



White Paper

Meeting SOX and GLBA Compliance

**A Guide to Automating User Authentication
and Document Integrity**

CONTENTS

Overview3

SOX, GLBA, and the Impact on IT.....3

Digging Out From Under SOX and GLBA - the Trust Factor.....4

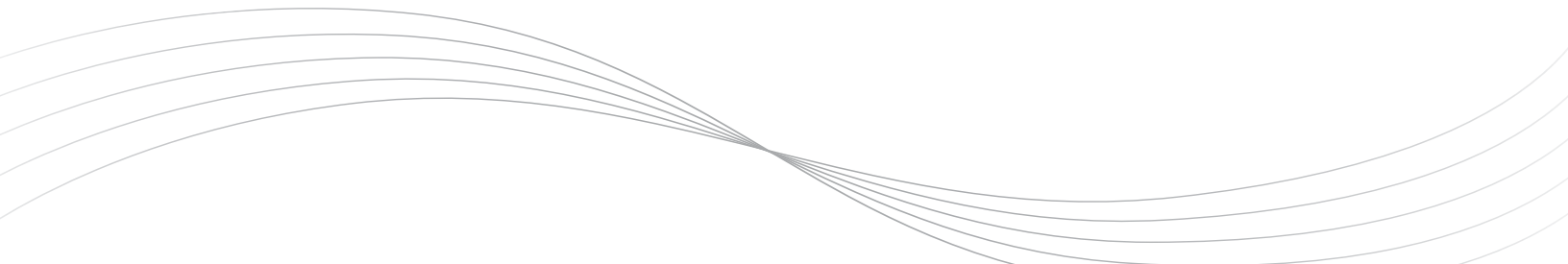
Compliance Equals Security: Three Key Security Concepts.....4

Enabling Trusted and Compliant Transactions.....6

The Paperless Paper Trail7

The GeoTrust Advantage.....7

Conclusion9



OVERVIEW

To comply with the Sarbanes-Oxley Act (SOX) and the Gramm-Leach-Bliley Act (GLBA) organizations must be able to protect data from unauthorized access (confidentiality), ensure that documents are what they say they are (integrity), while offering the flexibility of selective access and portability (availability). This can be a sizable challenge, taking into account the demands of a mobile workforce and the need to cater to business partners and customers, all requesting remote access to a multiplicity of internal IT applications.

In addition, regulations like SOX and GLBA spell out what businesses can and cannot do when it comes to financial reporting, client confidentiality, and document integrity. However, what the regulations do not provide is guidance on how to implement the proper processes and controls to make all this happen - and how to make it as painless as possible. Clearly, IT professionals are not compliance specialists, yet they are being asked to find technological solutions to regulatory issues. Fortunately, new automated security solutions can serve as the foundation for compliance initiatives.

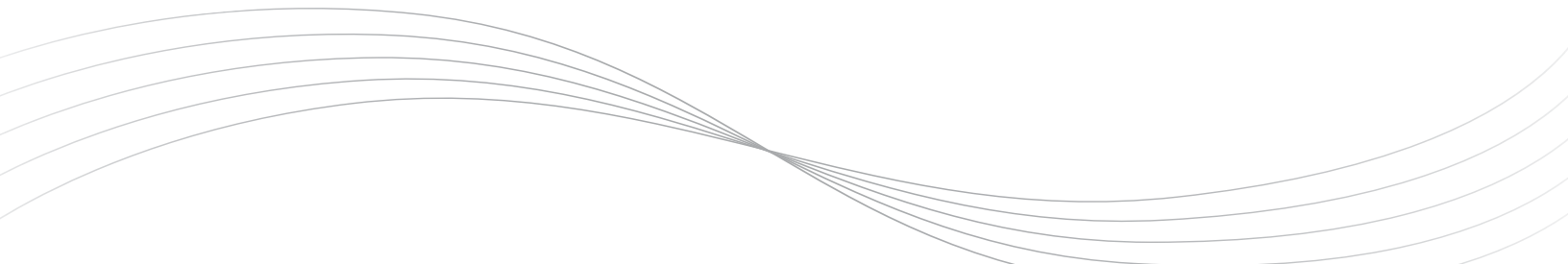
In the past, an audit meant that employees would be working late on the days leading up to the audit. Passing the audit meant being in compliance on the day of the audit, and important changes were often implemented at the last minute. Today SOX and GLBA require that organizations must be compliant at all times. And the only way to do that is to automate key aspects of security such as user authentication and document integrity.

SOX, GLBA, AND THE IMPACT ON IT

SOX and GLBA focus on two different areas of corporate accountability. As it translates to IT, SOX is essentially a data management and corporate governance problem, while GLBA is a security issue. SOX requires publicly-held companies to implement internal controls over their financial filings, in order to assure the accuracy of those filings. Moreover, it holds the executives who sign off on those filings personally accountable if the filings are misleading or inaccurate, with penalties of up to \$5 million or 20 years in prison. GLBA, on the other hand, seeks to bolster the confidentiality and integrity of consumer records. At first glance, it may be thought that these problems should be addressed separately, but they have key commonalities that should be handled together, which is why IT should develop a unified strategy when complying with these regulations.

Risks and Opportunities

While the Internet represents opportunity for enterprises to extend their reach, integrate their community of employees, business partners and customers, and reduce costs by using inexpensive public networks, it also represents risks for enterprises because it is open, anonymous and insecure. Business, however, cannot thrive any longer in the same open, non-confidential and anonymous environment, and that is why the government has stepped in with a range of new regulations.



Seizing the Internet opportunity while securely addressing its risks has been the challenge and promise of security infrastructures for a decade. However, corporate and government networks are still penetrated. When consumer data is stolen or patient records are compromised a business risks losing the trust of that single consumer. In addition, since many regulations require the public disclosure of such incidents, a business could also jeopardize its status as a trustworthy organization.

Even though SOX and GLBA regulations place new burdens on IT, they could represent a unique opportunity for an organization. By following the mandate of these regulations to use appropriate security measures and instill accountability in a cost-effective, coherent manner, the organization might well have a distinct advantage over those competitors who have failed to fully comply with the regulations.

DIGGING OUT FROM UNDER SOX AND GLBA - THE TRUST FACTOR

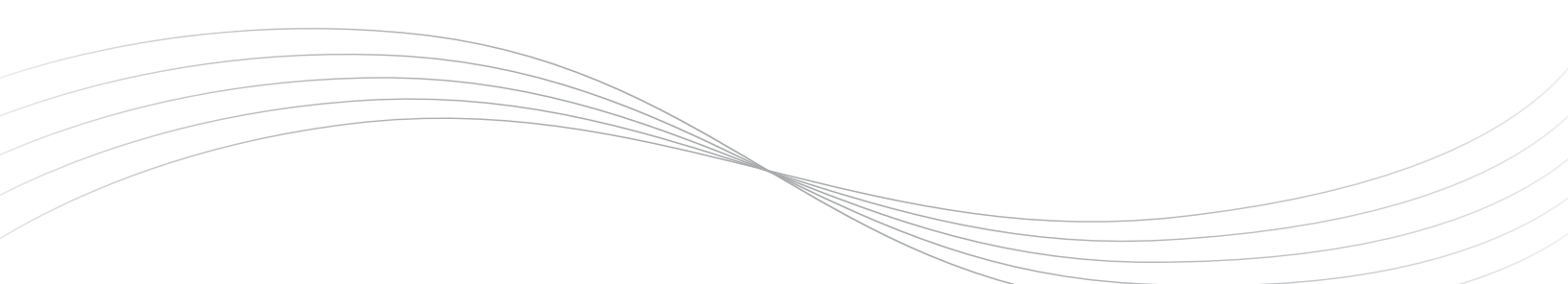
The intent of both SOX and GLBA can be summed up in one word - trust. Investors need to be able to trust that a public company's financial statements are accurate. Similarly, in this age of identity theft, customers need to be able to trust that organizations they do business with keep their sensitive information protected and private. Moreover, since something like an inaccurate credit report can adversely affect a person's future, organizations must ensure that the data they collect and maintain is accurate.

Section 404 of the SOX act speaks directly to the trust issue. This section focuses on a company's internal controls and their impact on a company's financial filings. For IT the two most important aspects of complying with Section 404 are identity and integrity. If key executives must verify that filings are accurate, then it is important that they know that the right person signed off on the right document. Similarly, they must manage the access to that document and ensure that it has not been tampered with after the fact. In other words, they need a way to trust that the document is what it says it is.

GLBA also deals with trust. The purpose of GLBA is to protect a consumer's personal, confidential data. When consumers give their information to a bank or credit card company, they need to be able to trust that their data is protected. The key to meeting both of these objectives is implementing an automated, reliable method for the authentication of users, and the ongoing integrity and security of their important documents. A manual approach will not only overwhelm an IT staff, but due to its cumbersome and error-prone nature, it is hard to audit and could very well put an organization out of compliance.

COMPLIANCE EQUALS SECURITY: THREE KEY SECURITY CONCEPTS

Confidentiality, integrity and availability - those key security concepts should be the foundation of IT's compliance strategy. If an organization's security solution protects data from unauthorized access (confidentiality), while ensuring that documents are what they say they are (integrity), it can't lose track of the third concept: availability.



If application availability is sacrificed to security, an organization may achieve compliance, but business will suffer because documents and applications will not be readily available to those who need them in a timely manner.

Confidentiality. GLBA directs financial institutions to protect “Personally Identifiable Financial Information” (PIFI). PIFI covers a variety of information types, including information provided to obtain a credit card or loan; information that results from a financial service transaction; or information obtained about consumers in order to provide them with financial products or services. GLBA requires financial organizations to implement a security process that protects PIFI from being accessed by unauthorized people. User name and password protection, which is the method by which much of this information has been protected in the past, is certainly not enough and will likely lead to incidents that threaten to place an organization out of compliance.

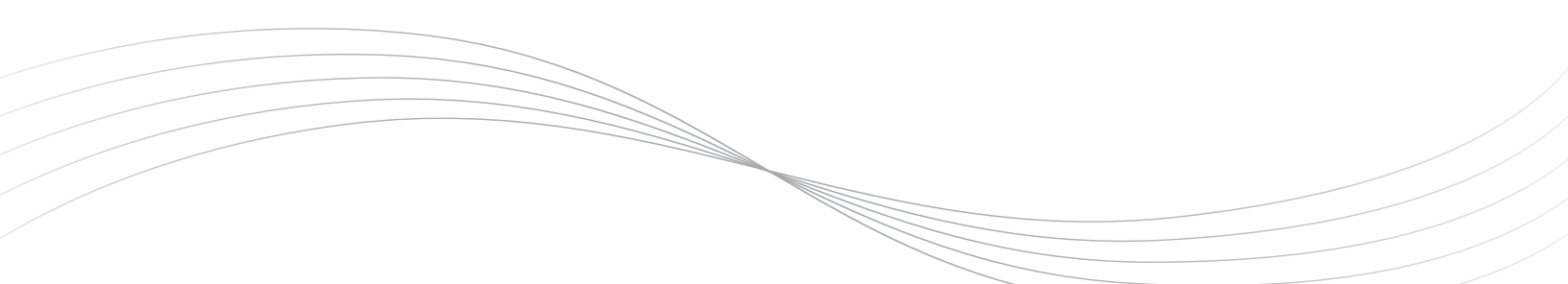
Integrity. A common defense used by executives embroiled in recent corporate scandals is that they did not know what was going on within their own companies. SOX seeks to eliminate this problem by improving the process of corporate disclosure and financial reporting. One key piece of this new accounting process is to ensure document integrity. If a CFO must sign off on a key document, how can anyone prove that he is actually the person who signed that document? Is the signature itself enough? Under SOX, it isn't.

Section 302 of SOX places the following demands on corporate executives: 1) executives must personally review the financial reports they sign, 2) executives who sign documents must, to the best of their knowledge, certify that those documents are accurate and do not contain misleading or false information, 3) executives must ensure the accuracy of their financial statements, and 4) executives are responsible for implementing and maintaining internal controls over financial disclosures and reports.

The problem with these SOX mandates is that of proof, or the audit trail. In the past, being in compliance meant being compliant on the day the auditors showed up. Now, not only must a business show compliance that day, but it must also prove it has been in compliance all along. Without a systematic method for ensuring document integrity, this is a near impossibility.

Availability. Finally, if any measures taken to establish the confidentiality of data and to maintain the integrity of that data undermine application availability, then the price of compliance is a steep one.

What is required is a manageable, cost-effective means for authenticating users and maintaining data integrity. A managed service is one way to relieve the compliance burden, but whether outsourced or addressed in-house, automation is key. Without automation, IT resources are shifted away from business goals to meet regulatory mandates.



ENABLING TRUSTED AND COMPLIANT TRANSACTIONS

In today's connected businesses, it is important to allow someone from outside of the organization to access internal applications. Mobile and remote workers, partners and customers may all need to access various internal applications. In the past, this was accomplished through the use of a browser and user-names and passwords, VPNs or time-synchronized tokens.

There are problems with all of these approaches. User names and passwords are so notoriously weak that they can threaten compliance with many regulations. The effectiveness of VPNs is undermined when logging on requires only a user name and password, as is the case with many VPN solutions. Many organizations have considered distributing time-based tokens that generate a random number the user must supply along with a PIN at login time. But at up to \$55 each, traditional time-synchronous tokens are not cost effective enough to be widely deployed. These are just the sort of security weaknesses that led to regulations like GLBA.

An authentication method that is easy to deploy, affordable, and convenient is the use of digital client certificates. Based on public key infrastructure (PKI) encryption technology, client certificates are an ideal means for achieving authentication and meeting compliance with SOX and GLBA. Where unsophisticated hackers can often guess user names and passwords, even supercomputers can't break PKI. So why isn't everyone using PKI?

PKI is highly complicated, costly, and difficult to manage, especially in a large, distributed enterprise. PKI requires a Registration Authority (RA), Certificate Authority (CA), key management and recovery software, an administrator and a help desk to support end users. An IT staff already burdened by regulations like SOX and GLBA will be hard pressed to take on the task of administering and maintaining something as complex as PKI.

However, by outsourcing client certificates and PKI management to a trusted Certificate Authority, organizations can retain complete control over the entire certificate lifecycle, including enrollment, renewal and revocation. At the same time centralized key generation, private-key backup and distributed key recovery ensure maximum security and protection of private keys.

What is the easiest and most cost effective method for an organization to implement client certificates? A managed PKI certificate service cuts expensive internal PKI costs significantly by softening the burden on internal resources, placing the operational burden on the Certificate Authority, and eliminating technology (such as PKI) obsolescence because the system is built and maintained centrally. And most importantly, browsers and email clients have trusted Certificate Authority root keys embedded in them when they are shipped so that individual (client) certificates signed by one of these CA roots will be automatically accepted with no unfriendly warning dialogs.

Once the user obtains a client certificate from a RA that electronic credential is passed from client to server machine, becoming the user's electronic identity. Digital certificates provide a highly

secure authentication mechanism, and when coupled with user name and password they are an extremely secure multi-factor authentication method. For added portability, most credentials can also be installed on a smart card or USB-based token.

THE PAPERLESS PAPER TRAIL

Equally important as determining that users are who they say they are is proving that documents are what they appear to be. How can it be proven that a specific CFO has indeed signed off on an important financial statement, as SOX requires? If an organization is audited, how can it be shown that customer records have not been tampered with, as GLBA demands?

The key is adding authentication and a standard to ensure documentation integrity. This sounds like yet another cumbersome new security burden, but, fortunately, it is not. Businesses, government agencies, and educational institutions all share information electronically. Key documents are handled online, and this practice has become nearly universal.

However, identity theft, online fraud and hacking all threaten the viability of electronic documentation. Incompatible security technologies and desktops make sharing secure online documents cumbersome and inconsistent. As a result, documents that leave the organization are often unprotected, and recipients are rarely assured of a document's integrity or the author's identity. Until now, this has seemed more of an inconvenience, a cost of doing business, than a real threat to the bottom line. However, if an organization can't verify the integrity of a document, it may very well fail its next compliance audit.

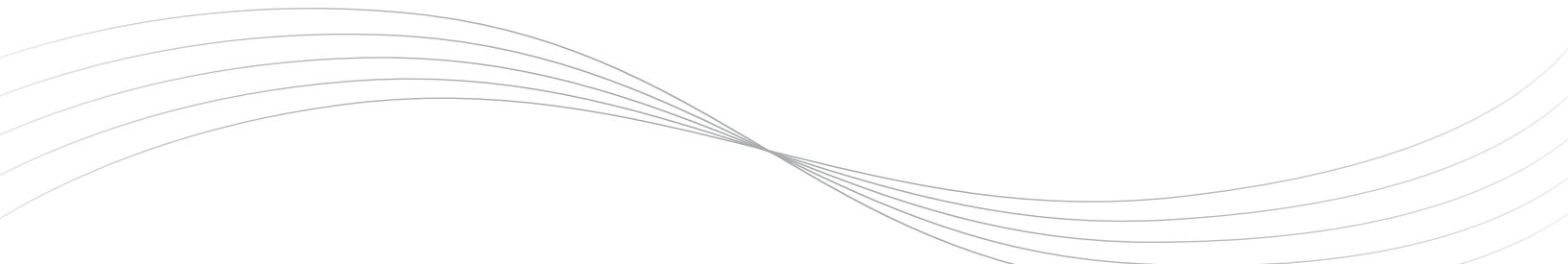
Fortunately, e-documents are slowly being standardized. Adobe® is a nearly ubiquitous source for electronic documentation, and anyone with an Internet connection can download Adobe Reader for free. By adding new security measures to Adobe, the electronic document can be a real cornerstone to compliance efforts, rather than an Achilles' heel.

THE GEOTRUST ADVANTAGE

GeoTrust True Credentials® is the first second-generation managed PKI service - a service that provides the protection of PKI at a fraction of the cost of maintaining PKI in-house. With a very low initial investment, True Credentials allows an organization to outsource the complex task of authenticating a disparate user base, one consisting of centralized employees, mobile employees, customers and partners.

True Credentials® Digital Certificates

True Credentials client certificates provide two-factor authentication and the cryptographic functions necessary to encrypt all online transactions. A fully-managed service, it addresses the inherent security risks typically associated with simple password schemes, without any expensive hardware, infrastructure or set-up costs. With a very low initial investment, True Credentials allows you to outsource the complex task of issuing credentials to a vast user base.



Typical implementations of True Credentials start with GeoTrust cutting a private Intermediate Certificate Authority (ICA) on behalf of the enterprise. This ICA is issued off the GeoTrust Root Certificate Authority providing the enterprise and its end users with the best of both worlds: widespread ubiquity and private branding. And since 99% of all browsers and email clients have the GeoTrust certificate authority root keys embedded in them when they are shipped, individual (client) certificates signed by the GeoTrust CA roots will be automatically accepted with no unfriendly warning dialogs.

The administrator designated by the organization is authenticated and an HTML interface dedicated to the administrator is created. Next, the institutionally-branded user-facing web site for delivery of digital certificates is created; policies and procedures for key recovery (lost user certificate), revocation (people who are no longer customers) and renewal (one-year expiration) are put in place; and then True Credentials is ready to be deployed. True Credentials includes a management interface that provides a secure administrative portal and a clean, simple operational web interface for delivering certificates to users in an automated and "factory-like" operation.

After an individual requiring a digital identity has been authenticated by the organization, the certificate can be delivered. The user receives an email with an HTML link to a page hosted by GeoTrust. This page can be branded with the look-and-feel of the financial institutions pages for consistency. The certificate is then delivered to the user's browser (the browser is the standard way to get a new certificate into the operating system's certificate store).

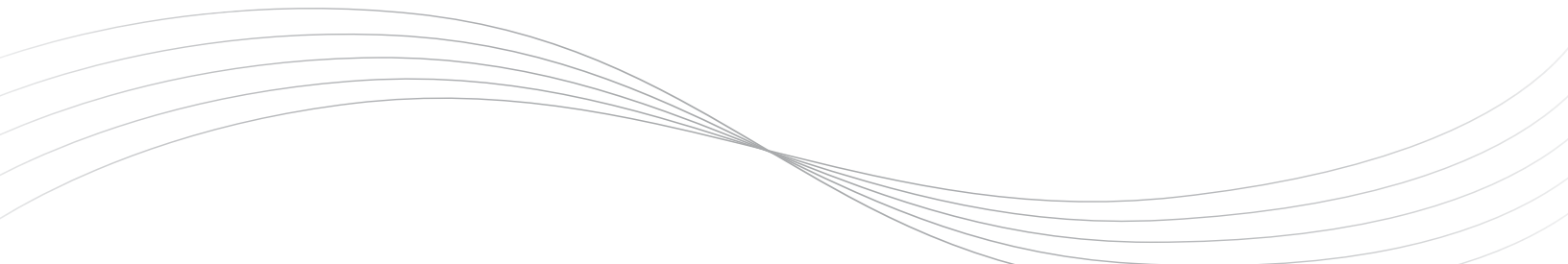
What's equally important when it comes to SOX and GLBA is that managed PKI services establish the necessary controls to prove that critical data is secure, while providing an audit trail to show an organization has been compliant all along.

Flexibility and portability is the key. Users can access this strong form of authentication from anywhere at anytime, so long as they have a browser. Without any special client software or token hardware, the enterprise achieves strong, two-factor authentication that is flexible, portable, cost-effective and easy to use. For organizations that already have smart cards or tokens, there is no need to abandon that investment. True Credentials is compatible with both smart cards and tokens, adding an additional level of security, while providing centralized control and auditing.

Moreover, GeoTrust True Credentials can be used to secure email, instant messaging, e-commerce applications, and more - all without any special hardware or proprietary client software.

Adobe® Certified Document Services

Together with Adobe, GeoTrust has developed Certified Document Services (CDS), a solution that allows authors to create and publish Adobe Portable File (PDF) documents that certify to recipients that the author's identity has been verified by a trusted organization and that the document has not been altered. The solution allows organizations to engage in secure and reliable document exchange, while meeting the strictures of regulations like SOX.



Because this solution was developed in conjunction with Adobe, the CDS certificate is designed to be validated automatically when the file is opened by Adobe Reader or Acrobat. Relying parties don't need to decide for themselves whether the issuing Certificate Authority is trustworthy or not, since Adobe can automatically verify the validity of CDS certificates, displaying a message to the receiving party that the signature and/or contents have been validated. In addition, CDS signing ensures the highest level of document integrity and verification because the user's digital credentials must be stored on a cryptographic hardware device, and they must be issued by a WebTrust certificate authority using strict guidelines.

This server-based solution can handle the high volumes of documents generated by even the largest enterprise, and since it incorporates time-stamping and revocation checking, CDS certification will stand up to even the toughest audits.

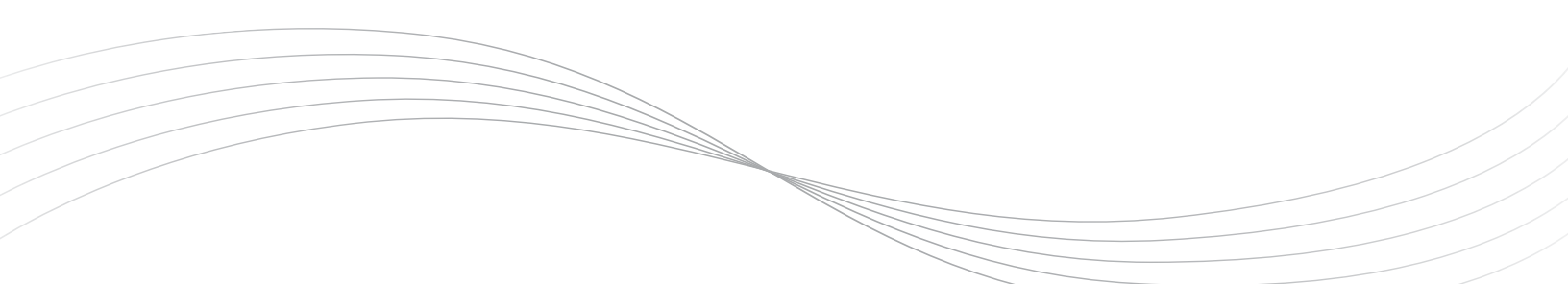
CONCLUSION

In the aftermath of recent corporate scandals, consumers and commercial customers lost trust in the organizations they do business with. Regulations such as SOX and GLBA were enacted to restore trust and to make trust a common business practice.

With these regulations, it's not enough for an organization to be compliant when it is audited. Instead, they must prove that they have been compliant all along, and the only way to do that is to automate key aspects of security, such as user authentication and document integrity.

From Fortune 500 companies to smaller businesses, government agencies and universities, GeoTrust solutions allow secure and quick deployment of globally trusted client certificates and certified documents, while eliminating the burden and expense of maintaining an in-house Certificate Authority. These highly scalable and cost-effective services are ideal for any organization that needs to manage multiple client certificates or create document files that clearly certify to the recipient that their identity has been verified by a trusted organization and that any documents sent have not been altered.

Now, when an auditor asks about the confidentiality of customer information, GeoTrust customers can point out that the data is protected by our strong, two-factor authentication using True Credentials client certificates. And when an auditor asks if a financial statement was signed by the right executive at the right time, our customers can point to the document itself, since the GeoTrust CDS service will keep track of that information for them. And when an auditor asks whether or not customers have a systematic approach to authentication and document security, you can say, "Yes."





117 Kendrick Street, Suite 350
Needham, MA 02494
Phone: (781) 292-4100
Toll Free: (800) 944-0492
Fax: (781) 444-3961
E-mail: info@geotrust.com
www.geotrust.com

WP-SOX-0206 © GeoTrust, Inc. All rights reserved. All specifications subject to change without notice. GeoTrust, the GeoTrust corporate logo, and True Credentials are marks of GeoTrust, Inc. All other trademarks referenced herein are the property of their respective owners.