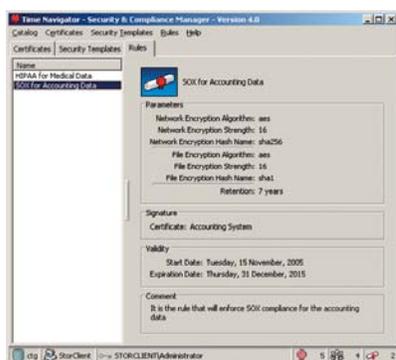# TIMEnavigator™

Security and Compliance Manager

INTRODUCING ADVANCED SECURITY
INTO YOUR DATA PROTECTION INFRASTRUCTURE

The digitalization of critical information has eased transactions and made recordkeeping and other tasks a great deal more efficient, but digitalization has also invited a huge number of internal and external risks that threaten the privacy and authenticity of personal and other data. In recognition of these very real threats to the sanctity of critical data, regulations like the Sarbanes-Oxley, HIPAA and Basel II dictate the need to provide secure backup and non-repudiated archiving.

Atempo is at the forefront as a means to control how data is treated, stored and secured against tampering and theft. Time Navigator Security and Compliance Manager (SCM) not only encrypts and decrypts the data in-place and on-the-network, but also integrates a digital signature system and digital certificates that include hierarchical key management. Encryption, digital certificates, key management, and activity trails intelligently applied to data with the aid of compliance templates forms the basis of a holistic, multi-layered storage security paradigm capable of meeting multi-dimensional security threats.

Applying the predefined Sarbanes Oxley rule with the backup of your financial data will help you comply with this regulation

KEY BENEFITS

Eavesdropping Prevention
Time Navigator SCM puts in place security mechanisms using public-key cryptography and encryption methods. It is the guarantee that the confidentially of your most important digital assets is not compromised while the information is transferred over a public or a private network or while it is stored on disk or tape.

Tamper Detection
Digital signatures are used in public-key cryptography to show and prove that data has not been altered. Applying a digital signature to the business critical information to backup before it leaves the primary storage is the best method to, upon arrival to the storage media, detect if it has been tampered with or if it is still intact.

Prevention of Impersonation
Using digital certificates and advanced authentication mechanisms, the recipient of the data sent by Time Navigator SCM can verify the sender's identity and confirm that the information comes from a trusted origin. When deploying Time Navigator SCM, a hierarchical key management infrastructure is put in place. IT professional can control which data can be backed up or restored by which individual.

Facilitating Compliance to Regulations in the Data Protection Area
Time Navigator SCM offers a set of compliance templates specifically designed to help companies meet compliance requirements related to data protection and archiving of sensitive digital assets. Implementing Time Navigator SCM in the data protection infrastructure is a significant step toward complying with the regulations imposed to a specific industry.

« Without security, information lifecycle management is dead-on-arrival. Atempo's Security and Compliance Manager provides a business-driven approach to protecting and securing your data. »

Jon Oltsik
Senior Analyst
Enterprise Strategy Group

ESg Enterprise Strategy group

Atempo

TIMEnavigator™

Security and Compliance Manager

KEY FEATURES

Advanced File & Network Encryption/Decryption Capabilities

Time Navigator SCM leverages public-key cryptography and offers a wide range of strong and certified ciphers to encrypt data to backup before it leaves the primary storage. Data remains encrypted while it is stored on any selected storage media for optimum security throughout its lifecycle. Whether it resides on disk or tape it will be impossible for a third party to read the company business critical information.

While it is traveling on the network from its primary storage location to the storage media, information is exposed to security threats and potential hackers. It has been proven that more than 50% of security attacks occurred on private networks. Time Navigator SCM offers strong encryption capabilities to secure data transfers. By building a secure tunnel, Time Navigator SCM protects digital assets and prevents any malicious third party from reading it while transferred from one storage media to the other.

Digital Signatures

Public-key cryptography uses digital signatures to help keep data intact. The methodology used to detect data alteration relies on a function called one-way-hash. Time Navigator SCM applies this function to the backup data to create a digital signature. Both the information to backup and the digital signature are sent over the network. When the data reaches its destination, a new hash is created from the data received and compared with the original hash proving the non-alteration of the information.

Hierarchical Key Management Capability

Time Navigator SCM leverages digital certificates as a proof of a person's or a server's identity. Implementing a hierarchical certificate infrastructure addresses the problem of impersonation and ensures that the information backed up or recovered has been sent by a trusted computer. The same mechanism is also used to prove that individuals trying to recover data are allowed to do so.

Compliance Templates

Time Navigator SCM offers a set of templates designed to meet specific compliance rules. Atempo has implemented these templates with each specific regulation in mind. Each template contains the encryption and hash algorithms recommended and authorized by the regulations; it also sets compliant retention periods for the selected data and the length of the passwords that are used to encrypt/decrypt the information.

Deep integration with the backup and archive classes

The key advantage of Time Navigator SCM is that all the security features are directly applied to the classes of data created when the backup environment is configured. It provides users with the flexibility to apply different level of security depending on the value of the information that needs to be protected and introduces the notion of "Secure Backup".

Audit Trails

All the regulations in place today require the creation and record of detailed audit trails regarding the activity on the regulated information. When a set of data has been selected in a backup class and a security rule is associated to it, Time Navigator SCM records all activity and stores it as a secured file in case of an audit.

ENCRYPTION ALGORITHMS AND COMPLIANCE TEMPLATES

Time Navigator Version	Encryption Algorithms	Hash Algorithms	Signature Algorithms	Compliance Templates
Time Navigator Enterprise Edition Version 4.01 and higher	AES CAST5 Triple DES TwoFish Blowfish	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Whirlpool Tiger	DSA RSA	Sarbanes-Oxley SEC 17.a HIPAA Basel II

ABOUT ATEMPO

Atempo is the leader in trusted information lifecycle management. Atempo's solution enables corporations to protect all their digital assets and secure those assets against tampering and theft over their information lifecycle. Atempo's Time Navigator software suite delivers enterprise-wide secure data protection and storage security, enabling corporations to meet critical business requirements including digital privacy, regulatory compliance, non-repudiated long-term archiving, and business continuity. Founded in 1992, Atempo has more than 2300 customers worldwide, with a sales and support network exceeding 100 resellers. The company's dual headquarters are in Palo Alto, CA, and Paris, France.

Learn more about Atempo and its "Trusted ILM" vision at www.atempo.com

groupe2milf1.com

Australia
Tel: +61 2 9025 3936

France
Tel: +33 (0) 1 64 86 83 00

Germany
Tel: +49 (0) 711 67400 330

The Netherlands
Tel: +31 (0) 70 4 16 17 04

Korea
Tel: +82-(0)2-2052-1189

Singapore
Tel: +65 6430 6728

Spain
Tel: +34 91 788 2617

United Kingdom
Tel: +44 (0) 208 610 6012

USA
Tel: +1 (650) 494-2600

Atempo