

## Why Use Electronic Transactions Instead of Paper?

### *Electronic Signatures, Identity Credentialing, Digital Timestamps and Content Authentication*

#### Introduction

By allowing the exchange of information more quickly, easily, and dependably than ever before, the Internet has forever changed the way we do business.

That revolution is now making a handwritten signature on a paper document part of the past. Why spend time or money printing, faxing, physically delivering and storing paper documents, when you can accomplish better results in just a few minutes with a web based solution? In fact, today's electronic alternatives are not just analogous to, but clearly *superior* to, their paper equivalents. Indeed, the options offered by new technologies not only provide greater security than traditional forms, but facilitate authenticated transactions in better ways than paper permits. These new technologies make critical transactions faster and more convenient, but they also substantially improve control, security, and verifiability beyond anything previously possible.

Just as email revolutionized the business world a few years ago, secure electronic document management solutions are now changing the way the world conducts business transactions. More companies and government entities, regardless of size, are adopting these solutions proving that it is simple to make a business case for electronic signature with identity credentialing, document authentication, secure document exchange and electronic storage.

#### Why should we move away from paper documents?

- **Security:** Handwritten signatures and signed paper documents can be easily forged with existing technology. It is easy to create a document that looks as good as the original.
- **Efficiency and productivity:** Business cycles can be substantially streamlined and reduced - templates and forms can be easily shared and integrated together with an electronic signature solution.
- **Flexibility:** Physical distance becomes meaningless.
- **Cost reduction:** No printing, faxing, delivering, or physical storage of documents reducing overhead costs.

In fact, moving towards an electronic transaction opens the door to a much more efficient way to ensure secure document transactions. Not only does the act of signing the document become more secure and efficient, but the entire process of managing the document, from its generation to the final storage of the document improves tenfold, addressing these common paper management pitfalls:

- **Increasing costs of managing paper documents:** When you add the cumulative costs of mailing, the retention of signed documents, and print equipment, the costs of managing paperwork is staggering. As a token, the New England Journal of Medicine determined in a 2004 article that 31% of all health care costs are related to paperwork; which amounted to \$500Billion in 2004 alone.

- **Complex storage and retrieval management systems:** as the amount of paper grows, the complexity to manage the documents grows exponentially. According to the Delphi Group, knowledge workers use up to 25% of their work time searching for information. In addition, if several people need to have access to the stored documents, then one single physical repository might be neither effective, nor practical.
- **Cost of lost efficiency:** The time you spend printing, signing, sending and filing paper documents can be used in a more efficient way, actually adding value to the business, instead of spending the time in administrative activities.
- **The impact on the environment:** Every paper process has a environmental effects, from cutting down forests to manufacture paper, to the pollution generated by the paper manufacturer, through the carbon costs of transporting and storing paper; going paperless helps us all reduce our carbon footprint which helps the global environment.

An electronic transaction is designed to create a provable connection between a document and the people who have signed it. That means that not only the signature is authenticated, but the document content as well. This process requires that the document itself is analyzed to make sure that it has not been modified from the moment it was sent out to start a signature workflow, to any point of time after the document was signed. This unique characteristic allows for a more secure document management solution than is available with paper transactions, ie. **Electronic Content Authentication**

Electronic authentication is also superior to paper-based authentication in several key ways:

- Electronic authentication guarantees the integrity of the original document content as well as the signatures it bears.
- It guarantees the integrity of the content at any point during a document's lifespan, not just at completion. For example, an academic, inventor or scientist can sign and authenticate every step of creating a research paper, from first draft to publication, thus proactively establishing ownership of the original intellectual property or work effort.
- It establishes a chain of custody of a critical document by recording the identity of everyone who views or changes it. This is a necessary step to proving compliance with financial or health care regulatory requirements, as well as a useful tool to protect the confidentiality of proprietary business information.
- It certifies the time at which events occurred exactly like content authentication is required to secure the electronic signature process, a time stamp is utilized to seal the document. This time stamp can be used to determine the time when a document was signed by each one of the recipients, or it can be used to determine at what time the content of a document was certified and sealed.
- Finally, it is faster and more cost-effective than paper equivalents. Electronic transactions, electronic content authentication, sealing and time stamping do not require multiple copies, overnight deliveries or messenger services that add costs for each set of copies, or an appointment with use of a notary public to witness each signature. It allows signers to be anywhere there is Internet service, instead of having to meet to conclude the transaction.

All these tools that should be part of a world class electronic transaction service can be used together to securely sign a document or they can be used independently to electronically seal and time stamp a document as a prior step before being stored. In that case, an audit trail is kept in a secure e-vault so that any viewing event can be registered and any attempt to tamper with the document will invalidate it.

## **What to consider when evaluating an electronic signature solution:**

There is a clear business case for electronic transactions. However, there are several questions an enterprise or a government entity should carefully consider when analyzing an electronic transaction and content authentication solution.

### **The service characteristics:**

1. **Trust factor:** Are the transactions secure? Tamper-proof? Authenticated? Timestamped by a trusted authority? Verifiable and irrefutable? For especially-sensitive and critical communications such as contracts, content rights management, and other legal notifications, making the transition from traditionally paper-based formats to digital ones also means educating end-users that they have control of the document's integrity at every point in the document workflow.
2. **Identity verification:** In addition to assuring that the document is sealed and signed in a secure environment, many regulations require verification that the person who signs the document is the intended signer – through identity verification or identity credentialing. Most of the solutions in the market overlook this important part of the process, relying only on the email address of the person they are trying to reach. But email access is not tamper-proof, so identity verification by a reliable third party provides additional legal credibility that the signer is authentic.
3. **System flexibility:** Familiarity with paper documents paired with the resistance to change of human nature makes adoption of fully electronic transactions a slow process within some corporations. To address this adoption, the electronic solution must offer a secure fax signature alternative. That provides the option to fax the document to the recipient, who manually signs it, and then faxes back to the secure server. The secure server automatically transforms it to an e-document simultaneously time stamping, sealing and securely storing for reference.
4. **Legal and regulatory concerns:** The solution has to deliver unique identity credentials that are legally enforceable and regulatory compliant. The records must be authenticated, the signer's intention has to be evident, their identity must be undisputable and last but not least, there has to be irrefutable proof that the content of the document has not changed in any step of the signature process, or at any point of time after the signature event.

## The internal entity requirements:

5. **System requirements.** Would you rather use a web based solution? In that case, there is no additional hardware or software requirement, and the implementation is usually very fast. Or you prefer to download a solution to your computer?
6. **Business needs:** Do you need a simple one time signature event per document, or you have documents that go through more complex signature flows? Where would you rather store the documents? With a third party secure e-vaulting, or internally?
7. **Internal education:** Even though electronic transactions are demonstrably more efficient and productive, people are usually reluctant to change, in part due to the simple comfort of familiarity. Adoption can be enhanced and accelerated through internal publicity and training, showing senior level management's buy-in to the selected product as-well-as emphasis of the benefits to the company and the individual employees.

## Is it legal?

Over the last decade, most countries around the world have passed regulations stating that electronic signatures and electronic transactions are permissible and legally binding. In the U.S., these regulations and guidelines include the 2000 Electronic Signature in Global and National Commerce Act (ESIGN) the 1998 Government Paperwork Elimination Act (GPEA), the 1999 Uniform Electronic Transaction Act (UETA) and the US FDA 21 CFR Part 11.

The ESIGN Act defines electronic signatures and describes their use and legality in interstate and foreign commerce. It also clarifies that electronic signatures are considered the equivalent of an ink signature, depending on the situation.

In addition, many local and regional governments, as well as transnational entities like the United Nations and the European Union, have also approved the use of electronic signatures on documents ranging from tax returns to college applications.

Although regulations about allowable forms and formats vary from state to state and country to country, an electronic signature is generally defined as one that uniquely identifies the signer, is created by the signer, and cannot be used by anyone else. Many definitions also require the signature to be linked to the relevant data in a way that reveals whether the data has been altered and therefore whether the signature is still valid.

Several cases involving e-signature have already been upheld in a Court of Law, among them:

In the *Vinhnee vs. American Express*, CC-04-1284-KMoP (“American Express”) the court stated that authenticating electronic records, in principle, poses the same issues as for paper records with the only difference being the format in which the record is maintained. *Id.* The proponent of the record must demonstrate that the record retrieved from the file (whether paper or electronic) is the same record that was originally placed in the file. *Id.* (citing FRE 901(a)).

On October 16, 2006 the Southern District of New York upheld an arbitration clause in an electronic contract. In *Bar-Ayal v. Time Warner Cable Inc.*, 03 CV 9905 (KMW) (S.D.N.Y. Oct. 16, 2006), the Court ruled that Click” Deemed Legally Binding Assent to Lengthy Contract.

## **Authentidate’s approach to content integrity verification and electronic signatures**

Authentidate’s AuthentiProof service ensures the provision of a world class secure electronic document transaction service. Authentidate’s solution ensures that sensitive and critical documents are audited, signed and stored according to the legal requirements of United States legal statutes and laws.

Authentidate’s electronic transactions, electronic signature service and transaction management tools can be described answering the following questions:

### **Who, What, When, Where, How**

#### **Who: Identity Credentialing**

User authentication is the process guaranteeing that the people who sign a document are who they say they are and confirming that they alone are authorized to view, change, and approve the document. It requires the verification of the person’s unique credentials, which in a very basic way can be done verifying username and password.

In order to provide an irrefutable proof of identity, Authentidate includes two additional layers of verification, utilizing related information from a trusted credentialing entity, such as Experian, and the option to define a secret access code that is conveyed to the recipient separately.

#### **What: Document Authentication**

Data authentication is the process of verifying that the information contained in a signed document has not changed since it was signed, linking the signatures to the document in a way that reveals any attempts to alter or tamper with it.



To provide irrefutable evidence of electronic content integrity and tamper-evidence, Authentidate’s compliant solutions utilize the AuthentiProof™ seal. We incorporate the AuthentiProof seal into all of our solutions to secure as well as to verify content integrity at each step of an electronic signature or electronic transaction. This unique security ensures that no attempt to change a document will go undetected. Even a small change will invalidate the signed document that has been tampered. The AuthentiProof record is stored for seven years in the Authentidate data repository and can be used to verify that the content of the original file, form or document has not been altered.

Authentidate ensures the highest level of trust, not only through the signature process, but in the subsequent document management and storage process. In fact, AuthentiProof complies with the UETA statute as well as the ESign Law.

## **When: Time Stamping and Audit Trail**

A key differentiating factor in Authentidate's solutions is a two-tiered audit trail capability for all actions. The first tier provides for a log of each event performed by a user and the order in which each event was performed.

The second tier incorporates an additional logging of activities as part of the AuthentiProof authentication audit trail that allows for verification of authenticity and for non-repudiation. This tier utilizes the time and date stamping servers that are compliant with IETF RFC 3161 Internet X.509 Public Key Infrastructure Time Stamp Protocol. The time and date stamping service also takes into consideration the UPU (Universal Postal Union) standards on Interface Specification (S43-3).

The content authentication and time stamping can be used separately from the electronic signature option, allowing sealing and certifying for a secure document management solution. Copyrighted content, legal documents or any content that requires tamper protection can be sealed and certified with the AuthentiProof seal. An Audit trail of the content will then become available.

## **Where: Document Flow**

The sender of the document might need a simple document transaction sequence, where he needs to send it to all the recipients at the same time; or the business transaction might require a more complex document transaction sequence, where one recipient needs to sign before the next signature is requested.

The AuthentiProof solution allows the sender of the document to define the appropriate transaction sequence to fit its particular needs, for each transaction event.

## **How: Intention to Sign**

The signature process must show without any doubt that the person intended to sign the document. Since a signature is the declaration of a person's intention to sign, the signature process must clearly be able to demonstrate that fact. With Authentidate's solutions, the recipient of the document has to go through several clicks to clearly accept, first the delivery of the document, and then each one of the requested signatures. The sender of the document receives notification on each of these events.

In addition, to make the transition from traditionally paper-based formats to digital ones is seamless, Authentidate's service allows for easy selection of either e-sign or fax sign.

## Customer support

With over 20 years of experience in the secure document management area in highly regulated markets, Authentidate is in unique position to provide you with the tools and support to make any paperless initiative a success. Our customer support team and product support is highly rated by our clients.

Our solutions team will help you develop the business case to ensure internal support, identify the challenges you face and work with your team to determine the way to solve those challenges.

Authentidate's web based solutions permit easy and fast deployment, without any additional investment in hardware or software, allowing a quick and hassle-free implementation of an electronic transaction, e-signature and/or content authentication solution.

## Which industries and market segments stand to benefit most from electronic transactions?

Current technology not only enables secure and trusted electronic authentication, it makes it possible to store, search, retrieve, and verify authenticated documents quickly and easily. This is especially valuable for certain markets:

- Heavily regulated industries like **pharmaceuticals, healthcare and finance** risk significant fines and other penalties if they do not maintain detailed, verifiable records to prove compliance. In particular, insurance companies, lenders and banks are heavy users of secured electronic documents
- Companies and individuals in **law, scientific research and technology development** need to refer repeatedly to certain documents and be confident that they have not changed. This also applies to common functions like human resources and purchasing in almost every industry.
- Businesses like **construction and manufacturing** that work with a wide range of vendors and suppliers can improve customer service and cut time-to-market by streamlining the contracting process.
- Any businesses or organizations that are document-intensive, such as those in **real estate, government, and education**, wrestle daily with the time and expense involved in printing, managing, and storing reams of hard copy.
- **Human Resources** paperwork signed by newly hired employees or changes in employee status should incorporate content authentication and identity credentialing of the electronic signature just as any other legal document or contract.
- Businesses in any industry with **multiple offices across a wide geographic area** need to share critical information confidentially and without fear of unauthorized changes.

In addition, environmental concerns and pressures in coming years are likely to promote (or require) alternatives to paper for businesses of all types and sizes. The government paperless initiative, the e-prescription program are examples of this important trend.

## **About Authentidate Holding Corp.**

Authentidate Holding Corp. is a worldwide provider of secure health information exchange, workflow management services and telehealth solutions. The company's software and web-based services enable healthcare organizations and other enterprises to increase revenues, reduce costs and enhance patient care by eliminating paper and manual work steps from clinical and administrative processes. The web-based services are delivered as Software as a Service (SaaS), and only require that customers have an Internet connection and web browser. The company's healthcare customers and users include leading homecare companies, health systems and physician groups. These organizations utilize the company's products and services to coordinate care for patients outside of acute-care.

For more information, visit the company's website at <http://www.authentidate.com>.

## **About the AuthentiProof Service**

The AuthentiProof service enables users to verify authenticity, provide tamper detection, and date and timestamp electronic content, documents and files. The record of the content authenticity is stored by the AuthentiProof service, assuring a backup verification service for up to seven years from an AuthentiProof seal's attachment to an electronic file to ensure trusted non-repudiation of content.

## **Summary**

Online technology has revolutionized business communications. So why do we still revert to paper to conduct the most critical aspects of our business transactions? This report explores the electronic equivalents to handwritten signatures, certified mail, and other authentication elements needed for contracts, legal correspondence, and compliance-related documentation. Learn how platforms like Inscribe from Authentidate are not just analogous to, but superior to, traditional methods.

- What assures that electronic transactions and electronic signatures are legal
- Why these technologies are superior to their paper equivalents
- How to use them for improved productivity and security