Solutions for Borderless Banking

KTeller Biometric Identification Suite

In the current financial transactions world, whether huge or small transactions require the outmost verification of the bearer. Thus many financial institutions face this challenges of authentication that the clients are whom they claim to be and that their identity is truly theirs.

KENEX proposes to you KTELLER which consists of a robust USB Optical Fingerprint scanner connected to a standard office computer (preferably at the teller terminals) and KTELLER clients (Customers) authentication management software loaded on the same computer on your Local Area Network (LAN).

KTELLER operations Scope and Benefits

For client registration, KTELLER system captures and verifies users' fingerprints and stores them in a central database. This procedure is done onetime and requires the clients to be present.

During the registration process, the clients' accompanying documents such as national ID or Passport can be scanned and associated with the specific enrolled client.

After enrollment, the system has a maker checker facility in which the enrolled clients have to be approved by a high level officer before they can be authenticated.

For authentication, the KTELLER system uses fingerprint biometrics scanner device to capture the client fingerprint and certify against existing template. If found matching, the teller can proceed with the transaction and if not the client is blocked from carrying out a transaction.

Further, the system has a utility to "blacklist" block the customers from making a transactions unless approved by an individual with higher authority e.g. the supervisor or bank branch manager.

For management, the system will automate transaction processing, and assist in decision making for the various parties in the decision making tree within the organization.

Below is a diagram illustrating how KTELLER system can be deployed on a bank and its branches
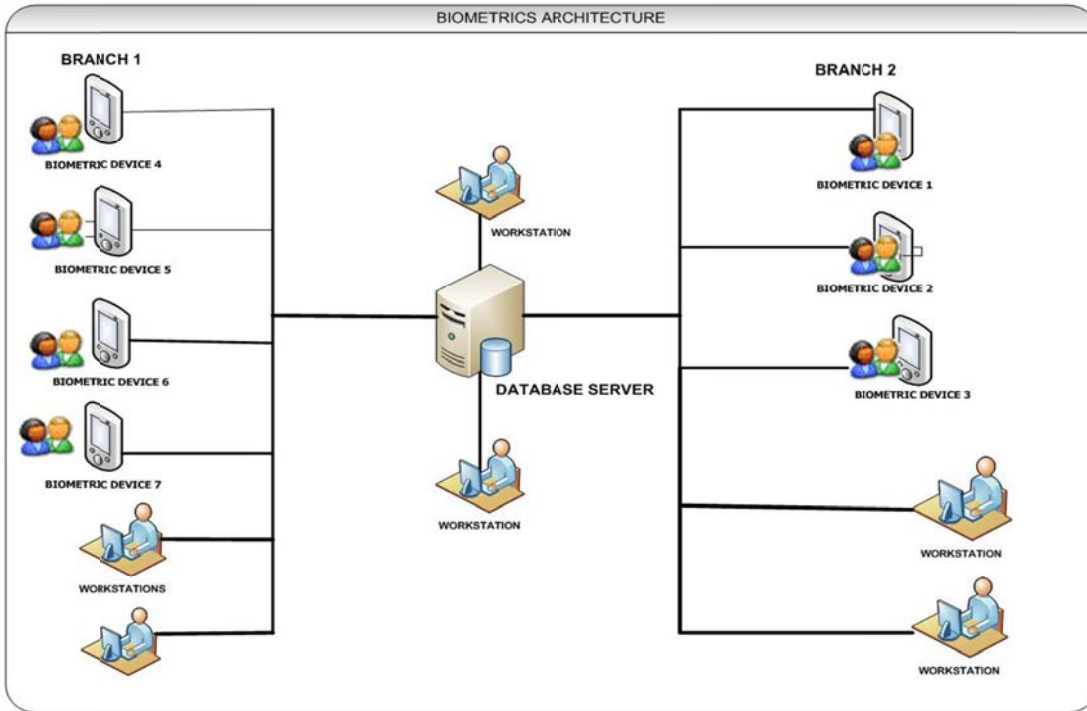
KTELLER Fingerprint Scanner - Fingkey Hamster III

It can be connected to PC along with a normal mouse or keyboard

KENEX © 2015

KTELLER   Security

The system enhances the security aspect by enforcing the following

- Access to system is controlled through use of user name and password.

- There is Dual authorization of user names and passwords for the users created in the system by the administrator.

- The system has a feature for enforcing password change for a new user after 1st log on or whenever the administrator has modified his/her system access rights

- User's passwords are stored in encrypted format and meet the minimum password complexity defined in terms of length, characters, case sensitivity, etc.

- The system has three levels of operations to facilitate maker-checker functionality of the system i.e.

    o Administrator – who setups up system parameters and users management

    o Approval – who counterchecks registered client details

    o Data – who registers the client details

- The system has a robust and extensive audit trail which is only viewable to administrator and cannot be deleted. Its accessible centrally across the branch network

- System users can be configured to use biometric logon instead of password – optional

Contact us on kenex@kenexnbi.com for further details