



White Paper

Electronic Document Security: A Guide to Certified Digital Signatures

Powered by  **GeoTrust**

CONTENTS

Overview3

Trust Issues3

So, How Can You Trust E-Documents?.....4

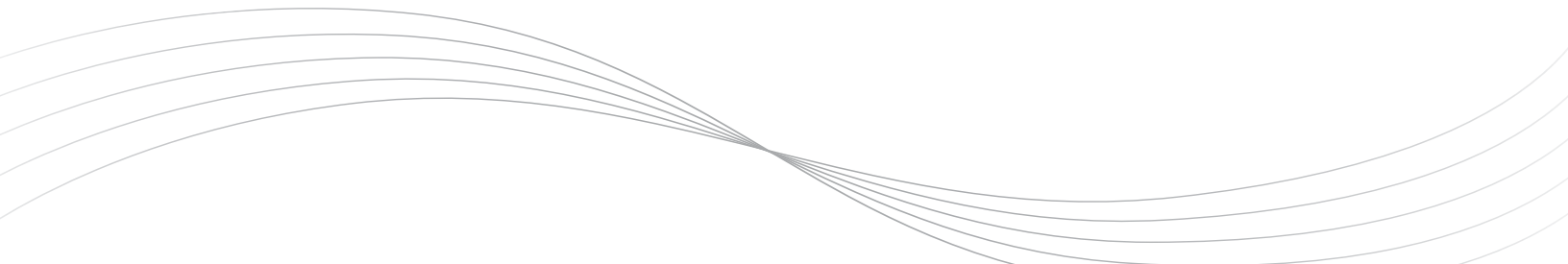
The Good News: PKI for Document Security5

Legality of PKI-based Digital Signatures6

Certified Digital Signatures for Adobe.....7

Case Study: Penn State University.....10

Conclusion.....11



OVERVIEW

Every single day, government organizations, educational institutions and enterprises, both large and small, move their business processes on-line. The benefits of collaborative efficiencies, significant cost reduction opportunities, higher levels of service to customers and compliance with regulatory mandates more than justify any time and effort involved. However, in moving away from the physical world, where paper provided a perception of security, organizations must ensure that the electronic replacement not only retains this critical characteristic in the eyes of their stakeholders, but builds upon it, to create an even stronger reliance on electronic documents in the future.

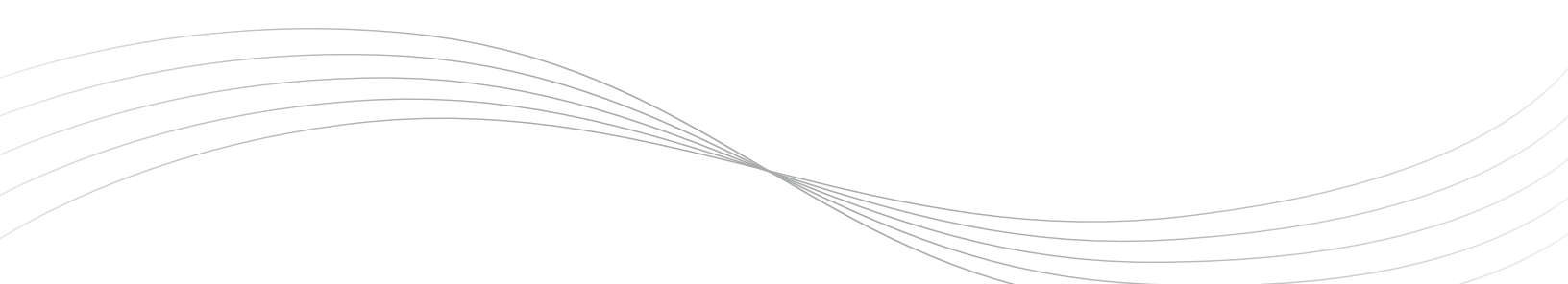
So how can enterprises ensure that trust and security are woven into the very fabric of their electronic documentation? How for instance does a consumer verify that a product recall notice was indeed issued by the manufacturer or distributor responsible for the recall? How does an employer verify an applicant's electronic transcript? How do they verify that the information contained within the transcript has not been tampered with or more crucially that the person actually attended the school in the first place?

Many organizations find themselves at the base of a learning curve, incorrectly viewing the need to secure electronic documents as a major barrier to adoption rather than as a business opportunity. Providing a simple and effective method of document integrity checking together with an intuitive indication of the author and organization behind the document offers a clear opportunity to strengthen brand awareness and increase brand loyalty.

TRUST ISSUES

But just having a way to build trust into documents is not sufficient by itself. The method must also be one that organizations and users will accept. For users, it must be effortless and intuitively simple. For organizations, it must be inexpensive, scalable, and easy to integrate within the existing infrastructure. And, in fact, these attributes are the model for the Certified Document Service (CDS) now available from GeoTrust (a VeriSign company) and Adobe. Here is a look at the trust issues this service addresses, and how it does so.

Any solution for making e-documents more trusted must overcome two key obstacles. The first is that the Internet is a virtual medium, so it lacks the customary physical safeguards people rely on every day to establish trust. The second is that the damage from cyber deception is real, widespread, widely publicized, and expensive. People have good reason to be suspicious of online documents, especially since most of the familiar ways people check authenticity cannot be replicated in the virtual world.



Communicating critical information to a broad audience presents real problems with real consequences. Phishing, identity theft and document forgeries have eroded customer trust in electronic communications. A fraudulent press release, for example, can cause a company's securities to rise or fall dramatically in price - allowing a buyer or short seller to receive a fast windfall. PairGain, Emulex, and Bank of America are all companies that have been publicly identified as victims of "press release fraud." Most cyber crime victims, of course - whether individuals or organizations - do not wish to advertise so publicly, as to do so would be brand suicide. This means that the actual number of attacks is probably much greater than just online forms at bank or merchant web sites.

Notice that the same qualities that make e-documents less desirable from a trust standpoint - such as the ease of doing business anonymously - are often the same qualities that spur organizations to use e-documents in the first place. It's almost as if the more efficiencies organizations derive from using e-documents, the greater the resistance they encounter against using them.

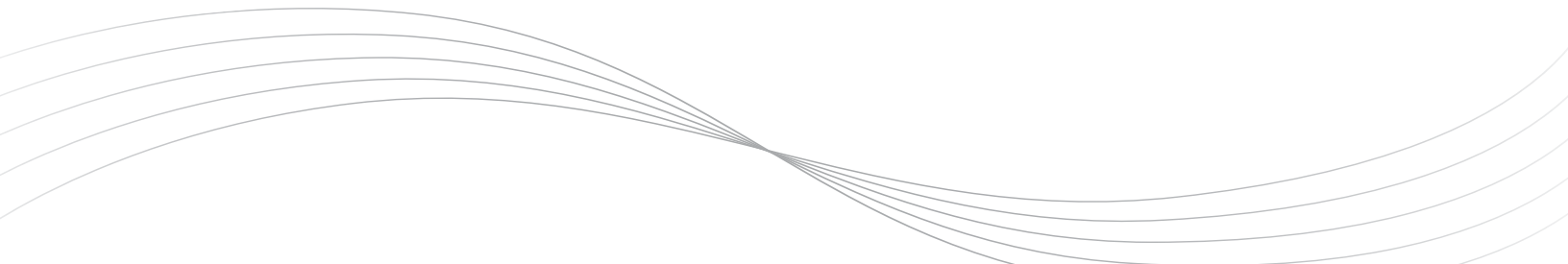
SO, HOW CAN YOU TRUST E-DOCUMENTS?

Even this brief sample of security issues shows why many people and organizations have trouble trusting documents they download, view, and store in their computers.

What these issues also demonstrate is that making the Internet secure is a huge task - one that is not likely to be accomplished soon. That means that any solution for making electronic documents trustworthy, must work in an environment you can't trust. Trust must be so much a part of the document that if that trust is somehow breached, the document becomes tamper evident. The irony is that a paper document may still be trusted, even if fakery is technically possible. In the virtual world - as long as fakery is technically possible - electronic documents won't be trusted.

New processes customized for electronic information and workflow, are needed to ensure critical document authenticity and integrity. Critical among these is a simple, effective and legally-binding means for digitally signing documents. If organizations are to increase the use of electronic documents and digital signatures, as well as meet the privacy requirements as set out by law, they must be able to establish and maintain document security as follows:

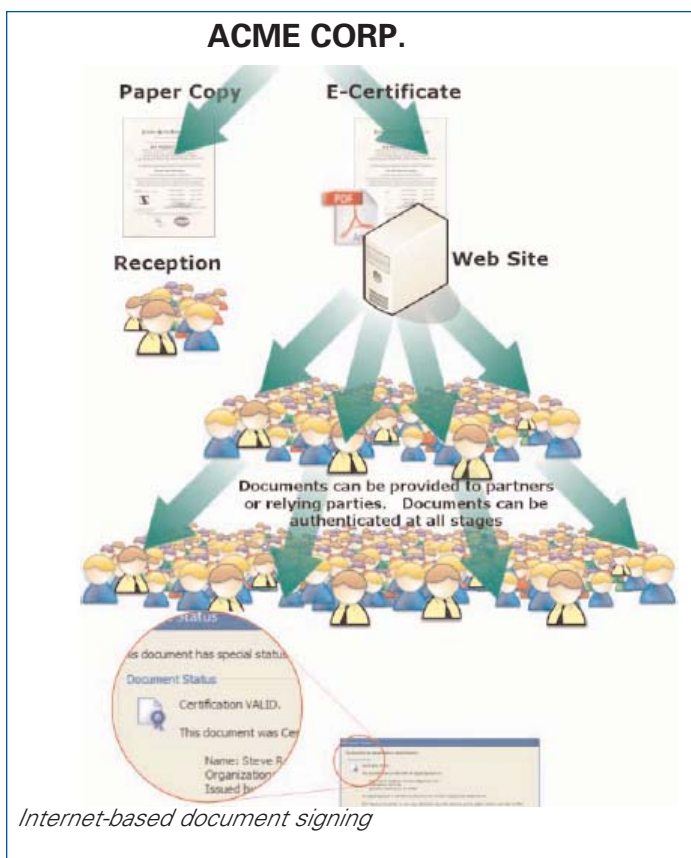
- Authenticity - Provide assurances that the document truly comes from the stated author.
- Integrity - Detect unintentional or malicious document alteration. (Many signature disputes arise over the principle of integrity. Signers don't disclaim their signature, rather they maintain the document is different from that at the time they signed it.)
- Non-repudiation - prevent authors or senders from refuting a document they have signed. (Especially important in the case of time-sensitive documents like Stock Analyst reports where the author's claims were made during a specific time and date.)



- Security persistence - Maintain document security throughout a business process. (This property allows signatures to be retrieved and verified at any time in the future.)
- Ease of use - Make it easy to receive secure documents across all platforms. (This means that the signature can be verified by the recipient without reference to an application maintained by another party.)
- Confidentiality - Optionally, protect content from unauthorized access so that only the intended audience can view it.

THE GOOD NEWS: PKI FOR DOCUMENT SECURITY

The good news is that security experts have known for years how to make electronic documents more trustworthy. It is the same technology used by financial institutions and intelligence agencies to transmit sensitive information - whether in closed, highly secure networks or out in the "open" over wireless links. That technology is called PKI, or public key infrastructure. Basically, the way PKI works is by using keys, or digital codes, to sign and encrypt documents.



"Signing" a document before it goes out over the network scrambles the document so that you need a matching key to unscramble the document and open it. Signing the document also adds a certificate that shows both the signer's identity and the identity of a trusted third party - a certificate authority (CA) - that can vouch for the identity of the key holder. The mere act of opening the document proves three things:

1. The person or organization whose identity appears in the certificate is the one whose key signed the document
2. That identity corresponds to the name of a trusted key holder on a list at the certificate authority
3. The document has not been altered (otherwise key and content would not match)

The reason PKI is "public" is that the key used to decrypt the document is publicly available, while the key used to sign (and encrypt) the document is private - known only to the signer. Anyone with the public key can open the document, thus proving the signer used a corresponding private key and that the document had not been altered after it was signed. If both keys were private it would not be possible to distribute documents widely, because not everyone would have the private key. In Internet applications you want to be able to distribute documents anonymously, yet maintain trust - a requirement satisfied by PKI's digital signature.

LEGALITY OF PKI-BASED DIGITAL SIGNATURES

PKI is now widely proven and digital signatures have become legal in most parts of the world during the past couple of years.

Section 101(a) of the ESIGN act (October 1, 2000), provides that "notwithstanding any statute, regulation, or other rule of law with respect to any transaction in or affecting interstate or foreign commerce,

1. A signature, contract, or other record relating to such transactions may not be denied legal effect validity, or enforceability solely because it is in electronic form, and
2. A contract relating to such transaction may not be denied legal effect validity, or enforceability solely because an electronic signature or electronic record was used in its formation."

ESIGN does not define the details of how e-signatures will be implemented or regulated. States and Federal agencies do that. Shortly after ESIGN, the U.S. Department of Justice (DOJ) published a document entitled "Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies," (November, 2000). Essentially, what the DOJ says is that you can use an e-signature to establish trust if it meets certain technical standards:

A well-designed electronic process should ordinarily be able to provide the same information as the paper system; who submitted the information; what information was submitted; when the information was submitted; and whether all the relevant information was retrieved. (p. 6)

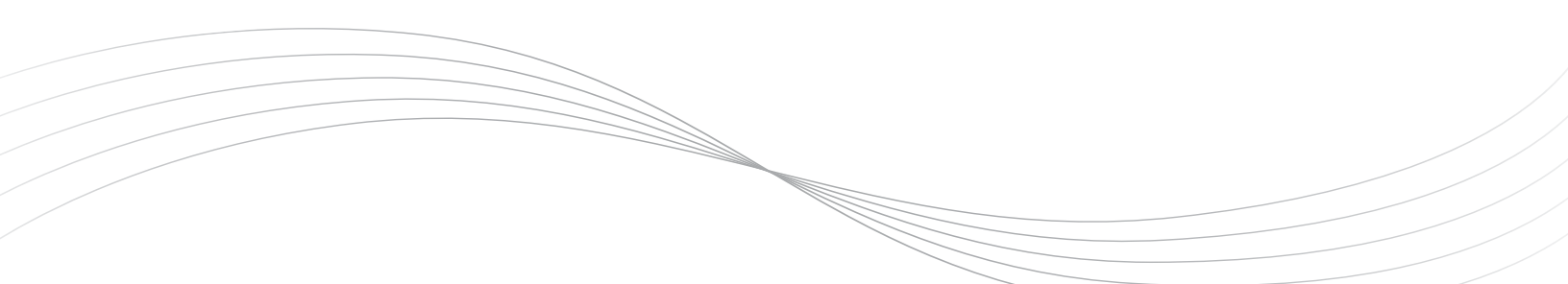
DOJ also notes that:

Agencies should ensure that their electronic processing captures all relevant information, such as ... whether the document was subsequently amended, and, if so, the source, date, and content of the alteration. (p. 10)

The DOJ acknowledges a key point about e-signatures - they are not only equivalent to paper signatures, they hold an important advantage over paper signatures when it comes to trust: ...a digital signature on a document can cryptographically bind the signature to the entire document, whereas a written signature on the last page of such a document may leave questions as to which of the preceding pages are part of the signed document. (p. 4).

Globally, the EU Directive 1999/93/EC for Digital Signatures allow for a basic digital signature: any form of digital data that is attached to the original electronic information. Under such a definition, for example, a picture of the signer pasted into a Word document is sufficient. This is the equivalent, in paper documents, to placing an "X" or stamp in the signature area. Obviously, the biggest weakness with an "X", typed name, picture or similar such methods is in that there is no way of preventing others from using the same method to forge documents.

The EU Directive recognized this vulnerability and defined in the Directive a stronger type of electronic signature, the Advanced electronic signature. Although the Directive had done its best to remain technology-neutral, only PKI Based Digital Signatures meet the requirements for such



signatures. Advanced electronic signatures provide not only stronger user authentication, but also protect the integrity of the data signed, thus ensuring non-repudiation of the transaction by the signer. This goes along way towards creating both a legally binding and legally admissible signature.

But if a PKI can cryptographically bind documents to digital signatures (and thereby establish trust), why hasn't PKI been implemented more widely? Why don't all companies and individuals use PKIs to prove the documents they send are authentic? Decades after PKI was invented, and years after ESIGN became law, most digital documents are still unsigned. Why is that?

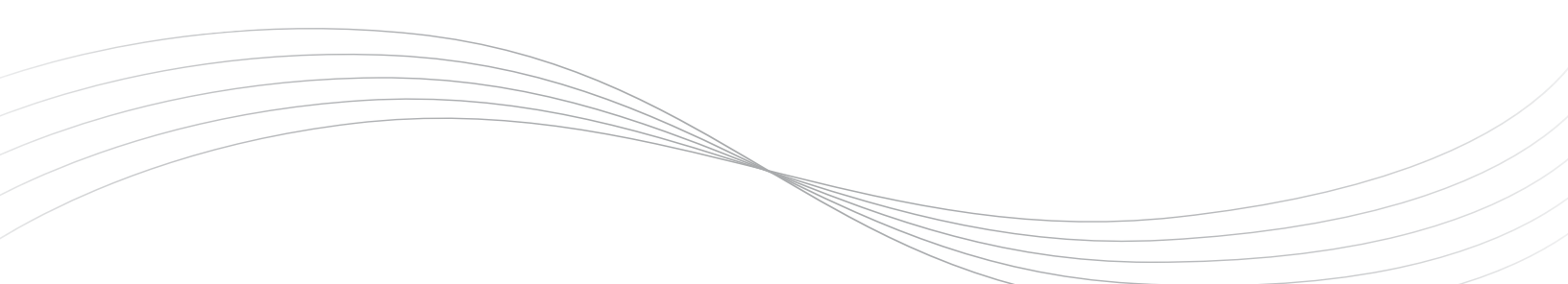
The bad news about PKI is that it is an infrastructure - and as such is expensive and hard to implement. Although financial networks and intelligence agencies can afford them, most other organizations can't. And even if a company did set up its own PKI, that would still leave open the question of how to exchange documents "outside" the infrastructure. If I have the software to create, sign, and authenticate documents using one organization's PKI, will that same software work for another organization's PKI? Will the keys for each PKI be compatible? Every PKI has a Certificate Authority (CA) that registers and validates the signers of documents whose signatures incorporate its particular certificate. Would one CA's certificate be trusted by another CA? What about the software for signing and authenticating? Internet users need solutions that are as universal as the Internet itself. How do you make something like trust, which requires a quality of privacy, universal?

CERTIFIED DIGITAL SIGNATURES FOR ADOBE

GeoTrust and Adobe have helped to solve this problem by making the same PKI available to all users of Adobe Acrobat (Version 7.0 and above) and Adobe Acrobat Reader (Version 6.0 and above). GeoTrust is a Certificate Authority - so PDFs signed by GeoTrust certificate holders (using off-the-shelf Adobe Acrobat or Adobe Document Security Server) can be authenticated by any user of Adobe Reader. Since Adobe Reader is free and ubiquitous, virtually any user on any computer can authenticate documents signed with GeoTrust keys.

To get a GeoTrust Certified Document Service (CDS) certificate, the user either registers online directly from GeoTrust or, alternatively, with an organization who has purchased an Enterprise Managed PKI Service from GeoTrust. The reason an organization might want to purchase this Service is so that it can both quickly certify multiple user certificates and / or large numbers of PDFs, such as bank statements or financial reports while acting as Registration Authorities for their GeoTrust vetted organization. The Enterprise Service is equipped to handle both desk-top signing using Acrobat and Server-based signing using Adobe Document Security Server.

Through a simple web-based portal, Registration Authorities allow GeoTrust (acting as the Certificate Authority) to bind the user's identity via a digital certificate (and the CA) to your private key. Once you sign a document (by clicking "sign" in Acrobat), a relying party can automatically validate who you are and that your private key signed the document.



MEETING DIVERSE INDUSTRY NEEDS

Certification Bodies

- The ANSI-ASQ National Accreditation Board (ANAB)**, the organization responsible for accrediting certification bodies for quality management and environmental management systems in the U.S., turned to GeoTrust to prevent certification bodies from fraudulently claiming to be accredited by displaying a modified accreditation document. "Our number one priority is to ensure a high level of protection for the accreditation certificates that we send out to U.S. certification bodies," said Bob King, president of ANAB. "We chose the GeoTrust/Adobe-based signature verification because it allows us to raise the level of security and reduce risk for customers engaging in trade worldwide, while at the same time eliminating the inefficient process of issuing accredited paper certificates."
- ISACert**, a global certification body serving the entire food industry, with clients including 7,000 farmers, food processing companies and restaurants recently adopted CDS. The agency produces over 10,000 high-value or confidential documents per year that include contracts, revenue reports and letters, as well as certificates to prove compliance with hygiene codes, environmental standards and quality systems.

Pharmaceutical Companies

- Orexigen Therapeutics, Inc.**, a privately held, clinical-stage pharmaceutical company focusing on obesity, adopted CDS to sign clinical, regulatory and legal documents. "We have a dispersed executive team communicating sensitive clinical and legal information with contractors around the country, so changing our manual, paper intensive process of certifying documents to a virtual process has significantly increased efficiency," said Anthony McKinney, chief operating officer at Orexigen Therapeutics. "A key to our success has been the ease and convenience with which document recipients can authenticate documents signed with GeoTrust's certified signing services."

The relying party simply opens the PDF and instantly receives a validation message regarding the trustworthiness of the signature. Additionally, the relying party can click on the signature box within your document and retrieve the certification status (i.e., a time-stamp of authorship, revocation check of the author's certificate). The relying party can also view signature properties, such as certificate details, your contact information, and the validation method. If the document has been altered after it was signed, a big red "X" appears across its pages. Valid documents are easily identified with a large Blue Ribbon indicating trust.



Document is Valid



Validity Unknown



Document is Invalid

The digital certificate and key itself are software, and in the case of desk-top signing that utilize Acrobat Standard or Professional are securely stored on a FIPS 140-1 level II USB token device. The user can plug the USB token into any computer with a USB port and sign documents if Adobe Acrobat and associated drivers are installed. Server-based signing used in conjunction with Adobe Document Security Server securely store private keys in a FIPS 140-1 level III hardware security module. If the key is lost or stolen, the user simply contacts GeoTrust and the certificate is revoked, so that the Adobe Reader and Acrobat no longer validates further signing with this certificate.

Because of the partnership between GeoTrust and Adobe, users of Adobe Acrobat can sign digital documents with the same ease-of-use and confidence they would have if signing paper documents. Those documents could be:

- Financial and banking documents** such as mortgage applications, brokerage transactions, promissory notes, loan applications and any other documents driven by high-value transactions
- Legal documents** such as power of attorney, wills, trusts, and settlement and arbitration agreements
- Real estate documents** such as deeds, purchase and sales agreements, rental applications, and leases

MEETING DIVERSE INDUSTRY NEEDS cont.

Engineering and Architecture Firms

- **SiteSafe**, an engineering company providing radio frequency health and safety solutions assist to organizations that are required to comply with Federal Communications Commission (FCC) and the Occupational Safety & Health Administration (OSHA), uses CDS to sign engineering documents for electronic storage and transfer. "When evaluating products, we found that the need to provide a separate public 'key' for each document was cumbersome and did not meet our business model, since some documents would be passed to other interested parties. CDS provides the security and convenience we needed," said Klaus Bender, vice president of RF Engineering, SiteSafe.
- **Alpine Engineered Products**, a leading worldwide supplier of technology-driven products and services for the building component industry, adopted the GeoTrust CDS product to digitally sign engineering drawings to provide building departments, partners and clients with the high assurance that is required in content-sensitive drawings.

- **Healthcare documents** that contain highly sensitive information such as medical records and health care proxies
- **Government documents** such as patent and trademark applications, copyright forms, grant proposals, tax returns and IRS forms
- **Engineering and architectural documents** such as blueprints and specifications that need to be certified
- **Certificates of compliance and accreditation** that are published over the Internet
- **And other general business or personal communications** that are delivered electronically and need to be verified as legitimate

Best of all, organizations can now leverage their valuable technology assets much more fully and productively. Increasingly, they will have the opportunity to maintain entirely digital workflows - without the "drag" of paper. That reduces the cost of handling documents, increases workflow velocity, reduces error rate, and allows for deployment of information that is far more tailored to meet specific opportunities and needs. Perhaps, most importantly, trusted documents send a powerful message about the type of organizations behind them: that these organizations are up to date and that they can be trusted.

Certified documents expand the value of digital signatures and differ significantly from standard digitally signed ones. For example, although Adobe® Acrobat® allows authors to sign PDFs with any x.509 v3 digital certificate, this isn't the same as signing a PDF document with a digital certificate issued from GeoTrust. A True Credentials for Adobe Acrobat certificate is signed by the GeoTrust for Adobe Certificate Authority (CA) that has been issued by the Adobe trusted root and embedded in Adobe Reader and Acrobat, versions 6.0 and higher. Only certificates issued from this hierarchy will receive the certified signature validation mark automatically when opened with Adobe Reader or Acrobat.

With non-CDS signatures, a user must explicitly "trust" the author of a document. With CDS signatures, trust is built-in to the Adobe Reader and no additional software download or configuration is required by the recipient of a certified document to validate its authenticity. Because CDS takes advantage of the worldwide acceptance of Adobe Reader authorized users on any platform can always access protected files without the cost of installing desktop software.



INDUSTRY: Education

CHALLENGES:

- Ensure validity of student transcripts
- Provide open, standards-based service for delivering electronic transcripts
- Track delivery and receipt of transcripts

SOLUTION: Penn State is providing an online certified transcript service to alumni worldwide via:

- Digital Signature Technology
- Document Generation
- Process Management

RESULTS:

- Accelerated production and delivery of transcripts by more than 99%
- Reallocated administrative time to other student services
- Improved integrity and reliability of transcripts
- Anticipated full ROI within one year of deployment

CASE STUDY: PENN STATE

One of the best examples of how e-documents can cut costs and remove bottlenecks is in recruiting - whether for business or graduate school. Decisions can be made faster if decision makers do not have to wait for paper transcripts to arrive in the mail (after being printed and stuffed into envelopes). Transcripts often require official seals be imprinted on them, an additional step that adds further costs and delays. Yet despite this precaution, these paper documents can still be easily forged (and often are). That's why many employers perform background checks to verify a potential employee's documentation - another step which, again, increases costs and further delays decision-making.

On the other hand, if transcripts are sent electronically, they become available almost immediately. And, with proper digital authentication, they could be accepted with a higher level of trust than paper transcripts.

An example of an institution that has switched to electronic transcripts is Pennsylvania State University. According to J. James Wager, assistant vice president for undergraduate education and university registrar, Penn State is inundated with transcript requests.

"Each year, Penn State receives about 120,000 requests from students and alumni who need copies of their transcripts," he says. "Employers, graduate schools, and professional certifying agencies require a high level of certainty that the academic credential was issued by Penn State, not a 'diploma mill,' and that the document has not been altered."

Penn State addressed both problems with a single solution: the academic version of CDS, GeoTrust's Certified Transcript Service. CTS allows college registrars, admissions offices and departments to create certified Adobe PDF transcripts. When a recipient opens a transcript with the free Adobe Acrobat Reader, the Reader displays a visible verification sign. That means the academic institution's identity was verified by a trusted organization and that the transcript has not been altered unscrupulously.

If, however, the verification sign is missing, then the recipient knows the transcript is suspect. Likewise, if someone not associated with the Penn State registrar's office tries to fake the document the recipient is also alerted. (A large red "X" appears across the face of the document.) The same thing would also occur if an unauthorized employee attempted to transmit the transcript.

CONCLUSION

Because worldwide organizations rely on rapid, easy information sharing, they are bringing document based business processes online to improve the quality, efficiency and cost-effectiveness of their operations. But the use of electronic documents must not compromise the integrity, authenticity or privacy of information. Organizations must protect documents at all times - and provide assurances of document confidentiality, authorization, accountability, authenticity, integrity, and non repudiation.

Digital signature capabilities enable important documents and information to be published inside and outside an organization with added assurances that the information arrives exactly as it was intended. Only PKI based electronic signatures, such as Certified Document Services from GeoTrust, offer stronger technology to protect against forgery by providing data integrity, author authenticity and non-repudiation.

