**Bank File Transfer As-Built**

Contents

[1 Introduction 3](#_Toc144198580)

[2 Create SSH Keys for SFTP Connection 3](#_Toc144198581)

[3 Create PGP Keys for File Decryption 3](#_Toc144198582)

[4 Setup Azure Environment 4](#_Toc144198583)

[4.1 Define Resource Names 4](#_Toc144198584)

[4.2 Azure Subscription 4](#_Toc144198585)

[4.3 Resource Group 4](#_Toc144198586)

[4.4 Public IP Address 5](#_Toc144198587)

[4.5 Virtual Network 5](#_Toc144198588)

[4.6 NAT Gateway 6](#_Toc144198589)

[4.7 Network Security Group – Prod 7](#_Toc144198590)

[4.8 Network Security Group – Test 9](#_Toc144198591)

[4.9 Key Vault – Prod 11](#_Toc144198592)

[4.10 Key Vault – Test 12](#_Toc144198593)

[4.11 App Service Plan –Prod 13](#_Toc144198594)

[4.12 App Service Plan – Test 13](#_Toc144198595)

[4.13 Function App – Prod 14](#_Toc144198596)

[4.14 Function App – Test 15](#_Toc144198597)

[4.15 Storage Account – Prod 16](#_Toc144198598)

[4.16 Storage Account – Test 17](#_Toc144198599)

[5 Configure Key Vault 18](#_Toc144198600)

[5.1 Enable Managed Identity for Function App 18](#_Toc144198601)

[5.2 Configure Key Vault Access Control 18](#_Toc144198602)

[5.3 Add Keys As Secrets to the Key Vault 19](#_Toc144198603)

[5.4 Create Key Vault Reference in Function App Configuration 20](#_Toc144198604)

[6 Function App Functions 21](#_Toc144198605)

[6.1 GetFileListFromBank 21](#_Toc144198606)

[6.2 GetFileFromBank 22](#_Toc144198607)

[6.3 SendFileToBank 22](#_Toc144198608)

[6.4 DeleteFileFromBank 23](#_Toc144198609)

[6.5 EncryptFileForBank 23](#_Toc144198610)

[6.6 DecryptFileForBank 24](#_Toc144198611)

[7 Function App Deployment 25](#_Toc144198612)

[8 Update Production PGP Keys 26](#_Toc144198613)

[8.1 Update ANZ Production PGP Key 26](#_Toc144198614)

# Introduction

This document describes the configuration values for each Azure Resource created for the Bank Transfer Function App. Please note that although the sections in this document are arranged as close to resource creation sequence as possible, some resources reference each other, and can only be updated to reference each other when both resources are created.

If this document is passed to Fusion5 clients for them to create the resources themselves, the naming convention in this document is then only for suggestion. The clients can use their own naming convention as long as they clearly document the names of each resource created.

# Create SSH Keys for SFTP Connection

The steps below can be used for generating keys for any banks and any environments for SFTP connection.

1. Download putty 0.78 installer from <https://www.puttygen.com/download-putty> and install on local computer.
2. Run and configure the settings:

Type of key to generate: RSA

Number of bits: 2048

1. Select Key -> Generate key pair.
2. Save private key as **{bank initials}\_{environment}.ppk**. Allow to save without passphrase.
3. Select Conversions -> Export OpenSSH key. Allow to save without passphrase.
4. Save public key as **{bank initials}\_{environment}\_multiline.pub**.
5. Copy the public key from screen which is a single line key and save as **{bank initials}\_{environment}\_singleline.pub**.
6. Zip up both public key files with password and send them to the bank. They will configure their side of the FTP with the key files.

# Create PGP Keys for File Decryption

1. Download Kleopatra Gpg4win 4.1.0 installer from <https://www.gpg4win.org> and install on local computer.
2. Select File -> New OpenPGP Key Pair.
3. Provide the following information:

* Name: {Company Name} - BC Integration
* Email: {Company email address}
* Don’t use passphrase

1. Click **Advanced Settings**…
2. Select RSA 2048 bits. Also tick +RSA and select 2048 bits. In the Certificate Usage section have everything ticked except **Authentication** and **Valid until**. Then click OK and OK. This then creates a new OpenPGP certification.
3. Right-click the certificate and select **Export…** to export the public key.
4. Right-click the certificate again and select **Backup Secret Keys…** to export the private key.

# Setup Azure Environment

A typical secured setup for running the Bank File Transfer Function App is depicted in the diagram below.

A screenshot of a computer

Description automatically generated

The following subsections provides detailed information about the configuration of these Azure resources.

## Define Resource Names

For the naming conventions below:

* {region} is the initials of a region. E.g. Australia East -> ae.
* {org} is the short form of customer organisation name. E.g. Plain Strategies Ltd -> psl.

|  |  |
| --- | --- |
| **Resource Type** | **Resource Naming Convention** |
| Resource Group | rg-bankfiletrans-{region} |
| Public IP Address | ip-bankfiletrans-{region} |
| NAT Gateway | natg-bankfiletrans-{region} |
| Virtual Network | vnet-bankfiletrans-{region} |
| Subnet – Prod (Under Virtual Network) | snet-bankfiletrans-{region} |
| Subnet – Test (Under Virtual Network) | snet-bankfiletrans-{region}-test |
| Network Security Group – Prod | nsg-bankfiletrans-{region} |
| Network Security Group – Test | nsg-bankfiletrans-{region}-test |
| Key Vault – Prod | kv-bft-{org}-{region} |
| Key Vault – Test | kv-bft-{org}-{region}-test |
| App Service Plan – Prod | asp-bankfiletrans-{region} |
| App Service Plan – Test | asp-bankfiletrans-{region}- test |
| Function App – Prod | fapp-bankfiletrans-{org}-{region} |
| Function App – Test | fapp-bankfiletrans-{org}-{region}-test |
| Storage Account – Prod | Stobankfiletrans{org} |
| Storage Account – Test | Stobankfiletrans{org}test |

## Azure Subscription

Create a new Azure Subscription or decide on which existing Subscription to be used to host the resources. All required resources are to be created inside this subscription.

|  |  |
| --- | --- |
| **Subscription Name** |  |
| **Subscription ID** |  |

## Resource Group

Create a new resource group to contain all required resources. Note that one resource group will contain both production and test environment resources, because there will be only one Virtual Network and one public IP address resource used by resources of both environments.

|  |  |
| --- | --- |
| **Resource Group Name** | rg-bankfiletrans-{region} |
| **Region** | E.g. Australia East |

## Public IP Address

The public IP address is used as an outbound address to connect to the banks’ FTP servers. The address is provided to the banks to be whitelisted.

|  |  |
| --- | --- |
| **Resource Name** | ip-bankfiletrans-{region} |
| **Region** | E.g. Australia East |
| **IP address** | Provided by Azure |
| **SKU** | Standard |
| **Tier** | Regional |
| **Associated to** | natg-bankfiletrans-{region} (NAT Gateway resource name when available) |
| **IP Address Assignment** | Static |

## Virtual Network

A virtual network is set up to allow the Azure resources to communicate to each other securely.

|  |  |
| --- | --- |
| **Resource Name** | vnet-bankfiletrans-{region} |
| **Region** | E.g. Australia East |
| **Address space** | 10.0.0.0/16 |
| **DNS servers** | Azure provided DNS service |
| **Subnets** | 3 |
| **Encryption** | Disabled |
| **DDoS protection plan** | Not configured |
| **Firewall** | Not configured |
|  | |
| **Subnet Name** | Default |
| **Subnet address range** | 10.0.0.0/24 |
| **NAT gateway** | None |
| **Network security group** | None |
| **Route table** | None |
|  | |
| **Subnet Name** | snet-bankfiletrans-{region} |
| **Subnet address range** | 10.0.1.0/24 |
| **NAT gateway** | natg-bankfiletrans-{region} |
| **Network security group** | nsg-bankfiletrans-{region} |
| **Route table** | None |
|  | |
| **Subnet Name** | snet-bankfiletrans-{region}-test |
| **Subnet address range** | 10.0.2.0/24 |
| **NAT gateway** | natg-bankfiletrans-{region} |
| **Network security group** | nsg-bankfiletrans-{region}-test |
| **Route table** | None |

## NAT Gateway

A NAT gateway is the only access point for Azure resources to connect to the world outside of the Virtual Network.

|  |  |
| --- | --- |
| **Resource Name** | natg-bankfiletrans-{region} |
| **Region** | E.g. Australia East |
| **Outbound IP** | ip-bankfiletrans-{region} |
| **Virtual network** | vnet-bankfiletrans-{region} |
| **Subnets** | E.g.  snet-bankfiletrans-{region}  snet-bankfiletrans-{region}-test |

## Network Security Group – Prod

A Network Security Group was created to allow resources to access each other within the Vnet.

|  |  |
| --- | --- |
| **Resource Name** | nsg-bankfiletrans-{region} |
| **Region** | E.g. Australia East |
| **Subnets** | snet-bankfiletrans-{region} |

**Inbound Security Rules**

|  |  |
| --- | --- |
| **Rule Name** | DenyAllInbound |
| **Source** | Any |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Deny |
| **Priority** | 4095 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowAzureLoadbalancer |
| **Source** | Service Tag |
| **Source service tag** | AzureLoadBalancer |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4094 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowVnettoVnet |
| **Source** | Service Tag |
| **Source service tag** | VirtualNetwork |
| **Source port ranges** | \* |
| **Destination** | Service Tag |
| **Destination service tag** | VirtualNetwork |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4093 |

|  |  |
| --- | --- |
| **Rule Name** | AllowDynamics365BusinessCentral |
| **Source** | Service Tag |
| **Source service tag** | Dynamics365BusinessCentral |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4090 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowKeyVault |
| **Source** | Service Tag |
| **Source service tag** | AzureKeyVault |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4091 |

## Network Security Group – Test

A Network Security Group was created to allow resources to access each other within the Vnet.

|  |  |
| --- | --- |
| **Resource Name** | nsg-bankfiletrans-{region}-test |
| **Region** | E.g. Australia East |
| **Subnets** | snet-bankfiletrans-{region}-test |

**Inbound Security Rules**

|  |  |
| --- | --- |
| **Rule Name** | DenyAllInbound |
| **Source** | Any |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Deny |
| **Priority** | 4095 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowAzureLoadbalancer |
| **Source** | Service Tag |
| **Source service tag** | AzureLoadBalancer |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4094 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowVnettoVnet |
| **Source** | Service Tag |
| **Source service tag** | VirtualNetwork |
| **Source port ranges** | \* |
| **Destination** | Service Tag |
| **Destination service tag** | VirtualNetwork |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4093 |

|  |  |
| --- | --- |
| **Rule Name** | AllowDynamics365BusinessCentral |
| **Source** | Service Tag |
| **Source service tag** | Dynamics365BusinessCentral |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4090 |

|  |  |
| --- | --- |
|  | **MAY NOT NEED THIS RULE** |
| **Rule Name** | AllowKeyVault |
| **Source** | Service Tag |
| **Source service tag** | AzureKeyVault |
| **Source port ranges** | \* |
| **Destination** | Any |
| **Service** | Custom |
| **Destination port ranges** | \* |
| **Protocol** | Any |
| **Action** | Allow |
| **Priority** | 4091 |

## Key Vault – Prod

A Key Vault was primarily created to store RSA SHA-2 keys for connecting to the bank’s FTP servers. However, it may be used to store some other secret keys as well.

|  |  |
| --- | --- |
| **Resource Name (Max 24 chars)** | kv-bft-{org} |
| **Region** | E.g. Australia East |
| **Sku (Pricing tier)** | Standard |
| **Vault URI** | https://kv-bft-{org}.vault.azure.net/ |
| **Soft-delete** | Enabled |
| **Purge protection** | Disabled |
| **Access configuration** | Azure role-based control  Add role “Key Vault Secrets User” to:   * fapp-bankfiletrans-{org}-{region} (function app managed identity) * Fusion5 support account |
| **Networking: Firewall and virtual networks** | Allow public access from specific virtual networks and IP addresses  Add existing virtual network: vnet-bankfiletrans-{region}  Subnet: snet-bankfiletrans-{region} |
| **Firewall** | Add function app Inbound and Outbound IP addresses after function app is created. E.g.  nnn.nnn.nnn.nnn/32 (the public IP address)  nnn.nnn.nnn.nnn/32 (function app inbound IP)  To be able to see the Secrets, add your own IP address as well. |
| **Exception** | Allow trusted Microsoft services to bypass this firewall |

## Key Vault – Test

Create a Key Vault to store RSA SHA-2 keys for connecting to the bank’s SFTP servers and any other secret keys.

|  |  |
| --- | --- |
| **Resource Name (Max 24 chars)** | kv-bft-{org}-test |
| **Region** | E.g. Australia East |
| **Sku (Pricing tier)** | Standard |
| **Vault URI** | https://kv-bft-{org}-test.vault.azure.net/ |
| **Soft-delete** | Enabled |
| **Purge protection** | Disabled |
| **Access configuration** | Azure role-based control  Add role “Key Vault Secrets User” to:   * fapp-bankfiletrans-{org}-{region}-test (function app managed identity) * Fusion5 support account |
| **Networking: Firewall and virtual networks** | Allow public access from specific virtual networks and IP addresses  Add existing virtual network: vnet-bankfiletrans-{region}  Subnet: snet-bankfiletrans-{region}-test |
| **Firewall** | Add function app Inbound and Outbound IP addresses after function app is created. E.g.  nnn.nnn.nnn.nnn/32 (the public IP address)  nnn.nnn.nnn.nnn/32 (function app inbound IP)  To be able to see the Secrets, add your own IP address as well. |
| **Exception** | Allow trusted Microsoft services to bypass this firewall |

## App Service Plan – Prod

Associated with the App Services of the Function Apps for App Service scaling.

|  |  |
| --- | --- |
| **Resource Name** | asp-bankfiletrans-{region} |
| **Region** | E.g. Australia East |
| **Pricing plan** | S1 |

## App Service Plan – Test

Associated with the App Services of the Function Apps for App Service scaling.

|  |  |
| --- | --- |
| **Resource Name** | asp-bankfiletrans-{region}-test |
| **Region** | E.g. Australia East |
| **Pricing plan** | B1 |

## Function App – Prod

The functions are used as a bridge between Business Central and the banks’ FTP servers for transferring files to and from. During creation of the function app, an App Service Plan and a Storage Account will also be created.

|  |  |
| --- | --- |
| **Resource Name** | fapp-bankfiletrans-{org}-{region} |
| **Region** | E.g. Australia East |
| **URL** | https://fapp-bankfiletrans-{org}-{region}.azurewebsites.net |
| **Operating System** | Windows |
| **Runtime stack** | .NET |
| **Version** | 6 (LTS) |
| **Operating System** | Windows |
| **Hosting options and plans** | App service plan |
| **App Service Plan** | asp-bankfiletrans-{region} |
| **Storage (Refer to 3.15)** | |
| **Networking** | |
| **Access restriction** | On - Allow public access.   * Has a ‘Deny all’ rule with priority 2147483647. * Add rule: * Name: AllowBC * Priority: 200 * Action: Allow * Description: AllowBC * Service Tag: Dynamics365BusinessCentral * HTTP headers filter settings: All left blank |
| **App assigned address** | Off |
| **Private endpoints** | Off |
| **Inbound address** | Function App IP Address shown on Properties page |
| **Vnet integration** | On  Vnet: vnet-bankfiletrans-{region}  Subnet: snet-bankfiletrans-{region} |
| **Hybrid connections** | Off |
| **Outbound addresses** | The Public IP and many more |
| **NAT gateway** | On |
| **Network security group** | nsg-bankfiletrans-{region} |

## Function App – Test

The functions are used as a bridge between Business Central and the banks’ FTP servers for transferring files to and from. During creation of the function app, an App Service Plan and a Storage Account will also be created.

|  |  |
| --- | --- |
| **Resource Name** | fapp-bankfiletrans-{org}-{region}-test |
| **Region** | E.g. Australia East |
| **URL** | https://fapp-bankfiletrans-{org}-{region}-test.azurewebsites.net |
| **Operating System** | Windows |
| **Runtime stack** | .NET |
| **Version** | 6 (LTS) |
| **Operating System** | Windows |
| **Hosting options and plans** | App service plan |
| **App Service Plan** | asp-bankfiletrans-{region}-test |
| **Networking** | |
| **Access restriction** | On - Allow public access.   * Has a ‘Deny all’ rule with priority 2147483647. * Add rule: * Name: AllowBC * Priority: 200 * Action: Allow * Description: AllowBC * Service Tag: Dynamics365BusinessCentral * HTTP headers filter settings: All left blank |
| **App assigned address** | Off |
| **Private endpoints** | Off |
| **Inbound address** | Function App IP Address shown on Properties page |
| **Vnet integration** | On  Vnet: vnet-bankfiletrans-{region}  Subnet: snet-bankfiletrans-{region}-test |
| **Hybrid connections** | Off |
| **Outbound addresses** | The Public IP and many more |
| **NAT gateway** | On |
| **Network security group** | nsg-bankfiletrans-{region}-test |

## Storage Account – Prod

The Storage Account is created during provisioning of the Function App for hosting web job resources. We can use the same storage account to store private and public key files.

|  |  |
| --- | --- |
| **Resource Name** | Stobankfiletrans{org} |
| **Region** | E.g. Australia East |
| **Performance** | Standard |
| **Replication** | Locally-redundant storage (LRS) |
| **Networking** | Enabled from selected virtual networks and IP addresses.  Add existing virtual network: vnet-app-ae  Subnet: snet-prod-ae  Add Function App’s Inbound and Outbound IP addresses. E.g.  nnn.nnn.nnn.nnn/32 (the public IP address)  nnn.nnn.nnn.nnn/32 (function app inbound IP) |
| **Containers** | Create new container called **keyfiles**. All private and public key files for FTP connection and PGP encryption will be uploaded to this container. At the time of writing this document, the five files below were uploaded to this container:  **SFTP Private Keys**   * Private key we generated for customer   **PGP Keys**   * Private key we generated for customer * Public Keys supplied by banks |

## Storage Account – Test

The Storage Account is created during provisioning of the Function App for hosting web job resources. We can use the same storage account to store private and public key files.

|  |  |
| --- | --- |
| **Resource Name** | Stobankfiletranstest{org} |
| **Region** | E.g. Australia East |
| **Performance** | Standard |
| **Replication** | Locally-redundant storage (LRS) |
| **Networking** | Enabled from selected virtual networks and IP addresses.  Add existing virtual network: vnet-bankfiletrans-{region}  Subnet: snet-bankfiletrans-{region}-test  Add Function App’s Inbound and Outbound IP addresses. E.g.  nnn.nnn.nnn.nnn/32 (the public IP address)  nnn.nnn.nnn.nnn/32 (function app inbound IP) |
| **Containers** | Create new container called **keyfiles**. All private and public key files for FTP connection and PGP encryption will be uploaded to this container. At the time of writing this document, the five files below were uploaded to this container:  **SFTP Private Keys**   * Private key we generated for customer   **PGP Keys**   * Private key we generated for customer * Public Keys supplied by banks |

# Configure Key Vault

We need to configure access to the Key Vault for the Function App so the Function App’s code can easily retrieve the secret keys from the Key Vault. Then we need to add the RSA SHA-2 keys as secrets to the Key Vault.

## Enable Managed Identity for Function App

1. Go to the Function App and go to Settings -> Identity and turn on System assigned identity. This will create a managed identity with the same name as the function app. E.g. fapp-bankfiletrans-{org}-{region}.

## Configure Key Vault Access Control

1. Go to the Key Vault and go to **Access control (IAM)**.
2. Add a new Role Assignment, and grant **Key Vault Secrets User** role to the Funsion5 support account.
3. Add a new Role Assignment, and grant **Key Vault Secrets User** role to the managed identity created in 5.1.

## Add Keys As Secrets to the Key Vault

There are two Key Vaults. One for the production environment and one for the test environment. Each Key Vault will have a set of secrets described in this section.

In the Key Vault, go to Objects -> Secrets, then add the secrets with the following information. (Set Upload options to Manual when adding the secrets.)

|  |  |
| --- | --- |
| **Name** | BlobConnString |
| **Content type** | Blob Storage Connection String |
| **Secret value** | Get from the Storage Account -> Access keys -> Connection string. |

|  |  |
| --- | --- |
| **Name** | BlobContainer |
| **Content type** | Blob Storage Container that contains the private key files |
| **Secret value** | keyfiles |

|  |  |
| --- | --- |
| **Name** | PGPPrivateKeyFile |
| **Content type** | Private Key File for PGP decryption |
| **Secret value** | (Name of the PGP Private Key file we generated for customer) |

For each bank, create a set of these secrets:

|  |  |
| --- | --- |
| **Name** | {BANK}SFTPHost |
| **Content type** | SFTP Host Name |
| **Secret value** | (As provided by the bank) |

|  |  |
| --- | --- |
| **Name** | {BANK}SFTPUser |
| **Content type** | SFTP Username |
| **Secret value** | (As provided by the bank) |

|  |  |
| --- | --- |
| **Name** | {BANK}SFTPPrivateKeyFile |
| **Content type** | Private Key File for accessing SFTP |
| **Secret value** | (Name of the SFTP Private Key file) |

|  |  |
| --- | --- |
| **Name** | {BANK}PGPPublicKeyFile |
| **Content type** | Public Key File for PGP encryption |
| **Secret value** | (Name of the PGP Public Key file provided by the bank) |

## Create Key Vault Reference in Function App Configuration

There are two Function Apps. One for the production environment and one for the test environment. Each Function App will have a set of key vault references defined in the Configuration section.

***IMPORTANT:*** *Every time a Key Vault secret is updated, the Key Vault reference needs to be saved again manually to ensure the reference is updated.*

Go to the Function App, then go to Deployment -> Configuration and add the following application settings. (Note that the bank names are in all caps to simplify function apps coding.)

|  |  |
| --- | --- |
| **Name** | BlobConnString |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName=BlobConnString) |

|  |  |
| --- | --- |
| **Name** | BlobContainer |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName=BlobContainer) |

|  |  |
| --- | --- |
| **Name** | PGPPrivateKeyFile |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName=PGPPrivateKeyFile) |

For each bank, create a set of these Key Vault References:

|  |  |
| --- | --- |
| **Name** | {BANK}-SFTPHost |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName={BANK}SFTPHost) |

|  |  |
| --- | --- |
| **Name** | {BANK}-SFTPUser |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName={BANK}SFTPUser) |

|  |  |
| --- | --- |
| **Name** | {BANK}-SFTPPrivateKeyFile |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName={BANK}SFTPPrivateKeyFile) |

|  |  |
| --- | --- |
| **Name** | {BANK}-PGPPublicKeyFile |
| **Value** | @Microsoft.KeyVault(VaultName=<key vault name>;SecretName={BANK}PGPPublicKeyFile) |

With these Key Vault References created, the function app code can then easily retrieve the secret values from the key vault just as retrieving configuration values from the environment variables. E.g.

sftpHost = Environment.GetEnvironmentVariable("{bank}SFTPHost");

# Function App Functions

|  |
| --- |
| **Note:**  **This section may change as the function app is currently going through enhancements.** |

The Function App will include these functions:

* GetFileListFromBank
* GetFileFromBank
* SendFileToBank
* DeleteFileFromBank
* EncryptFileForBank
* DecryptFileForBank

The full endpoint for calling the functions will be:

https://<function app url>/api/<function name>

When calling these functions, the caller should provide an x-functions-key in the HTTP Request Header. The value of the x-functions-key can be found in the Azure Portal, Function App -> App keys, as the default key.



The sections below describe the details of each function.

## GetFileListFromBank

|  |  |
| --- | --- |
| **Method** | GET |
| **Request Headers** | * x-functions-key |
| **Request Body** | None |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. * **folder**. Folder path for retrieving the list of files. E.g., IN/BankStatements. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | A multiline string containing one file name per line. |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ GetFileListFromBank?bank=anz&folder=bankstatements |

## GetFileFromBank

|  |  |
| --- | --- |
| **Method** | GET |
| **Request Headers** | * x-functions-key |
| **Request Body** | None |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. * **folder**. Folder path where the file is in. E.g., IN/BankStatements. * **filename**. * **enc**. “no” = No decryption required, else perform PGP decryption on the file while downloading. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | A multiline string containing the decrypted file content. |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ GetFileFromBank?bank=anz&folder=bankstatements &filename=bankstatement\_20230612.txt |

## SendFileToBank

|  |  |
| --- | --- |
| **Method** | POST |
| **Request Headers** | * x-functions-key |
| **Request Body** | String content of the file. This content will be PGP encrypted by the function before saving to the bank’s FTP folder. |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. * **folder**. Folder path to save the file into. E.g., OUT/Payments. * **filename**. Name of the file that will be saved to the bank’s FTP folder. * **enc**. “no” = No encryption required, else perform PGP encryption on the file while uploading. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | “Success” |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ SendFileToBank?bank=anz&folder=bankstatements &filename=payments\_20230612.txt |

## DeleteFileFromBank

|  |  |
| --- | --- |
| **Method** | POST |
| **Request Headers** | * x-functions-key |
| **Request Body** | None |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. * **folder**. Folder path where the file is in. E.g., IN/BankStatements. * **filename**. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | “Success” |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ DeleteFileFromBank?bank=anz&folder=bankstatements &filename=bankstatement\_20230612.txt |

## EncryptFileForBank

|  |  |
| --- | --- |
| **Method** | POST |
| **Request Headers** | * x-functions-key |
| **Request Body** | String content of the file. This content will be PGP encrypted by the function. |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | PGP encrypted file content. |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ EncryptFileForBank?bank=anz |

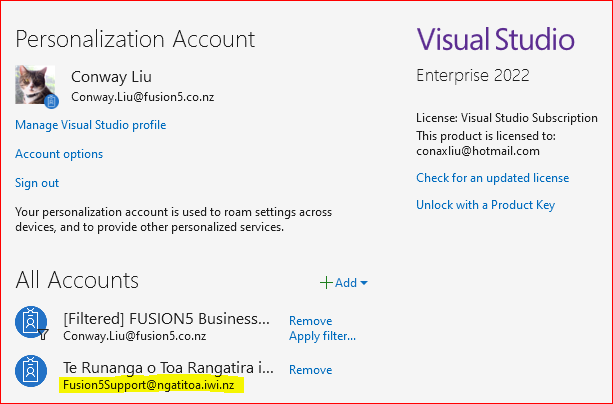
## DecryptFileForBank

|  |  |
| --- | --- |
| **Method** | POST |
| **Request Headers** | * x-functions-key |
| **Request Body** | Encrypted string content of the. This content will be PGP decrypted by the function. |
| **Query String Parameters** | * **bank**. E.g., anz, westpac…etc. |
| **Return HTTP Status** | * 200: Success * 400: Function detected invalid request submitted, including missing Function App configuration settings. * 401: Unauthorized likely due to invalid x-functions-key. |
| **Response Body (Success)** | Decrypted plain text file content. |
| **Response Body (Error)** | A string starts with “ERROR:” and the description of the error. |
| **Example** | https:// fapp-bankfiletrans-{org}-{region}.azurewebsites.net/api/ EncryptFileForBank?bank=anz |

# Function App Deployment

The function app can be deployed directly from within Visual Studio 2022. The solution can be cloned from <https://dev.azure.com/Fusion5BC/Fusion5%20BC%20Azure%20Functionalities/_git/Fusion5%20BankFileTransfer>

Ensure you have added the appropriate Fusion5 Support Account to your Visual Studio, otherwise Visual Studio will not be able to properly publish the function app to the customer’s Azure environment. E.g.



Once the solution is cloned, build the solution to ensure it can be built successfully. Then right-click on the project name and select Publish. Check the details on the screen to ensure you are publishing to the correct tenant and environment. Create a new publishing profile for the tenant and environment if not yet exist, then click the Publish button.

A screenshot of a computer

Description automatically generated

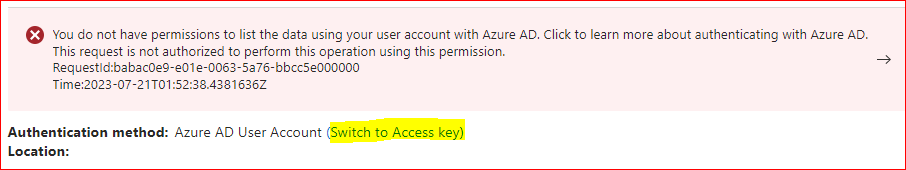
Note that this function app is not setup to run locally, since the banks have only whitelisted the IP address of the function app running in Azure.

# Update Production PGP Keys

The public PGP keys provided by some banks may have an expiry date. ANZ, for example, provides public PGP keys that last for five years each time. When it’s near the expiry date, ANZ will notify customers to update the key to ensure systems continue to work properly.

## Update ANZ Production PGP Key

To update the production public PGP key from ANZ, follow the steps below:

1. Download the latest key file from [ANZ Online Resources](https://www.anz.com/institutional/digital-services/online-resources/), in the accordion section of 'Fileactive PGP key'. Unless ANZ changes the name of the key file, It would be named as **fileactive-pgp-public-key.pub**.
2. Login to Azure using the Fusion5 Support Account.
3. Locate the Storage Account resource **stobankfiletrans**, browse to Containers, and into the ‘keyfiles’ folder.
4. If you see an error message ‘You do not have permissions to list the data….’, click the ‘Switch to Access key’ link.  
   
5. Download the existing ANZ key file for backup, then delete the key file from the folder.
6. Upload the new ANZ key file to overwrite the existing key file.

If the name of the new key file is different from the current key file name, follow the steps below to further update the configurations:

1. Locate the Key Vault resource **kv-bankfiletrans-{org}{region}**, browse to Secrets.
2. Click into the **ANZPGPPublicKeyFile** secret, then click **+New Version**.
3. Enter the following details:

|  |  |
| --- | --- |
| **Secret value** | <the file name of the new PGP key file> |
| **Content type** | Public Key File for PGP encryption |

Theoretically this should be all we need to do. However, because the function app’s configuration settings seem to cache reference values, it may still provide old setting values to the app. So we need to force a refresh of the configuration setting values.

1. Locate the Function App resource **fapp-bankfiletrans-{org}-{region}**, browse to Configuration.
2. Click into the **ANZ-PGPPublicKeyFile** setting, rename the setting name to something else, e.g., **ANZ-PGPPublicKeyFileS**, then click OK.
3. Click Save at the top of the page.
4. Repeat steps 5 and 6, but this time rename the setting name back to **ANZ-PGPPublicKeyFile**.