

Compliances

I. Achieving Sarbanes-Oxley Compliance with Tutis Biometric Logon

Information security is only a small part of the directives within the Sarbanes-Oxley (SOX) Act, but SOX has become a large part of information security for the organizations it applies to. After corporate scandals such as Enron, WorldCom, Tyco International and others threatened the economy and shook investor confidence, the US Congress passed the Public Company Accounting Reform and Investor Protection Act (PL 170-204), more commonly referred to as Sarbanes-Oxley.

Comprehensive Security as a Solution

Part of achieving and maintaining compliance with the SOX requirements is to ensure that only authorized individuals have access to sensitive internal data. Tutis Biometric Logon enterprise security solution provides a unique offering for achieving SOX compliance – and strengthening network security – by:

- Using strong authentication to ensure that individuals who access the network, applications, and portable devices like laptops are indeed who they claim to be, enabling you to tighten user access controls and enhance the security and integrity of your sensitive data.

TBL strong authentication provides an efficient solution for achieving SOX compliance by offering a comprehensive management free authentication solution for an organization's needs, including:

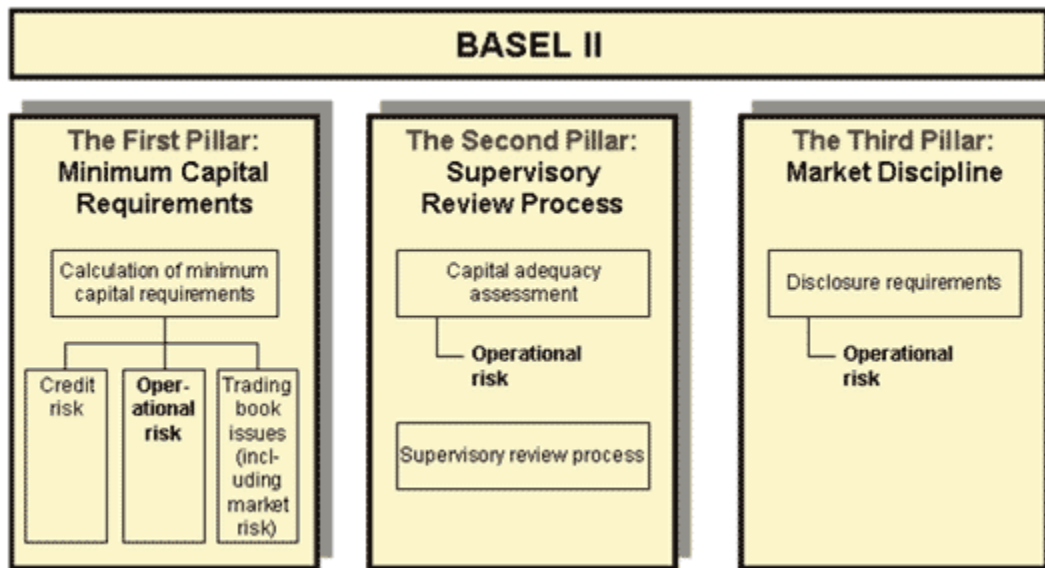
- Secure access to the company's network, computers, and applications
- Secure information transactions, email and documents
- Secure password management
- Secure physical access
- Complete Audit trail for Accesses & Encryptions

II. Achieving Basel II Security Compliance with Tutis Biometric Logon

The Basel II Accord, which went into affect in member countries by year-end 2006, is based on three pillars, designed to ensure that banks effectively monitor risk and implement sufficient risk-management practices to protect the institution.

The three pillars are:

1. Minimum Capital Requirements: describes the calculation for regulatory capital, credit, operational and market risks
2. Supervision: creates a framework of supervisory oversight and review processes to encourage better risk practices and to reduce other risks
3. Market Discipline: requires banks to disclose capital structure, risk exposures and capital adequacy in detail



The focus of each of the three pillars is the reduction of operational risk. The committee defines operational risk as "loss resulting from inadequate or failed internal processes, people and systems or from external events." Member banks are subject to a capital charge to cover unexpected losses, but the amount of the capital charge can be reduced if the bank can demonstrate to regulators that they have sound operational risk management procedures implemented.

Strong Security as a Solution

One of the primary elements of managing risk is to have an effective network defense system. Tutis Biometric Logon Enterprise security solution, protect your network resources and reduce operational risk by:

- Preventing unauthorized access to data by ensuring that individuals who access the network and applications are indeed who they claim to be, allowing you to tighten user access controls and enhance the security of your sensitive data.

Tutis Biometric Logon and Basel II

Fingerprint based strong authentication helps banks meet Basel II standards by ensuring strong authentication security. TBL offering is based upon Biometric strong authentication solution, which can be implemented for all of the bank's users.

- Secure access to the bank's network preventing unauthorized access to classified data, such as customer account information. This classified can be encrypted and stored. AFID can grant access to authorized users.
- Secure transactions, e-mail and documents with secure Biometric encryption reduces operational risk by enabling transfer of sensitive data sensitive data over the net, proof of authentic access (ensures physical presence while encrypting or decrypting data and tracking encryption and decryption locations)
- Eliminates password management completely.
- Secure physical access by having a room of incorporating RFID technology to provide combined logical and physical access solutions in one software, lowering operational risk by preventing unauthorized physical access.
- Usage of Biometric technology & fingerprint credential management at Windows AD level enabling full enterprise-level automated deployment and life-cycle management of fingerprints, diminishing operational risk by reducing human intervention in fingerprint management activities.

III. FIPS(Federal Information Processing Standards) & Tutis Biometric Logon

These standards define the security requirements that must be satisfied by a **cryptographic** module used in a security system protecting information within IT systems. Though we don't use cryptography, the explanation will be a guide to how we help in FIPS though not according to the inking in script.

What is cryptography?

Cryptography simply means Transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.

Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption ; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different

But today's cryptography is more than secret writing, more than encryption and decryption. Authentication is as fundamental a part of our lives as privacy. We use authentication though out our everyday life, when we sign our name to some document for instance, and as we move to a world where our decisions and agreements are communicated electronically, we need to replicate these procedures.

Cryptography contains even more when we include some of the things cryptography enables us to do. With just a few basic tools it is possible to build elaborate schemes and protocols which allow us to pay using electronic money, to prove we know certain information without revealing the information itself, and to share a secret quantity in such a way that no fewer than three from a pool of five people (for instance) can reconstruct the secret.

Tutis Biometric Logon can be sighted in this context, as a FIPS enabler. It is very difficult for any person, device, mechanism or procedure to be able to reconstruct a fingerprint template accurately and use the same to decrypt a file.

IV. HIPAA & Tutis Biometric Logon

After many delays, healthcare organizations are now finally under an established HIPAA-mandated deadline (most must be in compliance soon) to safeguard their electronic protected health information (ePHI).

And while no single solution meets all the technical security requirements of HIPAA, Tutis Biometric Logon security product can help healthcare organizations comply with many* of the requirements. Following is a list of key security requirements in the final HIPAA Security Rule published in April 2003, as well as the applicable Tutis Biometric Logon feature:

Unique User Authentication

HIPPA mandates that the confidentiality of individually identifiable health data be protected by authentication of the users that access such records. Passwords, the most common authentication mechanism, have been shown to leave organizations highly vulnerable to breaches in security. This is because passwords are often written down and are easily guessed, stolen, shared, hacked, or reused.

Tutis Fingerprint based Server Authentication solution offers healthcare organization the following security capabilities for unique user authentication:

- Strong, two-factor authentication(can be invoked) without any extra manageability like token, smart cards etc
- Easier and more cost-effective to deploy (critical for the traditionally tight budgets of healthcare organizations), since a user is authenticated in Windows AD.

- Better user experience, especially with the fingerprint reader, which promotes increased compliance (healthcare workers are among the most resistant to security measures they consider intrusive or time-consuming)

Workstation Security

HIPAA requires that only authorized users be able to access workstations that contain electronic protected health information (ePHI). So they can very well use TBL standalone version.

Tutis provides healthcare organizations with two distinct yet complementary methods for workstation security:

- Lock down workstations with Tutis strong user authentication and built-in features like:
 - Secu Desktop
 - File / Folder encryption / decryption
- Secure Network logon that protects network access with TBL strong user authentication

Data Integrity

HIPAA requires that a healthcare organization ensure that data in its possession has not been altered or destroyed in an unauthorized manner.

- Data can be encrypted with basic document properties that continue to exist even after encryption
- Log file give a complete track of Encryption origin and Decryption destination.

V. PCI (Payment Card Industry) Data Security Standard(DSS) Compliance with TBL

Tutis Biometric Logon currently does not support this compliance, but we can consult on the same.

The Payment Card Industry Data Security Standard (PCI DSS) was created by the world's major credit card companies to protect customer data. The primary purpose of PCI DSS is the protection of credit card data by reducing fraud and theft.

PCI DSS mandates that any merchants or service providers that handle, transmit, store or process information concerning the major credit cards, or related card data, are required to meet PCI standards or face penalties and/or severance by the credit card companies.

PCI DSS is a proactive security standard that defines requirements for security management, policies, procedures, network architecture, software design and other security measures.

Currently, Tutis is not suited to meet PCI DSS requirements. Though, in lieu of acquiring any assignment in this concern we can provide unique and effective security solutions for merchants and service providers that can meet PCI standards.

There are six primary areas covered by PCI DSS, divided into 12 requirements, with each being met by

1. Build and maintain a secure network
 - Install and maintain firewall configurations (Not our perview)

- Do not use vendor-supplied or default passwords
replace weak passwords with strong, two-factor fingerprint authentication
and also eliminates the need for risky and costly password maintenance
schemes
- 2. Protect cardholder data
 - Protect stored data

 - Encrypted transmissions of cardholder data across public networks
- 3. Maintain a vulnerability management program
 - Use and regularly update anti-virus software

 - Consult to develop and maintain secure systems and applications
- 4. Implement Strong Access Control Measures
 - Restrict access to "need-to-know"

 - Assign unique IDs to each person with computer access

 - Restrict physical access to cardholder data
- 5. Regularly monitor and test networks
- 6. Maintain an Information Security Policy