

account**2**account



Account2Account (A2A) Integration Guide

Version 1.2

DOCUMENT REVISION INFORMATION

Version	Date	Revision Information
0.1	19/04/2012	Initial draft.
0.2	16/05/2012	Updated with internal feedback.
0.3	28/05/2012	Updated with internal feedback.
1.0	08/06/2012	Release version.
1.1	17/09/2012	Updated screenshots, added FAQ section, new banks added.
1.2	03/07/2013	Updated Banks list, screenshots, FAQ & overview section. Added statement fields and reconciliation, A2A Customisation section.

RELATED DOCUMENTS

Version	Document Title	Link/Location

COPYRIGHT

© Copyright 2013, Direct Payment Solutions (DPS) Limited
98 Anzac Avenue
PO Box 8400
Auckland, 1035
New Zealand
www.paymentexpress.com

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the express written permission of Direct Payment Solutions.

PROPRIETY NOTICE

The information described in this document is proprietary and confidential to Direct Payment Solutions (DPS). Any unauthorised use of this material is expressly prohibited except as authorised by Direct Payment Solutions in writing.

CONTENTS

1	Overview	1
1.1	Supported Banks.....	3
1.2	How it works.....	3
1.3	Test Accounts	3
1.4	Sample Code	4
1.5	Basic Communication	4
2	Technical Specification	5
2.1	Transaction Request.....	5
2.1.1	Generate Request.....	5
2.1.2	Request.....	6
2.2	Transaction Response	7
2.2.1	ProcessResponse	7
2.2.2	Response	8
3	A2A Screens	9
3.1	Bank Selection	9
3.2	Authentication	10
3.3	Additional Authentication.....	11
3.4	Account Selection	12
3.5	Payment Details	13
3.6	Payment Result.....	14
4	Statement Fields and Reconciliation	15
5	PX Pay Comparison.....	15
6	A2A Customisation.....	16
7	FAQ.....	17
9	Appendix.....	21
9.1	Contact DPS	21

1 OVERVIEW

Account2Account (A2A) provides a solution for merchants to accept payments directly into their bank account by creating a one-off online payment using the customer's online banking portal. This sort of facility is already widely used where a merchant provides their bank account details and customers pay by creating a one-off payment via their online banking portal.

The key difference is that with DPS A2A, the one-off payment is created on a secure page hosted at DPS. DPS can authoritatively inform the merchant when a payment is created and the customer is redirected back to the merchant's website once payment is created. This means that the merchant website receives the transaction outcome in real-time. Goods can then be shipped on the receipt of funds to the merchant's bank account (or at the merchant's discretion).

As with any transaction processed via the DPS gateway, all transaction details are logged and are made available on Payline® for reporting and reconciliation purposes. A2A also supports custom hosted configuration which means the merchant will have the ability to make certain changes on the styles (for more information, please refer to [A2A Customisation section](#)).

A2A is also an extension of DPS' PX Pay 2.0 which provides merchants with an alternative payment option to card oriented payments and using the same hosted payments page architecture.

There are two ways of how A2A can be integrated:

- A2A Standalone
- A2A via PxPay 2.0

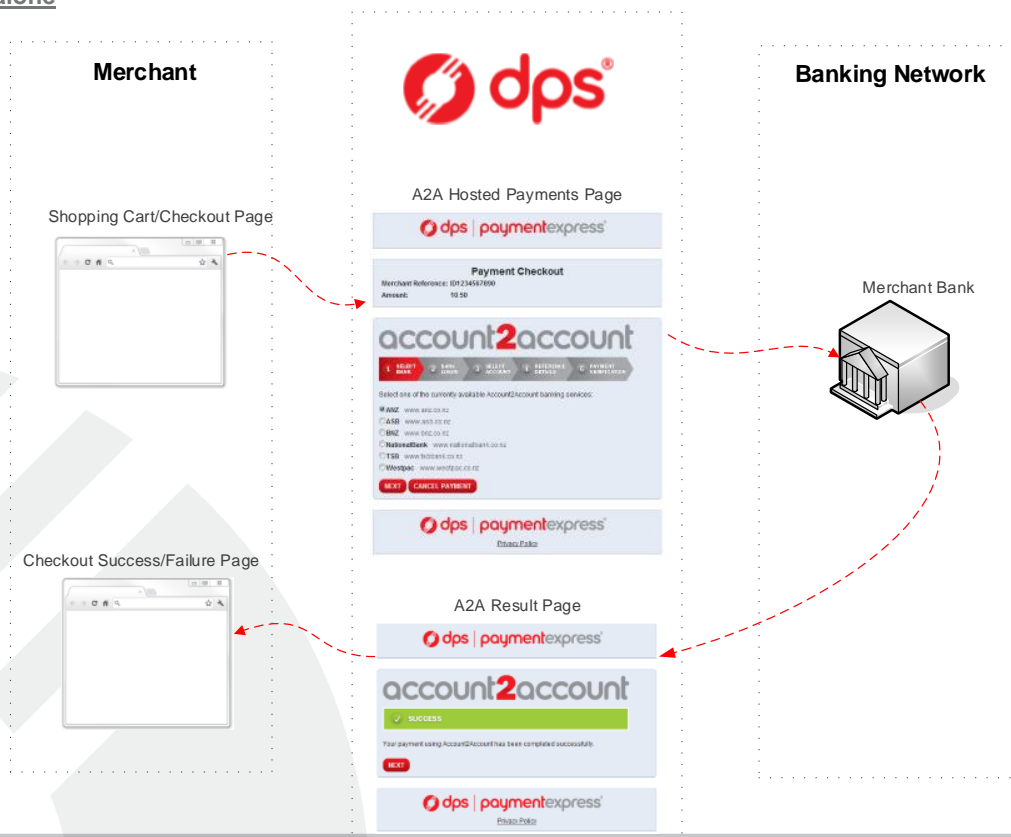
We will be focusing on the A2A standalone integration in this document.

Note: The integration process is very similar to the PxPay integration. For the merchants already integrated and familiar with PxPay please refer to [PxPay Comparison Section](#) for PxPay & A2A differences.

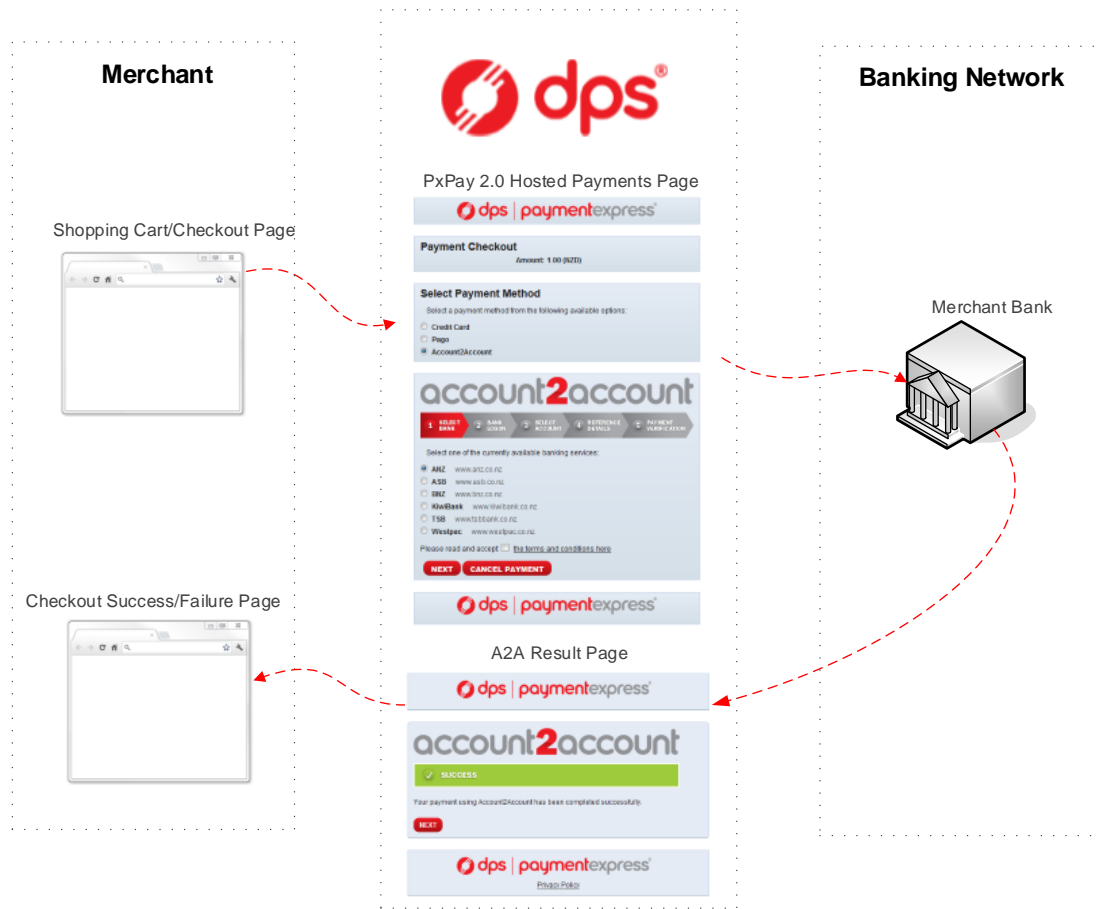
NOTE: Please ensure that your integration support LAX versioning

A basic demo of this service can be found at the link here. https://www.dpsdemo.com/a2a_demo/a2ademo_home.htm

A2A standalone



A2A via PxPay 2.0



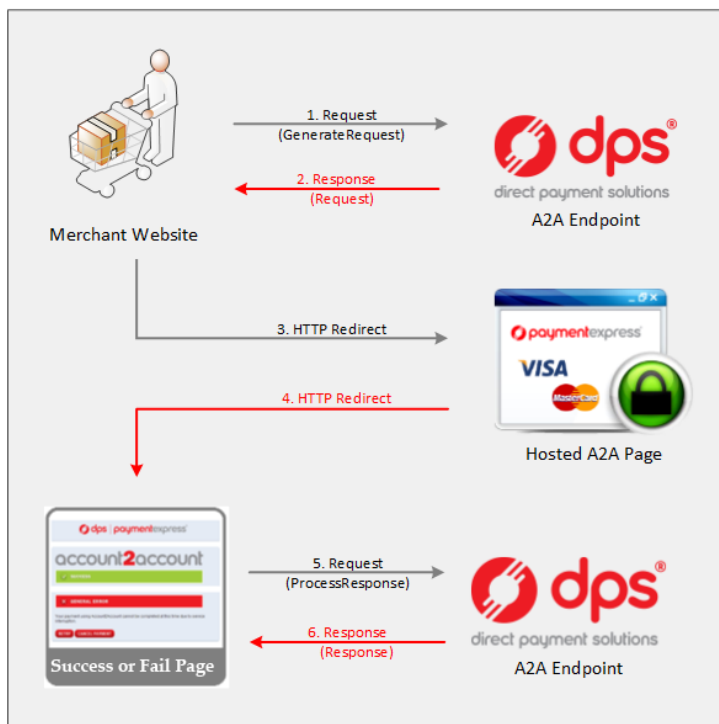
1.1 SUPPORTED BANKS

The banks currently supported by A2A are:

ANZ	www.anz.co.nz
ASB	www.asb.co.nz
Bank of New Zealand	www.bnz.co.nz
Kiwibank	www.kiwibank.co.nz
TSB	www.tsbbank.co.nz
Westpac	www.westpac.co.nz

1.2 HOW IT WORKS

A2A Process Flow



1. To process a transaction, A2A allows merchants to send XML requests to Payment Express® via HTTPS posts to <https://sec.paymentexpress.com/pxaccess/pxa2a.aspx>
2. DPS responds with a unique URI (encrypted URL) for an SSL secure payments page.
3. The merchant shopping cart uses the returned URI to redirect the customer to the secure DPS hosted payments page.
4. The customer will be prompted to login to their bank account and follow the standard steps to make a one-off online payment. The transaction result is displayed and the user is automatically redirected back to the merchant's website (success or fail page). The transaction details are also sent in this step. Transaction details are encrypted and can only be decrypted by using the provided PX Pay username and PX Pay key.
5. To extract the transaction details from the encrypted result string, the merchant sends the result string to DPS (same address as step 1) along with their PX Pay username and PX Pay key.
6. The transaction results and other transaction details are decrypted and sent back to the merchant as a standard XML response (note: data is non-sensitive information).

1.3 TEST ACCOUNTS

Live bank accounts are required for testing. If you wish to test A2A please send request to sales@paymentexpress.com.

DPS Support will require a live merchant bank account number (e.g. 01-1234-5678910-00). This is the bank account number that the funds will be transferred into.

Note that you will only be able to receive payments in your bank accounts local currency, i.e. A BNZ merchant account (even a multi-currency account) will only be able to process A2A payments using NZD.

Merchant can setup A2A with multiple bank account details each with different local currencies to have the ability to accept a wider range of currencies, and A2A will automatically select the correct account based on the transactions currency (As specified in the GenerateRequest message).

Account and currency mismatches will simply result in GenerateRequest failure.

1.4 SAMPLE CODE

Sample code is available in the following languages.

PHP cURL	PHP OpenSSL
ASP.Net 3.5 (C#)	ASP.Net 3.5 (VB)
Java	ColdFusion

All sample code can be downloaded from

www.paymentexpress.com/technical_resources/ecommerce_hosted/account2account.html

1.5 BASIC COMMUNICATION

Character data sent must be well formed XML.

The XML document must contain the required **opening** and **closing tags** that contains the whole document i.e. the root element.

Example: When generating the input XML document to begin a transaction request, the following GenerateRequest opening and closing tags must be present.

```
<GenerateRequest>
...
</GenerateRequest>
```

All tags must be **nested properly**. There must be an opening and a closing tag for all elements and the tags cannot overlap.

Example: Closing tags not complete.

```
</AmountInput - has no closing angle bracket, therefore the tag is not complete.
</AmountInput) - has a wrong closing bracket, therefore the tag is not complete.
```

The XML tags are **case sensitive** and **unique**. If a tag is submitted which is not recognized by DPS and is not a required element, it will be ignored and will not be returned in the response. If the tag is for a required element, an error may occur and a response code will be returned.

Example: If the AmountInput tag was sent with a lowercase “i” instead of an uppercase “I” and error will occur the response code “IU – Invalid Amount” will be returned.

```
<Amountinput>1.00</Amountinput> - Incorrect
<AmountInput>1.00</AmountInput> - Correct
```

If there is a possibility that a value will contain **invalid characters** (such as '&' and '>' in the cardholder name), please format the value using "HtmlEncoding", otherwise DPS will be unable to read the XML and will return an error (i.e. “Not acceptable input XML”).

Example, the following is invalid XML:

```
<GenerateRequest>
<TxnData1>Bill & Son</TxnData1>
<MerchantReference>Abc >> 123</MerchantReference>
</GenerateRequest>
```

The following is how it should be formatted.

```
<GenerateRequest>
<TxnData1>Bill &amp; Son</TxnData1>
<MerchantReference>Abc &gt;&gt; 123</MerchantReference>
</GenerateRequest>
```

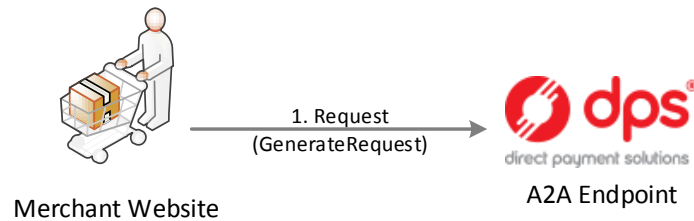

2 TECHNICAL SPECIFICATION

2.1 TRANSACTION REQUEST

2.1.1 Generate Request

GenerateRequest XML Document – To initiate a transaction the merchant posts the GenerateRequest to: <https://sec.paymentexpress.com/pxaccess/pxa2a.aspx> (Live).

Note, if you are using A2A via PxPay 2.0, you should be posting the GenerateRequest to: <https://sec.paymentexpress.com/pxaccess/pxpay.aspx> (Live).



The following is a list of the inputs elements applicable for a GenerateRequest.

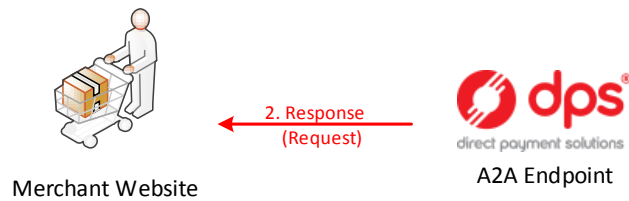
Input Element	Required	Datatype	Notes
PxPayUserId	Yes	BSTR Max 32 bytes	Use your A2A PX Pay username here
PxPayKey	Yes	BSTR Max 64 bytes	Use your A2A PX Pay key here
AmountInput	Yes	BSTR Max 13 characters	Transaction amount
CurrencyInput	Yes	BSTR Max 4 characters	Currently supports "NZD" only
EmailAddress	No	Max 255 bytes	
MerchantReference	Yes	BSTR Max 64 bytes	Reference value to appear on merchant bank statement
TxnData1	No	BSTR Max 255 bytes	Optional free text fields
TxnData2	No	BSTR Max 255 bytes	Optional free text fields
TxnData3	No	BSTR Max 255 bytes	Optional free text fields
TxnType	Yes	BSTR Max 8 Characters	Must be set to "Purchase"
TxnId	No	BSTR Max 16 bytes	Contains a unique, merchant application generated value that uniquely identifies the transaction.
UrlFail	Yes	BSTR Max 255 bytes	URL of page to redirect to if transaction failed. No parameters (&, ?) are permitted.
UrlSuccess	Yes	BSTR Max 255 bytes	URL of page to redirect to if transaction successful. No parameters (&, ?) are permitted.

Example:

```
<GenerateRequest>
<PxPayUserId>SampleA2AUser</PxPayUserId>
<PxPayKey>cff9bd6b6c7614bec6872182e5f1f5bcc531f1afb744f0bcaa00e82ad3b37f6d</PxPayKey>
<TxnType>Purchase</TxnType>
<AmountInput>1.00</AmountInput>
<CurrencyInput>NZD</CurrencyInput>
<EmailAddress>test@paymentexpress.com</EmailAddress>
<MerchantReference>SampleBusinessName</MerchantReference>
<TxnData1>John Doe</TxnData1>
<TxnData2>0211111111</TxnData2>
<TxnData3>98 Anzac Ave, Auckland 1010</TxnData3>
<TxnId>ABC12345678</TxnId>
<UrlSuccess>https://www.dpsdemo.com/SandboxSuccess.aspx</UrlSuccess>
<UrlFail>https://www.dpsdemo.com/SandboxSuccess.aspx</UrlFail>
</GenerateRequest>
```

2.1.2 Request

Request XML Document - Once the GenerateRequest has been processed a Request will be returned.



The URI returned can then be used to redirect the customer to the DPS Hosted Payments Page.

The following is a list of the output elements applicable for a Request.

Output Element	Datatype
valid [Attribute]	BSTR 1 character
URI	Datatype: BSTR

Example:

```
<Request valid="1">
<URI>https://sec.paymentexpress.com/pxmi3/EF4054F622D6C4C1B4F
9AEA59DC91CAD314D7F8C8A7C1D7A2B4C04CB8AA840B297A39069514956379</URI>
</Request>
```

2.2 TRANSACTION RESPONSE

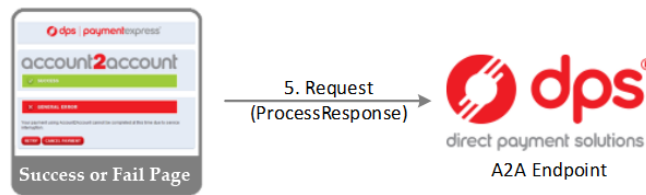
2.2.1 ProcessResponse

ProcessResponse XML Document – Once the user has submitted the payment and the transaction has been processed, the merchant now needs to obtain the transaction outcome and details.

When a user finishes the payment process the user is redirected to the merchant website. This URL has the result and userid appended to it e.g

<https://www.dpsdemo.com/a2a/pxpaysetup.aspx?result=0000840000100582bdc5b5e430bc5854&userid=SampleA2AUser>

To obtain the transaction details, the merchant sends the result string with their A2A PX Pay username and A2A PX Pay key in the ProcessResponse (Input XML Document).



The following is a list of the inputs elements applicable to the ProcessResponse.

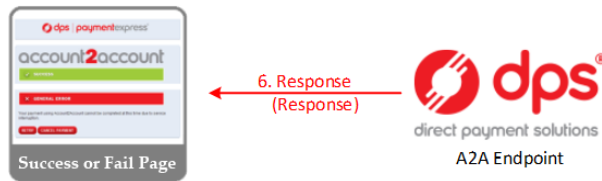
Input Element	Required	Datatype
PxPayUserId	Yes	BSTR Max 32 bytes
PxPayKey	Yes	BSTR Max 64 bytes
Response	Yes	Datatype: BSTR

Example:

```
<ProcessResponse>  
<PxPayUserId>SampleA2AUser</PxPayUserId>  
<PxPayKey>cff9bd6b6c7614bec6872182e5f1f5bcc531f1afb744f0bcaa00e82ad3b37f6d</PxPayKey>  
<Response>0000840000100582bdc5b5e430bc5854</Response>  
</ProcessResponse>
```

2.2.2 Response

Response XML Document - The Response will return the decrypted transaction results for the merchant to interpret.



The following is a list of the output elements applicable to the Response.

Output Element	Datatype
valid [Attribute]	BSTR 1 character
AmountSettlement	BSTR Max 13 characters
AuthCode	BSTR Max 22 characters
DpsTxnRef	BSTR Max 16 bytes
Success	Long
ResponseText	BSTR Max 32 bytes
ReCo	BSTR Max 2 characters
CurrencySettlement	BSTR Max 4 characters
TxnData1	BSTR Max 255 bytes

Output Element	Datatype
TxnData2	BSTR Max 255 bytes
TxnData3	BSTR Max 255 bytes
TxnType	BSTR Max 8 Characters
CurrencyInput	BSTR Max 4 characters
MerchantReference	BSTR Max 64 bytes
ClientInfo	BSTR Max 15 characters
A2aTxnStan	Long
TxnId	BSTR Max 16 bytes
EmailAddress	BSTR Max 255 bytes

Example:

```
<Response valid="1">
<Success>1</Success>
<TxnType>Purchase</TxnType>
<CurrencyInput>NZD</CurrencyInput>
<MerchantReference>Purchase Example</MerchantReference>
<TxnData1></TxnData1>
<TxnData2></TxnData2>
<TxnData3></TxnData3>
<AuthCode>113837</AuthCode>
<ClientInfo>192.168.1.111</ClientInfo>
<TxnId>P03E57DA8A9DD700</TxnId>
<EmailAddress></EmailAddress>
<A2aTxnStan>15<A2aTxnStan>
<DpsTxnRef>000000060495729b</DpsTxnRef>
<AmountSettlement>1.00</AmountSettlement>
<CurrencySettlement>NZD</CurrencySettlement>
<DateSettlement>20100924</DateSettlement>
<ResponseText>APPROVED</ResponseText>
<ReCo>00<ReCo>
</Response>
```

3 A2A SCREENS

3.1 BANK SELECTION

The bank selection screen is the first screen the user will see. The user will need to select their bank using the radio buttons and hit submit to go to the next screen.

Only available banks will be made visible on this screen. If a bank is down for maintenance or there is an integration issue between DPS and the bank, that particular bank will not be available on the list.

Note: The merchant reference, TxnData(1-3) and Amount fields are visible throughout the A2A payment process.

dps | paymentexpress

Payment Checkout

Merchant Reference: WP2KbMref1234

Amount: 1.01 (NZD)

account2account

1 SELECT BANK 2 BANK LOGON 3 SELECT ACCOUNT 4 REFERENCE DETAILS 5 PAYMENT VERIFICATION

Select one of the currently available banking services:

- ANZ** www.anz.co.nz
- ASB** www.asb.co.nz
- BNZ** www.bnz.co.nz
- KiwiBank** www.kiwibank.co.nz
- TSB** www.tsbbank.co.nz
- Westpac** www.westpac.co.nz

Please read and accept: [the terms and conditions here](#)

NEXT **CANCEL PAYMENT**


dps | paymentexpress


Note: Hitting the 'CANCEL PAYMENT' button will take the user back to the merchant failure URL.


Note: the style and options on the screen will be dependent on your custom hosted configuration.

3.2 AUTHENTICATION

This screen is the bank login page. User will be prompted to enter their bank username and password for authentication.


Payment Checkout
Merchant Reference: WP2KbMref1234
Amount: 1.01 (NZD)


1 SELECT BANK **2 BANK LOGON** **3 SELECT ACCOUNT** **4 REFERENCE DETAILS** **5 PAYMENT VERIFICATION**
Please review the following references that will appear on your statement:
Particulars: 00003DpsA2A
Code: DPS ANZ
Reference: WP2KbMref123
NEXT **CANCEL**



Note: Hitting the 'CANCEL' button will take the user back to the bank selection screen.

3.3 ADDITIONAL AUTHENTICATION

Depending on the user's bank, there might be additional layers of authentication. These screens can appear right after the first authentication screen or just prior to payment.

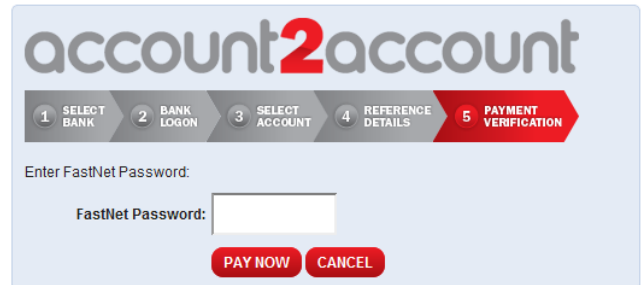
Here are some examples:

BNZ Netguard:



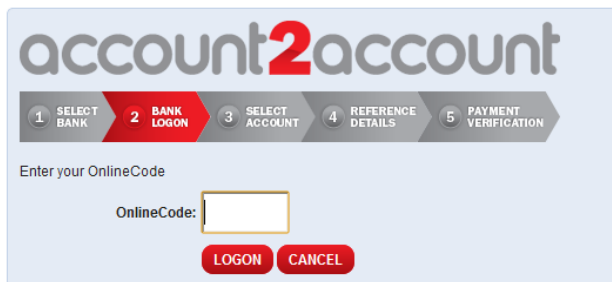
The BNZ Netguard authentication screen features the 'account2account' logo at the top. A progress bar below the logo shows five steps: 1. SELECT BANK, 2. BANK LOGON (highlighted in red), 3. SELECT ACCOUNT, 4. REFERENCE DETAILS, and 5. PAYMENT VERIFICATION. Below the progress bar, the text 'Netguard (serial number: 2050249)' is displayed. There are three vertical input fields labeled 'A7', 'E1', and 'E5'. At the bottom, there are two red buttons: 'LOGON' and 'CANCEL'.

ASB FastNet



The ASB FastNet authentication screen features the 'account2account' logo at the top. A progress bar below the logo shows five steps: 1. SELECT BANK, 2. BANK LOGON, 3. SELECT ACCOUNT, 4. REFERENCE DETAILS, and 5. PAYMENT VERIFICATION (highlighted in red). Below the progress bar, the text 'Enter FastNet Password:' is displayed. There is a text input field labeled 'FastNet Password:'. At the bottom, there are two red buttons: 'PAY NOW' and 'CANCEL'.

National Bank OnlineCode:




The National Bank OnlineCode authentication screen features the 'account2account' logo at the top. A progress bar below the logo shows five steps: 1. SELECT BANK, 2. BANK LOGON (highlighted in red), 3. SELECT ACCOUNT, 4. REFERENCE DETAILS, and 5. PAYMENT VERIFICATION. Below the progress bar, the text 'Enter your OnlineCode' is displayed. There is a text input field labeled 'OnlineCode:'. At the bottom, there are two red buttons: 'LOGON' and 'CANCEL'.

Note: Hitting the 'CANCEL' button will take the user back to the bank selection screen.

3.4 ACCOUNT SELECTION

The account selection screen will display all available bank accounts that support one-off payments.



Payment Checkout

Merchant Reference: ID1234567890
Amount: 10.50


account2account

1 SELECT BANK 2 BANK LOGON **3 SELECT ACCOUNT** 4 REFERENCE DETAILS 5 PAYMENT VERIFICATION

Select an account for the payment to be made from:

12-3456-1234567-89 \$15.13

SELECT **CANCEL**





[Privacy Policy](#)


Note: Hitting the 'CANCEL' button will take the user back to the bank selection screen.

3.5 PAYMENT DETAILS

Any reference information for the payment can be entered on the payment details screen. Fields are optional or mandatory depending on the user's bank.


Payment Checkout
Merchant Reference: WP2KbMref1234
Amount: 1.01 (NZD)


1 SELECT BANK **2 BANK LOGON** **3 SELECT ACCOUNT** **4 REFERENCE DETAILS** **5 PAYMENT VERIFICATION**
Please review the following references that will appear on your statement:
Particulars: 000003DpsA2A
Code: DPS ANZ
Reference: WP2KbMref123
NEXT **CANCEL**



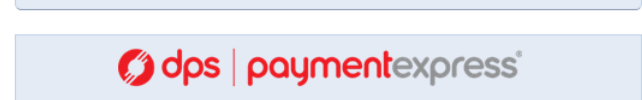
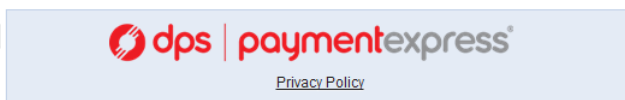
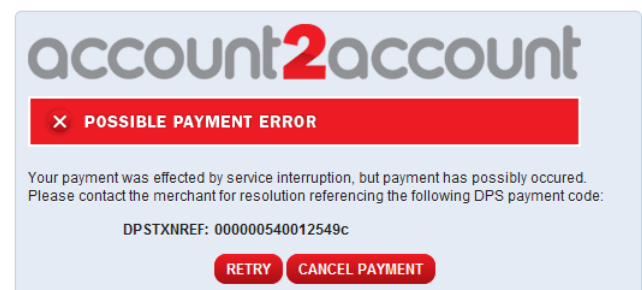
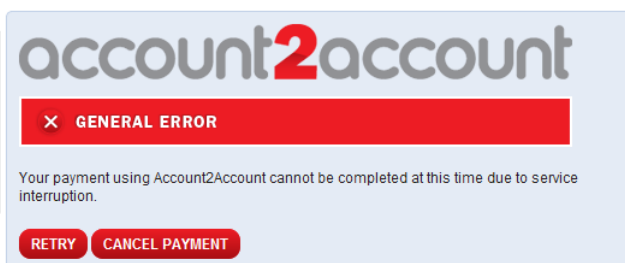
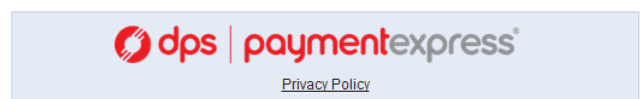
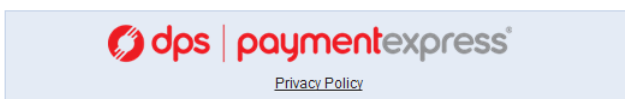
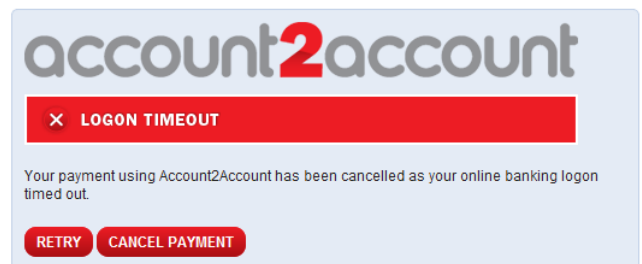
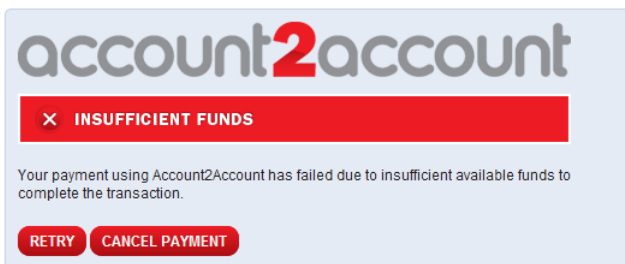
Note: Hitting the 'CANCEL' button will take the user back to the bank selection screen.

3.6 PAYMENT RESULT

The final screen of the A2A payment process. The outcome of the transaction is displayed to the user. The user is redirected to the merchant's success or failure URL when the 'OK' button is clicked.



Other potential results:



Note: Hitting the 'RETRY' button will take the user back to the bank selection screen. Hitting 'CANCEL PAYMENT' will take the user back to the merchant failure URL.

4 STATEMENT FIELDS AND RECONCILIATION

For Account2Account statement reconciliation processes please note the following.

Particulars field contains 6 digits rolling number (Stan) and string "DPSA2A". The Stan also appears in your Payline transaction records.

Please note the rolling number will roll over after it reaches a value of "999,999".

Code field contains your merchant account name (max 12 characters).

Reference field contains first 12 characters of Merchant Reference.

The following is an example of the Merchant Bank's Particular, Code and Reference fields:

Merchant Reference: "Order1234567"

Merchant account name: "TheShop"

Your fields will be for example:

Particulars: "000001DPSA2A"

Code: "TheShop"

Reference: "Order1234567"

5 PX PAY COMPARISON

A2A and PX Pay integrations are very similar. The key factor is that the A2A user is setup and configured differently at DPS.

Merchants who are already using PX Pay should be able to re-use existing PX Pay implementation with a few minor changes.

1. Set TxnType to 'Purchase' only.
2. Change DPS endpoint address to <https://sec.paymentexpress.com/pxaccess/pxa2a.aspx> (for A2A standalone).
3. Change PxPayUserId (if different).
4. Change PxPayKey (if different).

Other notable difference is:

- A2A does not support tokenisation.

6 A2A CUSTOMISATION

Merchants will have the ability to make certain changes on the A2A styles from the “Setup Custom Features” screen available on Payline®. (Please contact sales@paymentexpress.com if you do not have a Payline account and/or the Custom hosted screen available on your Payline portal.)

➤ Your Setup Custom Features screen will look like this:

For the above fields you can:

- Hide/unhide
 - Give a customised name
- From the A2A Specific tag, you will be able to turn on/off the A2A terms and conditions link, A2A info link, DPS A2A Brand Logo, add additional text and to give a customised name for the LabelA2AReferenceCode field.

➤ You will be able change the interface styles on the Page Style tag. There are 6 pre-set styles available.

➤ You will be able to preview your styles from the preview page.

Please note, not all functions on the “Setup Custom Features” screen are applicable for A2A standalone. Other customisable options are only available for PxPay 2.0.

7 FAQ

What is Account2Account?

Account2Account (A2A) is an e-commerce solution that allows merchants to accept online bank transfers as an alternative to credit card based payments.

Why use Account2Account?

Account2Account provides an alternative online payment option for customers without credit cards, or for customers who prefer paying via online bank transfer. Coupling Account2Account with DPS' credit card based payment products create a powerful solution that enables merchants to give their customers more ways to securely pay for goods and services online.

Who can use Account2Account?

Account2Account can be used by anyone who has access to online bank transfer functionality with a supported bank listed on page 2.

Do I need to download or install anything to use Account2Account?

No. There is no download necessary for customers to use Account2Account. All Account2Account software is hosted securely at DPS. Merchants will need to integrate to the Account2Account specification as per this document.

Does using Account2Account cost me anything?

For customers there is no cost to make payments using Account2Account, although online bank transfers fees may be applied by the customer's bank. For merchants please consult your account manager regarding your rate plan.

How does Account2Account work?

Account2Account provides a solution for merchants to accept payments directly into their bank account by creating a one-off online payment using the customer's online banking portal. This sort of facility is already widely used where a merchant provides their bank account details and customers pay by creating a one-off payment manually via their online banking portal. The key difference is that with Account2Account, the one-off payment is created on a secure page hosted at DPS. DPS can authoritatively inform the merchant when a payment is created and the customer is redirected back to the merchant's website once payment is created.

In terms of the customer experience, the customer will be redirected to a DPS hosted payments page when payment is ready to be taken. The customer simply selects their bank, follows the prompts and once the payment process is complete, the customer will be redirected back to the merchant website.

A basic demo of this service can be found at the link below.

https://www.dpsdemo.com/a2a_demo/a2ademo_home.htm

Is Account2Account secure?

The Account2Account page is securely hosted at DPS who are a Level 1 service provider and is compliant to PCI DSS Version 2.0.

Abiding by the comprehensive set of requirements of PCI DSS means that DPS use the latest security technologies to ensure the safe handling of all sensitive data. During the course of the Account2Account payment process, DPS does not store any of the customer's bank account information such as banking identifier or password. The same security features setup on the customer's bank account such as additional authentication methods are prompted during the course of the Account2Account payment process. Basically the same security technologies exposed by the banks are supported by Account2Account.

Visit link below to view our PCI DSS Compliance Certificate.

http://www.paymentexpress.com/getattachment/About/PCI_DSS/DPS_NZ_PCI_Cert.pdf.aspx/

Does Account2Account store any of my bank credential information?

No – DPS Account2Account will never store any bank credential information. The information is inputted by the customer and is used to enable and facilitate the payment transfer only and will not be recorded.

When will I see funds in my merchant account?

Settlement of funds is handled by the banks. This will be no different from a standard bank transfer payment created manually via the customers online bank portal. Funds usually settle on the next business day.

Can I ship goods or provide the service once Account2Account has provided an APPROVED response?

This is up to the merchant's discretion. This is because some banks allow their customers to cancel online payments before the transfer is actually settled. This means that there is a window where the customer if they wish to, could have made a payment via Account2Account and then cancel the payment manually via their own online banking portal before settlement. This risk can be mitigated by shipping goods/services once funds have settled.

What do I do if I need to refund a customer?

Merchants who need to refund their customers who have paid by Account2Account will need to refund via their merchant bank.

Can I test my Account2Account integration with test credentials?

No – Account2Account can only be used with live account details.

What are the possible A2A payment results?

Payment Result	Description
Success	Payment have been processed successfully
Insufficient Funds	Payment using A2A has failed due to insufficient available funds to complete the transaction
Logon Timeout	Payment using A2A has been cancelled as your online banking logon timed out.
General Error	Payment using A2A cannot be completed at this time due to service interruption
Possible Payment Error	Payment was effected by service interruption, but payment has possibly occurred.

8 ELEMENT DESCRIPTIONS

A2aTxnStan

The unique 6 digits reference for a2a transactions (Stan). Please note it will roll over after it reaches a value of "999,999".

AmountSettlement

The amount of funds settled for the transaction.

AuthCode

Authorisation code returned for approved transactions from the acquirer.

AmountInput

The AmountInput field specifies the total Purchase or Auth amount.

Format is d.cc where d is dollar amount (no currency indicator) and cc is cents amount. For example, \$1.80 (one dollar and eighty cents) is represented as "1.80", not "1.8". A string value is used rather than the conventional currency datatype to allow for easy integration with web applications. The maximum value allowable is "999999.99" however acquirer or card limits may be lower than this amount.

When submitting transactions for currencies with no decimal division of units such as the Japanese Yen (JPY), the AmountInput must be in an appropriate format e.g. "1000" for 1000 Yen. If "1000.00" is submitted in AmountInput with CurrencyInput set to JPY, an error will occur and response code "IU" will be returned.

CurrencyInput

The CurrencyInput field is used to specify the currency to be used e.g. "NZD" or "AUD".

NZD New Zealand Dollar

AUD Australian Dollar

CurrencySettlement

Used to specify the currency that was used for the transaction: AUD, NZD etc.

ClientInfo

The IP address of the user who processed the transaction.

DpsTxnRef

A DpsTxnRef is returned for every transaction. If the transaction was approved, DpsTxnRef can be used as input to a Refund transaction i.e. used to specify a transaction for refund without supplying the original card number and expiry date.

EmailAddress

The EmailAddress field can be used to store a customer's email address and will be returned in the transaction response. The response data along with the email address can then be used by the merchant to generate a notification/receipt email for the customer. This is an optional field.

MerchantReference

The Merchant Reference field is a free text field used to store a reference against a transaction. The merchant reference allows users to easily find and identify the transaction in Payline transaction query and DPS reports. The merchant reference is returned in the transaction response, which can be used interpreted by the merchant website. Common uses for the merchant reference field are invoice and order numbers. This is an optional field.

PxPayUserId

The PxPayUserId is a unique username to identify your customer account. This username will be setup by our Payment Express® Activations team and issued with your development account. The standard format used for Dev PxPayUserId is 'merchanname_dev' e.g. dps_dev.

PxPayKey

The PxPayKey is a unique 64 character key to identify customer account and used to encrypt the transaction request with 3DES to protect the transaction information. This key will be setup by our Payment Express® Activations team and issued with your development account.

Response

The Response field should contain the encrypted URL response from DPS, which can be obtained from the "result" parameter in the URL string that is returned to your response page.

ResponseText

Response Text associated with the response code of the transaction.

Success

Indicates success or failure of the transaction. A value of 0 indicates the transaction was declined or there was an error. A value of 1 indicates the transaction was approved.

TxnData1, TxnData2, TxnData3

The TxnData fields are free text fields that can be used to store information against a transaction. This can be used to store information such as customer name, address, phone number etc. This data is then returned in the transaction response and can also be retrieved from DPS reports. This is an optional field.

Note: storing large strings of information in the TxnData fields can cause the URI returned in the Request (Response) to exceed the max URL length for some browsers.

TxnType

The TxnType must be "Purchase".

TxnId

Contains a unique, merchant application generated value that uniquely identifies the transaction. Used by Payment Express® to check for a duplicate transaction generated from Merchant web site. If a duplicate is detected (same TxnId is used for an approved transaction within the previous 48 hours), the transaction is not retried, but an "approved" message is displayed and the merchant site is informed of the result.

UrlFail

Url of page to redirect to if transaction failed. No parameters (&, ?) are permitted.

UrlSuccess

Url of page to redirect to if transaction successful. No parameters (&, ?) are permitted.

URI

The URI field returns the URL including the encrypted transaction request that you will need to redirect the user to.

Valid

The valid field indicates whether the initial request was valid or invalid i.e. "1" for valid and "0" for invalid.

9 APPENDIX

9.1 CONTACT DPS

International	+64 9 309 4693
Australia	1 800 006 254 or +61 2 8268 7700
Hong Kong	+852 3 678 6766
New Zealand	0800 PAYMENT (729 6368) or 09 309 4693
Singapore	+65 3 158 1353
South Africa	+27 10 500 8784
United Kingdom	+44 (0) 20 3176 5551
USA	+1 310 670 7299