



Establishing Trust with Online Processes

Securing documents with Adobe[®] Certified Document Services

August 2010

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2010 Entrust. All rights reserved

Table of Contents

1	Reluctance to Adopt Online Processes	1
2	Why Move Processes Online?	1
	Dramatic Cost Savings	1
	Customer Loyalty.....	1
	Faster Response Times	2
	An Ecological Alternative.....	2
3	Establishing Trust in Electronic Documents	2
4	Adobe Certified Document Services	3
5	Adobe CDS — From a Reader Perspective.....	4
6	Adobe CDS — From an Author Perspective	7
	Types of Signing.....	7
	Individual Manual Signing.....	7
	Group Manual Signing.....	8
	Enterprise (Group Automatic) Signing.....	8
7	Real-World Applications of Adobe CDS.....	9
	Healthcare	9
	Education.....	9
	Government	10
	Insurance & Finance.....	11
8	The Legality of Digital Signatures	12
9	Adobe CDS Secures Online Processes.....	13
10	About Entrust	13

1 Reluctance to Adopt Online Processes

Now more than ever, organizations have reasons for moving processes online — cost-savings, environmental responsibility, faster response times and more.

But electronic transactions and communication can carry the perception of insecurity. The public is bombarded with information on phishing attacks, viruses, malware and online identity theft. Although it does occur, they rarely hear about the same attacks happening with physical mail.

This has led to skepticism in electronically delivered information. Customers want to be sure that the invoice they received is from the actual vendor; they want to be sure that academic records haven't been altered; they need to know that medical records haven't been intercepted.

As a result, the onus has been placed on organizations to establish trust and validity with their stakeholders. Without a widely accepted and available technology, the adoption of more sensitive online processes has been slow.

In response, Adobe's Certified Document Services (CDS) provides a method to authenticate and verify the legitimacy of PDFs via digital signature technology that offers proven non-repudiation and is widely accessible. The challenge is to demonstrate the trust and benefits of online processes.

2 Why Move Processes Online?

Dramatic Cost Savings

A recent study by the Hackett Group demonstrated that e-invoicing can save organizations 80 percent in reduced invoice-processing costs versus paper invoices. Their research also discovered that solving invoice discrepancies improved by 70 percent, which means a faster time-to-payment.

Consider that U.S. businesses spend between \$20 and \$30 billion annually on paper-invoicing alone — generating 26 billion bills and spending \$17 billion in postage¹ — the cost-savings opportunities are high. More than just invoices, any time an organization has to print a document for distribution, increased costs result.

Beyond the cost of printing and distributing paper, there's also the consideration of retaining and storing paper records. One only needs to visit their local land registrar to see an example of the complexity and volumes of paper for searching and maintenance.

Customer Loyalty

Customers are demanding online resources. In today's highly mobile, highly connected world, customers want access to their information from many different devices in many different locations. By meeting this demand and moving paper processes online, customers become loyal and less likely to seek services from paper-only competitors.

¹ "Quantifying the Benefits of Electronic Invoice Presentation and Payment," The Hackett Group, October, 21, 2005.

Faster Response Times

Beyond simply saving money, organizations and their stakeholders will appreciate the benefit of improved response times. Any time a process requires a paper format, the progression stops while the product is printed, processed and delivered. This lag can mean stale information — stakeholders often require instantaneous data.

For organizations, this can mean better cash flow from faster payments, improved customer satisfaction by providing immediate service and greater customer loyalty.

An Ecological Alternative

Many companies are committed to reducing their carbon footprint. This is partially due to pressures from consumers and government regulations, but also to be better corporate citizens.

Consider that the average invoice uses three pages of paper (including the envelope) and multiply that by the number of invoices processed each day, month or year — the ecological savings piles up. And that's just invoices. Statements, confirmations, transcripts, plans and records also contribute to the paper consumption.

In a typical year, the United States consumes 8 million tons of office paper. That's the equivalent of 178 million trees, which provide a source of clean oxygen.² When one considers the environmental costs to *produce* that same amount of paper, 152.6 billion gallons of water is wasted and 18.2 billion tons of solid waste is created.³ Those staggering numbers, based on research completed by the Environmental Defense Fund's Paper Task Force, make a strong case for moving paper processes online.

3 Establishing Trust in Electronic Documents

Adobe Systems Inc. pioneered the idea of creating documents in a portable format that could be read but not edited by recipients. Since that time, PDF has become a formal ISO open standard (ISO 32000) available on multiple platforms with more than 1,800 vendors offering PDF-based solutions.⁴ With more than 250 million PDF documents on the Web today, the format has become the tool of choice for deploying read-only documents.

As PDF documents became popular, commercial solutions appeared on the market that allowed altering of these read-only documents. Users began demanding greater security assurance that their documents weren't being seen by unauthorized users or altered after creation.

The PDF standard evolved in two ways to accommodate these needs: a username/password feature was implemented to encrypt and decrypt the document to prevent viewing from unauthorized recipients; and the ability for an author to add a digital signature to the document was included.

While encryption was weak at first, updated versions featured robust encryption. Later versions of Adobe[®] Acrobat[®] also included digital rights management (DRM) capabilities.

² "[Green Procurement Requirements and the Use of 100% Post Consumer Fiber Paper](#)," Raymond Paulson; NADEP North Island, Environmental Program Office, U.S. Navy; 2005.

³ Environmental impact estimates were made using the Environmental Defense Fund Paper Calculator. For more information visit <http://www.papercalculator.org>.

⁴ "[Adobe Portable Document Format \(PDF\): Product Details](#)," Adobe Systems, Inc.

Organizations have been using digital signatures for years to protect electronic documents. With public key infrastructure (PKI), an author uses his key or digital code to apply a signature to a document. That code or key applies a hashing algorithm to the entire document to compute a digital signature.

If any part of the document changes, that digital signature would no longer compute. The signature also shows the identity of the signer and the certification authority (CA) that created the key. As well, it includes the public key that allows the signature to be verified. While the author signed the document with a private key available only to him, the certificate in the document contains a public key that allows any recipient to validate the document.

The downside of these digital signatures is twofold. Generating and authenticating these certificates can be costly and complex since not all companies want to deploy a PKI infrastructure. More importantly, the user must possess the necessary tools and knowledge to “trust” the CA that signed the document. Security-conscious organizations understand that novice end-users can’t be expected to verify and trust signatures.

Organizations must assume users can’t/won’t download or configure applications in order to verify electronic documents. This is especially true when we ask readers to trust an unfamiliar CA. It also becomes difficult for readers to easily confirm the validity of the digital signature.

4 Adobe Certified Document Services

Adobe recognized the apprehension end-users were having with digitally signed PDF documents. With the tools to verify and view certificates built into the ubiquitous Adobe Reader, they also identified an opportunity to solve a significant barrier in the uptake of digital signatures.

Adobe Certified Document Services (CDS) is a relatively new platform offering available in the Acrobat 6.0 product family. Using digital signature technology, CDS provides recipients with assurances that certified PDF documents are authentic — that they did indeed originate from their stated author and the portions of the document signed by the author have not been modified since authoring.

Entrust Certificates for Adobe CDS enable organizations to easily apply digital signatures to documents — individually and in bulk — and have them be readily apparent to the reader.

To enable this capability, Adobe partnered with Entrust to provide certification authority (CA) services, including all registration authority (RA) functionality. Entrust’s CA has been “chained” to Adobe’s CA to provide trust services on behalf of Adobe. Once registered, the author is verified by Entrust and issued a digital ID to certify documents to be used in Adobe Acrobat, Reader and LiveCycle products.

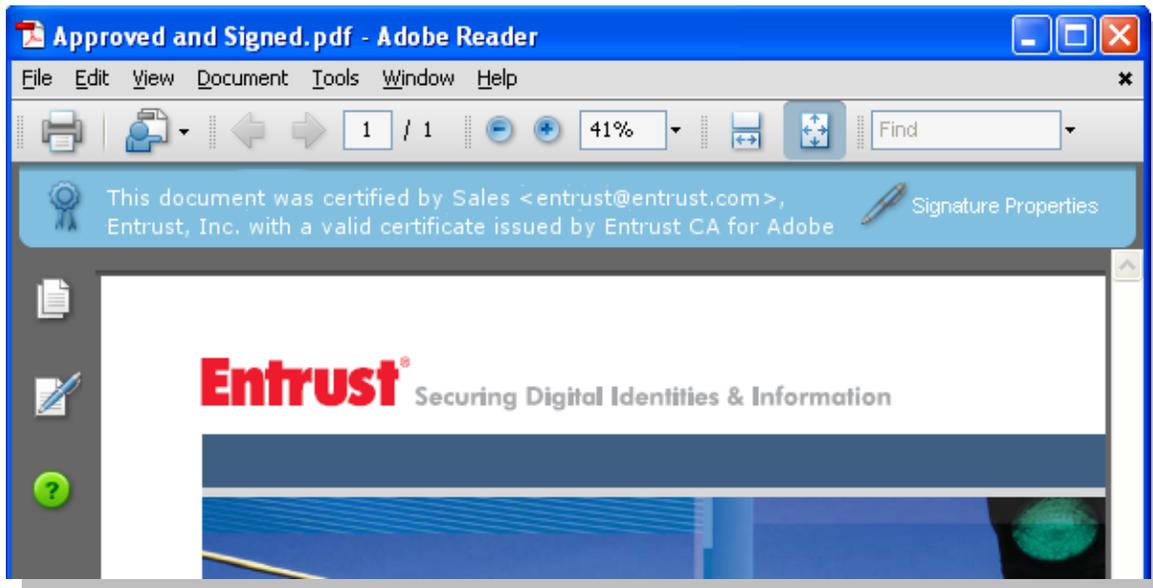
When a document is signed with an Adobe CDS certificate, the author’s identity and the document content is verified each time a PDF document is opened. In recent versions of Acrobat Reader, a blue ribbon appears at the top of the document clearly indicating the identity of the author and whether the document has been verified.

5 Adobe CDS — From a Reader Perspective

Each time a user opens a PDF that was certified with a CDS certificate, a visual ribbon is displayed across the top of the application. This ribbon is not on the document itself, but appears as an additional toolbar within Acrobat Reader (Version 6 or greater).

A Valid Signature

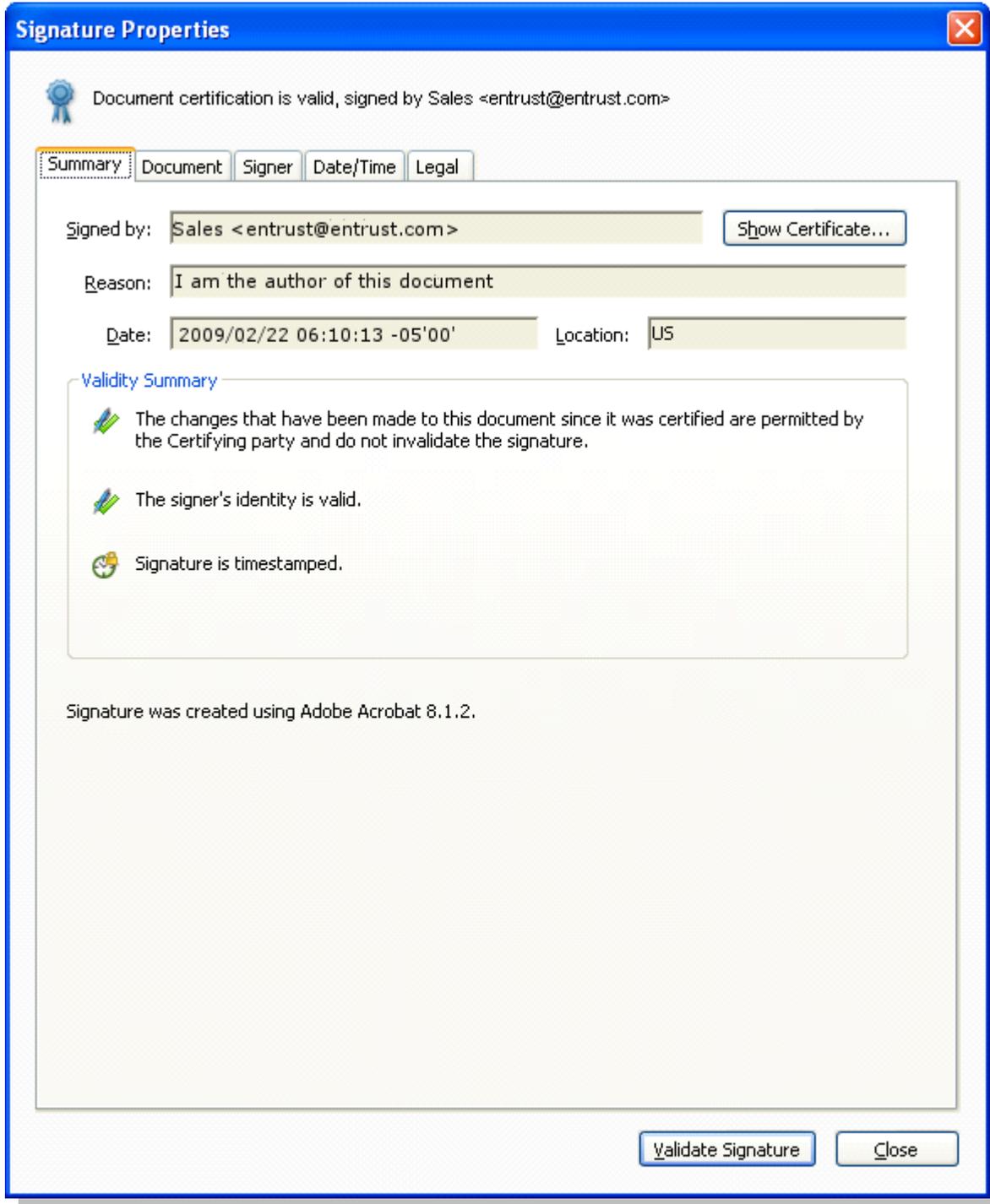
Once the integrity and validity of the signature is successfully verified, a blue ribbon icon appears on the ribbon (pictured below). This is a **certification signature**, which verifies the author and the integrity of the document. Because the document is confirmed to be the exact document that was signed by the author, it is known as **non-repudiation**.



Users can further verify the signature by clicking on “**Signature Properties**” (the pen) to the right of the ribbon. This displays the signature information detailed in the image on the next page.

The **Signature Properties** dialog provides another indicator of trust, but also further information. The *timestamp* (time, date) of the signature may also be important, especially with time-sensitive documents such as letters of offer, payments or invoices. Additional information, including the reason the document was digitally signed, is also available.

Another type of signature that may appear in a document is an **approval signature** where a signature appears within a document to indicate an author or reviewer's approval.

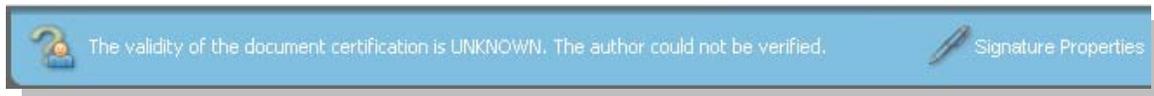




The author can create spaces where multiple Adobe CDS certificate users can sign their approval to a document. This is ideal for use in workflow applications or where multiple signatures are required. The signature uses the same visual icons to verify, in real-time, that the signature is authentic.

Validity Not Confirmed

If a reader is offline or if Acrobat Reader is unable to verify the signature, a question mark symbol will appear indicating trust could not be established.



Before relying on this signature, readers should establish trust with the author.

Invalid Signature

If a document has been compromised, an obvious symbol appears in the ribbon:



This symbol indicates that the document had been corrupted or changed since it was originally signed.

6 Adobe CDS — From an Author Perspective

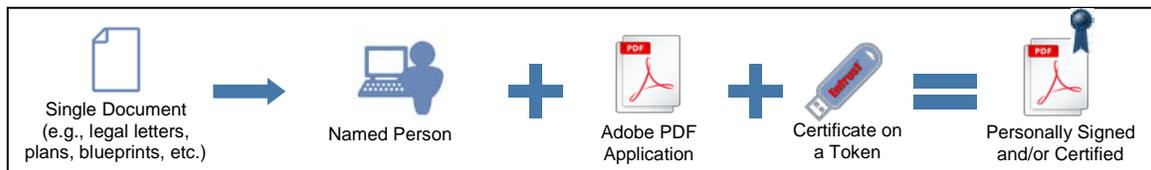
Creating and establishing trust with recipients is simple and different types of CDS certificates are available depending on the application.

Types of Signing

Depending on the use case, there are two types of signing (manual, automatic) and three types of signers (departments, organizations, individuals). Add to the mix that you can use CDS for certifying and/or signing, and documents can be set up for workflow applications with multiple signers, and there are countless combinations.

Individual Manual Signing

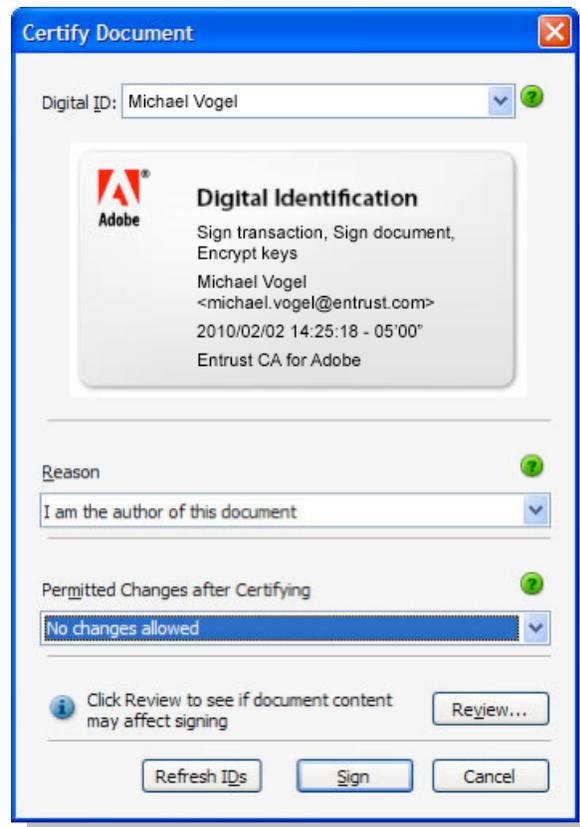
Individual manual-signing certificates are stored on a security token and used by individuals in organizations that need to sign documents on an ad-hoc basis. Examples of individual manual signatures are approvals on documents in a workflow, an individual signing a contract or form, or authors of sensitive documents signing their authenticity such as blueprints, specifications, finance reports and important letters.



To sign a document, the author simply “distills” the document into PDF format, certifies it first (providing the document doesn’t already have a signature on it), determine which parts of the document can/cannot be changed and signs it.

Sometimes an author will want to circulate a document for other approvals. In this scenario, the author can specify how and who can sign the document after the author has signed it.

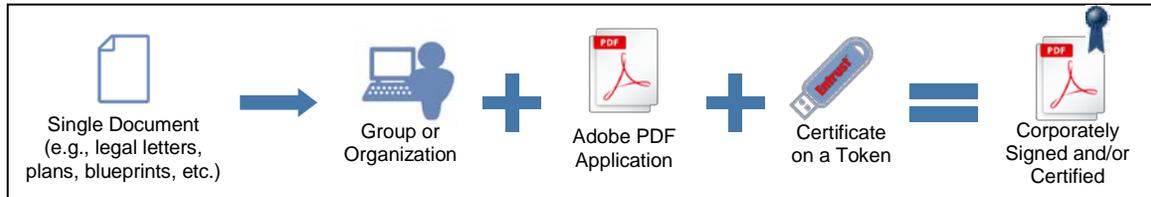
The image to the right depicts setting the preferences to certify a document.



Group Manual Signing

Group manual signing is similar to individual signing except that the signature and certification on the document is from an organizational group rather than an individual. These certificates are primarily used when a department is providing ad-hoc document certification and do not want to sign a specific name to it.

For example, the *planning office* of a municipality may want to provide approval/certification of documents for the public and want to sign it from the department. Or, a legal team may want to sign documents on an ad-hoc basis from the *legal department*.



To sign documents from a group, the same process is followed as an individual manual signing, except that a different CDS certificate is used.

Enterprise (Group Automatic) Signing

Automatic certification and signing is used when a large number of documents require certification and/or signing on a regular basis through an automated process. Typically, organizations use an application like Adobe LiveCycle[®] to manage signing. Adobe LiveCycle ES (Enterprise Suite) software is an integrated server solution for data capture, information assurance, document output, process management and content services.

Examples of automated group signing are regularly scheduled statements, invoices, certificates, quotes, employment records and transcripts, to name a few.

Signing automatically is largely dependent on the server software (e.g., LiveCycle). Enterprise CDS certificates are available on a secure Hardware Security Module (HSM) only and are available in the following versions:

- Enterprise Lite — Up to 40,000 signatures annually
- Enterprise Pro — Unlimited signatures

7 Real-World Applications of Adobe CDS

Healthcare

The healthcare industry has been under increasing pressure to reduce cost and provide a more streamlined approach to patient care and product delivery. A natural response to these pressures is to move documents online, but healthcare organizations have been slow to adopt electronic records. Released in March 2009, a 2008 study by the New England Journal of Medicine found that only nine percent of U.S. hospitals have implemented health information technology.⁵

There is immense opportunity to streamline security and improve the flow of information by moving healthcare records online. In the US, the Health Insurance Portability and Accountability Act (HIPAA) specifies that data corroboration, including the use of check sum, and digital signatures should be used to ensure data integrity.⁶ Adobe CDS documents provide full-document digital signatures and ensure the entire document has not been altered, thus providing compliance to this aspect of HIPAA. Similar laws exist in other countries for healthcare.

Within healthcare, the pharmaceutical industry requires secure electronic signatures when new drugs are brought to market. Information from clinical trials, quality control records and scientific data consume an immense amount of paperwork that could be easily brought online.

The U.S. Food and Drug Administration (FDA) recognized the need for a secure way to submit drug information, especially in light of revelations that paper signatures were at risk for falsification. The Code of Federal Regulations (CFR) Title 21 Part 11 deals with guidelines on electronic records and electronic signatures in the US. It defines the criteria under which electronic signatures can be considered valid.

Beyond simply bringing drugs to market, it also defined electronic signatures for ongoing clinical information and pharmaceutical manufacturing. Adobe CDS certificates are ideal for certifying and signing FDA paperwork because full-document validation is required. Although not mandatory, a timestamp is strongly recommended.⁷ Entrust Certificates for Adobe CDS provide a time-stamping feature.

Education

Several processes in the educational space have been under consideration for automation but have been stymied by the need for secure, trustworthy automation.

For example, the process to automate transcripts could save mountains of paperwork, but these transcripts are notorious for becoming falsified. Usually the need for a transcript is for employment purposes, so a fast turnaround is crucial. Educational institutions, however, need to reduce costs on courier and mail services.

By enabling Adobe CDS certificates, the transcripts can be certified and signed by registrar offices in a fraction of the time and cost it normally takes educational institutes to carry out the same task. Delivery of these transcripts can now be accomplished electronically.

Extending beyond transcripts, certified and signed documents can also be used by universities for extending admission letters, financial aid documents, grant letters and even diplomas.

⁵ ["U.S. Hospitals Slow to Adopt E-Records,"](#) Jacob Goldstein, The Wall Street Journal, March 26, 2009.

⁶ ["Health Insurance Portability and Accountability Act of 1996; Public Law 104-191,"](#) 104th United U.S. Congress.

⁷ ["Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application,"](#) U.S. Food and Drug Administration, August 2003.

Government

Governments around the world have enabled legislation to varying degrees that define what is acceptable for a digital signature. Now that legislation is in place, applications abound where a certified document would allow governments to interact better with citizens.

Digital signatures have been available to government departments and agencies for some time, but were often focused on signing for internal use. Having digital signatures available for citizen use was problematic because citizens did not likely have the technology and know-how readily available.

Adobe CDS certificate-signing takes away the complexity of digital signatures for recipients because most citizens who have access to a personal computer likely have Adobe Acrobat or Reader reading capabilities. Now that CDS certificate applications are possible, the opportunities are endless, some examples of government-citizen applications are:

- **Patent documentation** to ensure that the author of the document has certified and not altered the document and that the patent grant has not been altered.
- **Real estate transactions.** Every real estate transaction requires a mountain of paperwork including land survey documents, land transfer tax documents, agreements of sale and purchase, title search documentation and municipal tax documents to name a few. All of these highly sensitive documents not only need to be certified, sometimes they need an electronic approval signature.
- **Copyright forms.** Signing and certifying copyright forms not only ensures they do not change, but also adds a timestamp to resolve disputes on the first use.
- **Tax returns.** Every government has them. It would make sense to offer them in a downloadable format that citizens can trust.
- **Forms.** All departments in all levels of government have forms for citizens to fill out. Certifying forms using Adobe CDS certificates assures citizens that they have authorized forms.
- **Permits.** Municipal governments require building permits for most work that citizens and contractors want to carry out. On the one hand, contractors can certify the required engineering documents and submit them online in addition to approval signatures on the certified online forms. On the other hand, citizens can download certified forms to apply for permits themselves. To avoid fraudulent permits, the municipality can deliver certified and signed permits to the applicants electronically.
- **Census.** Delivering census information and reports as well as sending out census forms can be easily accomplished with Adobe CDS certificates.

Insurance & Finance

Banks all over the world are reeling from financial difficulties from the collapse of bad credit and the decline of the world economy. Shoring up costs has become a priority for the struggling sector and that can mean automation and moving processes online.

The biggest boost to these efforts in the United States was the passing of the Electronic Signatures in Global and National Commerce Act (ESIGN), which essentially validates the legality of proper digital signatures.

Similar legislation acknowledged the validity of digital signatures in other countries. This provides the confidence of a legal basis for financial institutions when utilizing digital signatures in online processes.

Some examples of these processes are:

- Trading instructions
- Loan applications
- Credit investigation
- Loan processing
- Mortgage papers
- Insurance applications and claims
- Trading confirmations
- Insurance/bank statements

The potential savings is tremendous, yet not without challenges. One such obstacle is that digital signatures have to “live,” in some cases, for up to 30 years. Fortunately, Adobe CDS certificates feature signing details such as the online certificate status protocol (OCSP) that allows the signature to live on in perpetuity.

Another challenge that the financial services industry faces is increased regulations such as Sarbanes-Oxley (or SOX). A key aspect of SOX regulation is the necessity to bind critical transactions to key employees in an auditable format.

Adobe CDS certificates directly address this need by tying the author’s digital signature and timestamp to prove information was made available (or reviewed) at the right critical times. These digitally signed PDFs provide a perfect audit trail.

8 The Legality of Digital Signatures

The legality of digital signatures varies based on jurisdiction, but, in general, digital signatures are legally accepted in most jurisdictions.⁸

In the U.S., the Electronic Signatures in Global and National Commerce Act (ESIGN) facilitates the use of electronic records and signatures by ensuring the validity and legal effect of contracts entered into electronically.

Although every state has at least one law pertaining to electronic signatures,⁹ the federal law indicates that a contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form.” The ESIGN legislation, while leaving many details ambiguous, contained the key element that wasn’t covered by law: digital signatures under the proper circumstances are valid.

In Canada, PIPEDA distinguishes between the generic “electronic signature” and the “secure electronic signature.” Federal secure electronic signature regulations make it clear that a secure electronic signature is a digital signature created and verified in a specific manner.

In the UK, electronic signatures were given legal status in the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002, which provided a framework for digital signatures.

Beyond standard digital signatures, the UK has also defined the concept of Advanced Electronic Signatures (AES), which is considered more secure and is as legal as a handwritten signature. The broad definition of AES signatures are that they are identifiers, uniquely assigned, under sole control of the signor, verifies that no changes are made after signing (non-repudiation), and are secured by a certification authority who complies by strict regulations.

Many other countries have adopted the United Nations Commission on International Trade Law (UNCITRAL) Model Law on E-Commerce, which was ratified in 2001. The UNCITRAL Model Law defines e-signatures, although some member jurisdictions have added their own twists to it.

⁸ [“Digital Electronics Signature Laws and Regulations Around the World,”](#) ComliancesForum.com.

⁹ [“Digital Signature Guidelines: Tutorial Footnotes, No. 29,”](#) American Bar Association.

9 Adobe CDS Secures Online Processes

There's little doubt that migrating to online processes saves money, reduces waste, increases efficiency and speeds communication. The primary objective is enhancing the trust and reputation associated with these online services, electronic documents and Web-based processes.

Fortunately, Adobe's Certified Document Services (CDS) solves the major barrier for mass adoption of electronic documents and information — trust. Already successful in other applications, this standard is the universal method to authenticate and verify the legitimacy of PDFs via digital signature technology that offers proven non-repudiation.

In support of Adobe's initiative for securing paperless initiatives, Entrust offers specialized SSL digital certificates that provide assurance for electronic documents.

Accessible and affordable, Entrust Certificates for Adobe CDS enable organizations to digitally sign Adobe PDF files with confidence. Recipients can feel more confident by seeing the visual trust indicators that verify who published the document and whether it has been altered.

The capabilities of Entrust Certificates for Adobe CDS are optimal for organizations who share sensitive or official information electronically, including statements, invoices, legal documents, engineering plans and diagrams, diplomas, charters and more.

Entrust Certificates for Adobe CDS provide real-time document authentication for any Adobe PDF, which Entrust confirms as the trusted verification provider.

10 About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.