SMARTPay System

The SMARTPay System is designed to provide a secure electronic messaging system to financial institutions to interact with peers or clients. It will facilitate exchange of financial messages between remote branches of the same institution, between different institutions and also for passing on payment instructions from corporate clients to Financial Institutions/bodies.

The System is formulated with the security requirements of financial messaging in mind. It enables production and transmission of secure messages across computer networks over regions in a country or even overseas. The messages are encrypted and use the most secure RSA key system based on PKI technology. The access to the system is restricted using smart card readers or bio-metric control systems or both depending upon the users security requirements. Moreover, a very strong and exhaustive audit trail keeps track of the usage of the system by individual users.

Each message created and sent in the system follows the 6 eyes principle making collusion of users very difficult. The user set up module allows a wide choice of delegation that makes it possible to minimize possibility of abuse of the system by users.

Economically, the system aims at empowering the corporate clients with the ability to undertake their own EFT and RTGS transaction handling and at the same time downsizing the bank operational tasks pertaining management of corporate clients transactions.

Smart Card & Bio-Metric Controls

The system controls access using smart cards and/or finger print reader methods to control access. The smart cards system is both affordable and amenable to control at the central point. The card to be issued to a particular user can be configured with the required secret codes at a central point and issued to the users along with a PIN (personal identification number) that may be changed at any time by the user to ensure absolute confidentiality.

The finger-print reader technology makes it more rigorous since it is not possible for another unauthorized person using a stolen access instrument. The above security requirements are essential for all categories of users such as Verifiers and Authorizers.

Other categories of users such as System Administrators are not allowed to create or verify any messages.

Straight Through Processing

The system has features that support integration with a wide range of systems such as Internet/sms banking, SWIFT, RTGS and Banking & Accounting Systems.

A range of reports allows for proper supervision, audit and reconciliation as well as exception reports. Optionally, it offers Anti Money Laundering filtering and reporting.

Contact us on kenex@kenexnbi.com for further details