Payment Page

IPP's Hosted Payment Page (HPP) is a standalone payment page which is not integrated into your application / website. This means the transaction data such as transaction amount and customer reference is entered on screen by the customer / agent. Transactions are processed in real-time and a response displayed to the screen however, a notification is not sent in real-time upon completion of the transaction. Transaction results can be viewed and downloaded in the IPP reporting facility, PRM.

### Integrated Hosted Payment Page

IPP's integrated Hosted Payment Page (iHPP) provides you with the ability to accept credit card and bank account payments on your website in real-time. The iHPP is device agnostic rendering responsively for web, mobile and table devices. You can also use iHPP to store your customer's card data for future use, see details on tokenisation below.

The iHPP is integrated into your website and accepts transaction data such as amount and customer references prior to the customer entering their card details. Transactions are processed in real-time and a response displayed to the screen. A notification of the transaction result is sent back to you in real-time for update of internal systems.

### Tokenisation

IPP offer a tokenisation solution which allows merchant's to store their customer's card data against a unique reference called a token in IPP's secure PCI-DSS compliant system. The token can subsequently be submitted by the merchant for future recurring or one-click payment requests. Once the token is submitted by the merchant, IPP will look up the corresponding card data and process the transaction as normal.

This removes the need for the merchant to store card data in their system minimising their PCI DSS scope and ensuring ongoing compliance against maturing standards.

This is an additional service and must be enabled on your account prior to successfully tokenising card data. If you are interested in this service, please contact us for further information. If you require tokenisation of bank account details, please contact IPP.

## 4 Solution Overview

### 4.1 iHPP Process

#### 4.1.1 iHPP Process Overview

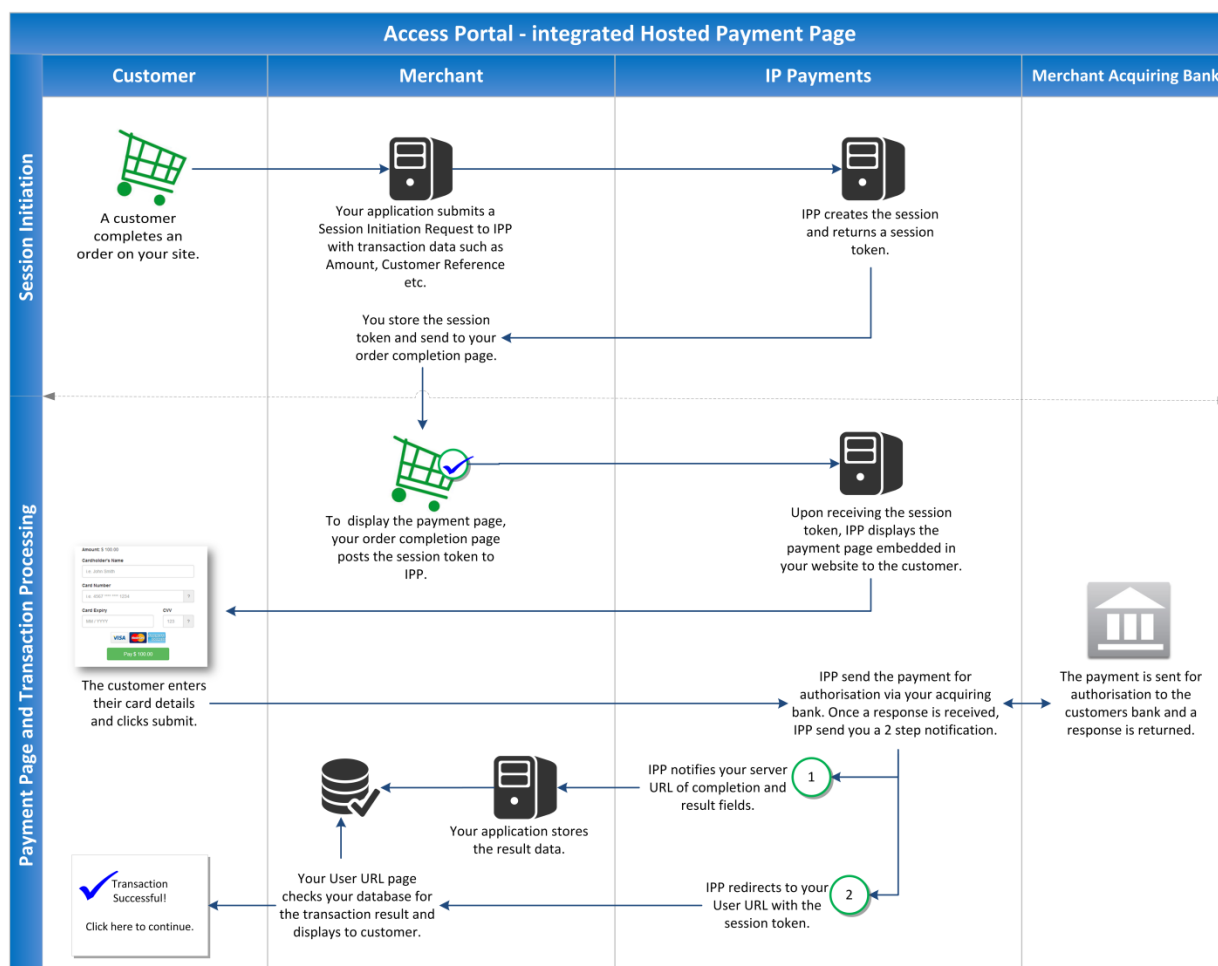
The following process outlines how you can use IPP's iHPP to carry out single submission transaction requests to debit a customer for a single payment. The same process is used for tokenisation with some additional request and response fields, debiting the customer for their initial payment and storing their card details for future payment requests.

##### 4.1.1.1 Single Submission Payments / Tokenisation

The processing of online transactions via iHPP follows the following sequence:

1. Session Initiation
2. Payment Page and Transaction Processing.

Please see diagram and transaction flow description below:



#### Session Initiation

1. A customer completes an order on your site and proceeds to your order completion page.
2. Your application generates and submits a session initiation request to IPP using a HTTP POST with the necessary transaction data required for IPP to complete the transaction, such as your account

credentials (Username, Password), transaction amount, customer reference, the response URLs (ServerURL, UserURL) where IPP will return the transaction response to. If you are implementing tokenisation, you will also submit the additional tokenisation request fields needed for IPP to store the customers card for future use.

3. IPP will create the session once all the necessary data is received and send back a secure session token (SST).

#### Payment Page and Transaction Processing

4. You can then display the IPP payment page embedded in an iframe on your order completion page by submitting the SST in a HTTP POST to IPP.
5. The customer enters their card details on the IPP payment page and clicks submit.
6. IPP sends the payment for authorisation to your acquiring bank who connect via the schemes (Visa, MC, Amex or Diners) to the customers issuing bank who checks the customers balance, card data, etc. The transaction response is passed back via the same route to IPP. If you are utilising tokenisation, IPP will store the card data against a token ready to be used for future payment requests (Tokenisation occurs for successful and declined transaction response).
7. IPP sends back two notification requests to you as follows:
  - a. IPP sends back the result fields using a HTTP POST to your "ServerURL" (submitted by you in the request.) Your application stores the result data in your database. Result data will include any data submitted to IPP in the request along with the transaction result. For tokenisation it will also include the token reference which you can store against the customer reference for future payment requests.
  - b. IPP sends a second notification to your "USERURL" (submitted by you in the request) with the SST. You can then query your database with the SST to get the transaction result stored from the first notification. Once you have the result, you can display the necessary response text to the customer.

#### 4.1.1.2 Tokenisation – future payment requests

Please see section Tokenisation for further information on the transaction submission methods on tokenised cards and data migration of any existing card data you may have.

### 4.1.2 Session Initiation

#### 4.1.2.1 Request

The POST generated by your server is submitted to the IPP server URL; see section Environments which details the URLs for the test and production environments.

The following table lists the values that your server must POST to IPP to initiate the session.

Merchant Server POST to IPP – Server Session Initiation				
Value	Max length	Data type	Mandatory / Optional	Description
UserName	32	AlphaNumeric	M	API Username
Password	16	AlphaNumeric	M	API Password
Amount	10	Numeric	M	Amount entered in cent value e.g. \$55.00 = 5500  Please note the amount field is not required for tokenise only transactions. Please see section Payment Page Functionality for further information on tokenise only.



SessionID	64	Alphanumeric	M	Merchant's unique session identifier. Maintain this session identifier throughout the life of the transaction.
SessionKey	64	Alphanumeric	M	<p>Generated by the merchant, can be any value e.g. random generated number, timestamp etc.</p> <p>The session key is to be included for security and authentication purposes. This Key should only be passed to IPP's server and should not be sent to your front end. IPP will return the SessionKey to your ServerURL in the transaction response once the payment has been processed. If you do not receive a SessionKey or receive an invalid SessionKey, then this should be treated as a possible fraudulent transaction. IP Payments needs to be notified of this event along with your internal teams for investigation.</p>
ServerURL	512	AlphaNumeric	M	<p>This value must be Base 64 encoded.</p> <p>The URL of your server that IPP will POST the first notification to including the transaction result data.</p> <p>If you do not require data to be sent to the ServerURL, please leave this field empty.</p>
UserURL	512	AlphaNumeric	M	<p>This value must be Base 64 encoded.</p> <p>The URL to force the user browser to POST to; this is the second notification.</p>
DL	32	AlphaNumeric	M	<p>This value is used to specify the styling and functionality IPP should display to your customer. Please see section Payment Page Functionality for full details on DL value.</p> <p>DL values will be confirmed by IPP upon account setup.</p>
AccountNumber	16	AlphaNumeric	O	<p>This value dictates which account the transaction will be processed through. Refer to section Account Hierarchy.</p> <p>If this value is not populated, the transaction will be processed to the account tied to the username field.</p>
CustRef	64	AlphaNumeric	M	A reference for the transaction sent by you for reporting purposes.

CustNumber	64	AlphaNumeric	O	An additional reference for the transaction sent by you for reporting purposes.
Email	64	Text	O	<p>An additional reference for the transaction sent by you for reporting purposes.</p> <p>Please note IP Payments can enable this field to send an email receipt to the email address entered in this field. Please contact IP Payments if you require this service.</p>
Reference1	32	Text	O	<p>This field name can be changed to something more suitable to your company for example "AccountID". Please advise IPP if you wish to change it.</p> <p>An additional reference that can be sent by you for reporting purposes e.g. a customer identifier unique to your system. Stored for payment requests only i.e. not for the tokenise only transaction. This will be available to view and download with the transaction details in our reporting tool, PRM.</p>
Reference2	64	Text	O	<p>This field name can be changed to something more suitable to your company for example "AccountID". Please advise IPP if you wish to change it.</p> <p>An additional reference that can be sent by you for reporting purposes e.g. a customer identifier unique to your system. Stored for payment requests only i.e. not for the tokenise only transaction. This will be available to view and download with the transaction details in our reporting tool, PRM.</p>
Reference3	128	Text	O	<p>This field name can be changed to something more suitable to your company for example "AccountID". Please advise IPP if you wish to change it.</p> <p>An additional reference that can be sent by you for reporting purposes e.g. a customer identifier unique to your system. Stored for payment requests only i.e. not for the tokenise only transaction. This will be available to view and download with the transaction details in our reporting tool, PRM.</p>
Reference4	1024	Text	O	This field name can be changed to something more suitable to your company for example "AccountID". Please advise IPP

				<p>if you wish to change it.</p> <p>An additional reference that can be sent by you for reporting purposes e.g. a customer identifier unique to your system. Stored for payment requests only i.e. not for the tokenise only transaction. This will be available to view and download with the transaction details in our reporting tool, PRM.</p>
Reference5	1024	Text	O	<p>This field name can be changed to something more suitable to your company for example "AccountID". Please advise IPP if you wish to change it.</p> <p>An additional reference that can be sent by you for reporting purposes e.g. a customer identifier unique to your system. Stored for payment requests only i.e. not for the tokenise only transaction. This will be available to view and download with the transaction details in our reporting tool, PRM.</p>
Stylename	64	Alphanumeric	O	<p>IPP offer the ability to have multiple CSS styles for the same payment page. This can be useful if you have multiple brands with different styling.</p> <p>Please see section <b>Payment</b> Page Design for further details.</p>
UserDeclinedURL	512	AlphaNumeric	O	<p>IPP offer the ability to have a cancel button on your payment page. By default this page will redirect to the UserURL. If you wish this button to redirect to a different page other than the UserURL, you can specify the UserDeclinedURL in this field. If your customer selects the cancel button on the payment page, the page will be redirected to the declined URL.</p> <p>Please note if you send a value in this field, all responses for declined transactions will be sent to this URL including cancelled transactions and transactions which have been declined by the bank.</p> <p>Please see section Cancel Button for further information.</p>
<b>Tokenisation fields</b> <i>Additional fields only required for tokenising the card. Not required if tokenisation is not being implemented by the merchant.</i>				
CustomerStorage Number	32	AlphaNumeric	O	<p>The account against which to store the token. Please see section</p>

				Account Hierarchy.
--	--	--	--	--------------------

#### 4.1.2.1.1 Preferred Submission Method – POST

IPP prefer the use of the POST method when submitting the session initiation as it is a more secure method of integration. Although GET is not the preferred method of integration, this is also an option. Please note you cannot use GET in the user's browser to submit the initial request data described above. If GET is being used for the initial submission, it must come from a server where the request data cannot be seen by the end user in the URL bar.

#### 4.1.2.2 Response

IPP returns the secure session token if the session initiation is successful, or an error description if the session cannot be initiated. This result is presented as XML parsable HTML. The value of SessionStored is 'True' if the session was initiated and stored correctly.

IPP Server to Merchant Server Result - Server Session Initiation				
Element name	Max size	Format	Description	Example Response
SessionStored	64	AlphaNumeric	Value that can be either True or False	True
SessionStoredError	256	AlphaNumeric	Textual description of the error. This field will only be populated if the SessionStored value is False.	Invalid username or password.
SST	64	AlphaNumeric	Secure Session Token. This field will only be populated if the SessionStored value is True.	3skygj450xenmtrg4bbyoimh

Example of the html returned upon successful session initiation:

```
<html>
<body>
<form>
<input type="hidden" name="SessionStored" value="True" />
<input type="hidden" name="SessionStoredError" value="" />
<input type="hidden" name="SST" value="3skygj450xenmtrg4bbyoimh" />
</form>
</body>
</html>
```

Example of the html returned upon failed session initiation:

```
<html>
<body>
<form>
<input type="hidden" name="SessionStored" value="False" />
<input type="hidden" name="SessionStoredError" value="Invalid username or password" />
<input type="hidden" name="SST" value="" />
</form>
</body>
</html>
```

### 4.1.3 Payment Page and Transaction Processing

#### 4.1.3.1 Request

Once the session is established, your backend application notifies your website which then POSTs (GET also supported) the Session ID and Secure Session Token to IPP's server URL.

The following table lists the values that your application forces the customer's browser to POST/GET to IPP.

User Browser POST to IPP Server		
Value	Max length	Description
SessionId	64	Merchant's unique session identifier. Defined by the merchant in the session initiation request.
SST	64	The Secure Session Token. Provided by IPP in the session initiation response.

Upon posting the above values to the necessary URL, the payment page will be displayed. This can be embedded in your website using an iFrame solution. The customer will be required to enter the following payment details into the payment form.

- Cardholder name
- Card number
- Security Code (CVV)
- Expiry date

#### 4.1.3.2 Response

IPP provides notification of the transaction completion to you in two steps.

1. The first step is a server to server post between IPP and your application providing a more robust and secure way of sending the transaction response data to you.
2. The second step redirects the customer back to your website where they are notified of the transaction result.

#### Notification of completion – Step 1

The IPP server POSTs the response to your server using the 'ServerURL' as supplied by you in the session initiation. The following table lists the response values that IPP will POST to your server. The response data should be stored in your database and made accessible to your website.

IPP Server POST to Merchant Server		
Value	Max length	Description
Result	1	0 = Declined 1 = Approved 2 = In progress 3 = Session Expired
Receipt	8	The IPP receipt number generated for this transaction
DeclinedCode	3	If result = 0, then this will be the reason for the declined transaction as an error code. Error codes are listed in the Appendix. If result = 1, then this will be blank

DeclinedMessage	256	If result = 0, then this will be the textual description of the error. If result = 1, then this will be blank.
SST	64	The Secure Session Token.
SessionKey	64	The session key submitted by you only to IPP in the session initiation request.
SessionId	64	Merchant unique session identifier
MaskedCard	16	The masked credit card number. This will show first 6 and last 4 digits of card number. E.g. 123456*****4321
ExpiryDate	5	The credit card expiry date. Format: MM/YY
CardHolderName	64	The card holder name (if captured)
CardType	16	E.g. MasterCard, Visa, American Express, Diners
CardSubType	64	A value can be passed back giving further details on the card. This field is only returned if you have the CardSubType functionality enabled. Please see section Card SubType Recognition for further information.
TxDateTime	19	The transaction date/time. Format: YYYY-MM-DD HH:MM:SS E.g. 2010-01-20 18:32:30
CustNumber	64	An additional reference for the transaction sent by you for reporting purposes.
CustRef	64	Merchant Reference for the transaction
Amount	10	Transaction amount in cent value e.g. \$55.00 = 5500. This is the originally submitted amount and does not include any surcharge amount that may have been applied by IPP.
Surcharge	10	Surcharge amount applied to the transaction in cent value. This is only populated if surcharging is enabled on your account. Please see section Surcharging for further information.
AmountIncludingSurcharge	10	Transaction amount plus surcharge amount applied to the transaction in cent value. This is only populated if surcharging is enabled on your account. Please see section Surcharging for further information.
SettlementDate	10	The settlement date of the transaction returned in the following format YYYY-MM-DD.
Reference1	32	Additional optional reference submitted by you in the transaction request.
Reference2	64	Additional optional reference submitted by you in the transaction request.
Reference3	128	Additional optional reference submitted by you in the transaction request.
Reference4	256	Additional optional reference submitted by you in the transaction request.
Reference5	1024	Additional optional reference submitted by you in the transaction request.

**AU Bank Account fields**

*Additional fields returned in the response after processing AU Bank Account Transactions.*

Acctitle	60	Bank account holder name.
AccRouting	6	Bank account BSB.  For NZ direct debit processing, this will include Bank and Branch Codes
Accno	16	Bank account number.  For NZ direct debit processing, this will include NZ Account number and Suffix

**Tokenisation fields**

*Additional fields returned in the response after tokenising the card.*

Token	16	Token generated by IPP to uniquely identify this customer/credit card. (not to be confused with the secure session token)
TokenResult	1	0 - Failed Tokenisation, 1 - Successful Tokenisation  Please note: TokenDeclinedCode and TokenDeclinedMessage will be blank for TokenResult of 1 (Successful tokenisation).  If Querying the Access Portal Session (using SST, SessionID and Query=true), the following results are also possible:  2 (Session In Progress), 3 (Session expired)
TokenDeclinedCode	3	Please see possible decline codes below: <ul style="list-style-type: none"> <li>• 110</li> <li>• 998</li> </ul>
TokenDeclinedMessage	256	The message sent depends on the 3 values for TokenDeclinedCode: <ul style="list-style-type: none"> <li>• 0 : "System Exception"</li> <li>• 110: "Invalid Credit Card Number"</li> <li>• 998: "Transaction Payment Cancelled"</li> </ul>

**Notification of completion – Step 2**

IPP redirect to the 'UserURL' as supplied in the Session Initiation request and POST's the SessionID and SST. Your UserURL page can use these details to access the transaction results stored in your database from the first notification.

The following table lists the values that IPP will POST to your server when redirecting to your UserURL.

**User Browser POST to Merchant Server**

Value	Max length	Description
SessionId	64	Merchant unique session identifier. Defined by the merchant in the session initiation request.
SST	64	The Secure Session Token. Provided by IPP in the session initiation response.

Once your UserURL page receives the transaction result, it can display the details to the customer.

#### 4.1.4 Query a Transaction

You can query the results of a transaction by submitting a POST or GET request as detailed below. You can use this query method until the secure session token (SST) expires (24 hours after it was created). If you need to query the transaction after this period, you can submit a query API request. Please see our API integration guide for further information.

##### 4.1.4.1 Request

**URL:** https://<IPP server>/access/index.aspx?

**Fields to be submitted:**

Merchant Server GET to IPP – Transaction Query				
Value	Max length	Data type	Mandatory / Optional	Description
UserName	32	AlphaNumeric	M	API Username
Password	16	AlphaNumeric	M	API Password
SST	64	AlphaNumeric	M	The Secure Session Token
SessionId	64	AlphaNumeric	M	IPP Client Unique session identifier
Query	5	Alpha	M	Value set to true

##### Example Query:

Structure:

https://<IPP server>/access/index.aspx?UserName=<account login>&Password=<account password>&SST=<secure session token>&SessionId=<SessionId>&Query=true

Example:

https://demo.ippayments.com.au/access/index.aspx?UserName=ippci.ipp.api&Password=zxcv1234&SST=b82cc30f-67b6-4e9c-a151-b542dcfa5c0f&SessionId=ippci\_b46ef0e7-7011-4c2d-bc27-348379345375&Query=true

##### 4.1.4.2 Response

The response fields returned will be the same as the fields returned in the Notification 1 step of the response; see defined response fields in section Payment Page and Transaction Processing Response. Please see an example of the html returned for the Query transaction.

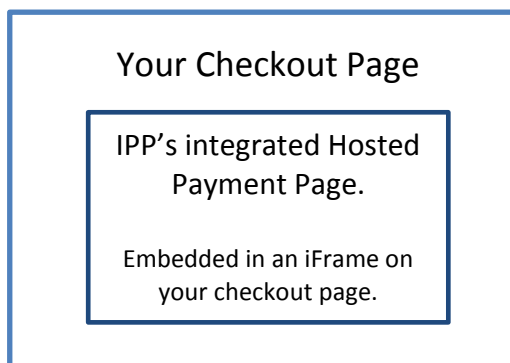
```
<html>
<body>
<form>
<input type="hidden" name="SessionId" value="ippci_b46ef0e7-7011-4c2d-bc27-348379345375" />
<input type="hidden" name="SST" value="b82cc30f-67b6-4e9c-a151-b542dcfa5c0f" />
<input type="hidden" name="SessionKey" value="" />
<input type="hidden" name="CustRef" value="NA" />
<input type="hidden" name="CustNumber" value="123455" />
<input type="hidden" name="Amount" value="100" />
<input type="hidden" name="Surcharge" value="" />
<input type="hidden" name="AmountIncludingSurchargeSurcharge" value="100" />
<input type="hidden" name="Result" value="0" />
<input type="hidden" name="DeclinedCode" value="01" />
```



```
<input type="hidden" name="DeclinedMessage" value="Refer+Card+Issuer" />
<input type="hidden" name="Receipt" value="87855444" />
<input type="hidden" name="TxDateTime" value="2012-10-26+13%3a32%3a14" />
<input type="hidden" name="SettlementDate" value="2012-10-26" />
<input type="hidden" name="MaskedCard" value="424242*****4242" />
<input type="hidden" name="CardHolderName" value="donald" />
<input type="hidden" name="ExpiryDate" value="02/14" />
<input type="hidden" name="CardType" value="Visa" />
<input type="hidden" name="Reference1" value="" />
<input type="hidden" name="Reference5" value="" />
<input type="hidden" name="Reference2" value="" />
<input type="hidden" name="Reference3" value="" />
<input type="hidden" name="Reference4" value="" />
<input type="hidden" name="Email" value="" />
</form>
</body>
</html>
```

## 4.2 Payment Page Design

With IPP's iHPP solution, you can embed the IPP payment form in your checkout page using an iFrame and is device agnostic rendering responsively for web, mobile and tablet devices. This allows you to keep control of the branding and design on your checkout page as only the payment form is hosted and controlled by IPP. Please see wireframe below of how this would be implemented.



### 4.2.1 Standard Payment Page

IPP offers a payment form with standard styling and the following form fields:

- Cardholder name
- Credit card number
- Expiry date
- Security code

Please see a sample of the standard form and examples of how the payment page can be embedded in your website in Appendix Standard iHPP Design and Examples.

### 4.2.2 Modified Payment Page

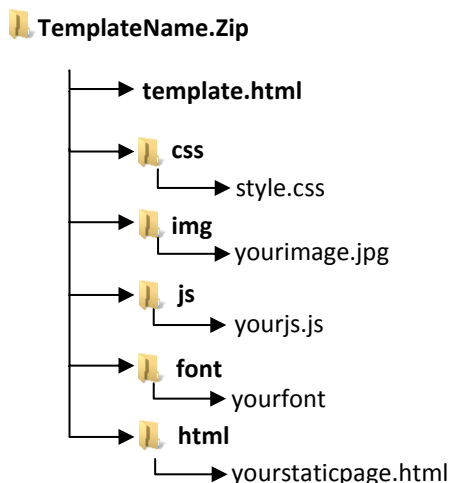
Rather than using the standard payment page, you also have the option to build your own version of the iHPP. The IPP iHPP is extremely flexible allowing you to define the structure and style of the payment page and even allows you to choose the fields you'd like the customer to populate on the form.

To build your own version of the iHPP, you will need to create a style template in the structure detailed below. The style template will be hosted by IPP and will need to be submitted to us prior to your account set up.

The template will be made up of a HTML page detailing the fields and structure of the form as well as any supporting files such as CSS and JS files and images referenced in the HTML page.

### 4.2.2.1 Template format

Please note IPP can provide a sample template structure including a sample HTML page to assist with your implementation. The template's images, style sheets and html file must be packaged in a zip file with the below folder and should be no larger than 1MB.



These folders and files will need to be submitted in the format outlined below.

Name	Type	Description
TemplateName.zip	Folder	<p>The zipped folder containing all the template pages and sub folders. The folder name can be chosen by you and should be Alphanumeric.</p> <p>Please note this folder name will be used as part of the DL value submitted in the HPP URL when processing a transaction. Please see section Payment Page Functionality for further information.</p>
template.html	HTML file	<p>A HTML file containing the structure of the payment form, reference JS, img, CSS and static HTML files contained in the other template folders.</p> <p>The HTML page must contain only one form tag. The form tag may contain "class" attribute. Any other attributes will be either removed or replaced by IPP.</p> <p>If a DOCTYPE element is not included in the template.html, IPP will automatically add it.</p>
css	Folder	Sub-folder containing CSS file(s).
style.css	CSS file	CSS file containing the styling information for the HTML page and payment form.
img	Folder	Sub-folder containing images.
yourimage.jpg	File	<p>Any image files you wish to include on your payment page and are relatively referenced in your html file (thus require IPP to host the image) should be stored in this folder. Any image name and format is acceptable once it has been referenced correctly in your html page.</p> <p>Please note the total template zip cannot exceed 1MB in size.</p>
js	Folder	Sub-folder containing JS file(s).

yourjs.js	JS file	JS file containing the code to perform particular tasks. Please note all JS will be screened prior to upload.
font	Folder	Sub-folder containing font file(s).
yourfont	File	Any custom font files you would like to use on your payment page. You can specify any font formats for various browsers. Please note this is not necessary for standard fonts used. This is only required if you are using a custom font.
html	Folder	Sub-folder containing any static html pages referenced by the template.html page.
Yourstaticpage.html	File	Any static HTML which you would like to include in the template. This may include help text or terms and conditions etc.

#### 4.2.2.2 HTML Page Format

Please see guidelines below for the html template page.

- The HTML must be XHTML compliant and all the html tags must be closed properly.
- A DOCTYPE element must be specified in the html page. If this has not been specified then by default the XHTML 1.0 Transitional DTD will be used i.e. the converted html will contain the below declarations. This can affect how your page and CSS is rendered.
  - `<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">`
  - `<html xmlns="http://www.w3.org/1999/xhtml">`
- The HTML page must contain only one form tag. The form tag may contain "class" attribute. Any other attributes will be either removed or replaced by IPP.

##### 4.2.2.2.1 Payment Form Fields

As described above, when building the HTML page for your iHPP you can choose the fields you wish to include on your payment form. A full list of the fields you can use on the form is detailed in the table below. You also have the option of pre-populating these fields using data passed through in the session initiation request.

The payment form fields Card Number, CCV, expiry month and expiry year must be placed on the payment form as input fields i.e. you cannot pre-populate these fields through the session initiation request. The customer must enter this data on the IPP payment form.

All other payment form fields can be:

- Passed in the session initiation in post fields so the customer does not see the data.
- Not passed in the session initiation and shown as input fields on the payment form. By default all fields on the form will be mandatory however optional fields can be made optional by having their validation removed. See section **Error! Reference source not found..**
- Passed in the session initiation and shown to the customer i.e. if you want to pass the amount to the payment page but display it to the customer. To do this you would need to implement the following:
  - **In the HTML Template:** When creating the template, ensure the required field is included in the form on HTML page with the corresponding CSS class name. The form field can be an input field if you want to allow the customer to change the data or a span field if you want to show the data to the customer for informational purposes.
  - **In the HTML Template:** Add the attribute "fill" to the end of the field class name to show the value passed in the session initiation request. For example, if the html page contains an amount text box that needs to be pre-populated using the amount value from session initiation request then the following tag should be included in the html template page – `<input type="text" class="amount fill" />`.
  - **In the Session Initiation Request:** When implementing the session initiation request, ensure the correct request field name is sent in the session initiation request for example "amount".

Please see list of all available fields that can be displayed / passed to on the payment form. Detailed also are their corresponding CSS class names required to build your CSS file and the session initiation request names.

Field name	Session Initiation Request Name	CSS Class Name	Mandatory /Optional	Pre-populate from session initiation request?	Comments
Card Number	N/A	ccnumber	M	N	For credit card payments, this field must be included on the form and entered by the customer.
CCV	N/A	ccv	M	N	For credit card payments, this field must be included on the form and entered by the customer.
Card Expiry Month	N/A	expm	M	N	For credit card payments, this field must be included on the form and entered by the customer.
Card Expiry Year	N/A	expy	M	N	For credit card payments, this field must be included on the form and entered by the customer.
Cardholder Name	cardholderna me	cardholdern ame	O	Y	Generally included on the payment form.
Amount	amount	amount	O	Y	<p>Please note the amount field should not be included on the payment page when tokenising card details only (tokenise only) i.e. when a purchase / pre-auth request is not submitted.</p> <p>Please note this field becomes mandatory if the amount is not submitted in the session initiation request.</p>
Customer Reference	custref	custref	O	Y	This field can have additional validation applied. Please see section Form Validation and Error Messages for more information.
Customer Number	custnumber	custnumber	O	Y	This field can have additional validation applied. Please see section Form Validation and Error Messages for more information.

Email	email	email	O	Y	Please note IP Payments can enable this field to send an email receipt to the email address entered in this field. Please contact IP Payments if you require this service.
Reference 1	*Reference1	*Reference1	O	Y	*Please note this field name can be changed as per your preference. If changed the new name should be passed in the session initiation and used as the class name.
Reference2	*Reference2	*Reference2	O	Y	*Please note this field name can be changed as per your preference. If changed the new name should be passed in the session initiation and used as the class name.
Reference3	*Reference3	*Reference3	O	Y	*Please note this field name can be changed as per your preference. If changed the new name should be passed in the session initiation and used as the class name.
Reference4	*Reference4	*Reference4	O	Y	*Please note this field name can be changed as per your preference. If changed the new name should be passed in the session initiation and used as the class name.
Reference5	*Reference5	*Reference5	O	Y	*Please note this field name can be changed as per your preference. If changed the new name should be passed in the session initiation and used as the class name.
Stylename	Stylename	[Stylename]	O	Y	Please see section <b>Using Multiple CSS Styles</b> for further information on this field.
Cancel Button	cancelurl	[cancelurl]	O	Y	Please see section Cancel Button for further information on this field.
Surcharge	N/A	Surcharge	O	N	Please see section Dynamic Display of Surcharge for further information.

AmountIncludingSurcharge	N/A	AmountIncludingSurcharge	O	N	Please see section Dynamic Display of Surcharge for further information.
<b>AU Bank Account Fields</b> <i>Additional fields only required for AU Bank Account Transactions.</i>					
Acctitle	N/A	acctitle	O	N	Bank account holder name.  For bank account payments this field must be included on the form and entered by the customer.
Accrouting	N/A	accrouting	O	N	Bank account BSB.  For bank account payments this field must be included on the form and entered by the customer.
Accno	N/A	accno	O	N	Bank account number.  For bank account payments this field must be included on the form and entered by the customer.
<b>NZ Bank Account Fields</b> <i>Additional fields only required for NZ Bank Account Transactions.</i>					
NZbankno	N/A	nzbankno	O	N	NA Bank Account Name  For NZ bank account payments this field must be included on the form and entered by the customer.
NZbranchno	N/A	nzbranchno	O	N	NZ Bank Account Branch Code.  For NZ bank account payments this field must be included on the form and entered by the customer.
NZaccno	N/A	nzaccno	O	N	NZ Bank Account Number  For NZ bank account payments this field must be included on the form and entered by the customer.

NZaccsuffix	N/A	nzaccsuffix	O	N	<b>NZ Bank Account Suffix</b>  For NZ bank account payments this field must be included on the form and entered by the customer.
-------------	-----	-------------	---	---	--

#### 4.2.2.2.1.1 Submit Button

- The HTML template page must contain a single form element which triggers the form submission.
- This must have the CSS class - "submitbtn".
- This element can be an html image, hyperlink, button (input type="button") or a submit button (input type="submit"). For example:

#### 4.2.2.2.1.2 Cancel Button

IPP offer the ability to include a cancel button on your payment page which allows customers to easily cancel the payment and get redirected back to either the UserURL or a different URL called UserDeclinedURL. To include the functionality on your page:

- You must include a cancel button as part of your HTML template. The cancel button on the HTML template page must have the CSS class "cancelbtn". This element can be an html image, hyperlink or form button. For example: <a href="cancelbtn">Cancel</a>
- The cancel button will redirect to a URL specified in the session initiation. By default it will redirect to the UserURL where all other transaction responses are redirected to. If you wish this button to redirect to a different page other than the UserURL, you can specify a value in the UserDeclinedURL. In this scenario, when your customer selects the cancel button on the payment page, the page will be redirected to the declined URL. Please note if you send a value in the UserDeclinedURL field, all responses for declined transactions will be sent to this URL including cancelled transactions and transactions which have been declined by the bank.

#### 4.2.2.2.1.3 Card Type Recognition

IPP can display your accepted card types on the payment page and dynamically highlight the customers entered card type. To include this on your page a <span> element with a new class called 'ccimglist' needs to be added to your template HTML page. The list of cards will be shown automatically based your preconfigured account settings.

For example: <span class="ccimglist"></span>

#### 4.2.2.2.1.4 Card SubType Recognition

IPP provides the ability to receive a real time response field which will contain a predefined value for the card entered on the payment page. Within our transaction management tool, you can upload a file containing specific BIN data and set the values to be returned if the card number matches or doesn't match the BIN's on file. For example, if you wish to differentiate between debit and credit cards, you can upload a BIN file of debit BIN's, set the matched value as Debit and the unmatched value as Credit. When the customers processes the transaction on iHPP, the response field CardSubType will be returned in the response with the value of Direct if the customer has used a direct debit card.

Please contact IPP for further information on this feature.

#### 4.2.2.2.1.5 Dynamic Surcharge Display

IPP allows you to dynamically display any applied surcharge in real time on the payment page as your customer enters their credit card number. The Surcharge amount and AmountIncludingSurcharge to be paid can be displayed by adding new fields (span, label) to your HTML page.



- To display surcharge amount, you will need to add a new class called '**surcharge**'. For example `<span class="surcharge"></span>`
- To display the AmountIncludingSurcharge to be paid (i.e. transaction amount plus surcharge amount), you will need to add a new class called "AmountIncludingSurcharge". For example `<span class="AmountIncludingSurcharge"></span>`

The Surcharge amount will be calculated using the values entered in the cardnumber and amount fields. The amount field will be sent in session initiation request or entered by the customer on the payment page depending on your integration.

#### 4.2.2.2.1.6 ReCaptcha

IPP offer the ability to protect your payment page from spam and abuse by using Googles ReCaptcha. Instead of entering complicated captcha code, the reCaptcha allows you to easily distinguish human users from bots by directly asking your customer whether or not they are robots. Where the reCaptcha detects any suspicious activities on your payment page, it will generate a test that humans can pass but computers cannot. Your customers have to prove that they were human and not a computer by correctly deciphering the character or choosing the images required.

- To use this functionality on your page a new class called '**captchaimg**' needs to be added to your template HTML page. For example: `<img src="" class="captchaimg" alt="captcha" />`

#### 4.2.2.2.2 Defining Form Fields as Mandatory or Optional

Fields specified above as optional can be made mandatory or optional on the payment form i.e. the customer will be required to enter a value. This cannot be changed for mandatory fields.

By default any field included on the payment form will be mandatory so to make a field optional use the CSS class attribute "opt" at the end of the field's class name. For example, if you want the email field to appear on the payment form but it should not be mandatory then you must specify "opt" attribute in the HTML template as follows:

```
<input type="text" class="email opt" />
```

#### 4.2.2.2.3 Per-populate Form Fields

Fields can be pre-populated on the payment form by adding the attribute "fill" to the end of the field class name. For example, if the html page contains a customer number text box that needs to be pre-populated using the custnumber value from session initiation request then you must specify the "fill" attribute in the HTML template as follows:

```
< input type="text" class="custnumber fill" >
```

#### 4.2.2.2.4 Styling Form Validation Errors

You can be flexible with the placement of your form validation errors on the payment page. See a list of form validation errors in section Form Validation and Error Messages.

The error message text can be specified in your HTML page by adding the suffix "-err" to the end of the fields class name. For example:

- ccnumber-err
- cardholdername-err
- ccv-err
- expm-err expy-err
- email-err

Please see example below:

```
<input type="text" class="email opt" />
<span class="ccv-err"></span>
```

The above HTML would display an input text box for email. If an error should appear the error message would appear in the <span> below.

#### 4.2.2.2.5 Using Multiple CSS Styles

IPP offer the ability to have multiple CSS styles for the same HTML page. This can be useful if you have multiple brands with different styling that will use the same HTML form structure. The following items must be completed to use this functionality:

- The template must be submitted with a HTML page that contains a special tag called [stylename] where the CSS is normally declared. For example,

```
<head>
  <link rel="stylesheet" type="text/css" href="[stylename].css">
</head>
```
- The [stylename] tag is used as a placeholder for the CSS file name. All CSS files should be packaged in the Zipped template folder and provided to IPP for upload.
- During session initiation, you can specify the CSS file you wish to use in the "Stylename" request field.

Please note, if you require a different payment page structure, you can submit a different template zip folder with the appropriate changes to the HTML file.

#### 4.2.2.2.6 Reference to External Content

IPP allows you to include references to external content as part of your template. JS, CSS and font files hosted on the following Content Delivery Network (CDN) URL's are accepted as part of your template.

- <https://cdnjs.cloudflare.com/>
- <https://maxcdn.bootstrapcdn.com/>
- <https://netdna.bootstrapcdn.com/>
- <https://code.jquery.com/>
- <https://ajax.googleapis.com/>
- <https://ajax.aspnetcdn.com/>
- <https://fonts.googleapis.com>
- <https://ajax.microsoft.com/>
- <https://cdn.jsdelivr.net/>
- <https://yastatic.net/>
- <https://yui.yahooapis.com/>
- <https://cdn.jsdelivr.net/>
- <http://code.ionicframework.com/>
- <https://oss.maxcdn.com/>

## 4.3 Payment Page Functionality

### 4.3.1 DL Naming Convention

Once your account is enabled with one or more of the below functionalities, you can specify which styling and functionality you want the payment page to carry out based on the “DL” value submitted in the session initiation request.

The DL value will be created using the following naming convention:

- TemplateName\_Functionality

With this naming convention, there are 2 elements separated by a “\_” character. Each element is derived from the following references:

- The “TemplateName” references the name of the zip folder containing your styling template (see section Payment Page Design).
- The “Functionality” references the functionality you require the payment page to carry out once the customer clicks submit. Please see a list of functionalities provided on the standard payment page in section Functionality Options. Please note your account must be enabled for each piece of functionality prior to use on your payment page.

### 4.3.2 Functionality Options

Your account will be enabled with one or more of the below functionalities based on your requirements.

- Credit card processing – pre-auth or purchase
- Direct debit processing
- Tokenisation – storage of credit card details where IPP generate the unique reference.
- Customer registration – storage of credit card or bank account details where the merchant generates the unique reference.

See details table below.

Payment Page Functionality		
Name	Description	Functionality name <i>Example DL values below. DL values to be confirmed with IPP prior to account setup.</i>
Purchase	<ul style="list-style-type: none"> <li>• Process a real time purchase transaction when the customer clicks submit.</li> <li>• If the purchase is successful, the customer’s card will be debited the transaction amount.</li> </ul>	Functionality name: Purchase  <i>Example DL value – Style1_Purchase</i>
PreAuth	<ul style="list-style-type: none"> <li>• Process a real time pre-auth transaction when the customer clicks submit.</li> <li>• If the pre-auth is successful, the transaction amount will be reserved only on the customer’s card.</li> <li>• Please note you must submit a follow up transaction called a capture to debit the customers card. A capture request is an xml transaction submitted to our API (see section Reference Documents).</li> </ul>	Functionality name: Pre-Auth  <i>Example DL value – Style1_PreAuth</i>
Direct Debit	<ul style="list-style-type: none"> <li>• Process a direct debit transaction using your customers’ bank account details.</li> </ul>	Functionality name: Direct Debit  <i>Example DL value – Style1_directdebit</i>

Tokenisation – card / bank account details storage		
Purchase-Tokenise	<ul style="list-style-type: none"> <li>Store the customer's card details and process a purchase transaction when the customer clicks submit.</li> <li>If the purchase is successful, the customer's card will be debited the transaction amount.</li> <li>A token will be passed back in the transaction response for use in future transactions.</li> </ul>	<p>Functionality name: Purchase-Tokenise</p> <p><i>Example DL value – Style1_ Purchase-Tokenise</i></p>
PreAuth-Tokenise	<ul style="list-style-type: none"> <li>Store the customer's card details and process a pre-auth transaction when the customer clicks submit.</li> <li>If the pre-auth is successful, the transaction amount will be reserved only on the customer's card.</li> <li>Please note you must submit a follow up transaction called a capture to debit the customers card. A capture request is an xml transaction submitted to our API (see section Reference Documents).</li> <li>A token will be passed back in the transaction response for use in future transactions.</li> </ul>	<p>Functionality name: PreAuth-Tokenisation</p> <p><i>Example DL value – Style1_ PreAuth-Tokenise</i></p>
Tokenise	<ul style="list-style-type: none"> <li>Store the customer's card details when the customer clicks submit. No payment request will be submitted.</li> <li>A token will be passed back in the transaction response for use in future transactions.</li> </ul>	<p>Functionality name: Tokenisation</p> <p><i>Example DL value – Style1_ Tokenise</i></p>
Customer registration – card / bank account details storage		
Card Registration	<ul style="list-style-type: none"> <li>Store the customer's card details against a unique reference - CustNumber - when the customer clicks submit. With this functionality type, no payment request will be submitted.</li> <li>The registered CustNumber can be used for processing future transactions.</li> </ul>	<p>Functionality name: Card Registration</p> <p><i>Example DL value – Style1_ registercc</i></p>
Pre-Auth and Card Registration	<ul style="list-style-type: none"> <li>Store the customer's card details against a unique reference – CustNumber - and process a pre-auth transaction when the customer clicks submit.</li> <li>If the pre-auth is successful, the transaction amount will be reserved only on the customer's card.</li> <li>Please note you must submit a follow up transaction called a capture to debit the customers card. A capture request is an xml transaction submitted to our API (see section Reference Documents).</li> <li>The registered CustNumber can be used for processing future transactions.</li> </ul>	<p>Functionality name: Pre-Auth and Card Registration</p> <p><i>Example DL value – Style1_preauthregistercc</i></p>
Purchase and Card Registration	<ul style="list-style-type: none"> <li>Store the customer's card details against a unique reference – CustNumber - and process a purchase transaction when the customer clicks submit.</li> <li>If the purchase is successful, the customer's card will be debited the transaction amount.</li> <li>The registered CustNumber can be used for processing future transactions.</li> </ul>	<p>Functionality name: Purchase and Card Registration</p> <p><i>Example DL value – Style1_purchaseregistercc</i></p>

Bank Account Registration	<ul style="list-style-type: none"> <li>Store the customer's bank account details against the unique reference CustNumber when the customer clicks submit. No payment request will be submitted.</li> <li>The registered CustNumber can be used for processing future transactions.</li> </ul>	Functionality name: Bank Account Registration  <i>Example DL value – Style1_registerba</i>
Direct Debit and Bank Account Registration	<ul style="list-style-type: none"> <li>Store the customer's bank account details against the unique reference CustNumber when the customer clicks submit.</li> <li>Process a direct debit transaction using your customers' bank account details.</li> <li>The registered CustNumber can be used for processing future transactions.</li> </ul>	Functionality name: Direct Debit and Bank Account Registration  <i>Example DL value – Style1_directdebitregisterba</i>

### 4.3.3 Form Validation and Error Messages

The standard and modified payment page uses the following form validation and error messages.

Form Validation and Error Messages.		
Field Name	Validation	Error Message example
Cardholder's Name	<ul style="list-style-type: none"> <li>Validate the cardholder Name text field requires a value</li> </ul>	Cardholder's Name requires a value.
Card Number	<ul style="list-style-type: none"> <li>Validate a correct card number has been entered.</li> <li>Validate the card type entered is accepted.</li> </ul>	<ul style="list-style-type: none"> <li>You must enter a valid credit card number</li> <li>You must enter a valid credit card number - incorrect number of digits</li> <li>The card you have entered is not accepted. Please try another credit card</li> <li>&lt;Card type&gt; is not accepted. Please try another credit card</li> </ul>
Card Expiry	<ul style="list-style-type: none"> <li>Validate the expiry date text field has a value.</li> <li>Expiry date needs to be in the format MM/YYYY.</li> </ul>	<ul style="list-style-type: none"> <li>Expiry date requires a value</li> </ul> The expiry date you have entered appears invalid
CVV	<ul style="list-style-type: none"> <li>Validate the CVV text field has a value.</li> <li>Validate the CVV entered value is numeric.</li> <li>Validate the length of the entered value depending on the card type.</li> </ul>	<ul style="list-style-type: none"> <li>CVV requires a value</li> <li>CVV must be numeric</li> <li>CVV must be 4 digits (Amex)</li> <li>CVV must be 3 digits (Visa, MC)</li> </ul>
CustNumber	The following validations can be enabled at your request. <ul style="list-style-type: none"> <li>Validate a min and max length of the entered value</li> <li>Validate the Custnumber entered value is numeric only.</li> </ul>	<ul style="list-style-type: none"> <li>Customer Number is not valid</li> </ul>

	<ul style="list-style-type: none"> <li>Validate the Custnumber against a pre-defined check digit routine.</li> </ul>	
CustRef	<p>The following validations can be enabled at your request.</p> <ul style="list-style-type: none"> <li>Validate a min and max length of the entered value</li> <li>Validate the CustRef entered value is numeric only.</li> <li>Validate the CustRef against a pre-defined check digit routine.</li> </ul>	<ul style="list-style-type: none"> <li>Customer Number is not valid</li> </ul>

#### 4.3.4 Tokenisation

As described above, IPP offers a tokenisation solution which allows merchant's to store their customer's card data against a unique reference called a token in IPP's secure PCI-DSS compliant system. Section iHPP Process describes how you can implement the storage of card data on a payment request made by a new customer.

See info below on the submission methods IPP offer for processing future token payment requests. Please note tokenisation is an additional service and must be enabled on your account prior to successfully tokenising card data.

Once you have carried out an initial transaction for a customer and stored the card details against a token reference, you can process future payment requests using the stored token in the following scenarios:

##### Stored payment method

- You can enhance your returning customers experience by presenting them with a masked version of their card number stored through a previous payment. If the customer decides to use the same card, you can submit the payment request using IPP's secure API. Please see Appendix Reference Documents for the documents required to implement this solution. If the customer decides they want to use a new card, you can send them to the IPP iHPP to enter their new card details.

##### Recurring payments

- You may require the facility to set up the customer for recurring payments for example if the customer needs to pay a monthly subscription. IPP provide a number of integration methods for recurring payments such as creating a schedule of payments, submission via batch, submission via API. Please see Appendix Reference Documents for additional information on the methods IPP offer for recurring payment submission or feel free to contact us to discuss your options.

##### 4.3.4.1 Token Format

The IPP token is unique for each card and will not display or bear any resemblance to the original credit card number. It will not display any part of the original credit card number in the token (e.g. the last 4 digits). The token is MOD 10 compliant (last digit will be a check digit).

Token format is: **9NNNNNNNNNNNNNNNC**

Token format		
Character	Position	Description
9	1	First digit - The first digit is "9" to differentiate the sequence from any credit card number as no credit card number starts with the digit "9"
NNNNNNNNNNNNNN	2-15	Random numeric string, 14 characters in length.

C	16	Check digit. Used in the MOD10 check.
---	----	---------------------------------------

IPP have the ability to accept different token formats if the above format does not meet your systems requirements. Please contact us for further information.

#### 4.3.4.2 Migration of Card Data

IPP can facilitate the migration of any existing card data you currently store to the IPP tokenisation database. This is done through a one-off bulk tokenisation file to be uploaded in PRM.

For more information on this process please see Appendix Reference Documents.

### 4.4 Account Hierarchy

IP Payments will set up your account based on brands or divisions in your company.

- Different divisions can also be set up for reporting purposes so specific user groups can only access certain division information.
- Each account will be setup with your Acquiring Merchant ID and supporting credentials which will dictate the bank account in which your funds will be settled by your acquirer.
- If you process in multiple currencies, a division will be set up for each currency.
- IPP can also tokenise card data at the top level of the merchant account or on a divisional level.

An example of how the account may be structured is detailed below. This example merchant has 2 divisions, each with its own Acquiring Merchant ID.

#### Division 1

- Division 1 is using the standard iHPP styling for credit / debit card processing.

#### Division 2

- Division 2 has a modified iHPP Design as they want to specify their own styling.
- They will be implementing credit card processing and tokenisation to provide a stored payment method for returning customers.
- Division 2 also has 2 brands and thus has 2 iHPP implementations to meet the styling specifications of each brand. The DL value submitted by Division 2 in the request will denote the styling specification and functionality to use.

#### Merchant Account Hierarchy

Top Level Merchant	Account Name	Account Number	Acquiring Merchant ID	Functionality required	iHPP #	iHPP	DL value
Merchant 1	Division1	TBC by IPP	TBC by Merchant	Purchase (See section 4.3.2Functionality Options for further info.)	1	Standard	Standard_Purchase
Merchant 1	Division2	TBC by IPP	TBC by Merchant	Purchase-NewToken (See section 4.3.2Functionality Options for further info.)	2	Modified template names: <ul style="list-style-type: none"> <li>• Style1</li> <li>• Style2</li> </ul>	Style1_Purchase-NewToken Style2_Purchase-NewToken

## 4.5 Surcharging

IPP provides you with the ability to surcharge your customers based on the card type they enter at the time of payment. This could be used for example if you wish to pass on the cost of payment processing to the customer. The card types supported for surcharging are:

- Visa
- MasterCard
- Amex
- Diners

By default no surcharge will be applied. If you wish to surcharge your customers then you will need to advise IPP prior to account setup, IPP will then set up the surcharge on your account. The following surcharge types can be implemented.

- A fixed amount surcharge by card type.
- A percentage of the payment amount surcharge by card type.

If surcharging is enabled on your account, the surcharge amount will be calculated once the customer submits their payment details for processing. This surcharge amount will be applied to the total transaction amount and the value of the applied surcharge will be returned back to you in the transaction response.

### 4.5.1 Dynamic Display of Surcharge

IPP allow you to dynamically display any applied surcharge in real time on the payment page as your customer enters their credit card number. Please see section Dynamic Surcharge Display.



## 5 Environments

### 5.1 Test Environment (Demo)

IPP provide access to a test environment known as Demo for user acceptance testing of your solution. This will be available to you once your solution has been agreed and deployed to the Demo environment. You can access this environment by implementing the solution integration as detailed in the solution components section. The following credentials will be required to access the demo environment.

Demo Account Credentials	
URL	<a href="https://demo.ippayments.com.au/access/index.aspx">https://demo.ippayments.com.au/access/index.aspx</a>
User Name	TBC by IPP once your solution is deployed to demo.
Password	TBC by IPP once your solution is deployed to demo.

### 5.2 Production Environment (Prod)

Once you have completed your UAT, IPP will provide access to our production environment so you can process live transactions. Please note you will require a merchant services agreement with an acquiring bank to process live credit card payments. Please contact IPP for further information.

The following credentials will be required to access the production environment.

Production Account Credentials	
URL	<a href="https://www.ippayments.com.au/access/index.aspx">https://www.ippayments.com.au/access/index.aspx</a>
User Name	TBC by IPP once your solution is deployed to prod.
Password	TBC by IPP once your solution is deployed to prod.

## 6 Appendix

### 6.1 Pre-requisites

- To process credit card payments you must have a merchant services agreement with an acquiring bank. Please contact IPP for further information if you do not have this agreement in place.
- To process bank account payments, you must have an APCA ID set up. Please contact IPP for further information if you do not have this agreement in place.

### 6.2 Reference Documents

See other guides below which may be useful in implementation of your solution. You can request these guides from IPP.

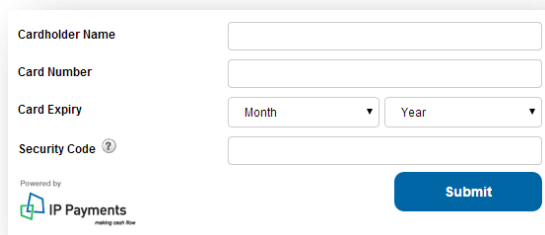
Document Name	Description
PRM User Guide	This document provides a guide to the functionality available in IP Payments reporting tool, Payment Relationship Manager (PRM).
Tokenisation integration Guide	This document outlines the integration methods for tokenisation for subsequent token and recurring payments.
Data Migration Guide	This document details the method used for migration of data such as card data to IPP.
API Integration Guide	This document describes the technical details required for integration using IPP's API.

## 6.3 Standard iHPP Design and Examples

Please see the design of the standard payment page below along with examples of how you can embed this into your checkout process in a web or mobile environment.

### Standard iHPP Design

IPP's iHPP is device agnostic rendering dynamically for web and mobile devices.




Cardholder Name

Card Number

Card Expiry

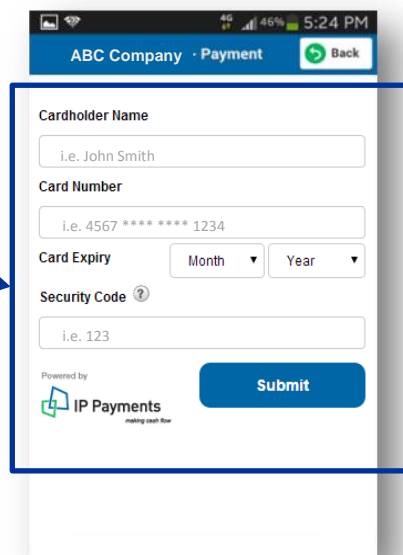
Security Code

Powered by  IP Payments making cash flow

**Submit**

### Mobile Application or Browser

IPP iHPP embedded in the merchant's mobile application using an iFrame.




ABC Company · Payment [Back](#)

Cardholder Name

Card Number

Card Expiry

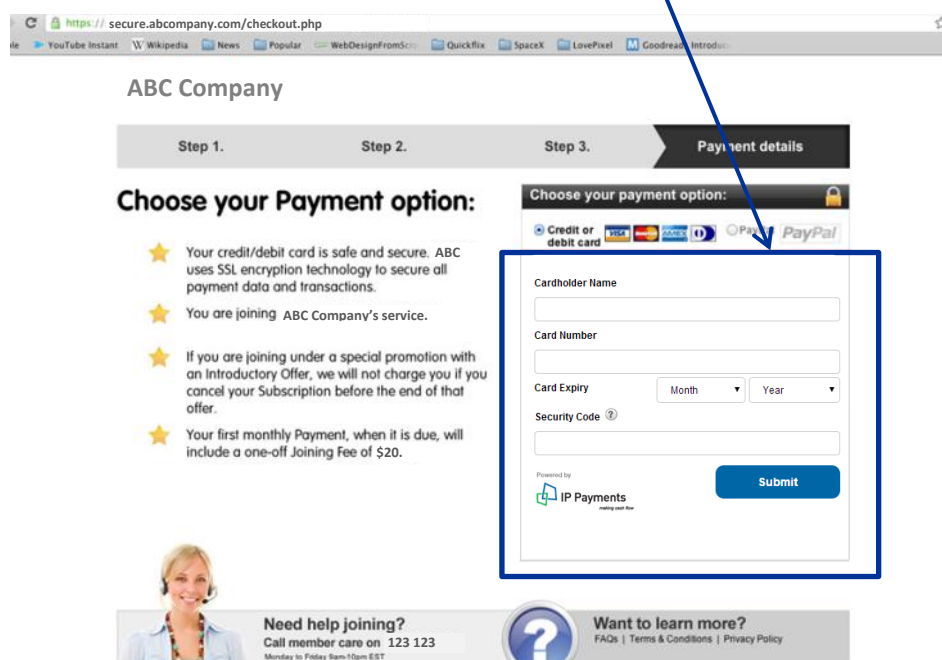
Security Code

Powered by  IP Payments making cash flow

**Submit**

### Web Browser

IPP iHPP embedded in the merchant's checkout page using an iFrame.



https://secure.abccompany.com/checkout.php


ABC Company

Step 1. Step 2. Step 3. **Payment details**

**Choose your Payment option:**

- ★ Your credit/debit card is safe and secure. ABC uses SSL encryption technology to secure all payment data and transactions.
- ★ You are joining ABC Company's service.
- ★ If you are joining under a special promotion with an introductory Offer, we will not charge you if you cancel your Subscription before the end of that offer.
- ★ Your first monthly Payment, when it is due, will include a one-off Joining Fee of \$20.

**Choose your payment option:**


☒ Credit or debit card  ☐ PayPal

Cardholder Name


Card Number


Card Expiry

Security Code

Powered by  IP Payments making cash flow

**Submit**

 **Need help joining?**  
Call member care on 123 123  
Monday to Friday 9am-5pm EST

 **Want to learn more?**  
FAQs | Terms & Conditions | Privacy Policy

## 6.4 Bank Response Codes

Codes 0 to 99 are generated by the bank. These common codes have been highlighted in the table below and are provided as is. IPP cannot guarantee that other codes will be received by the customer from the bank.

Code	Response text	Code	Response text
<b>Approved</b>			
00	Approved	08	Honour with ID
11	Approved VIP (not used)	16	Approved, Update Track 3 (not used)
77	Approved (ANZ only)		
<b>Declined</b>			
01	Refer to Card Issuer	41	Lost Card—Pick Up
02	Refer to Issuer's Special Conditions	42	No Universal Amount
03	Invalid Merchant	43	Stolen Card—Pick Up
04	Pick Up Card	44	No Investment Account
05	Do Not Honour	51	Insufficient Funds
06	Error	52	No Cheque Account
07	Pick Up Card, Special Conditions	53	No Savings Account
09	Request in Progress	54	Expired Card
10	Partial Amount Approved	55	Incorrect PIN
12	Invalid Transaction	56	No Card Record
13	Invalid Amount	57	Trans. Not Permitted to Cardholder
14	Invalid Card Number	58	Transaction not Permitted to Terminal
15	No Such Issuer	59	Suspected Fraud
17	Customer Cancellation	60	Card Acceptor Contact Acquirer
18	Customer Dispute	61	Exceeds Withdrawal Amount Limits
19	Re-enter Transaction	62	Restricted Card
20	Invalid Response	63	Security Violation
21	No Action Taken	64	Original Amount Incorrect
22	Suspected Malfunction	65	Exceeds Withdrawal Frequency Limit
23	Unacceptable Transaction Fee	66	Card Acceptor Call Acquirer Security
24	File Update not Supported by Receiver	67	Hard Capture—Pick Up Card at ATM
25	Unable to Locate Record on File	68	Response Received Too Late
26	Duplicate File Update Record	75	Allowable PIN Tries Exceeded
27	File Update Field Edit Error	86	ATM Malfunction
28	File Update File Locked Out	87	No Envelope Inserted
29	File Update not Successful	88	Unable to Dispense
30	Format Error	89	Administration Error
31	Bank not Supported by Switch	90	Cut-off in Progress
32	Completed Partially	91	Issuer or Switch is Inoperative
33	Expired Card—Pick Up	92	Financial Institution not Found
34	Suspected Fraud—Pick Up	93	Trans Cannot be Completed
35	Contact Acquirer—Pick Up	94	Duplicate Transmission
36	Restricted Card—Pick Up	95	Reconcile Error
37	Call Acquirer Security—Pick Up	96	System Malfunction
38	Allowable PIN Tries Exceeded	97	Reconciliation Totals Reset
39	No CREDIT Account	98	MAC Error
40	Requested Function not Supported	99	Reserved for National Use

## 6.5 IP Payments Declined Responses Codes

Codes above 99 are generated by IPP and are generally related to:

- configuration errors
- system exceptions

IPP recommends handling these by a generic “catch all” function that should be followed up with IP Payments

Code	Response text
100	System Exception
101	Invalid company identifier
102	Invalid account identifier
103	Invalid API username or password
104	Invalid transaction type identifier
105	Invalid channel identifier
106	Invalid currency identifier
107	Invalid transaction amount
109	No customer reference supplied
110	Invalid credit card number
111	Invalid credit card expiry date
119	Customer status not active
120	Account status not active
121	Account does not have any risk profile rules assigned
122	Registered customer details not found
124	CVN required but not supplied
150	Account not set up to accept supplied currency transactions
151	Account not set up correctly to accept supplied currency transactions
152	Account not set up to accept credit card transactions for the supplied credit card type
153	Account not set up to accept credit card transactions for the supplied amount
154	Merchant account details not set up correctly
155	Interface details not set up correctly
162	Risk profile rules failed
180	Exception encountered when retrieving the receipt number
181	Exception encountered when receiving transaction data from client
182	Exception encountered when creating transaction XML log
183	Exception parsing transaction XML
184	Exception validating transaction XML
190	Exception encountered when finding transaction identifier
191	Exception encountered when finding credit card interface to use
192	Exception encountered when submitting transaction to interface
200	Interface error
201	Interface Error with successful automatic reversal
500	Batch Record Exception
997	Remote Interface Exception
998	Transaction Payment Cancelled
999	Timeout when waiting for a response