TRUSTBANKCBS CORE BANKING SOFTWARE

TrustBankCBS Core Banking Software is a product of Trust Fintech Limited. We are a CMMi Level 5 Certified and ISO 27000 Certified Company.

User Administration & Security

Centralized User Administration and Security Management for financial organizations

Solution enables to customize and provide secure access, control various activities of users. Each role has a different access privileges. Solution helps to manage and administer of giving individual users within a system access to the tools they need at the right time. Provides seamless way to manage user identities and access all in one place for employees with varying roles and responsibilities. Administrators have access to a single console for all products. It can manage users and groups, what programs they have access to, and which applications you'll run within it.

It quickly manages local user accounts; User Management software is the tool of choice. It makes it easy for administrators to manage user accounts within any Domain. It offers the simplest way to manage information about local user accounts. It also enables the administrator to reset local user passwords and enable or disable account status. As an administrator, you can even remotely use the software to perform desired tasks.

Our framework offers with a fully functional user management system that gives an edge over competitors. This user management will be completely extendable. It is highly customized to meet your business needs. TrustBank CBS has facility to create user from existing employee. In this system allots dummy password to update his new password first time according to define password policy. Also defines user role, user password expiry, user over limit power. Assign different module rights to existing user. Assign module wise & role wise menu rights to user.

Strong password generation

Additional Biometric authentication facility for valid user access

Multiple system login not available.

Ideal duration limit set so that application can log out the user if the system remains ideal

Encrypted password

ID-Suraksha

Reduce Risk, Secure transactions, Protect business. If banks, financial institution are looking to enable secure access, facilitate two-factor authentication (2FA) and Single Sign-on (SSO), we have a solution that is simple, secure, user-friendly, and easy-to-integrate and supports organization's financial transactions with ID-Suraksha Device. Biometric authentication of Trust CBS is trusted by most of the financial institutions. Trust CBS with the help of ID-Suraksha provides 2 Factors Authentication for Users so as to ensure valid user access. It thus helps to strengthen security. According to RBI circular for 2 Factors Authentication, we design Biometric authentication for user security & to stop password hacking. In this process user first enter his manual password & then use biometric to login the application. Also for transaction authentication we use same activity. It is very easy to use & 100% secured other than OTP generation.

Biometric Sign-In Tools

Activate the biometric sign-in capabilities for convenience, security and protection against attacks and breaches.

Security Challenges in Financial Industry

Meet RBI, State and federally regulated compliance requirements with a trusted biometric solution.

2 Factor Authentications

Authenticate in an instant with a touch of your finger; security and convenience in one.

Preventing Data Breaches

Reduce data breach risk across the organization with biometric authentication.

Secured Shared Networks

Eliminates unauthorized access that puts your business at risk.

Audit Trail

A well-managed audit trails are key indicators of good internal business controls. Audit trails have transitioned from manual to automated electronic logs that make this historical information more accurate, readily accessible, and usable. Successful audit trails demand a top down commitment by upper management, affected departments, and IT personnel. The more quickly an abnormal change or addition to information is "red-flagged," the better the response to mitigate against negative influences such as cyber-threats, security breaches, data corruption, or misuse of information. This article will define an audit trail, what should be included, the importance of tracking this information, and how to best manage audit trail data. Then, we'll demonstrate sample audit trails that you may find in your business systems. Solution provides Audit Trails electronic records that chronologically catalog events or procedures to provide support documentation and history that is used to authenticate security and operational actions, or mitigate challenges. Records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations. Whether it is logging the design changes of a product build, keeping the record of financial transactions for banking institutions, an audit trail validates actions and outcomes. Audit trail records will contain details that include date, time, and user information associated with the transaction. Solution plays an important role in the general process of organization- or regulation-specific audit logs and trails. System itself has a unique and densely populated log process where the numerous and varied activities of users, systems, and applications are constantly monitored to prevent misuse, hacking, or corruption of information.

It has system for validation as an essential tool to analyse operations and technical controls for computer systems. Used to validate and monitor activity, an audit trail provides a tool to maintain information and system integrity. Solution maintains the log of every change in existing data such as old data, new data, machine ID, Change date, Change time, user histories and authentications.

Benefits

System has the ability to follow records back to their origin provides numerous benefits, including transparency and a defence of records for compliance, record integrity and accuracy, system protection from misuse or harm, and security of sensitive or vital information.

These are achieved through these four areas:

- **User Accountability**: A user is anyone who has access to the system. Implementing audit trails promotes appropriate user behavior, which can prevent the introduction of viruses, improper use of information, and unauthorized use or modifications. In addition, the user knows that their actions are automatically recorded and tied to their unique identity.
- **Reconstruction of Events**: When an investigation is warranted or triggered, the first step to remediate a problem is knowing the "when," the "how," and the "what" of the event. Visibility into this information can aid in problem detection and prevent future occurrences of things such as hacking, system failures, outages, or corruption of information.
- **Intrusion Detection**: Audit trails aid in identifying suspicious behavior or actions. Unauthorized access is a serious problem for most systems. Many regulations now have mandates for the security of information and maintaining confidentiality. Protection also extends to intellectual property, designs, personnel information, and financial records.
- **Other Problem Identification**: Through real-time monitoring, you can use automated audit logs to identify problems that indicate system implementation issues, operational issues, unusual or suspicious activities, or system and operator errors.

Digital Signing

In today's hyper-connected world, traditional methods of signing and authenticating documents are increasingly being replaced by technological innovations such as digital signatures in particular. It has the highest level security and acceptance.

Features

Authentication

They authenticate the source of messages. Since the ownership of a digital certificate is bound to a specific user, the signature shows that the user sent it.

Integrity

Sometimes, the sender and receiver of a message need an assurance that the message was not altered during transmission. A digital certificate provides this feature.

Non-Repudiation

A sender cannot deny sending a message which has a digital signature.

Added Security

With use of encryption verification technology, a digital signature offers the highest and most verifiable standard for identifying an individual by an electronic signature. The coded message in a digital signature uniquely identifies the signer and links him or her with a particular recorded document.

Global Acceptance and Legal Compliance

Countries are starting to accept digital signatures on legally binding documents because they understand that the security protocols offered by vendors are in compliance with international standards in the field.

Contact Details

NAGPUR OFFICE

Trust Fintech Limited

11/4, IT Park, Gayatri Nagar, Nagpur, India. PIN: 440022

Hemant Chafale, CEO & MD

Cell: +91-9422111446

Email: hchafale@softtrust.com

PUNE OFFICE

Trust Fintech Limited

101, Navkar Avenue, Building No. A-2 Bavdhan, Pune, India. PIN: 411021

Heramb Damle, Director

Cell: +91-9422111442

Email: hdamle@softtrust.com

MUMBAI OFFICE

Trust Fintech Limited

509, E Square, Subhash Road, Vile Parle, Mumbai, India. PIN: 400057

Anand Kane, Director

Cell: +91 7028990080

Email: anandkane@softtrust.com