CommonwealthBank

Using the CommBiz Automated Channel

CommBiz Automated - Technical Requirements

June 2011

Version 2.1

Contents

Version Control

Version	Date of changes	Details of version changes made
2.0.12	October 2010	Published version used for migrating clients.
2.1	June 2011	Updated specifications including Secure Transfer details.

Section 1 - Executive Summary

In 2010 the Bank integrated a range of new payment features into CommBiz, our premium online business banking platform. One of these functions is the ability to "automate" your connection to the Bank without the use of Bank proprietary software. This will allow you to enable straight through processing for your business banking needs.

To assist in the planning and management of your upgrade, the Bank will provide support through your Account Manager and a dedicated Implementation Manager as well as documentation similar to the document you are reading at present.

Below you will find detailed technical requirements, which your information technology team will be able to use in the provisioning of your new automated CommBiz solution. This service will automate and streamline the transfer of your data files to and from the bank using industry standard secure file transfer software and appliances.

A glossary has been provided in Appendix 2 to assist with technical terminology that is used in this document and also throughout your upgrade.

If you have any questions around these requirements or the engagement process, please contact your Account or Implementation Manager.

1. Information you need to send to the Bank

i. CommBiz set up

CommBiz Upgrade Client form: CommBiz, the Bank's premium Business Banking channel will be replacing all other legacy channels. As part of this upgrade, we will need to establish your business with CommBiz access. If you already have CommBiz, your existing service can used. We intend to provide you with the same level of access and functionality in CommBiz as you have in the current channel. To facilitate this process, we will be providing you with a pre-populated "CommBiz Upgrade Client Form", which will document your access and functions as used in the current legacy channel.

Please review this form, confirm that the information is correct and that you would like us to proceed to set up your facility in such a manner.

ii. Automated connection

The automated user: To achieve straight through processing, the Bank will create an "automated user" in CommBiz. This "automated user" will need to be linked to a staff member of your organisation. Along with other key users of the CommBiz User Interface (i.e. transaction Authorisers), the staff member linked to the "automated user" will need to complete a "know your customer" check. This will be completed by the Bank as part of the implementation process.

Public/Private keys: Using secure file transfer protocol (SFTP) requires the use of PKI public/private key pairs. To connect to the Bank you will need to generate and then provide the Bank with your public key. Technical details of this process are included Section 2 of this document and may be used by your IT department.

PGP key: For further file security, you may wish to digitally encrypt your files using PGP. Your IT department will have to provide your PGP public key to the Bank so we can encrypt the files you receive from the Bank. The Bank will provide you with its PGP public key so you can encrypt the files sent to the Bank. Therefore there are 2 separate keys for two separate functions.

2. Client CommBiz Automated Connection Testing

i. Connectivity testing

From July 2010, you will be able to initiate connectivity testing. Your automated facility will be placed in a “pilot” environment. Connectivity testing will be performed by sending files from your SFTP Server to this environment. Your Implementation Manager will help facilitate this transaction by providing your IT department with your “Client Logon” and with further technical details as outlined in Section 2. While in “pilot” mode, any files you send to your outbox will automatically be moved to your inbox so you can test your file retrieval scripts. Once we have confirmed that testing is successful, we will move your facility from the pilot environment to the CommBiz environment. The CommBiz environment will be placed on hold until the full CommBiz functionality is established and you are ready to upgrade to the automated channel (post October 2010).

ii. CommBiz file testing

The range of new payment features will be available in CommBiz in the last quarter of 2010. It is at this stage that the Bank will commence the upgrade process of moving your current payment processing from the current channels to CommBiz.   An indicative timeframe for your upgrade window should have been communicated to you by your Account or Implementation Manager. If you are still waiting for this information, please contact the Bank

In order to test payment files, your CommBiz facility will be established with a special “transaction purpose”. Straight through processing in CommBiz will be turned off, and all files sent will need to be manually authorised. You can setup specific CommBiz users to have access to this “transaction purpose” – this will enable you to manually authorise or reject files for testing purposes. During the initial phase of testing, you can use either small test files or your existing Production files. You can also look at scheduling your transmissions to and from the Bank.

Once testing is complete, straight through processing in CommBiz will be enabled and your “business as usual” transaction purpose will be applied to all subsequent files.

iii. User Acceptance Testing (UAT) period

UAT testing will commence once all CommBiz testing has been completed successfully. The Bank will provide suggested test cases and a UAT sign off sheet during the migration period. This will be completed with the assistance of an Implementation Manager.

The UAT period should not require more than one week.

3. Using the new CommBiz Automated Connection for your Transaction Processing

i. Go Live

Once your testing is completed and signed off, you are now ready to "go live". From this date you will use CommBiz as your primary channel to communicate with the Bank. In consultation with you, the Bank will disable your legacy channel in our environment so that there is no possibility of duplicate files being processed across channels.

ii. Removal of legacy channel

Once you are successfully using CommBiz for all your Business Banking needs, there will be no need to use the obsolete, legacy channels. At a time mutually agreed between you and your Implementation Manager, but not greater than 6 weeks after you have gone live, your Implementation Manager will arrange to have the legacy channel decommissioned and removed from your environment. To ensure this is completed successfully, the Bank's Implementations Manager will disable your legacy facility by changing configuration data in the legacy channel, as well as checking your schedule and making sure it is turned off.

4. Bank support

i. Implementation Managers

Your Implementation Manager will work with you throughout the upgrade process. Key tasks that they will be involved in will be:

- Planning for the upgrade
- CommBiz Service Configuration
- Providing advice on the steps you will need to follow to connect to the Bank
- Connectivity testing
- CommBiz file acceptance testing
- User Acceptance Testing

Whilst writing the connectivity script and configuring your SFTP Client or Server will be your IT department's responsibility, our Implementation Managers have the necessary skills to be used as a reference point for questions or approaches on how to complete these activities.

ii. CommBiz Helpdesk

The CommBiz Helpdesk is available 24hrs a day, 7 days a week, 365 days a year. Once you have your CommBiz connection up and running, the Helpdesk can answer questions about CommBiz functionality, connectivity and usability. The contact number is for the Helpdesk is 13 23 39.

5. Business Continuity Planning (BCP) recommendations

If the automated connectivity between you and the Bank is unavailable, the CommBiz web interface will be used as BCP and be made available for you to manually send and receive files.

For this reason we strongly recommend that you create at least four users within CommBiz who have access to the web interface. These four operators will be able to upload and approve payment files, in addition to downloading receivables information.

Finally, in your scripting of your SFTP Server, you will need to build in a failover option which will be invoked if the secure file transfer is unavailable on the Banks side. Within this scripting you may want to consider building in an automated email notification to your system administrator so they can be made aware that manual processing will need to commence.

For those clients using PGP encryption in the automated channel, you will need to remove the encryption from the file before CommBiz can manually accept the file.

Section 2 - Technical Details

1. Hardware / Software requirements

Requirement	Reason for use
SFTP or SCP Client or Server	An SFTP or SCP client or server is used to send or receive files to/from the bank. Refer to Appendix 3. SFTP and SCP are open standard file transfer protocols that use PKI public/private keys for security. The client or server must be able to use Open SSH 2048 bit RSA public keys.
WAN and LAN Connectivity	All files will be transferred over the internet. The quicker your upload and download speeds, the more efficient the file delivery will be. The files saved on your file servers will need to be accessible within your local area network (LAN) and must have the appropriate file permissions for the SFTP client or server to access them unattended.

2. Security and Communications Protocols

Requirement	Reason for use
CommBiz Automated Login ID (generated by the Bank)	Used as part of the SFTP client configuration to initiate the SFTP connection between you and the Bank. Refer to Appendix 3.
Generation of an Open SSH public/private key pair (2048 bit RSA) (generated by you)	You will need to generate an Open SSH public/private key pair to secure your SFTP/SCP sessions. Your 2048 bit RSA Open SSH public key must be provided to the Bank via email and is uploaded by us to the CommBiz server. The Open SSH public/private key pair must be generated from within your environment.
Bank to verify the digital fingerprint of the public key provided by you	We will also confirm with you, the fingerprint of the public key we receive, so you can seek independent verification that the key pair has originated from within your organisation.
Firewall changes	You may be required to add an outbound rule enabling your internal SFTP client or server through your firewall and outside your network to connect to the CommBank infrastructure over the internet. Connection details: IP Subnet: 140.168.0.0/16 TCP/IP Port: 22

3. Connecting to the Bank

To connect to the Bank the following activities will need to be undertaken by your technical team in the following order.

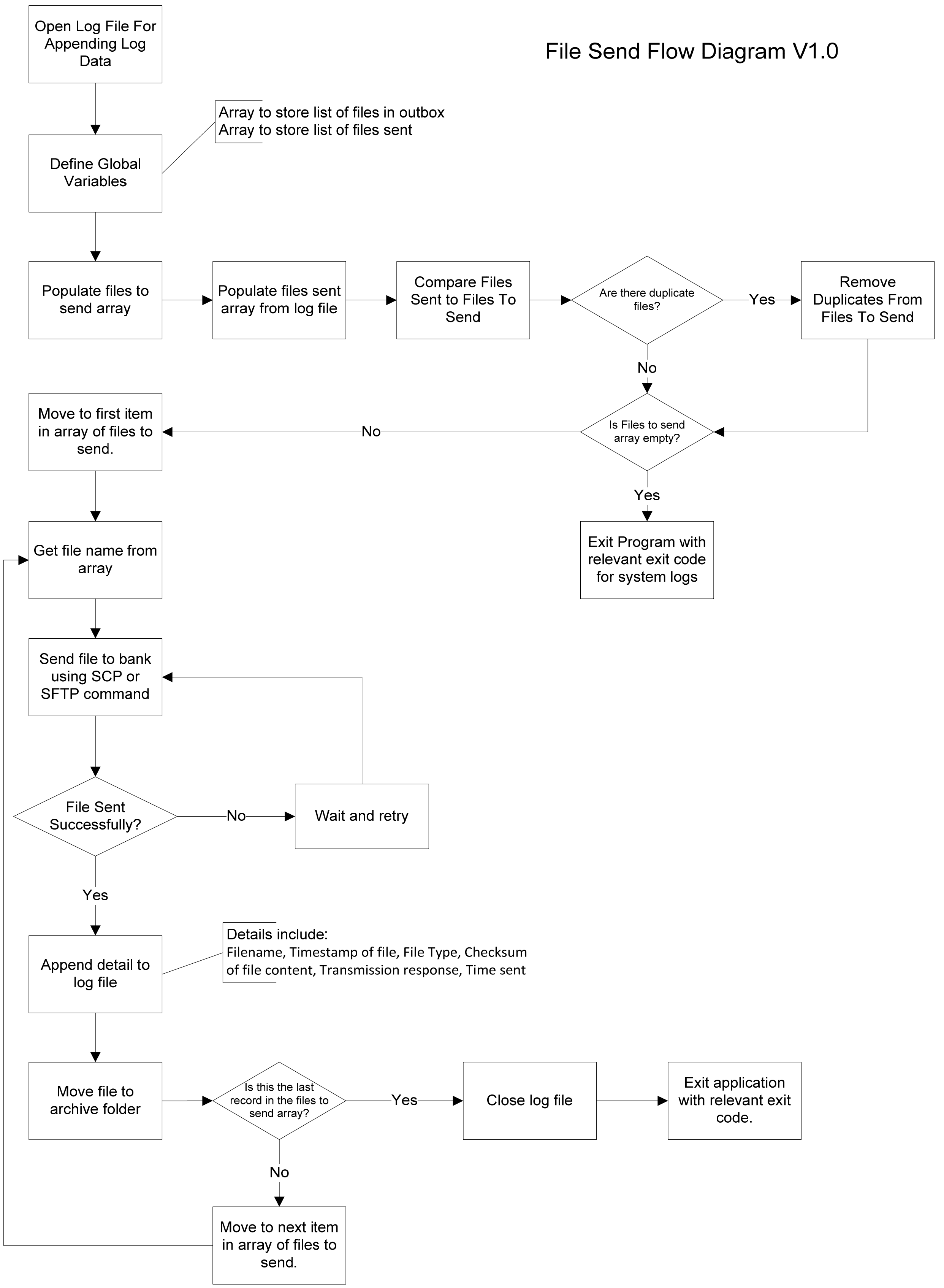
Activity	Reason / details
Create an OpenSSH public/private key pair (2048 bit RSA)	You will need to create an SSH key pair. You will keep the Private key secure on your network and in your SFTP/SCP client software, and provide the bank with the public key. Please email your public key to: ESImplementations@cba.com.au Your key needs to be an OpenSSH compatible 2048 bit RSA key. Once we have this key, we will call your company to advise receipt and verify authenticity. It is recommended that the email containing the public key is digitally signed to enhance security.
Establish a connection using your SFTP Client	You will need to create a new connection/site in your SFTP client or server software environment: **Site:** securetransfer.commbank.com.au **Login ID:** Provided to you by the Bank. *CommBiz Service ID preceded by 3 zeros (e.g. 000100002001)* **Load SSH Private key:** load the Private key into the SFTP client or server (this varies according to the program used)
Ensure your file formats are compatible	• Existing standard legacy file formats will be supported • Automated channel size limit - 100MB
Ensure your file names and file types meet the requirements	Please refer to Appendix 4 for the detailed file naming and file type requirements. • File name length max 173 characters; • Alphanumeric allowed; • Specific special characters allowed depends on Operating System; • WinZip/file compression is supported on the automated channel; • PGP also has compression capability.

Activity	Reason / details
Scripting your SFTP or SCP client or server connection	Scripting will be required to automate the connection to the Bank. Please refer to Appendix 1 for the flow charts that describe possible steps to be taken when scripting your solution. Optional considerations will be • PGP encryption and decryption **<u>Note:</u>** **/CommBiz/inbox** is used to collect files from the Bank (e.g. receivables, status files, BAI2). It is your responsibility to remove files from this directory once they have been downloaded successfully. **/CommBiz/outbox** folder is used to send files for processing by the bank. Files dropped in this folder will be moved to a processing area within The Bank. You will no longer have access to files delivered to this folder. Please also note that the inbox and outbox paths are case sensitive, and need to be referred to in code exactly as shown above. **While in “pilot” mode, any files you send to /CommBiz/outbox will automatically be moved to /CommBiz/inbox to facilitate testing and debugging of your upload and download scripts.**
Use of PGP encryption for additional security (optional)	PGP encryption can be used if you require increased security for delivering payment files to and/or retrieving receivables files from the Bank. To use PGP we need to exchange PGP public keys. Key elements include: • You must create a PGP private / public key pair. • You keep the PGP Private Key on your SFTP/SCP client. • You provide the Bank a copy of your public key. • The Bank will generate a PGP key pair, and send you the PGP public key. To encrypt files sent to you, the Bank will use your public key. To encrypt files sent to the Bank, you will need to use the Bank’s public key.

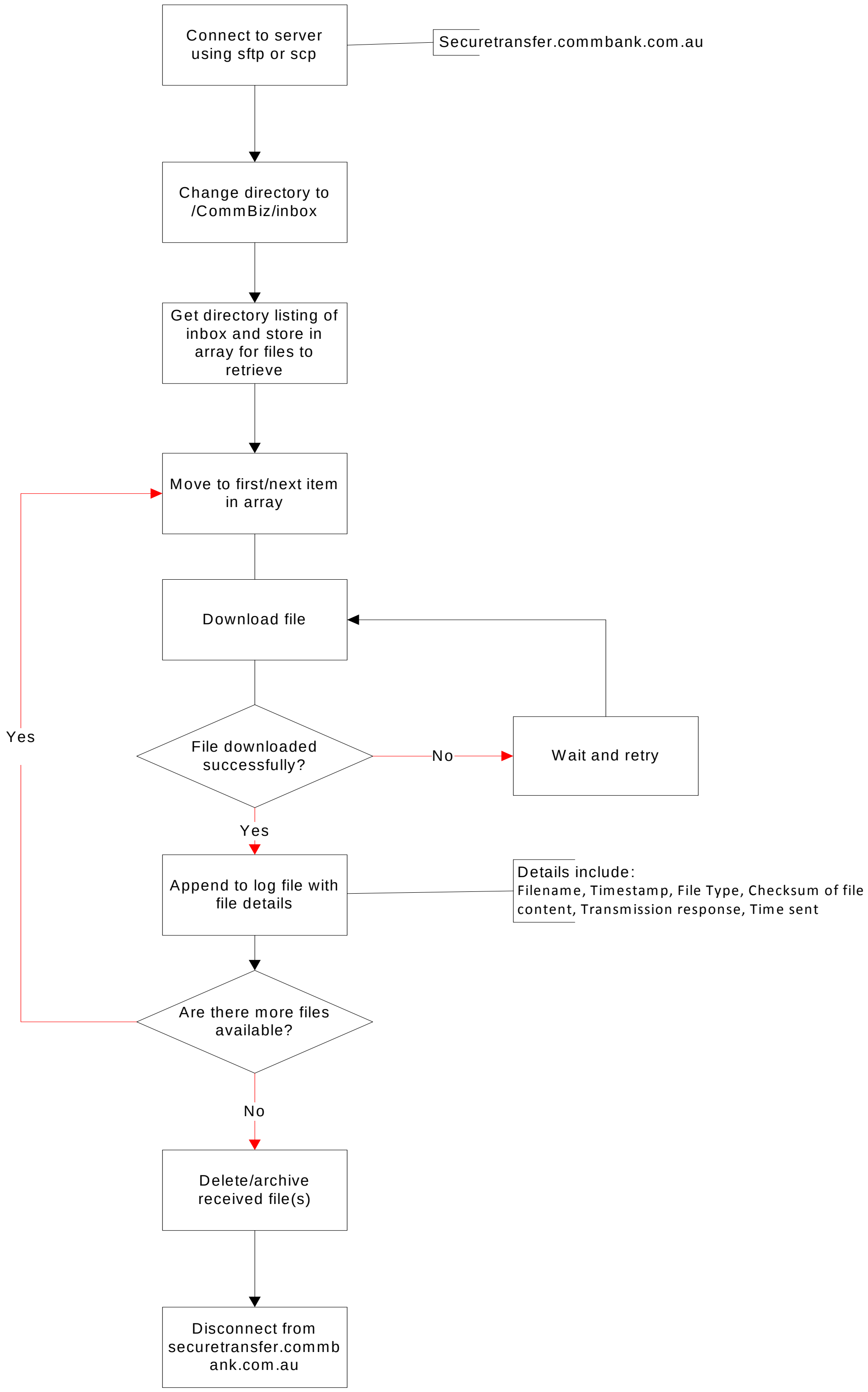
For further information please contact the following people:

Business related issues (Section 1 - Executive Summary)	- your Account Manager
Technical issues (Section 2 - Technical details)	- your Implementation Manager

Appendix 1 – Possible scripting flow charts


File Send Flow Diagram V1.0
Open Log File For Appending Log Data
Define Global Variables
Array to store list of files in outbox
Array to store list of files sent
Populate files to send array
Populate files sent array from log file
Compare Files Sent to Files To Send
Are there duplicate files?
Yes
Remove Duplicates From Files To Send
No
Is Files to send array empty?
No
Move to first item in array of files to send.
Yes
Exit Program with relevant exit code for system logs
Get file name from array
Send file to bank using SCP or SFTP command
File Sent Successfully?
No
Wait and retry
Yes
Append detail to log file
Details include:
Filename, Timestamp of file, File Type, Checksum of file content, Transmission response, Time sent
Move file to archive folder
Is this the last record in the files to send array?
Yes
Close log file
Exit application with relevant exit code.
No
Move to next item in array of files to send.

Downloading Receivables Files


Connect to server using sftp or scp
Securetransfer.commbank.com.au
Change directory to /CommBiz/inbox
Get directory listing of inbox and store in array for files to retrieve
Move to first/next item in array
Download file
File downloaded successfully?
No
Wait and retry
Yes
Append to log file with file details
Details include:
Filename, Timestamp, File Type, Checksum of file content, Transmission response, Time sent
Are there more files available?
Yes
No
Delete/archive received file(s)
Disconnect from securetransfer.commbank.com.au

Appendix 2 – Technical Definitions and Glossary

APCA	Australian Payments & Clearing Association
APF	Agency Payment Facility – a system that receives data from various sources, processes it and passes information files to EDTS
BECS	Bulk Electronic Clearing System
DDS	Demand Deposit System. Holds information relating to Demand Deposit Accounts.
DE (AUTOPAY)	The Bank's core Direct Entry System.
DE-NBFI	Direct Entry – Non-Bank Financial Institution. Similar to MA23 – a list from the DE system of entries processed to NBFI accounts.
eLockbox	Replacing "Off System BSB". Product known to customers as eLockbox. Product is when bank provides cm with their own BSB to manage receivables payments.
ERP	Enterprise Resource Planning. This software manages internal and external resources such as financials and HR. Examples include SAP, JDEdwards, SAGE and Microsoft Dynamics amongst many others.
Firewall	A firewall is a software program, hardware device or a combination of both that inspects and filters data transmitted to and from an organisation. It permits or denies access based on a set of rules administered by the organisation.
IP	Internet Protocol (IP) delivers data from source to destination based on their addresses. Much like post codes, street addresses and street numbers distinguish a home, IP addresses distinguish particular machines on a network.
Know Your Customer (KYC)	Under Anti Money Laundering /Counter Terrorism Finance legislation, KYC policy refers to documentation which sets out the Bank's approach to authenticating the customer's identity, ensuring that it can effectively identify, verify and monitor its customers and the financial transactions in which they engage. This is done with the aim of guarding against identity theft, illegal money laundering and terrorism financing, which are damaging both to the customer and the community at large.
LAN	A local area network (LAN) supplies network capability (e.g. internet, email) to a group of computers within close proximity, such as an office building or school
Login ID	Your Login ID is your CommBiz Service ID with 3 leading zeros. It is used to connect to the Bank's automated channel via your SFTP client
MA23	Generic name for a list out of the DE system of entries processed to a specific

	account number.
MIS	Management Information Systems. A system or process that provides information to aid management. Differs from regular information systems in that they're used to analyse other information systems used in day to day operations.
NBFI	Non-Bank Financial Institution. Transactions on accounts maintained by NBFI's with CBA. Includes accounts for overseas banks which do not operate commercially in Australia.
Network Ports	Ports enable multiple computer programs to communicate with other computers at the same time sharing a single physical network connection. For example your work PC uses port 23 for email, 80 or 8080 for HTTP and 443 for HTTPS. Ports are not physical – they are akin to lanes on a freeway. Port 1 would be the first lane, port 2 the second lane etc. Each lane/port is used for particular traffic types.
Open SSH	Open SSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
PGP	PGP is a data encryption and decryption standard. PGP is used to encrypt or digitally sign files (e.g. email, text files).
Ping	A command that's used to test connectivity or the existence of a computer. For example "ping securetransfer.commbank.com.au" Ping is commonly used with traceroute.
PKI (Public Key Infrastructure)	A system that uses digital certificates from certificate authorities that verify and authenticate the validity of each party in an internet transaction.
Protocol (aka Network Protocol, Communications Protocol)	Network protocols are set standards that define communications between network devices such as routers, much like human communication protocols help networks listen, understand and converse with each other. Examples of protocols include HTTP (web pages), HTTPS (secure web), SFTP, TCP and IP.
Proxy server	A proxy server acts as an intermediary for client requests seeking resources from another server (e.g. web pages, files). The proxy server evaluates the requests according to its filtering rules. The proxy server can often store commonly accessed data locally to speed up access to web pages in particular.
Routers	A router is similar to a modem in that it connects two or more computer networks. In most enterprise environments a router is a physical device that also has abilities in providing network security such as ip filtering (like a built in firewall)
RSA (drop key)	RSA refers to an algorithm for public-key cryptography first publicly described by cryptography researchers Rivest, Shamir and Adleman.
Scheduler (Job) aka batch	A job scheduler is an application that controls unattended background executions. Example of a job scheduler is backup a drive at a time interval at a

processing	specific day
SCP	SCP is an intelligent node that contains customer information in a database residing on a centralized network server. An SCP provides routing and other instructions to a service switching point (SSP).
Script	Scripts are executable files that control one or more software applications. Scripts are used to automate tasks (especially repetitive tasks). Scripts can be written for Unix, Linux and Windows platforms
SFTP (Secure File Transfer Protocol)	SFTP uses SSH to transfer files and encrypts both data and commands thus preventing passwords and information from being transmitted in human readable format over the network. Refer to Appendix 3.
Shell	A shell is an interface for users of an operating system. It is used to issue commands to the operating system. Shells can be command line (like a Unix terminal) or graphical (like Windows)
SSH	Secure Shell enables data to be exchanged between two networks via a secure channel. SSH operates on port 22 and ensures that the communication channel is secure
SSL (Secure Socket Layer)	A protocol of communication that uses a cryptographic system that has 2 keys to encrypt data - a public key known to everyone and a private/secret key known only to the recipient. It is most commonly used by web browsers and is recognised by https: in the address field.
TCP	Transmission Control Protocol (TCP) is a method of data delivery that includes error checking and flow control.
Traceroute	Traceroute (Unix/Linux) or tracert (Windows) commands displays the path from a client machine to a host machine. For example you can run a traceroute from your clients SFTP server to CommBiz. Each address in the list shown represents a networking device (e.g. router, firewall). This can be used to find out where connectivity fails.
Tumbleweed	This is the commercial name of the Bank's SFTP server that you will connect to. This product is provided by AxWay and is now called Secure Transport.

Appendix 3 – Secure Transfer Details

The following is a list of software that we know is suitable for connection to the bank:

SFTP clients:

- FDX 4.5.2
- FileZilla 3.0.0
- PuTTY SecureFile Transfer 0.60
- SCP and SFTP (shipped with Solaris 10)
- Tectia Client 5.3
- Tectia Client 6.0.7
- VanDyke SecureFX 6.2.1
- WinSCP 4.1.9

SSH servers for serverinitiated transfers:

- OpenSSH
- Synchrony Gateway 6.12
- Tectia Server 6.0.7
- VanDyke VShell 3.5.3

Firewall setup:

- Checkpoint Firewall NG 5.5

Proxy servers:

- Apache Reverse Proxy
- IBM Webseal 6
- MS ISA Server 2006
- MS ISA Server 2008
- SunOne Proxy Server 4.0

Appendix 4 – File Naming and File Type Conventions

For data files sent to the Bank, filenames must conform to:

- Only alphanumeric (numbers and letters), or;
- '.' (dot) or;
- '_'(underscore);
- Filenames should not contain spaces;
- Maximum client filename size should conform to a **maximum** of 173 characters"(inclusive of the file extension).

Payables Direct files (CO1, CO2, GOVT) must not have an extension of .meta

In addition to this, Payment File filenames should conform to Windows and UNIX system file naming requirements (that covers most other operating systems also). See below.

1. To support a WINDOWS operating system - FAT and NTFS – the following rules should be adhered to:
    a. / ? < > \ : * | " ^ are invalid. (These characters are deemed Invalid);
2. In addition to these characters, the following conventions are also illegal for Windows Systems:
    a. Placing a space at the end of the name;
    b. Placing a period at the end of the name.
3. To support the UNIX Operating System, the following rules should be adhered to:
    a. / invalid. Do not place a / in the filename. If a client places a slash, UNIX will attempt to interpret the slash characters as directory delineators;
    b. Payables Direct format files (CO1, CO2, GOVT) filenames should not have spaces (aka whitespace).

Acceptable file Extensions:

- If sending files via CommBiz Automated, then the following file extensions will fail and the file will be rejected:
    - JPEG, BMP, PDF, DOCX, ZIP.
- If using CommBiz GUI (Manual) to upload files and the file ends in ".zip", ".z" or ".gz" then it **must** be a compressed file.
- Irrespective of the upload method (Manual or Automated) CommBiz will reject the following file extensions:
    - WMZ, HTM, XLSX

End of Document