E-Banking with Atlas Design and Implementation Guidelines

I. Background

Headquarters bank accounts, HQ Zero Balance Accounts assigned to Country Offices, and many Country Offices local bank accounts utilize Host-to-Host (H2H) electronic banking interface EFT (with Bank of America) and FGT (using ISO20022). The H2H interface, however, cannot accommodate some country offices' local banks due to varied domestic banking requirements/regulations and resource challenges. FGT (Financial Gateway) was introduced in 2012 to automate the payment processing in ATLAS by leveraging ISO20022 standard for payment processing and acknowledgement under SWIFT FileAct protocol.

In the case where H2H interface cannot be implemented immediately for the Country Offices, other forms of local electronic banking interfaces are put in place, for example the use of Web E-Banking solutions offered by the banks.

While there are obvious benefits and potential efficiencies that E-Banking can provide, designing and implementing the interface must be in compliance with UNDP's internal control framework while ensuring that proper mechanisms are in place to protect data integrity as the data is transmitted from UNDP to the banks.

This document outlines the standards and requirements that need to be considered when designing and implementing E-Banking.

II. Process Overview

The payments data, once approved in the Atlas in accordance with the ICF, are extracted and delivered to bank using the following steps:

1. Vendor Payments/Staff payroll payments/T&E Payments are certified and approved in Atlas; Atlas generates payment instructions file.
2. Payment instructions are formatted to a layout agreed with the bank.
3. Payment instructions are sent to the bank.
4. Bank confirms receipt and status of payment instructions.

III. Common E-Banking Configurations

E-Banking facilities and capabilities vary from bank to bank. Below are the configurations that are commonly available.

Host to Host E-Banking (H2H) – Payment instruction files (EFT/FGT) are sent directly from the UNDP's server to the bank's file server. Data is encrypted and is transmitted through private networks. UNDP H2H interface with Bank of America is identified as EFT. FGT solution is used by leveraging UNDP's SWIFT membership and the use of SWIFT/FileAct connectivity to exchange data with other banks. The application uses a single, common, non-proprietary file format (ISO 20022) for payments processing. And electronic statements are reported using SWIFT MT940 format from the banks to UNDP.

Web E-Banking/online solutions – The bank provides online web application where clients can create individual payment instruction or upload a bulk payment file. Web E-Banking applications provide facilities for uploading pre-formatted payment instructions and then allow users to review and approve payments online. Users are provided with credentials by the bank with the ability to login using password and/or token.

IV. Design Considerations and Requirements

The following details the requirements and considerations that need to be taken at each step of the process.

1. Processing the payment file generated by Atlas

A payment file, Universal Flat File (UFF), is generated after running the AP Pay Cycle/ Payroll or T& E. The UFF contains the necessary information (e.g. payee, bank information, payment amount and payment mode) to create payment instructions.

In the case of fully implemented Host-to-Host, the UFF file is downloaded and passed to a routine that re-formats the file into a layout agreed with the bank. In order to avoid/to minimize the risk of having the UFF file being tampered with, technical configurations to integrate the download, format and upload routines into a single program must be in placed; thereby eliminating any manual intervention.

For payment monitoring purposes, it is useful to store the payment instructions into a local database. The payment status from the bank can be stored into the same database for record reconciliation.

2. Review and approval procedures for releasing payment instructions to the bank

Under Web E-Banking setup:
Prior to executing bulk uploading to the E-Banking platform, the 1st authorized user may need to reformat UNDP UFF file to meet that of the bank's requirements either manually or using a converter tool. The e-banking tool may also allow to modify the data, therefore a final verification to match the data with the original UFF file must be completed by the 1st user before the file is sent for approval to the 2nd authorized user. The 2nd authorized user is

responsible to review and reconcile the data loaded to the E-Banking with the original UNDP UFF file before any approval.

It is of the utmost important that the UFF file generated from Atlas is secured and not tampered with since Atlas does not offer encryption.

For Host-to-Host setup:
UNDP UFF file is electronically submitted from Atlas to the bank through interface, therefore it does not require any approval. It is however advisable to have the formatting program generate a control total report that can be reconciled with the Pay Cycle report – ensuring that the number of transactions and the total amount agree. Alternatively, a report can be generated if the transactions are saved into a database.

3. Data Transmission

For Web E-Banking, data transmission is usually taken care of by the bank's software as the web application is bank's proprietary solution and resides within their protected servers and usually transparent to the users. Still, it is useful to understand the mechanism in place how the data is protected after the payment file is uploaded. In addition, it should be made clear that the responsibility of ensuring data integrity in this case, for the most part would be the bank. The data should also be handled carefully by granting access to authorized staff within UNDP environment as the UFF file currently does not have built-in encryption or security in Atlas.

In the case of Host-to-Host setup, since we are pushing data to the bank's server, UNDP is responsible for ensuring data integrity until the data reaches the bank. There is a Straight-through-Process (STP) established without any manual process to communicate data between UNDP Server to Banks. It is hard, if not impossible, to fully guarantee data integrity that passes through public networks. Nonetheless, there are controls that can be implemented to guard data at acceptable levels. The payment instructions file should be encrypted using the bank's digital public key. Please refer to Appendix A, Public Key Encryption System. In addition, use of secured transport layer (scp/sftp, or ftp over SSL) is recommended instead of the regular unencrypted ftp session.

4. Receiving and processing bank's receipt confirmation and payments status

For Web E-Banking, the status of the payments is made available on the web platform.

For Host-to-Host, downloading the payment status from the bank's server is usually initiated by the client. Same as the payment file transmission, downloading payment status should follow the same encryption and secured transport mechanisms.

For further information, please contact David Jordan, OIMT at david.jordon@undp.org or Paul Gravenese, Treasury at paul.gravenese@undp.org

Appendix A. Public Key Encryption System

Public Key Encryption System is a widely accepted and highly trusted encryption system in which two complementary keys, called a key pair, are used to maintain secure communications. One of the keys is designated as a private key to which only the sender have access. The other is a public key that is exchanged with other users. Both the private and public keys are stored in a keyring files. Some systems refer to the private and public keys as confidential and open keys, respectively.

Only the sender has access to his private key, but in order to correspond with other users, he needs a copy of their public keys and they need a copy of his. The sender uses his private key to sign the documents he sends to others and to decrypt the files they send to him. Conversely, the addressee uses the public keys of others to encrypt the documents he sends to them and to verify their digital signatures. This way, it is guaranteed that only the addressee can decode the document, and that the addressee can be confident that the very sender who has signed it, sent the document.

Appendix B. Data Format and Controls

The bank designs the structure of the payment instructions file. It is worth confirming however that some controls are embedded into the file structure (e.g. hash totals, number of payments and total payment amount) that allows the bank to verify if the file is valid or not. This, for example, alerts and prevents the bank from processing an incomplete payment file.

In addition, for EFT/FGT payments, Atlas is configured to generate a unique payment reference number across all UNDP bank accounts. It should be agreed with the bank not to process payment request if a payment with the same reference number has already been received and processed. No special encryption protocols are needed in case of FGT payment files as SWIFT is more reliable and secured network which covers more public keys, digital certificates and digital signatures are variously used to authenticate senders and to validate the integrity of the messages sent.