

# DIGITAL SIGNATURES FOR ARCHITECTS' AND ENGINEERS' DRAWINGS

© Copyright 2005 LineType Software, Inc.

## The Need

Changes in communications and printing technology in the last decade have made possible new ways of reproducing architectural and engineering drawings that are of higher quality and potentially lower cost than traditional means of reproduction. In order for these new technologies to be fully implemented, however, a method must be devised of electronically affixing a signature and date to drawings that is acceptable to and approved by state architectural licensing boards.

## History

In the traditional printing work flow, a set of original drawings is produced, either hand-drawn or plotted from a CAD system. The registrant's seal is then applied to each sheet of drawings with a rubber stamp, and each sheet is hand-signed and dated by the registrant. Copies are then made of these original documents. The copies are distributed to project team members, while the originals are kept on file in the registrant's office.

In recent years, some state licensing boards have adopted rules allowing digital signatures and seals to be applied to drawings and specifications. Other boards are considering such rules. Although the requirements vary from state to state, typically the rules stipulate that the digital signature must be applied in a secure manner and that it be applied only by the registrant whose name is on the signature. Some boards leave the interpretation of "secure" undefined; others reference particular state or federal regulations governing the use of digital signatures.

This paper seeks to address some of the relevant issues and to suggest a method that is generally available, that can be employed by users of all CAD systems, and that will meet the requirements of state boards as a sufficiently secure process for digital signatures.

## Some Terms

There are several terms related to data security that may be helpful in this discussion.

### *Components of Data Security*

- Authentication - Are you who you say you are?
- Authorization - Are you sanctioned to perform this transaction?
- Privacy - Is this data protected from non-authorized persons?
- Data Integrity - Has the data been altered by a non-authorized person?
- Non-repudiation - Can it be proven who generated the data?

### *Encryption*

A method of ensuring the privacy of data. Data is typically encrypted and decrypted with a key.

### *Key Pair*

A pair of related numbers that is used to encrypt and decrypt data. The private key is kept secure on the owner's computer system. The public key is distributed to parties with whom the user is exchanging encrypted messages. Data encrypted with the private key can be decrypted with the public key, and vice versa.

### *Hash*

A unique number generated from the contents of a data file by a standard algorithm. The hash is an abbreviated digest of the contents of the file, and no two files will create the same hash.

### *digital certificate (digital ID)*

A link between an individual and a key pair. This link is made, verified, and maintained by a Certification Authority. Certification Authorities are typically independently audited businesses that provide and maintain these links (usually via the internet) for a fee. Similar to a state agency or board, the public can rely on the Certification Authority to provide truthful information that the individual's identity has been verified and that the public key is associated with this individual.

### *Digital Signature*

A cryptographic modification of data that provides for authentication, data integrity, and non-repudiation of the data. A digital signature is an encrypted string of numbers that is attached to a data file. The digital signature is generated through an algorithm that encrypts a digest or "hash" of the contents of the data file with the user's private key. The user's digital certificate is also included with the digital signature. The digital signature is a unique combination of the contents of the file and the private key belonging to the user who attached the digital signature. The digital signature can be verified using the public key, which is available to anyone who receives the signed message. Typically all the steps involved in generating and verifying digital signatures are handled transparently by software.

It is important to note that a digital signature is not a digital representation of a handwritten signature. A digital signature is a number that is attached to a data file, and it can only be read and interpreted by software that is designed to recognize and process it.

A distinction must also be made between encryption and digital signatures. A data file does not have to be encrypted for it to have a digital signature attached to it. The digital signature does not provide for privacy of the data, only for authentication, data integrity, and non-repudiation. If privacy is required, the data may be encrypted as an operation separate from the digital signature.

**Security of Architectural and Engineering Drawings**

In the traditional workflow, the security of drawings prepared by registrants relies on accepted legal conventions and on the actions of regulatory authorities. The elements of data security in this system are outlined below:

| <b>Security in the Traditional Workflow</b> |   |
|---|---|
| <b>Security Criteria</b>                    | <b>Method of Providing Security</b>   |
| Authentication                              | The registrant’s seal and signature identify the registrant. Security is dependent on good faith acceptance of the signature and seal and on penalties for violations. Forgery is simple to accomplish but is punishable by law.  |
| Authorization                               | Maintenance of registrant’s records by the Board are used to determine authorization, and enforcement of rules and law regarding professional conduct are used to address violations. Security depends on a trusted government authority and is therefore at a high level.  |
| Privacy                                     | Not legally required. The need for privacy of documents is determined by the registrant and the client and appropriate measures are taken to ensure privacy.  |
| Data Integrity                              | Original documents retained at registrant’s office provide a mechanism for verifying whether or not a set of prints has been modified without the registrant’s approval. The prints have to be compared to the originals to make this verification. Verification is not automatic or easy to accomplish, but is possible when needed. |
| Non-repudiation                             | Non-repudiation relies on the authentication of the registrant’s seal and signature and on the nature of practice. However, if a registrant were to destroy all originals and deny authorship of a drawing or set of drawings, it might be impossible to prove authorship.  |

## The New Workflow

A secure method of electronically affixing signatures must fit the procedures typically used in the architectural and engineering community, and the capabilities of plotting service providers. For the purposes of this discussion it is assumed that printing will be provided by a third-party service. The same principles could be applied to an in-house printer, however.

When CAD drawings are printed by a plotting service, first a plot file is generated from the CAD drawing file. The plot file is usually in one of several industry-standard formats, the most common being HPGL (Hewlett-Packard Graphics Language) and PDF (Portable Document Format). The plot file contains the information selected from the CAD file for printing, and is formatted for output. For the purposes of this discussion, it is assumed that PDF files are used for plotting.

There are several important differences between a CAD drawing file and a PDF file. The format of the CAD drawing file is dependent on the particular CAD system used, and it may represent building elements in a variety of ways. Walls may be represented by lines, or they may be three-dimensional graphic elements with material attributes or other information attached to them. There may be several possible views in each drawing file; for a three-dimensional drawing, it may be possible to view the objects in either plan, section, elevation, or detail views. A drawing may have several different sheet layouts in it at different locations, or there may be information in the drawing file that is not meant for plotted output and that will be excluded when a plot is made. In addition, it is relatively easy to modify the content of a drawing file – that is the whole purpose of CAD programs.

The PDF file, on the other hand, accurately represents the size, scale, and appearance of the plotted sheet. Only that graphic information that is intended for output is included, and line weights and colors are accurately described. The drawing file can be thought of as a database of information; the PDF file is a specific representation of that information as it is meant to be seen on a sheet of paper. And PDFs are more difficult to modify. Although there are PDF editing programs on the market, modifying a drawing by changing the PDF would be about as difficult as manually erasing lines from a printed sheet and drawing other lines in with a pen. Large-scale changes such as can be made with a CAD program are not easy to do.

Now once the PDF has been created, it is sent to the plotting service. Usually this is done over the internet, although files can also be copied to disks and hand-delivered. The plotting service opens the PDFs on their computer and sends them to their printers for output.

The crucial part of the new workflow is this last step. If an electronically-generated signature and date could be affixed to the drawing file or the PDF file, then when the PDFs are output by the plotting service, every set of drawings would be an original. There would not be one set of transparencies from which bluelines are run – instead, all sets of drawings would be output from the PDFs directly. An analogy may be made to a laser printer and a copy machine. If one original of a document is printed out on a laser printer, and then ten copies are made of it, that is similar to the traditional workflow. But if ten originals are printed out on the laser printer, each will have the same high quality and there will be no need for the additional step of using the copy machine.

In addition to providing higher-quality prints (because each is an “original”) this method will make it possible to securely transmit final, stamped and signed construction documents via the internet or email. The documents will be safeguarded against unauthorized changes or errors due to transmission, and the digital signature, unlike a simple scan of a written signature, will have full legal significance.

## **A New Workflow Using the Banjo™ Digital Signature Plug-in**

The new workflow uses the Banjo digital signature plug-in, developed by LineType Software, Inc., to increase the efficiency and convenience of the printing process while maintaining or enhancing the level of security provided by the traditional method.

The steps in this procedure are outlined below:

- Drawing files are edited as required. This step may be performed by the registrant or by an employee.
- A PDF of each sheet to be printed is created. This step may be performed by the registrant or by an employee. During plotting, an image of the registrant's seal may be applied to each PDF if allowed by current Board rules, or it may be applied later as part of the digital signature.
- Each PDF is opened and viewed by the registrant using Adobe Acrobat. The Banjo digital signature plug in is installed with Acrobat, and it is used to digitally sign the PDF files. The registrant's signature and date of signature are securely applied over the seal on each PDF, and a digital signature is attached to the file in conjunction with the image of the signature and date. A password is required for this step and therefore the digital signature can only be applied by the registrant.
- When all PDFs have been modified, they are sent to the plotting service via the internet. A password-protected account or folder on the plotting service computer will ensure that only authorized persons will be able to send files to the plotting service or have access to files that have been sent previously to the service.
- PDFs are retained on the registrant's computer system for archive purposes.
- At the plotting service, the Banjo plug-in has also been installed, using either Adobe Acrobat or the free Adobe Reader. Since the plotting service will only be reading and verifying signatures, not creating them, the Reader version may be all that is needed.
- The PDFs are individually read and automatically processed by the plotting service. The registrant's digital certificate is on record at the plotting service. If the digital certificate used to sign the PDFs is different from the one on record with the service, or if the service does not have the digital certificate for the registrant, then the image of the signature on the PDF will be automatically marked as invalid or unverified.
- If the PDF has been altered, either intentionally or unintentionally, since it was signed, the digital signature will appear as invalid.
- Only if the digital certificate matches and the PDF can be verified as unmodified will the signature appear as valid. These verification steps are performed automatically by the plotting software and do not require additional work from the plotting service employees.

This process depends on a different understanding of the concept of “original document.” Whereas in the traditional workflow the sealed and signed reproducible (vellum or other transparency) is the original, in the new workflow the sealed and signed PDF is the original. The PDF is archived on the registrant’s computer system in a manner analogous to saving the original transparencies.

**Digital Signatures and Images of Written Signatures**

The process outlined here is complicated by the fact that it uses both a digital signature (as defined in the section on data security) and an image of a written signature (as required by convention in the AEC industry). These are different concepts, serving different functions.

A digital signature is useful only for a digital document – it is generated and verified by computer software, so it is meaningless for a printed document. State licensing boards typically require a visible signature and seal on drawings. Codes officials and contractors also expect to see this on printed documents. The image of this seal and signature, may, if state regulations allow, be applied electronically. But this is not a digital signature. It is an electronic image of a written signature that is required to be affixed in a secure manner (with the digital signature supplying the security).

In this process, the digital signature is used as a means of authenticating the image of the written signature. The digital signature protects the integrity of the PDF until the PDF is output to paper, at which point the image of the written signature “takes over” as the statement of authenticity.

**Security in the New Workflow**

The elements of data security in the proposed system are outlined below. Security in all areas is equal to or greater than that provided by the traditional system:

| Security in the New Workflow |   |
|------------------------------|---|
| Security Criteria            | Method of Providing Security  |
| Authentication               | As with the traditional workflow, on the printed document the registrant’s seal and signature identify the registrant. The use of digital technology does not change the level of security of the printed document – someone can still forge a seal and a signature.<br>On the original PDF, however, the digital signature provides an additional level of authentication. The plotting service verifies the digital certificate and the digital signature when drawings are processed, and therefore is assured that the drawings have indeed been sent by the registrant and that they have not been tampered with. And the digital signature remains on the original PDF archived at the registrant’s office to verify that the registrant signed this original file. |
| Authorization                | Again, for the printed document authorization depends on the Board. Only the Board has the authority to determine who is authorized to sign and seal documents.<br>For the application of the digital signature, the Certification Authority verifies that the digital signature has been applied by an individual with a valid digital certificate.  |
| Privacy                      | The proposed process does not include encryption of the PDFs or any other files. If individual users decide that encryption is necessary, this can be easily accomplished using the encryption capabilities of PDF files.   |

|                 |   |
|-----------------|---|
| Data Integrity  | <p>Verification that the PDF has not been modified since it was sealed and signed is provided by the digital signature. If the file is modified either on the plotting service computer or in the registrant's office, the digital signature will no longer be valid and verifiable.</p> <p>For printed documents, the presence of the digitally signed PDF at the registrant's office provides the same mechanism for verifying data integrity as is provided by the traditional workflow. Prints that are suspected of unauthorized modification can be compared to the original images in the PDF.</p> |
| Non-repudiation | <p>The presence of the digital signature provides a method of determining who generated the PDF that cannot be repudiated by the registrant. Therefore if the PDF is available either on the plotting service computer or on the registrant's computer, authorship cannot be denied.</p> <p>As with the traditional workflow, if all PDFs are deleted and only paper prints are available, authorship cannot be definitively proven.</p>  |

## Questions and Answers

### Are digital signatures accepted under the law?

Yes. The *Electronic Signatures in Global and National Commerce Act (US E-SIGN ACT)* was signed into law by President Clinton in 2000. Although certain types of documents are excluded from this act (such as wills and court orders) the act does provide a legal basis for the use of digital signatures in architectural and engineering documents.

### What is the difference between this proposed method and the Digital Signature Extension sold by AutoDesk? Doesn't the AutoDesk product already provide these features?

The Digital Signature Extension from AutoDesk (and other products from different vendors) addresses a different need in a similar manner. The crucial difference is that the AutoDesk product attaches a digital signature to the CAD (DWG) file; the method proposed here attaches the signature to the PDF.

The Digital Signature Extension from AutoDesk is the appropriate product to use when an original CAD file (the DWG file) must be securely sent from one place to another and must be protected against changes. For instance, if an architect is sending base plans to a consultant and wants to ensure that nothing is changed by the consultant, then a digital signature applied to the DWG file is a good solution.

For the generation of *construction documents*, however, (in either electronic form or in a form to be plotted on paper), the method proposed in this paper has two important security advantages.

As described earlier in this document, there are basic differences between the CAD drawing file and the PDF file, the most important of which is that the CAD drawing file does not represent a printed document; it is a database of information, some of which may not be intended for output. The appearance of the drawing file depends on the CAD operator's selection of information to display at a certain time. Therefore if the registrant applies his signature to this file, he may not be able to determine exactly what he is taking responsibility for. When the drawing file is printed, additional information may be visible, or some critical information that was displayed at the time of signing may not be visible anymore. These appearance changes can occur without changing any of the contents of the drawing file, and so the signature would still be visible in the file.

A second problem with applying the signature to the CAD drawing file is that a plot file of some kind (a PDF or and HPGL) must still be made from it in order to send the drawing to a plotting service. When this file is made, the security functions attached to the drawing file are not transferred to the plot file. An image is made of the signature that is securely attached to the drawing file, but the plot file itself has no link to this security mechanism. Therefore it would be possible to modify the plot file with the image of the signature in it without there being any way to tell that this modification has taken place.

The proposed system avoids this problem by applying the image of the signature to the PDF rather than to the drawing file, and by applying a digital signature as well as an image of the written signature. The digital signature is the means of verifying that nothing has been changed in the PDF from the time that it is created until it is plotted and becomes a hard-copy document.

**If a PDF processed in this manner is tampered with, will the image of the registrant's signature still be visible in the PDF?**

Yes, but it will be marked as invalid. When the PDF is opened for processing by the plotting service software, the digital signature is verified automatically. If the PDF has been altered, the plotting service operator will be alerted that the file is not valid. Even if someone were to ignore this alert and print the file, the image of the signature will be marked as unverified or invalid and it will be obvious to anyone reviewing the drawings that the signature is not to be trusted.

**What is the potential for abuse with this system?**

As with the system currently in use, there is the possibility of abuse on a variety of levels. The overall level of security, however, is improved in the proposed system.

First of all, the electronic signing mechanism must be performed by the registrant in good faith. The use of a password-protected application to apply the digital signature and the image that goes along with it provides a way to secure this process, but if a registrant allows an employee to do the signing, there will not be any physical evidence of wrongdoing. This is similar to the current situation in which a registrant could allow an employee to sign his name on documents, and unless someone reports it there will be no way to know it has occurred. Security on this level is dependent on the professional conduct of the registrant.

Assuming that the signature has been securely applied and that the digital signature has been written to the file, there is very limited opportunity for abuse. A dedicated hacker could conceivably modify a PDF file, or could extract the image of the registrant's seal and written signature from the PDFs and use these to create a forged drawing file. It would be much easier, however, to simply re-create the image of the seal (as its general format and the license numbers of all registrants are public information) and forge the signature by hand.

Or, as is possible with the traditional system, an unscrupulous individual could obtain a set of signed and sealed paper plans from a job site, photocopy the seal and signature, and place them onto a new set of drawings.

Even if someone were to accomplish one of these types of forgery, the digital signature would protect the original PDFs and would expose the forger. If the original files were modified the digital signature would no longer be valid, and if a forged file were created, the forger would be unable to sign it with the registrant's private key. In either case the plotting service would be alerted to a possible security problem.

After the files are plotted and the prints of the drawings are in the field, it is possible that someone could try to modify one of the copies by hand and pass it off as valid. The only way to determine if this has occurred is to compare the altered drawing to a set of prints in the office, or to compare it to the digitally-signed archived PDF.

The digitally-signed PDF provides a level of authenticity even greater than the current system of using original transparencies, because the digital signature is time-stamped when it is applied. There can be no question that this is the original from which the copy was made, and no question about whether or not it has been modified in the time since.

### **What is the role of the plotting service in this process?**

In order to participate in this new workflow, the plotting service will be required to install software that can read and verify the digital signature on the PDF. Since the plotter service is only reading and verifying signatures, not creating the, either the full version of Adobe Acrobat (and the full version of Banjo) or the free Adobe Reader (and the Reader version of the Banjo plug-in) can be used to verify these signatures.

Because the verification procedures are performed automatically by the Banjo plug-in, extra work and responsibility would not be imposed on employees. Potential liability exposure could be reduced, because it would be very difficult to submit a forged digitally signed document, whereas it is relatively easy to submit a forged hand-signed document.

More important to security than software, though, are proper and well-defined procedures. There must be agreement between the registrant and the plotting service about digital signature use as well as what other types of plot files are acceptable. For instance, it is possible to scan a paper document (with a hand-applied seal and signature) and turn this into a PDF. Is the plotting service authorized by the registrant to plot this type of file? Or when a file such as this is received, should the plotting service alert the registrant to a possible fraud? These questions should be considered and answered at the beginning of the process.