

- 27 Finding Focus
- 42 Online Repositories
- 46 CART Roundtable
- 91 Secure Your Wireless Network

REPORTERS AND ELECTRONIC EVIDENCE

Page 36



s e c r e t s

19 5 3 18 5 20 19

o f t h e

15 6 256 20 8 5

d i g i t a l

4 9 7 9 20 1 12

s i g n a t u r e

19 9 7 14 1 20 21 18 5

What is a digital signature? And how can it protect my transcript?

Back during high school, when you spent hours lying on your bed and perfecting your signature, did you ever consider the purpose of your unique, special squiggle — other than being, oh, so sophisticated? How about today? When you sign a credit card receipt, rent check, or video rental form, what is the point of your special little scrawl?

You likely have some idea. It is a promise of a sort and, perhaps, a kind of proof that you made the mark. And you'd be correct with that answer. But consider, with the growing sophistication of today's technology, how easily someone else could reproduce your signature. Could you prove that the mark wasn't yours — especially on something serious, such as a loan document or a transcript? What if the document was faxed or e-mailed — or never printed at all? How could you or anyone else prove that the document was or was not authentically made or certified by you?

That issue is the driving essence behind the mysterious digital signature: How do you sign something that's not on paper?

What Is a Signature?

Many of you already have a digital signature, and you might even be using it to sign your transcripts. But you likely have no idea what it does, how it works, or why it is supposedly better than any other type of signature.

Although writing your name is the most common way of signing a document, you need to realize that you can still achieve the legal weight of a signature in other ways. Have you ever wondered why an illiterate person can still legally sign a document by just making an "X"? A person can do so because to "sign" something is an acknowledgment — a legal, affirmative act that serves three distinct purposes: authentication, integrity, and non-repudiation.

- *Authentication* (I signed that. This is *me*.) When you sign anything, you are affirming that you are the person making your special and authentic mark. No one else can make your mark. You are signing it and, by doing so, you

are confirming that you are signing the document.

- *Integrity* (This is what I did.) You always sign the *bottom of the last page* of a letter to mom or of a legal contract to indicate that all of the preceding text was written or wholly approved by *you*.

- *Nonrepudiation* (You signed that. Yes, you did!) Other people can look at your mark and hold you to your word. You cannot deny (or repudiate) that you made or approved the document because you signed it. You are on the hook for whatever was written.

These three purposes of a legal signature can be achieved by writing your name in ink (usually called a "wet signature.") But besides the "X," you might not have considered the other standard ways to sign a document. Embossing a seal onto a document, ink stamping a special mark, or even making a fancy wax seal with a piece of ribbon all can carry the weight — and serve the three purposes — of a signature. In fact, by accepting paper currency, you are recognizing the fancy engraving, watermark and, for some, even the smell of a bill as an authentic government document. That acceptance meets the three stated requirements, yes?

Do you know what the biggest problem with physical signatures is?

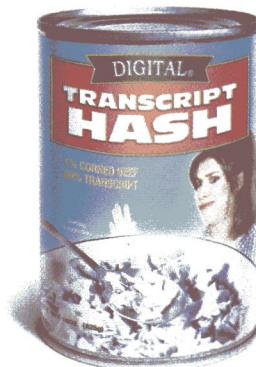
Unless you have seen a person's signature before or can trust someone else to vouch for its authenticity, you cannot know if it is really the genuine mark. A digital signature solves this problem.

What Is a Digital Signature?

We've all heard about digital signatures. But other than seeing something on our computer screen that says "digital signature valid," we have never seen one. We've not seen one because a digital signature isn't a single thing to behold like a stamp or a squiggle.

A digital signature is a combination of several tests that can be performed at any time to certify the integrity of a file.

Just to be clear, unlike what many people seem to believe, a digital signature *is not* a picture of signature on your computer screen.



ART BY ROBIN HUBER

Alex Kasperavicius is vice president of technology for Barkley Court Reporters in Los Angeles, Calif. This article is based on his presentation on digital signatures at the 2008 NCRA convention. Alex can be reached at alex@barkley.com.

FIGURE A:



The above picture of an ink-on-paper signature is not what people are talking about when they refer to a digital signature, even if it's on a computer screen.

The issue can get a little confusing because some software manufacturers like to reproduce a picture of an ink-on-paper signature to certify that the digital signature tests have passed. But the squiggly line on your computer screen is not a digital signature. The digital signature is the test itself.

The First Test: Hashing or "Digitally Binding" a Transcript

With a printed transcript, you physically bind the signature page to the rest of the transcript, thus making it difficult to separate. By signing the last page of a transcript, you, thereby, affirm the entire document. If someone breaks the binding, you know the integrity of the transcript can no longer be guaranteed.

A physical binding proves integrity for printed paper. But with a digital file, binding is achieved with a *hash* test.

Transcript Hash

Hash means "to cut up" (like corned beef hash), which is exactly what is done! The entire transcript is digitally cut up into many pieces.

Similar to cooking hash, digital hashing can be done in many different ways. While our computers use a very complex technique, in Figure B, I have created a very simple type of hash to illustrate how this works.

Notice that I focused on a very small portion of the transcript and cut up — or hashed — that small portion into individual characters. Then, I assigned values to letters of the alphabet (A = 1, B = 2, C = 3, and so on) and went through the portion writing the values under every letter. Likewise, a computer could go through the entire transcript, as I did with these 16 characters, and assign a value to each character. The final step is to add all of these character values together to get one (very long) number.

Ask yourself this question: What will happen to that long number if even one character were changed in the transcript?

Yes, the number would change! That is the essence of a digital signature. It's a way of proving that the document is completely intact by comparing the results of a hash.

The long number you get by adding up all the bits of the hash is called the "checksum." (Get it? Check the sum?)

When you verify a digital signature, your computer rehashes the transcript and compares the checksum it gets against the

FIGURE B: A Simple Hashed Transcript

STEP 1:

Let's say this is your transcript:

```

8      THE REPORTER: You do solemnly state
9  evidence you shall give in this matter shall
10 truth, the whole truth, and nothing but the
11 help you God.
12      MS. DAWSON: Yes.
13

```

STEP 2:

We'll focus on a small portion of it — just these 16 characters:

9 evidence you s

STEP 3:

We will cut up — or hash — the text into separate characters:

9 evidence you s

STEP 4:

Then, we assign each character a specific value:

9 evidence you s
38 256 5 22 9 4 5 14 3 5 256 25 15 21 256 19

STEP 5:

The sum of all those characters would change if even one character were altered.

one the signer made. If the checksums match, you know the file hasn't changed. But if the checksums don't match, you know that the file has been tampered with; then the digital signature breaks or becomes invalid.

Keep in mind that example is a very simple hashing technique that you could get around if you thought about it. Common digital signatures, however, use much more complex hashing techniques, and they break the file down into much smaller pieces at the bit level.

The Second Test: Who Is the Signer?

As mentioned earlier, one big problem with most signatures is recognition. How do you that know a signature is real if you've never seen it before?

The checksums in a digital signature can match, but how do you know that the person sending you the file is authentic? Just as in the physical world, you verify the signature using a third party whom you trust and who has seen the signature before.

In the world of digital signatures, these trusted third parties are called Certificate Authorities. Some you may have heard of are VeriSign, EnTrust, Go Daddy, and Comodo. These trusted third parties do the legwork to ensure that you really are who you say you are. This verification might involve looking you up in the phone book and calling your listed number; inspecting your driver's license, CSR license, business license, or other certification; or using some combination of those.

Once the certificate authority is satisfied that you are genuine, it will issue you a signing certificate that you can install on your computer, along with a password. Each time you digitally sign something, your signing certificate is used and leaves a special digital mark in the file.

When a digital signature is verified, in addition to the checksum test, that special mark is crosschecked with your issuing certificate authority to make sure your certificate has not been revoked.

You can revoke your digital signature if your signing certificate password is ever lost or compromised. Revoking your certificate is a nuclear option because it would break all of the signatures you made up until that time. But it's nice to know that you can do so if you believe someone has stolen your signing certificate and password and is digitally signing files under your name.

Ink-on-paper signatures can be forged, and stamps and seals can be stolen. But because digital signatures check the validity of the signature each time the document is opened, they offer a level of security never before available.

Are Digital Signatures Legal?

Although some agencies and software vendors are urging reporters to start using digital signatures exclusively, you need to remember that, in many situations, digital signatures do not certify the transcript.

The NCRA Committee on Professional Ethics Advisory No. 37 states: "Only a hard copy with the reporter's original signature page constitutes a certified record."

Since the advisory opinion was written, some states, such as Texas, have approved the use of digital signatures, but be careful. Always follow the law in your jurisdiction when producing originals or certified copies. In most cases, the law still requires an ink-on-paper signature page to be bound to the physically printed transcript.

In some jurisdictions, claiming to certify a transcript by using *only* a digital signature could put you and your client in the unenviable position of being the test case. Without statutory authority, a trial court would be justified in determining that a transcript without conventional written certification is inadmissible. Ultimately, an appeal to a state supreme court might reverse the holding, but the extended court battle would be expensive. Because you didn't follow the law, the costs could be passed to you.

Many people from various organizations are working to make the acceptance and legal status of digital signatures clear everywhere. This change will take legislation or the ruling of an appellate court. Although it seems inevitable that digital signatures will soon become as common as signing your name with a pen, in many places, acceptance is not yet the law. ■

What's the Value in Your Digital Signature?

BY SANDY BUNCH VANDERPOL

Can digital signatures add value to your transcripts?

Here is one reporter's story about how her clients embraced digital signatures.

"Do attorneys or the courts need digital signatures?" I asked myself when I made the decision to move forward on digitally signing transcripts. I really wasn't sure whether they wanted them, but I certainly understood that they needed them — especially in paperless cases and paperless

filings. We all know and understand that judicial jurisdictions have and will continue to move forward with e-filings of not only pleadings and motions but also with both court and deposition transcripts.

I certainly wasn't sure if marketing digital signatures on transcripts would bring value to my business but did feel strongly it would add quality to transcript. Quality is defined in this context as superiority of kind, an intellect of unquestioned quality,

Sandy Bunch VanderPol, RMR, CRR, is a freelancer in Lotus, Calif., and a member of NCRA's Technology Evaluation Committee.

or a degree or grade of excellence.

On a personal note, I'd like to share just one anecdotal story of how I've seen value in digital signatures. After promoting paperless discovery on an arbitration case I've been and still am working on, counsel now understand the value of digital signatures, this value being experienced by their whole litigation team, including their experts. It took a great deal of convincing to get one attorney to try something new; however, after trying it for the past year, he's my loudest convert to paperless depositions and digital signatures.

When I first approached counsel to try the paperless deposition discovery process in their arbitration, I explained the process of both digitally and electronically signing their digital transcripts. When I mentioned, in addition to their ASCII file for their litigation support program, they would also be getting a transcript in PDF that would have the authentication process of a digital signature, their eyes opened wide.

No big deal, you say, in states other than California. In California the PDF format is not the standard practice for the digital transcript, but it is the standard format in e-filing documents in our state by litigants. PDF is the legal standard for documents, but for many reasons reporters have not provided transcripts in this format to counsel or courts. I didn't expect this value of the PDF in promoting digital signatures to counsel, the value it added to their clients and their experts. I've learned that my PDF transcript (yes, digitally and electronically signed) gets sent to their clients and their experts and is printed from if they wish to have a full-sized transcript printed. PDF is the exact image of the official digital transcript. They can count on that fact — as long as my digital signature (through my RealLegal or VeriSign accounts — more on that later) indicates validity.

"I've never had a deposition reporter rise to the level you have of ensuring that the digital transcript is authentic," says one counsel involved in the case. Another counsel replied, "Yeah, I like that yellow emblem on the certificate page that tells me it's a valid transcript." Another value I discovered — bringing the highest standard to ensuring the integrity of the digital transcript, adding confidence in my clients' minds that they can rest assured I'll give them what they need.

Education is an important process in promoting digital signatures. Without saying a word, I promote every digitally signed transcript I send via e-mail or delivery via download from our transcript repository. I insert into my e-mail the following language: "To ensure the integrity of the attached digital transcript, it has been digitally signed using my VeriSign Digital Signature authenticity account. My digital signature confirms the authenticity and accuracy of this transcript. If there are any changes made to this transcript, this digital signature becomes invalid." Since many of my clients request an E-transcript, I will also in-

"I certainly wasn't sure if marketing digital signatures on transcripts would bring value to my business but did feel strongly it would add quality to transcript. Quality is defined in this context as superiority of kind, an intellect of unquestioned quality, a degree or grade of excellence."

clude the following language when sending the E-transcript file, "To ensure the integrity of the attached digital transcripts (PDF and PTX), they have been digitally signed using my VeriSign Digital Signature authenticity account and the RealLegal third-party digital signature account. My digital signature confirms the authenticity and accuracy of this transcript. If there are any changes made to this transcript, this digital signature becomes invalid."

Why are digital signatures important to our clients? In summary, digital signatures provide the foundation for proving that our digital transcript is reliable, is usable, and has integrity. This foundation has been based on best business practices

until recently, when Thomson West published "Signed, Sealed, Delivered: A White Paper on Digitally Signed Transcripts" prepared by E. Cristin O'Keeffe. The white paper states, in summary, "We believe that digitally signed and sealed transcripts will become the preferred format for filing with the federal courts and many state courts in the relatively near future." Within this white paper are citations to the Federal Rules of Civil Procedure, the Federal Rules of Evidence, a New York Appellate decision, and an Arizona Supreme Court decision, stating that a digital signature is valid and verifiable. You can get the entire white paper free through the RealLegal Web site by filling out the form at www.reallegal.com/digitalsignatures.asp.

In closing, I remind us all that the reporter's transcript initially concerned the integrity of the paper-based transcript, but today it includes transcripts in digital format. With the digital delivery method of our transcripts, there should be a method of preservation to ensure the identity of the digital signature and the integrity of the transcript. As far as identifying and authenticating the reporter's identity as it relates to the digital transcript, this is easily verified by the digital signature, reflecting the time and place of the signature, as well as third-party authentication in some situations — depending on the software you use to digitally sign. The integrity of the transcript as being complete and unaltered is also verified by the use of the digital signature. This integrity can be confirmed throughout the entire course of the existence of the digital transcript.

When making your decision to move to digital signatures, I hope you consider not only your job as you do it today but consider the future of our profession. After all, a signature on a paper transcript needs to be, at a minimum, equaled on a digital transcript. I submit that it's not only the legal environment that is moving full speed ahead into the digital world; it is every facet of our lives, both personal and professional. Yes, the reporting world is moving full speed ahead into the digital world. What comes after digital signatures for us? That's the challenge of our profession, keep stride with changing technology. ■