8 RULES FOR E-SIGNATURE SECURITY

A complete guide to making sure your e-signature service gives you the security and legal evidence you deserve.

SIGNiX

8 RULES FOR E-SIGNATURE SECURITY

By John B. Harris

John B. Harris joined the SIGNiX team as Director of Product Management in 2012. He focuses on rigorously tying customer needs, industry trends and technology innovations to specific product requirements, while also contributing to SIGNiX's marketing efforts and driving a product strategy that enhances SIGNiX's leadership position.

Most recently, John managed Adobe Systems' broad electronic signature and approval capabilities across a range of client and server-side products, from click-thru approvals to complex digital and certification signatures. He broadened Adobe's digital certificate trust programs in Adobe® Acrobat® and Reader® to include commercial and government certificates from around the world.

Harris also directed efforts to bring Adobe's enterprise power to bear on smartphones and tablets — technologies that have made a profound impact on user experiences in the past few years. Before working at Adobe, Harris spent 10 years managing biometric, encryption and strong authentication products at Sony Electronics and Thomson-CSF.

CONTENTS

WHAT YOU'LL LEARN IN THIS EBOOK

It's no secret that e-signatures are becoming popular across all industries. Electronic signatures can save your business money and make your office more efficient.

But in the rush to adopt e-signature technology, some people don't realize they're making a decision that could affect the security and legal standing of their company's contracts for decades.

If you adopt the wrong e-signature technology, you could be putting yourself, your customers and partners at risk.

In this eBook, we'll address the eight e-signature security rules to follow when you're evaluating e-signature vendors. You'll also learn the answers to questions like:

- What's the difference between a digital signature and an electronic signature?
- How can digital signatures protect documents against fraud?
- What security features should I look for in a vendor?
- What makes an electronic signature legal?

DIGITAL SIGNATURES VS. ELECTRONIC SIGNATURES

Rule 1: You should only use standards-based digital signatures to ensure the best security and legal evidence.

If you've spent any time researching e-signature technology, you've probably heard about a lot of different types of e-signatures. The term "electronic signature" (often shortened to "e-signature") is a blanket term that describes any technology that lets you sign a document online, but there are many sub-categories.

In this chapter, we'll tell you a little bit about the differences between electronic signatures and a specific type of e-signature technology called a "digital signature."

ELECTRONIC SIGNATURES

Electronic signatures have become popular because they allow users to sign documents on the web with a simple click of the mouse. In some products, users can even scan images of their signature or use their fingers to trace their handwritten signatures onto a document.

The simplicity of this signing process, combined with the fact that no software or hardware is required, has drawn significant interest to the technology for its potential to speed up workflows with less cost.

Unfortunately, there are no universal standards for electronic signatures. The technologies to protect a document once it has been signed vary widely, and the legal evidence to support each document is usually stored on the vendor's server instead of within the document.

This can be problematic if a document is challenged in court in the future, raising questions like:

- How do I know the service provider will be around in the future when I need to prove the signature in court?
- What assurance do I have that the service provider will not charge an

outrageous fee when I go to court and I need the service provider to turn over records and testify about how the service worked?

This presents a huge risk for businesses that deal with high-value transactions.

In fact, Forrester Research suggests that a good stress test to evaluate e-signature vendors is to imagine that the vendor disappears and see what evidence you have to support you in court. With most electronic signature vendors, that evidence is sparse at best if the vendor disappeared.

DIGITAL SIGNATURES

Digital signature technology has been used for decades, which means it is highly standardized and accepted. A digital signature essentially links a "fingerprint" of the document at the time of signing with an identity credential (a digital certificate), and the result is permanently embedded into the document.

A digital signature proves no fraud or tampering has taken place. The signature also identifies the signer and can provide other information about the time of signature, which provides significant legal evidence in the event that a document is challenged in court (a feature called "non-repudiation").

VIDEO: CLICK HERE TO SEE HOW DIGITAL SIGNATURES WORK

Because digital signatures are based on industry and international standards, signed documents contain all of the evidence you'd need to prove its authenticity. This means you don't have to rely on a vendor to give you evidence in the future. Digital signatures are also more widely accepted internationally than electronic signatures.

THE DANGERS OF VENDOR LOCK-IN

Rule 2: The integrity of the document and each individual signature should be verified without ever leaving the signed document.

WHAT IS VENDOR LOCK-IN?

You probably know from personal experience that changing from one service provider to another can be tough. Think about the last time you changed your Internet service or cell phone provider. It was probably a pain. Vendors don't want you to have a seamless transition from their product to a competitor's.

But you might not know that some less-scrupulous vendors build roadblocks specifically designed to lock customers into their service. That way, the company can raise their prices or change their policies without worrying too much about losing customers. This is something the technology industry calls "vendor lock-in."

"The problem is, when companies sit down to calculate the cost of using cloud computing services, they don't factor in the costs of migrating off the system — expenses which could be prohibitive and unexpected."

—Forbes

E-SIGNATURE VENDOR LOCK-IN

In the e-signature industry, vendor lock-in is often hidden in the signature verification process, when you go to prove the document is real and hasn't been tampered with.

Instead of embedding signature information into the document, many e-signature vendors' signatures are just an image with a link back to their website for verification.

What happens if you want to switch vendors? What if they go out of business, get acquired or decide to change their technology?

You're putting your company at significant risk if you have to rely on that one company to verify signatures on your documents for the lifetime of the documents themselves, which can sometimes span decades.

SET YOUR DOCUMENTS FREE

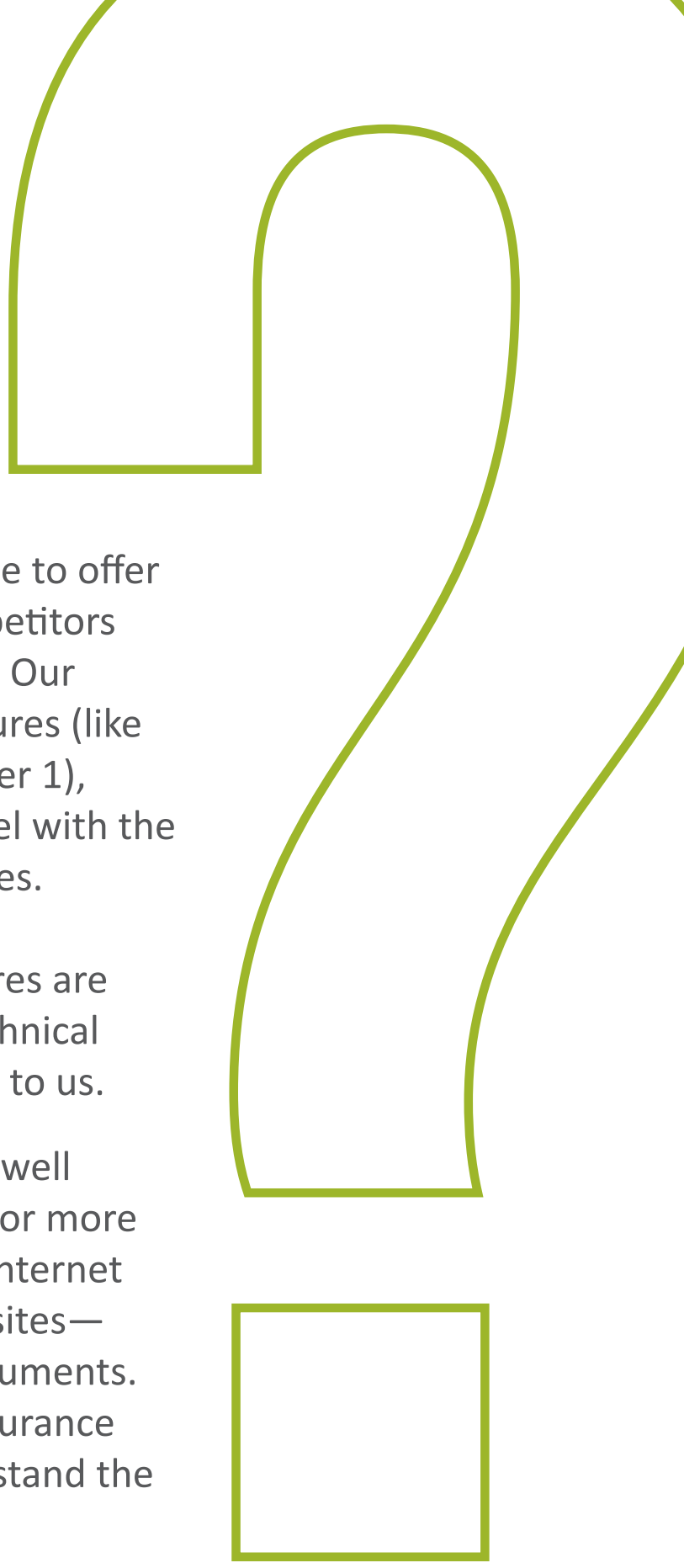
We think locking you into one technology is kind of sneaky. We'd much rather you keep using our service because you like our products, our customer service and the security we provide with our digital signatures.

That's why we offer something we call Vendor Freedom™.

Our digital signatures and their cryptographic information are embedded into each signed document, so you don't need to be a SIGNiX customer (or come back to our website) just to check if your documents are valid.

In fact, you don't even need to be connected to the Internet to verify your signatures!

HOW DO WE DO IT



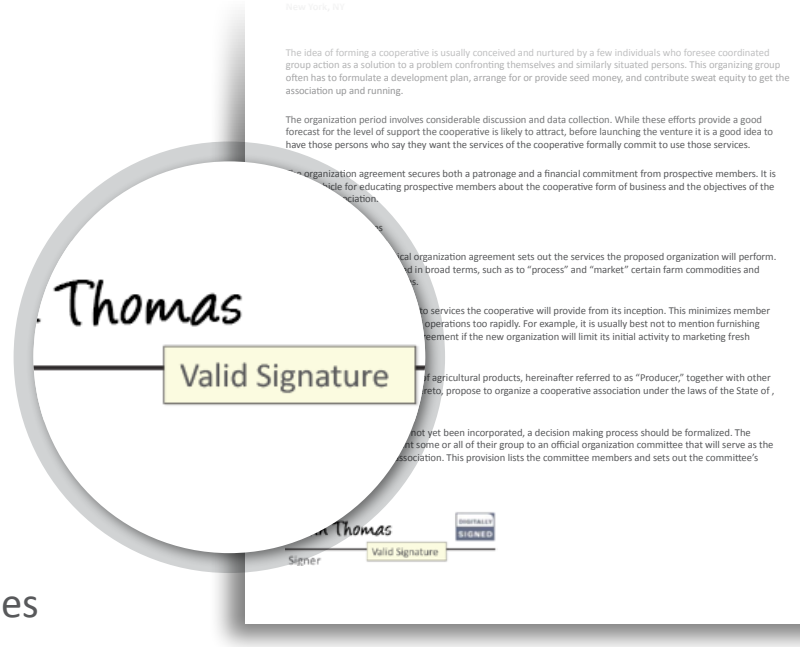
You might wonder how we're able to offer Vendor Freedom when our competitors can't. The key is in the signature! Our signatures are true digital signatures (like the ones we mentioned in Chapter 1), which means the signatures travel with the document no matter where it goes.

This also means that our signatures are based on actual documented technical standards that aren't proprietary to us.

In fact, this technology has been well known in the technology sector for more than 20 years. Every day on the Internet you use it to browse secure websites—we simply apply that to your documents. These standards give you the assurance that this trusted technology will stand the test of time.

Easy Verify™ by SIGNiX

SIGNiX-signed documents can be easily verified using free PDF reader software. There's no need for you to be online. All you have to do is hover over a signature to find out if the signature is valid. To see more information, simply click on the signature to open the Signature Properties dialog box.



This dialog box contains a rich set of information about the signature: the name of the signer, a timestamp of the signature, the nature of the document when it was signed and other technical details.

This is a quick and easy way to know if your documents have been tampered with. SIGNiX's documents also come with a highly detailed audit trail, which we'll tell you about more in Chapter 6.

Ineffective Verification

SIGNiX's digital signatures offer you verification offline and are embedded into the document. Contrast that with most other electronic signature vendors. Instead of including the data you need to prove the document is valid within the document itself, they send customers back to the vendor's own website to retrieve information about the signature.

The signature isn't embedded into the document—in fact, information about the signature is likely stored with the vendor.

And even though the vendor may let a customer download these documents, if there's ever a question about an individual's signature, the lack of information in their audit trails (as addressed in Chapters 6) means the customer always has to come back to the vendor, resulting in vendor lock-in (described earlier in this chapter).

The image below shows the link presented when you hover over a signature created by another vendor. Clicking on it opens a browser window, requiring that a recipient be online to get at any additional information.

Worse, if the vendor's website goes down or the vendor goes out of business, you wouldn't have any evidence to prove that your documents are valid.

STANDARDS-BASED TECHNOLOGY

Rule 3: Signatures must meet international requirements, be timestamped and based on actual, published standards so you can trust and validate signatures at any time in the future.

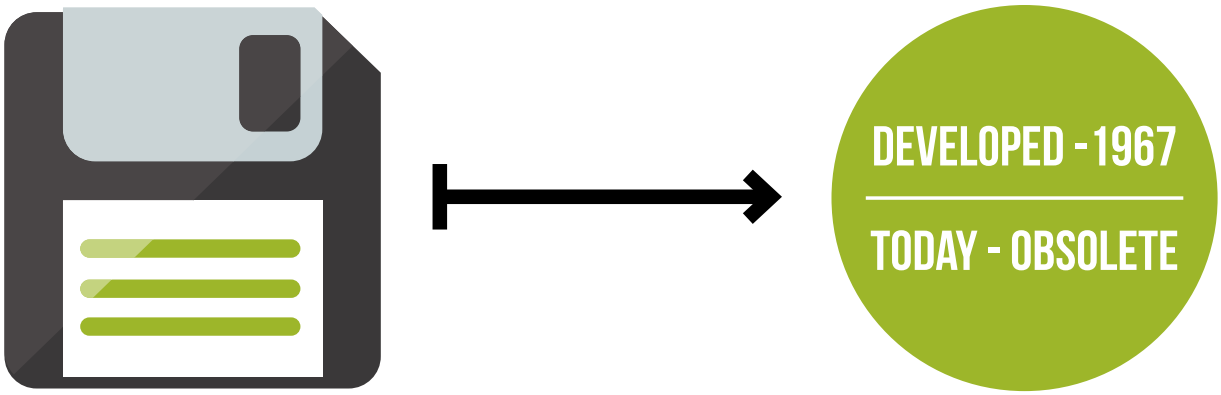
WILL YOUR E-SIGNATURE TECHNOLOGY BE OBSOLETE IN 10 YEARS?

Technology choices you make today could put your business at risk years down the road.

You remember the floppy disk, right? When they were developed back in 1967, it was cutting-edge technology. Before long, every computer had a floppy disk drive, and people couldn't imagine doing business without them.

Today, you'd be hard pressed to find an office that uses floppy disks. No one would even consider storing important information on a floppy disk, and you'd be in trouble if all of your company's documents were stored on floppies.

Compare the floppy disk to a technology that most of us use all the time—maps. Maps have existed for centuries, yet we still use them today. They've become much more advanced over the years (evolving from cave paintings all the way to



GPS smartphone apps), but if you picked up a map from thirty years ago, it would still be valid today (not including new roads, of course). You might need an expert to tell you what you're looking at, but the underlying "technology" that exists today will still be valid in 100 years.

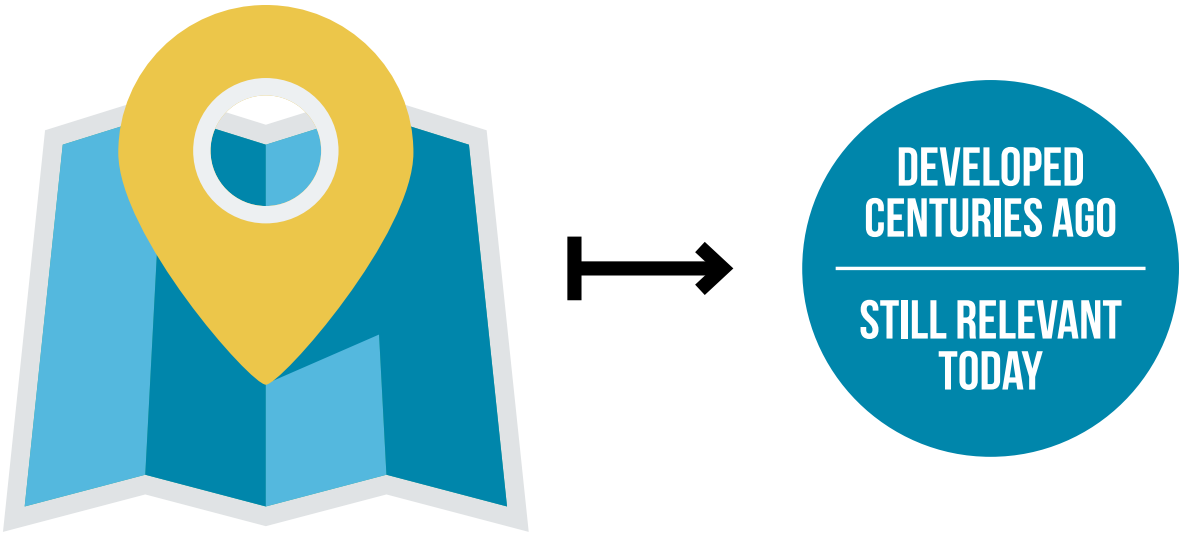
Why are we telling you this? Because if your e-signature technology is proprietary (not based on standards), it will eventually become obsolete, just like the floppy disk. Newer, better technology will take its place. It's just a fact of life. But if you use technology that's based on established standards, your signatures will still be readable and valid in 100 years—just like a map.

Only a select few e-signature vendors make sure your signed documents will be valid forever (though most will try to convince you they make the cut).

At SIGNiX, our signatures are based on documented technical standards that aren't proprietary to us. These standards have been well known in the technology sector for more than 20 years.

Our digital signatures and their cryptographic information are embedded into your signed documents, so you don't need to be a SIGNiX customer, or visit our website, just to check if they are valid. In fact, you don't even need to be connected to the Internet to verify your signatures!

With SIGNiX, each signature can be verified with any free PDF reader software. This software can read digital signatures (because they're based on standards) and let you know whether someone has tampered with your documents. You don't even have to be an IT expert to



see if documents have been altered. The software will show you a green checkmark if the document is valid or a red X or yellow exclamation mark if it has been altered.

E-signature vendors that don't use digital signature standards can't promise that your documents can be verified without their help. Instead of embedding the signatures into each document, they only give you a link to their website to try to prove if it's been tampered with. The link opens a new window and either shows you a version of your document that's stored on their servers or a web page with limited information about the transaction. Worst of all, some vendors only link to a generic page that gives you no information whatsoever about the signed document.

If their technology changes or they go out of business, your documents will be obsolete, just like a floppy disk.

Don't believe us? Try to verify one of "the other guys'" documents without an Internet connection. You'll be left with a "page not found" error. You can bet a judge and jury won't be convinced by an error message. If one of your signed documents can't be verified, it might be deemed inadmissible in court.

We can't overstate how important this issue is. Every document you receive signed with proprietary e-signature technology puts your company at more and more risk. Choose a standards-based digital signature product to protect your documents from the risk of becoming obsolete.

TAMPER EVIDENCE

Rule 4: To prevent tampering and fraud, any change in a document must trigger the document viewer to notify you of the change in real-time.

WHAT IS TAMPER EVIDENCE?

An electronic signature is only as good as the security that protects it. After all, what good is a contract if someone can easily change the terms after it's been signed?

That's why some electronic signature services offer a feature called "tamper evidence." If someone tries to change any part of the document (even something as simple as deleting a space or capitalizing a word), there's proof that changes took place.

However, these vendors may also apply that tamper-evident seal at some time *after* the document was actually signed, which means the tamper-evidence has nothing to do with the actual signatures.

With SIGNiX's digital signatures, documents are tamper-evident not just at the end of the signing process, but from the moment the transaction is created because each signature and initial includes a tamper-evident seal at the time of signing. This provides evidence that the first signer didn't alter the document before it was sent to the second signer. Pretty neat, right?

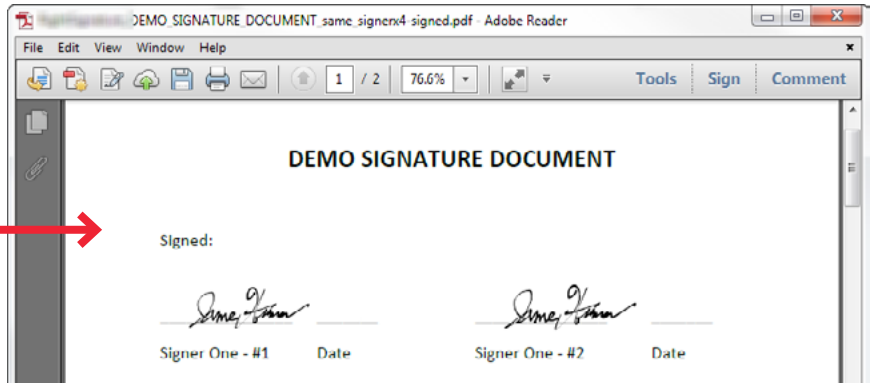
If you're dealing with important documents or high-value transactions, advanced tamper evidence is vital. In fact, many banks and credit unions require this kind of tamper evidence to protect their customers.

INEFFECTIVE TAMPER EVIDENCE

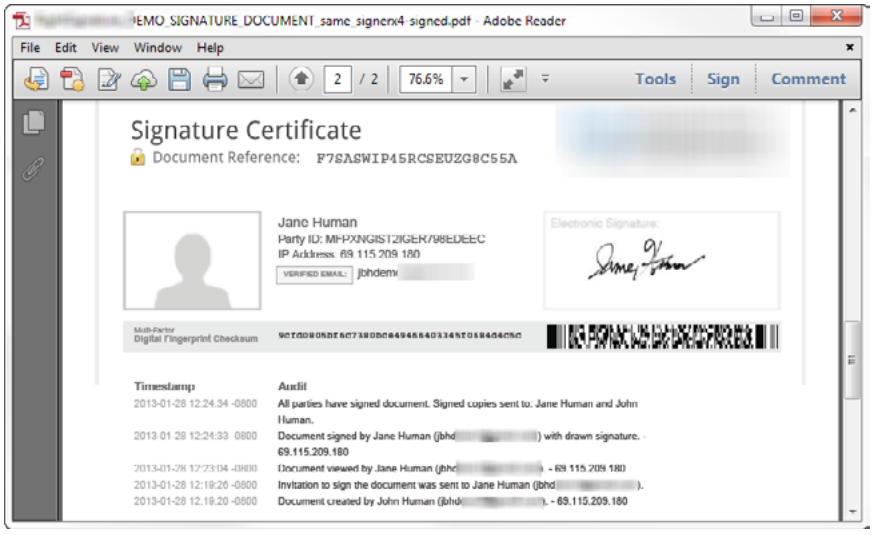
First we'll look at an example of what not to do when it comes to tamper evidence. In these screenshots, a document has been signed twice by a single person using another e-signature vendor's service. The first screen shows the signatures, but since there's no tamper-evidence applied to the document, there are no green checkmarks or any security feature or control on the document itself.

The second image contains all manner of seemingly secure elements including bar codes, 'checksums,' and a high-level audit trail (we'll talk about this more later), and thus seems to be protected from changes—but not everything is what it seems.

ORIGINAL SIGNED DOCUMENT



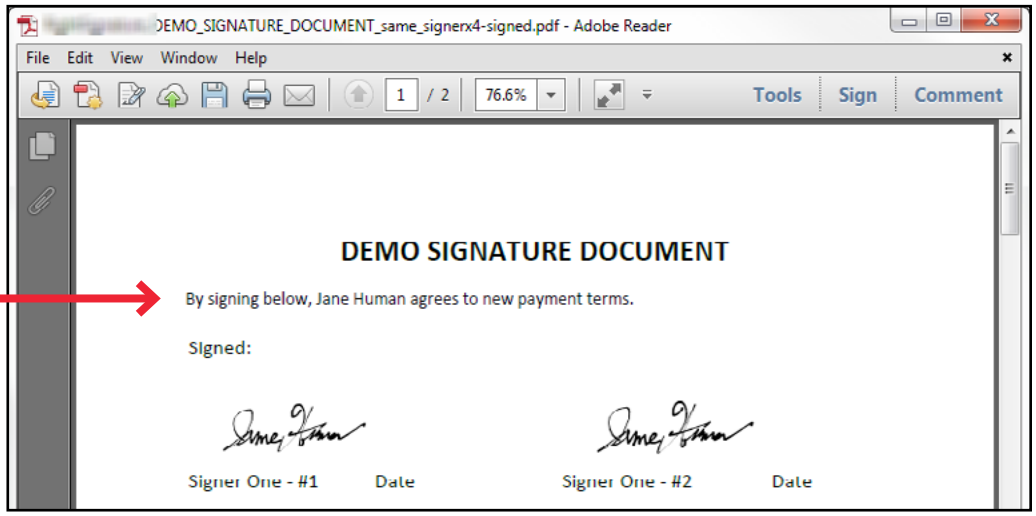
ORIGINAL AUDIT TRAIL



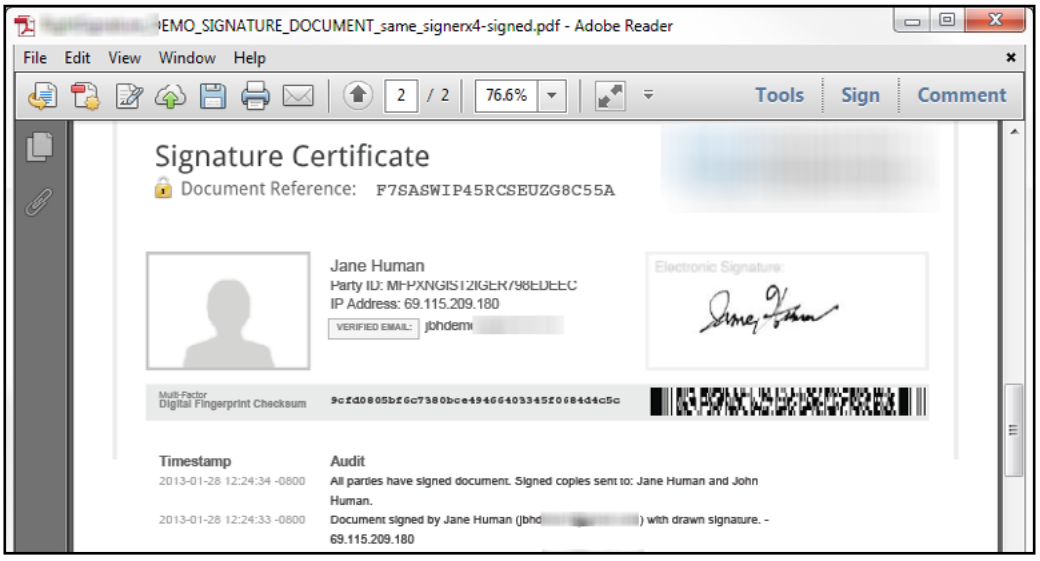
What happens to the document after a line of text is added to the PDF using tools provided by the PDF viewer itself? The images below show the results. Other than the additional line of text, there is no real-time indication that the document has changed considerably. Everything else remains exactly the same.

The security features touted by this vendor require the document recipient to take an active role in verifying the document. There is no information stored within the document to show a change was made—that information must be requested from the vendor, which assumes the vendor is still in business and won't charge you to access this information.

ADDED TEXT AGREES TO CHANGED TERMS



AUDIT TRAIL LOOKS EXACTLY THE SAME!



SECURE TAMPER EVIDENCE IN ACTION

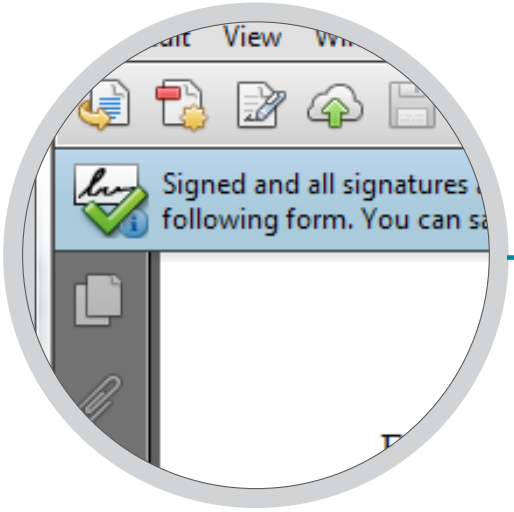
Compare that type of ineffective tamper evidence to the tamper safeguards provided by SIGNiX's digital signatures (which you can see in action on the next page).

As you can clearly see, any change in a document signed by SIGNiX will trigger the PDF viewer to notify you of the change, in real-time. They are embedded directly into the PDF and are available at any time, offline or online.

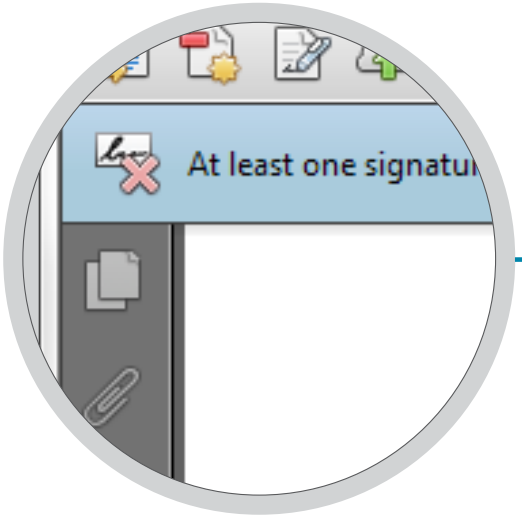
These layers of tamper evidence aren't always present in other e-signature solutions. Some don't even render their e-signed documents tamper evident, as we showed previously, making it possible for fraudsters to take a signed document, change the terms and try to pass off the altered version as the original.

Other e-signature vendors often use a different signature technology to tamper seal a document than is used to sign the document.

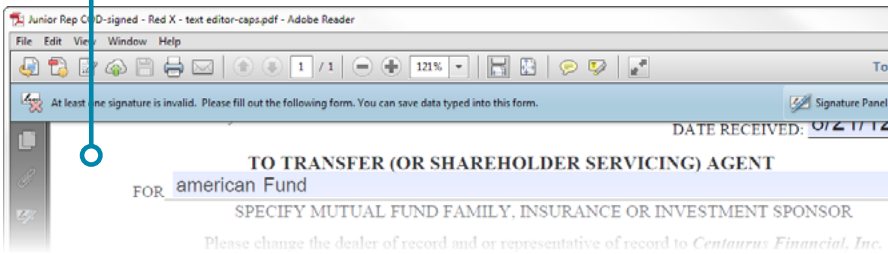
Moreover, they apply this seal only after each party has signed. Not only does this make it difficult to know if a document was altered in-transit, it can also produce inconsistencies in evidence, which we'll talk more about in Chapter 6.



This image shows an original, valid document signed with SIGNiX. The green checkmark clearly shows the integrity of the document.



Changing the capitalization of the word ‘American’ causes the validity status to change to a red X icon.



HOW TO MITIGATE LEGAL RISKS

Rule 5: Signed documents must meet or exceed the six criteria set by the American Bar Association.

ARE ELECTRONIC SIGNATURES LEGAL?

Laws in the United States are pretty broad about what counts as a legal electronic signature. But just because a technology is considered legal doesn't necessarily mean it will have enough evidence to stand up if it's challenged in court.

Luckily, you're not on your own to figure out if an electronic signature service meets your legal needs. The American Bar Association (ABA) had 70 lawyers spend four years developing a document called the Digital Signature Guidelines[1].

Here are six questions your e-signature vendor should be able to answer, based on the ABA guidelines.

1 DO I KNOW WHO SIGNED THE DOCUMENT?

Electronic signature services provide a variety of identity authentication options that can be tailored to fit the risk of the transaction. You can learn more about authentication options in Chapter 7.

> "The SIGNiX platform establishes a trustworthy process for binding the identity of an individual to a digital signature. This is crucially important."
>
> — **Timothy Reiniger**, a member of the Electronic Discovery and Digital Evidence Committee of the American Bar Association

1. http://www.signelec.com/content/download/digital_signature_guidelines.pdf

2 DO I KNOW THEY MEANT TO SIGN THE DOCUMENT?

> "The affixing of the signature should be an affirmative act which serves the ceremonial and approval functions of a signature and establishes the sense of having legally consummated a transaction."
>
> — Digital Signature Guidelines of the American Bar Association

The e-signature service must be able to prove the signer meant to sign the document. At SIGNiX, we require signers to enter their signing PIN for each signature and initial to clearly establish this intent to sign.

3 HAS THERE BEEN PROPER DISCLOSURE AND CONSENT?

It is critical that any electronic signature system be compliant with all requirements for consent for electronic delivery of documents as well as review and/or approval of necessary disclosures.

At SIGNiX, you can customize our standard disclosure language to meet your unique legal and compliance requirements. Our process also requires defined steps like a review or approval of necessary documents to be completed before allowing a signature to be applied, and this consent is recorded in the document's audit trail.

4 HAS THE DOCUMENT BEEN ALTERED?

The e-signature service must be able to prove the document hasn't been altered. See Chapter 4 to learn more about tamper evidence.

SIGNiX's solution includes technology — hashing, encryption and public key cryptography — to make it virtually impossible for a document to be altered without detection once the digital signature has been applied.

5 IS THE DOCUMENT ACCESSIBLE TO ALL SIGNERS?

Regulations and industries may require documents to be valid for many years. SIGNiX provides a verifiable version of the signed document and audit trail to customers and signers for storage, under their own best practices. SIGNiX can also provide permanent online access to documents for all individuals who have signed the document or have been given review rights.

Finally, SIGNiX-signed documents are rendered using the international standard PDF format, meaning documents will be accessible for many years to come.

6 CAN I PROVE THAT THE SIGNATURE FOLLOWS ALL OF THESE RULES?

A detailed audit trail of an electronic transaction, including facts like the time and date of each relevant activity, gives details that paper transactions can't provide. SIGNiX timestamps each signature and tracks all aspects of the electronic signing process. SIGNiX provides independent verification of all aspects necessary for non-repudiation of the transaction.

THE ANATOMY OF A COMPLETE AUDIT TRAIL

Rule 6: The system should have a robust and highly detailed way of tracking each and every signature as well as all other steps in the signing process with no inconsistencies.

THE IMPORTANCE OF AN AUDIT TRAIL

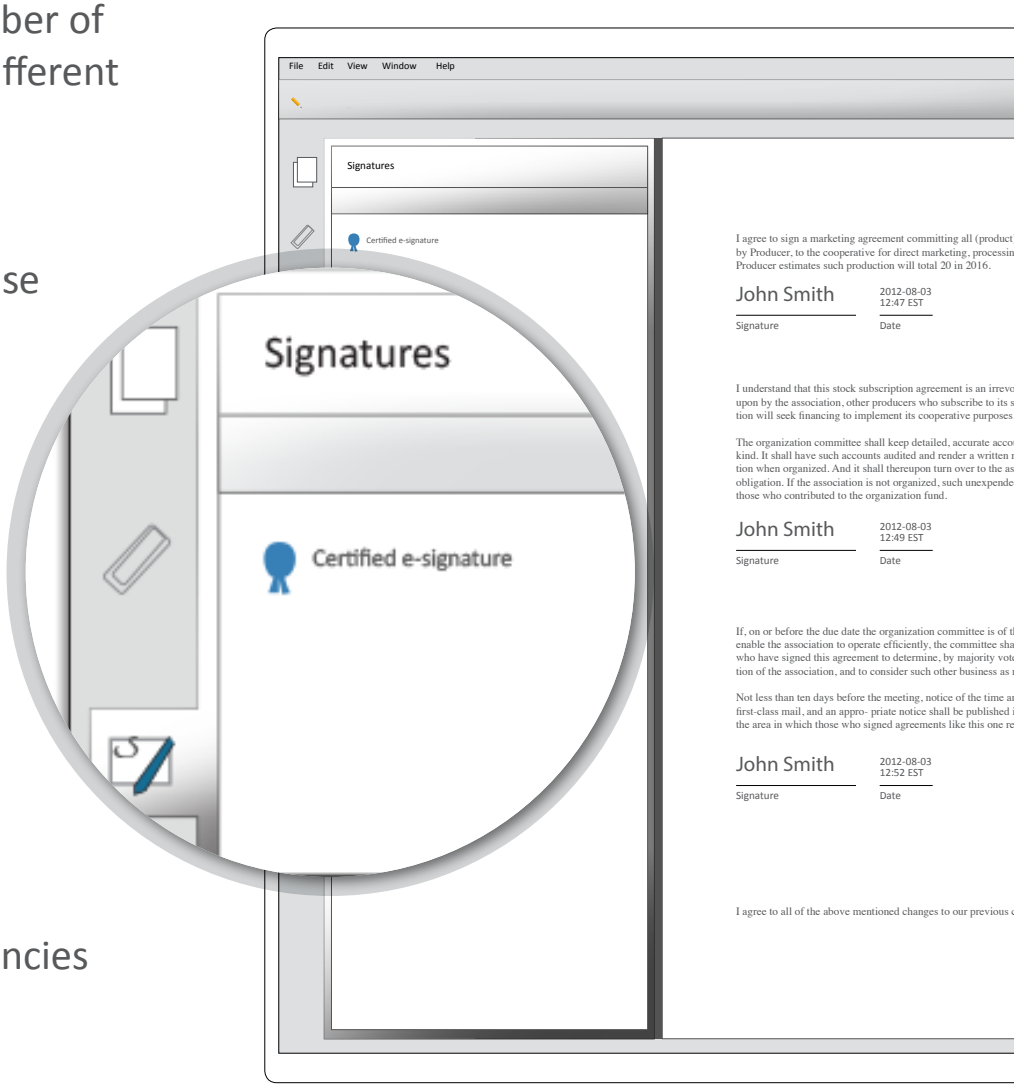
Some people are reluctant to use e-signature technology because they're afraid that signatures created online aren't legal. The truth is that e-signatures are just as legally binding as handwritten signatures. But that doesn't mean that all e-signature products are on an equal footing if a signature is challenged in court.

When someone claims "I didn't sign that," you need to know that your e-signature vendor has your back. Most e-signature companies use audit trails (sometimes also called an audit log or a certificate of completion) to track the steps of the signature process. The audit trail is a powerful tool that can prove who signed a document and when they signed it.

But some e-signature companies don't think it's important to log every event that happens to your documents. These audit trails don't tell the whole story of the life of your document. This lack of detail can put you at risk if your document comes under legal scrutiny.

INCONSISTENT AUDIT TRAILS

Take a look at the screenshot to the right. You'll notice that there are three signatures and an initial on the document, but there's only one signature in the signature panel. This can be confusing because the number of signatures represented is different depending where you look.



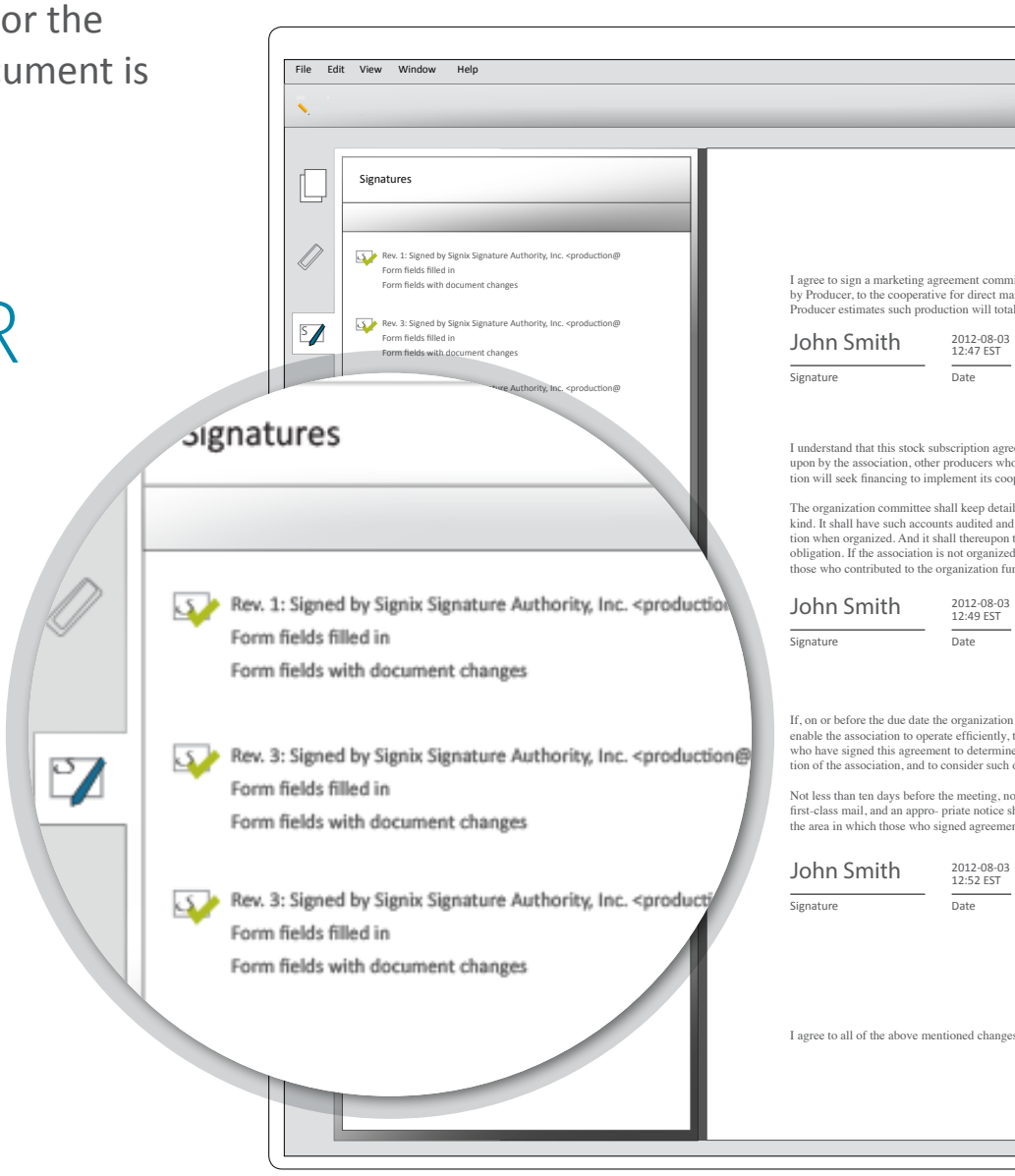
Why does this happen? E-signature vendors often use a different technology to tamper seal a document than is used to sign the document (as discussed in Chapter 4). They apply this seal only after everyone has signed. Not only does this make it difficult to find out if a document has been tampered with in transit, it also can produce inconsistencies in evidence.

You could have a document that contains 20 signatures, but the signature panel shown above would only display one signature.

This inconsistent evidence can be confusing both for the document's owner and for a court if the document is ever challenged. Does this represent only the last signature? Where did the other signatures go? What happens if the signer claims she signed signatures 1 and 2 but never signed signature 3? There's no separate evidence attached to the document or the audit trail to prove the document is genuine and tamper-free.

A SUPERIOR AUDIT TRAIL

Compare that with the consistency produced by SIGNiX's Total Audit™. There are three digital signatures on the document and three signatures represented in the signatures panel on the left.



HIGHLY DETAILED AUDIT TRAILS GIVE YOU THE BEST LEGAL DEFENSE

When it comes to electronic evidence, it's always best to have as much information to deal with as possible. That means that if an electronically signed document needs to stand up to scrutiny in today's courtrooms, it must also track and store all of the steps of the signature process, from set-up through signature to final document delivery.

Not only does this allow users to clearly track where any document is at a given time in a transaction, but having this detailed information on hand also means that companies can better defend against claims like, "I didn't sign that."

Most electronic signature services capture some sort of event history while a signature process is in motion, but the level of detail captured and stored can vary quite dramatically, sometimes barely providing enough detail to reconstruct the process at all. Some services simply append this information to the document, where it could be altered, or fail to include key data points, providing an opening for an attorney to create doubt about the transaction's authenticity.

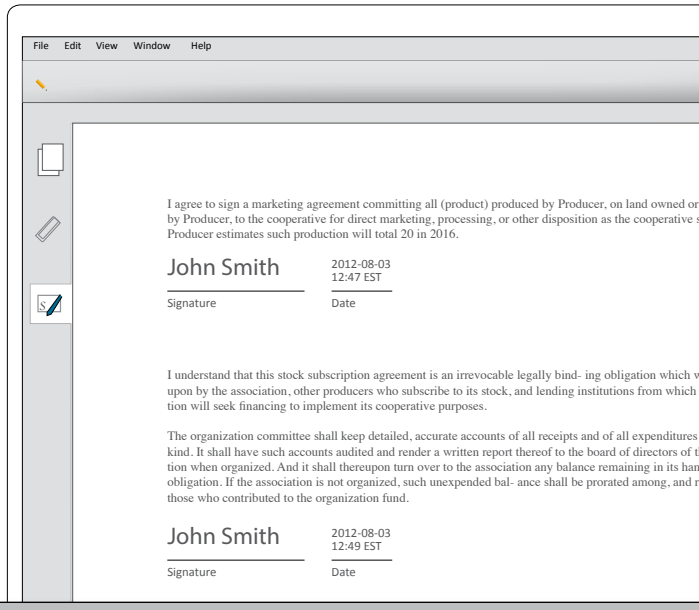
SIGNiX logs an extraordinary amount of detail about each transaction, using a feature called TotalAudit. This goes far beyond what many of other e-signature services choose to provide.

When we compare this wealth of features and granularity to other e-signature vendors, significant differences become apparent.

INCOMPLETE AUDIT TRAILS

Some e-signature vendors simplify the audit trail to such an extent that individual signatures are not listed on the audit trail, but instead a 'signing event' is listed which apparently consolidates all of the user's signatures in one line.

Let's see what this looks like in practice. Here, we're using the same document and vendor we used in the example mentioned in Chapter 6, with three signatures and one initial from John Smith. Next to that, you'll see the audit trail provided by the e-signature vendor.



Notice that the individual signatures are not listed in the audit trail (consistency issues like those mentioned in Chapter 6). If someone claims they didn't sign three signatures, there would be no legal evidence to prove otherwise.

Instead of the highly detailed metadata provided by the SIGNiX audit trail, this vendor provides only one line of information, including the time and date for when the transaction was started, who it was emailed to, when that

person looked at it, when it was 'signed,' and when the finished document was sent to the recipients.

Signatures are typically challenged at the signature level, not at the document or transaction level. Arguments revolve around a person alleging they did not sign off on a particular term of a contract or particular section, rather than the entire thing. If the evidence for these signatures is not in the audit trail, imagine how difficult it will be to prove that signature took place.

COMPREHENSIVE AUDIT TRAIL

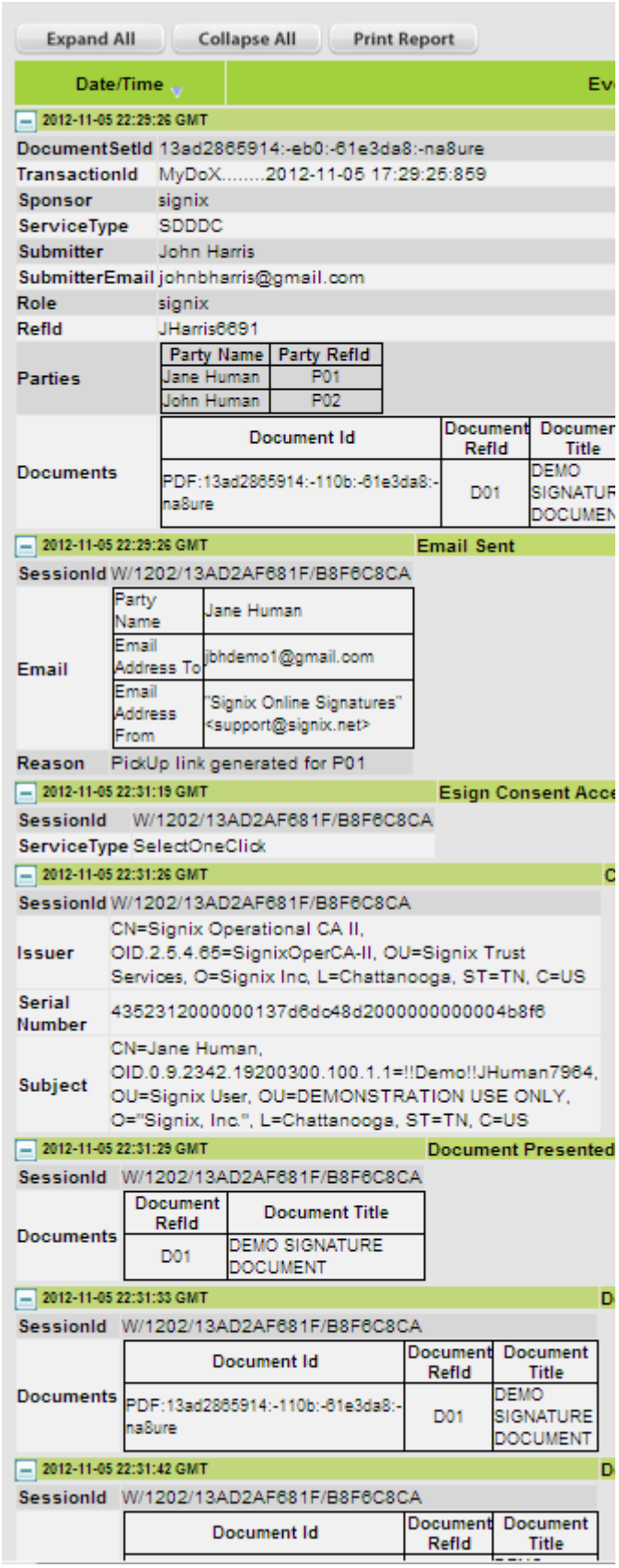
Compare that to the wealth of information provided by SIGNiX's TotalAudit. This feature logs all of the following information:

- Transaction creation
- Emails and notifications sent to any signer
- Signers consent to use e-signatures
- User authentication
- Documents viewed by each signer
- Signature creation (by each signer)
- Party agreement to/ acknowledgment of document
- Transaction completion
- Document downloads after signing
- Cancellations and opt outs
- Changed party information

By clicking on the plus sign beside each action, you can see a lot more information about the nature of the signing credential (and associated x.509 digital certificate).

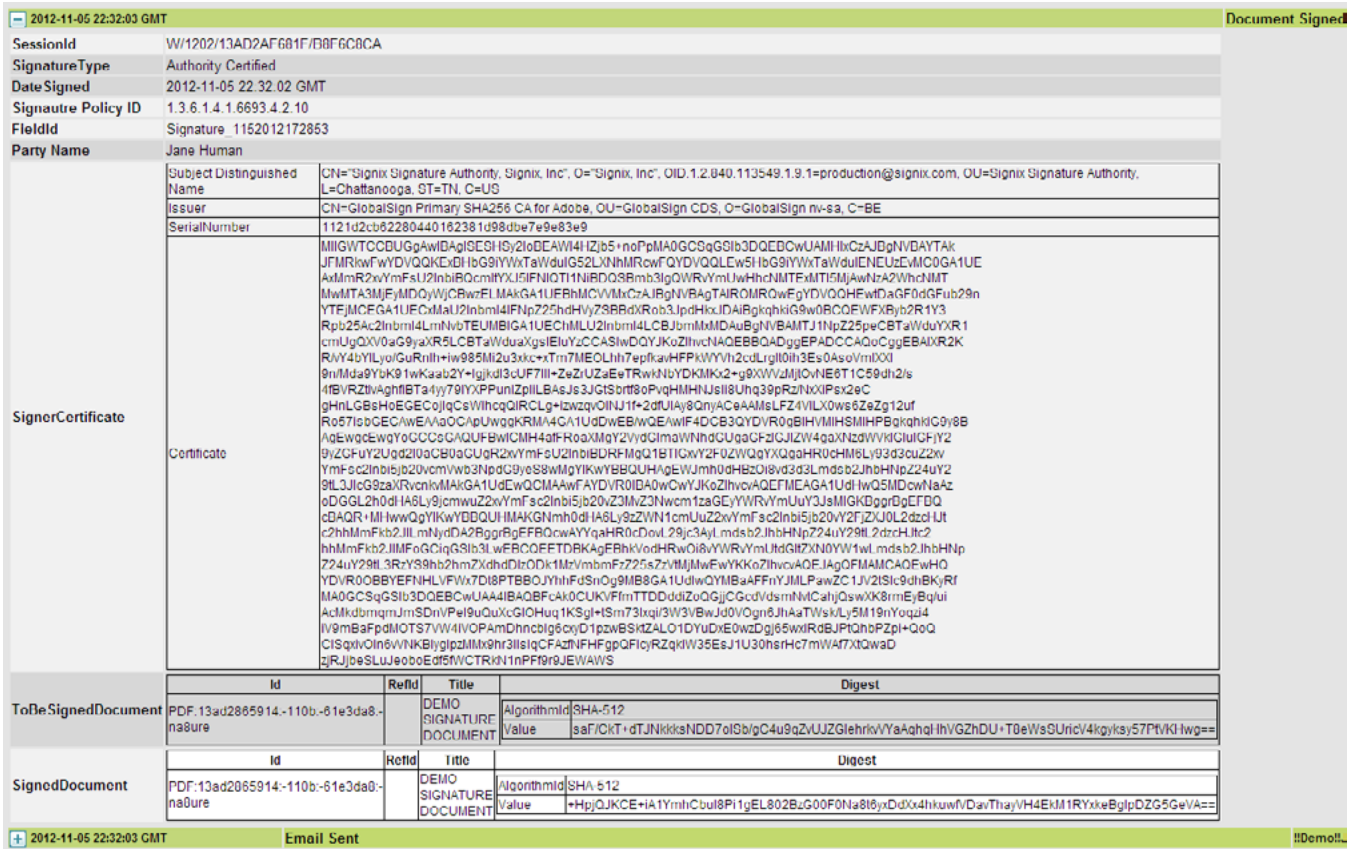
While this might look like gibberish to many people, a technical expert can easily read this information to verify every step in the document's lifecycle.

Since we use published cryptography and document standards to apply digital signatures to PDFs, this information (known variably as a message digest, hash or fingerprint) provides experts with the specific details needed to verify documents at any point in the transaction.



SIGNiX stores a digitally signed XML version of each audit trail (which can be fed into custom reporting solutions) and also makes them available to users in HTML and PDF formats. The information shown can be directly accessed from the transaction status tab in the MyDoX Document Center by clicking on View History.

Legal precedent over the past ten years has shown that insufficient evidence regarding the signature process and the integrity and custodianship of electronic documents can prompt the court to overturn signed agreements. And as time passes, the bar that electronic evidence has to meet will only rise.



2012-11-05 22:32:03 GMT					Document Signed
SessionId	W/1202/13AD2AF681F/D8F6C8CA				
SignatureType	Authority Certified				
DateSigned	2012-11-05 22:32:02 GMT				
Signautre Policy ID	1.3.6.1.4.1.6693.4.2.10				
FieldId	Signature_1152012172853				
Party Name	Jane Human				
SignerCertificate	Subject Distinguished Name	CN="Signix Signature Authority, Signix, Inc", O="Signix, Inc", OID.1.2.840.113549.1.9.1=production@signix.com, OU=Signix Signature Authority, L=Chattanooga, ST=TN, C=US			
	Issuer	CN=GlobalSign Primary SHA256 CA for Adobe, OU=GlobalSign CDS, O=GlobalSign nv-sa, C=BE			
	SerialNumber	1121d2cb62280440162381d98dbe7e9e83e9			
	Certificate	MIIGWTCCBUGgAwIBAgISESHG/y2IoDCAWI4HIZjb5+noPpMA0GCSqGSIb3DQEDCwUAMHIxCzAJBgNVBAYTAk JFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMRcwFQYDVQQLEw5HbG9iYWxTaWduIENEUzEvMC0GA1UE AxMmR2xvYmFsU2InbiBQcmltYXJ5IFNIQTI1NiBDQSBmb3IgQWRvYmUwHhcNMTExMTI5MjAwNzA2WhcNMT MwMTA3MjFyMDQyWjCBwzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAlROMRQwEgYDVQQHEwtDaGF0dGFub29n YTEjMCEGA1UEChMaU2lnbml4IFNpZ25hdHVyZSBRdXRob3JpdHkxIDAiBgkqhkiG9w0BCQEWFXByb2R1Y3 Rpb25Ac2lnbml4LmNvbTEUMBIGA1UEChMLU2lnbml4LCBJbmMxMDAuBgNVBAMTJ1NpZ25peCBTaWduYXR1 cmUgQXV0aG9yaXR5LCBTaWduaXgsIEluYzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIXR2K RAY4bYILyofGuRnlh+iw985Mi2u3xkc+xTm7MEOLhh7epfkavHFPkWYVh2cdLrgIt0ih3Es0AsoVmIXXI 9n/Mda9YbK91wKaab2Y+tgjkdI3cUF7III+ZeZrUZaEeTRwkNbYDKMKx2+g9XWVzMjtOvNE6T1C59dh2/s 4fBVRZtlvAghfIBTa4yy79IYXPPunIZpIILBAsJs3JGtSbrtf8oPvqHMHNJsII8Uhq39pRz/NXXIPsx2eC gHnLGBsHoEGECojIqCsWIhcqQIRCLg+lzwzqvOlNJ1f+2dfUIAy8QnyACeAAMsLFZ4VILX0ws6ZeZg12uf Ro57IcbCECAwEAAaOCApUwggKRMA4GA1UdDwEB/wQEAwIF4DCB3QYDVR0gBIHVMIHSMIHPBgkqhkiG9y8B AqEwgcEwgY0GCCsGAQUFBwICMH4afFRoaXMgY2VydGlmaWNhdGUgaGFzIGJlZW4gaXNzdWVkIGluIGFjY2 9yZGFuY2Ugd2l0aCBUaGUgR2xvYmFsU2lnbiBDRFMgQ1BTIGxvY2F0ZWQgYXQgaHR0cHM6Ly93d3cuZ2xv YmFsc2lnbi5jb20vcmVwb3NpdG9yeS8wMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY2 9tL3JlcG9zaXRvcnkvMAkGA1UdEwQCMAAwFAYDVR0lBA0wCwYJKoZIhvcvAQEFMEAGA1UdHwQ5MDcwNaAz oDGGL2h0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvZ3Nwcm1zaGEyYWRvYmUuY3JsMIGKBggrBgEFBQ cDAQR+MHwwQgYIKwYBBQUHMAKGNmh0dHA6Ly9zZWN1cmUuZ2xvYmFsc2lnbi5jb20vY2FjZXJ0L2dzcHJt c2hhMmFkb2.IlLmNydDA2BggrBgEFBQcwAYYqaHR0cDovL29jc3AyLmdsb2.IhbHNpZ24uY29tL2dzcHJtc2 hhMmFkb2.IlMFoGCiqGSIb3LwEBCQEFTDBKAgEBhkVodHRwOi8vWRvYmUtdGlfZN0YW1wL.mdsb2.IhbHNp Z24uY29tL3RzYS9hb2hmZXdhdDlzODk1MzVmbmFz725sZzVtMjMwEwYKKoZIhvcvAQEJAgQFMAMCAQEwHQ YDVR0OBBYEFNHLVFWx7Dt8PTBBOJYhhFdSnOg9MB8GA1UdIwQYMBaAFFnYJMLPawZC1JV2tSlc9dhBKyRf MA0GCSqGSIb3DQEBCwUAA4IBAQBFcAk0CUKVFfmTTDDddiZoQGjjCGcdVdsrmNvCahjQswXK8rmEyBq/ui AcMkdbrnqmJmSDnVPel9uQuXcGlOHuq1KSgI+tSm73Ixqi/3W3VBwJd0VOgn6JhAaTWsk/Ly5M19nYoqzi4 lV9mBaFpdMOTS7VW4IVOPAmDhncbIg6cxyD1pzwBSktZALO1DYuDxE0wzDgj65wxlRdBJPtQhbPZpI+QoQ CISqxlvOln6vVNKBlygIpzMMx9hr3IlsIqCFAzfNFHFgpQFlcyRZqklW35EsJ1U30hsrHc7mW4f7XtQwaD zjRJjbeSLuJeoboEdf5fWCTRkN1nPFt9r9JEWAWS				
ToBeSignedDocument	Id	PDF.13ad2865914.-110b.-61e3da8.-na8ure	RefId		
	Title	DEMO SIGNATURE DOCUMENT			
	Digest	AlgorithmId	SHA-512		
		Value	saF/CkT+dTJNkkksNDD7olSb/gC4u9qZvUJZGlehrkvVYaAqhqIihVGZhDU+T0eWsSUricV4kgyksy57PfVKl+wg==		
SignedDocument	Id	PDF.13ad2865914.-110b.-61e3da8.-na8ure	RefId		
	Title	DEMO SIGNATURE DOCUMENT			
	Digest	AlgorithmId	SHA-512		
		Value	+HpjOJKCE+iA1YmhCbuI8Pi1gEL802BzG00F0Na8t6yxDdXx4hkuwfvDavThayVH4EkM1RYxkeBgIpDZG5GeVA==		
2012-11-05 22:32:03 GMT	Email Sent				!!Demo!!..

KNOW YOUR SIGNER'S IDENTITY

Rule 7: Electronic signature vendors should offer a range of identity authentication options to verify signers' identities.

When it comes to doing business online, it's important to understand who you are doing business with. Face-to-face, you can rely on physical identification. But in remote situations, you can't typically fall back on these tried and true ways of authenticating signers.

This is where understanding risks comes into play. There may be some transactions that present little risk to an organization and others where the stakes are higher, depending on the value of a contract or the type of information being agreed to.

At SIGNiX, we know that not all of your documents come with the same amount of risk, which is why we offer a variety of ways to prove your signers' identities. In fact, our customers can assign different authentication methods to each party in the same transaction.

Here are the five authentication methods you can choose from:

1. BASIC, EMAIL-ONLY AUTHENTICATION

Description: Proves a user has access to a specific email address

Use Case: Limited situations, when level of risk is very low or in combination with other methods

In Operation: A user is sent an email with a link to the transaction. If the user receives the email and clicks on the link, SIGNiX considers the user 'authenticated,' and the transaction continues.

2. SUPPLIED QUESTIONS

Description: Leverages information known by the customer about the end user, including account number or other information not widely known outside the relationship between customer and end user

Use Case: Typically used alongside other authentication models to add additional strength

In Operation: An email gives the signer a link to the transaction. Once the signer consents to use e-signatures, they're asked to answer to questions generated by the customer, which could be shared secrets. If the user successfully answers the challenge questions, SIGNiX considers the user "authenticated," and the transaction continues.

3. SPONSORED / PASS-THRU

Description: Leverages authentication provided by an integrated partner's system

Use Case: Typical for integrated models where customer or partner already has trusted authentication models in place and prefers to rely on them based on desired user experience

In Operation: A user may or may not be sent an email with a link to the transaction, depending on the integration. Instead SIGNiX's client or partner authenticates the user within their own system, according to their own best practices. If the authentication is successful, SIGNiX will grant access to the transaction. In this model, the client/partner assumes responsibility for the authentication of the user.

4. SMS / TEXT MESSAGE ONE-TIME PASSWORD

Description: Sends a text message with a one-time password to a user's mobile phone to prove the signer has access to an email address and a specific cell phone number

Use Case: For customers looking for an inexpensive, convenient multifactor authentication with a low burden on the end user

In Operation: An email gives the signer a link to the transaction. Once the signer consents to use e-signatures, SIGNiX sends them a text message containing a random, one-time password. If the user enters the text message code correctly, SIGNiX considers the user "authenticated," and the transaction continues.

5. KNOWLEDGE-BASED AUTHENTICATION (KBA)

Description: Asks the user very specific questions about past residences, possessions and transactions based on 30 years of public databases to prove that a user possesses significantly privileged information

Use Case: This is the highest form of remote authentication available, and it's best for transactions where the identity of the signer must be abundantly clear, including loan documents, high value trades, tax returns or real estate closings

In Operation: An email gives the signer a link to the transaction. Once the user consents to use e-signatures, the user is first prompted for the last four digits of their social security number and date of birth. If they answer correctly, they're prompted with a set of four multiple choice questions. If the signer successfully answers the questions as outlined above, SIGNiX considers the user "authenticated," and the transaction continues.

THE SIGNIX ADVANTAGE

Rule 8: Pick SIGNiX to get the best document security and legal evidence (OK, this one is more of a guideline than a rule).

At SIGNiX, we pride ourselves in combining convenience with best-in-class security. In addition to the capabilities we've outlined throughout this eBook, we exclusively offer key benefits that can't be found with other e-signature vendors.

FLEXIBLE DOCUMENT STORAGE

Many firms prefer to store confidential client documents on their own servers, and SIGNiX's exclusive Flex Storage™ technology gives you this option since the necessary legal evidence is embedded in every document.

With Flex Storage, you can decide whether you want to store documents on our highly secure servers or within your own secured document management systems. All digital signatures and their validation information travel with the document and aren't inherently tied to the SIGNiX website.

At the end of the signing process, SIGNiX can give you the signed documents as well as the highly detailed audit trail (as mentioned in Chapter 6). These two elements comprise everything you would need to defend the legality of the signatures and agreements; there's no need to come back to us to collect additional information or verify signatures.

By allowing you to store these documents and their related event histories, SIGNiX gives you the opportunity to leverage and observe your own secure data policies. This also helps reduce privacy and other risks that often rise with third party storage of information. In fact, at the customer's request, we can electronically shred signed documents according to the latest Department of Defense specifications with no loss of legal evidence.

Other e-signature vendors either require you to check back with them to verify a signature (even if you've downloaded the signed document) or they provide inferior data in their audit trails, practically demanding that you return later to ask for additional information should the documents come into question.

SECURE ARCHITECTURE

At SIGNiX, we've always used true digital signatures since our inception ten years ago. We chose this technology because it recognized a key truth in business technology—sometimes you need to be both convenient and secure, not just one or the other.

SIGNiX combines the ease-of-use of a traditional e-signature

service (no software/hardware to install, all accessible via web browser) with the security and legal evidence provided by digital signatures.

SIGNiX applies a standards-based digital signature for each and every signature and initial on the document. This provides substantial legal evidence compared to competing technologies offered by other e-signature vendors.

The integrity of the document and each individual signature can be verified and information retrieved without ever leaving the signed document. The digital signatures we use are embedded directly into the PDF and available at any time.

SIGNiX's MyDoX™ and EnterpriseDoX™ products operate entirely via a Software-as-a-Service (SaaS) model, meaning you don't need to worry about installing software or managing hardware.

In the last few years, consumers have become comfortable with cloud-based services—just look at the success of services like Gmail, Spotify and Facebook. Likewise, enterprises have truly embraced the cloud due to the resulting cost savings, scalability, and improved security.

SECURE HOSTING

SIGNiX meets hosting provider meets the highly secure requirements of SSAE 16, the follow-on to the popular SAS 70 audit, which features a complex reporting matrix of physical, logical and personnel controls designed to protect the confidentiality and integrity of the information contained within the datacenter.

Within the datacenter, we use Federal Information Protection Standard 140-rated hardware security modules whose sole purpose is to keep cryptographic material such as signing credentials secure and protected.

These devices are equipped with systems right out of a spy film that cause the information within them to be erased if the device is tampered with rather than have that information leaked.

But we don't stop there:

- All of our XML-based audit log and event history information is protected with a tamper-evident seal.
- All communication with the SIGNiX service is handled via secure communication 256-bit SSL (which effectively uses the same technology as our digital signatures) within the browser, encrypting communication between the browser and the server.
- All documents are encrypted via AES 256 while at rest within our system.
- Documents can be shredded electronically according to DOD standard 5220.22-M.

SIGNiX takes the security of our service—and our customers' documents—very seriously.

INTERNATIONAL STANDARDS

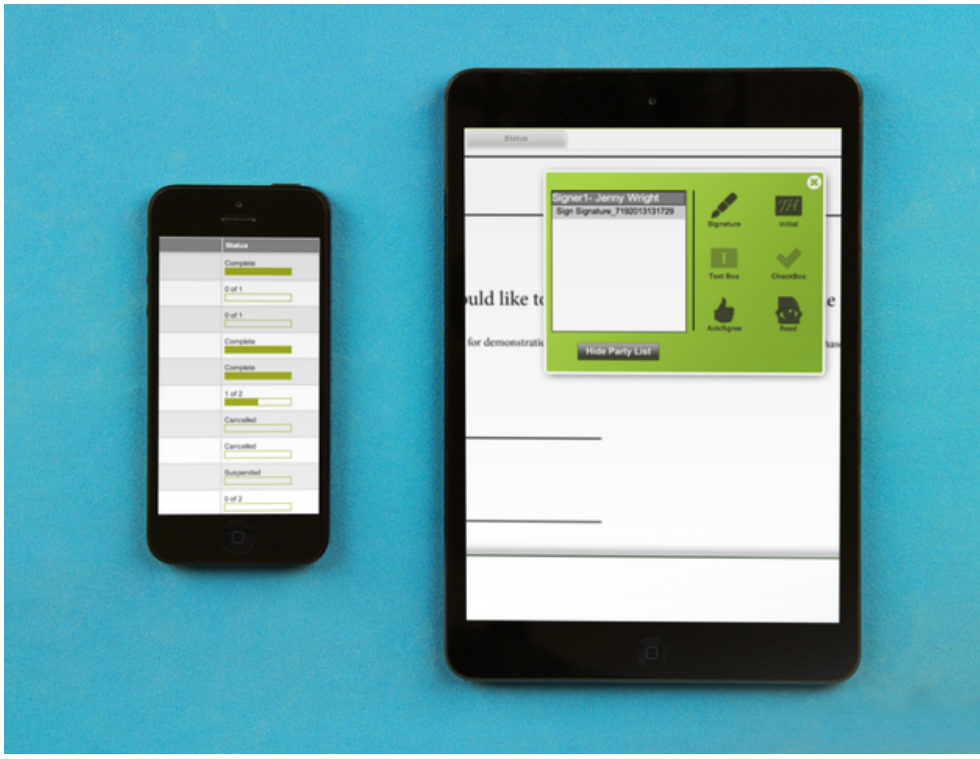
Signed documents may need to be trusted for five, ten, maybe even twenty years. Your documents may also need to be trusted across national and international borders. SIGNiX digital signatures meet international requirements, are time stamped and based on actual, published standards so you can trust and validate those signatures at any time in the future.

In fact, digital signatures are preferred not only by the United States government, whose employees use digital signature technology every day, but also internationally because these signatures are owned by no one company or country. In Europe and in many other countries around the world, digital signatures represent a class of electronic signatures called "advanced electronic signatures," and are given a stronger weight in law because of their inherent properties.

SIGNIX: WHERE SECURITY COMES FIRST

For more than a decade, we've been committed to providing the most secure and legally compliant online signature product available. This commitment has shaped every aspect of our product line, and it has made us the leader in many highly regulated industries.

Our digital signatures provide consistent evidence to ensure integrity of your signed documents today and into the future. Recipients need not be locked into SIGNiX to simply verify a signature. Freely available, standards-based PDF viewers allow users to see any changes made to a document in real-time, online or offline, allowing



enterprises to easily store documents in their own document repositories.

We authenticate users with a diverse set of methods that scale to meet your needs and risk profiles. We provide significant non-repudiation protection through a carefully vetted signing process and highly detailed audit trail.

We deploy our service through a provider audited to some of the highest standards in the industry.

Our technology is compliant with ESIGN, UETA, FINRA/SEC, Digital Signature Standards by National Institute of Standards and Technology, ETSI, 21 CFR Part 11, SSAE16, Health Insurance Portability and Accountability Act of 1996 (HIPAA), the IRS's IVES Electronic Signature Requirements, FHA Mortgage Letter 2014-03, and the Payment Card Industry Data Security Standard (PCI DSS).

SIGNiX has been certified as a compliant e-signature solution by the Insured Retirement Institute, the first vendor to have ever completed the rigorous requirements set by IRI.

The SIGNiX digital signature solution also exceeds the requirements for authentication, repudiation, admissibility, and other best practices set out by ACORD for electronic signatures in the insurance industry.

We know that signed documents are the foundation of any business, which is why we work diligently to offer the most secure and legally enforceable e-signature product on the market.

LEARN MORE TODAY!

Contact us today to learn more about SIGNiX and how our e-signature services reduce costs, speed up business and enhance document security.

Get A Quote **See How it Works**

Call 1.877.890.5350 x1048 or email info@signix.com