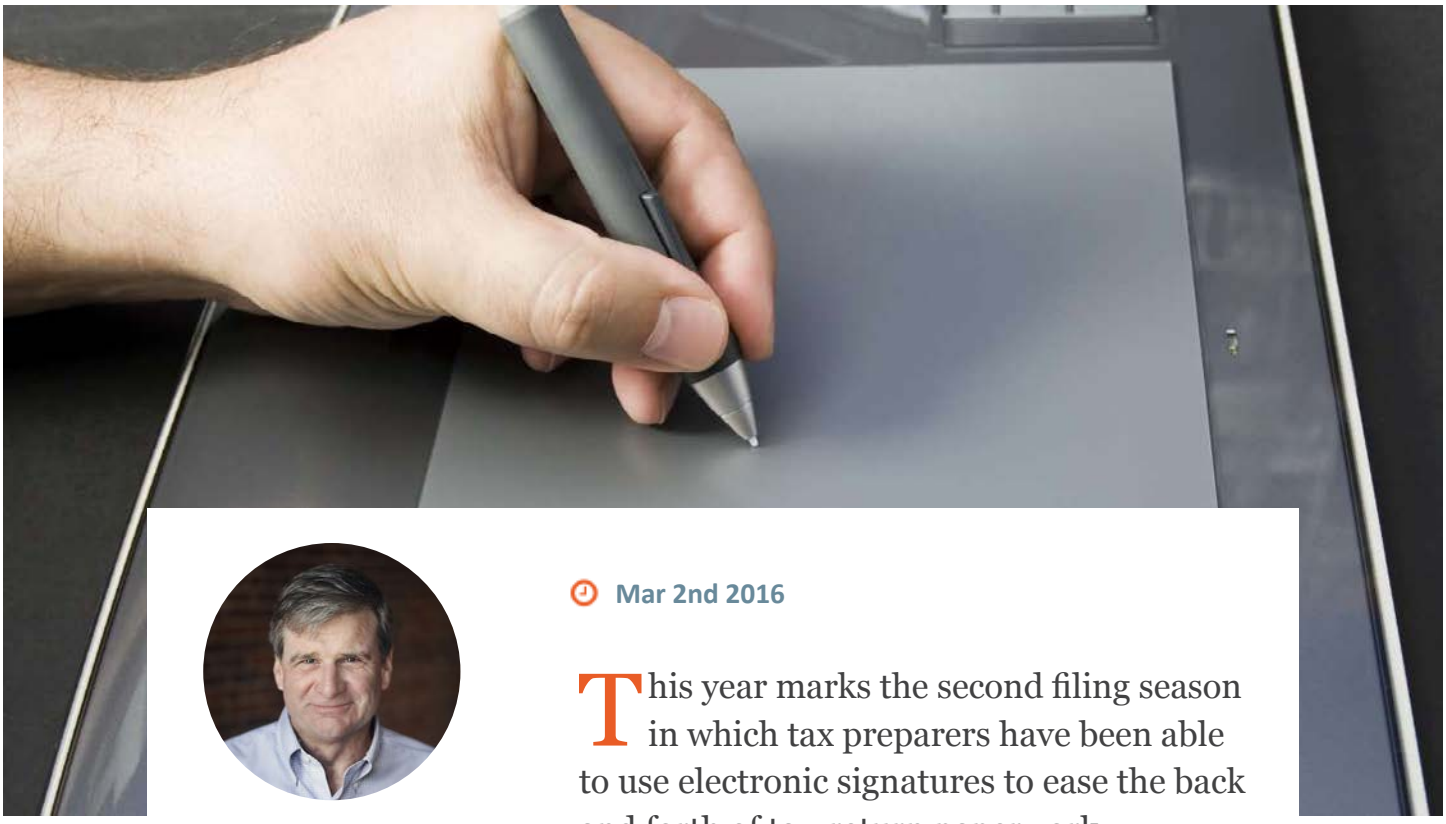
accountingWEB

How to Ensure a Seamless Tax Process with E-Signature Technology



Pem Guerry
Executive Vice President
SIGNiX

Columnist

Mar 2nd 2016

This year marks the second filing season in which tax preparers have been able to use electronic signatures to ease the back and forth of tax-return paperwork.

Prior to 2015's filing season, only handwritten signatures or signatures captured on signature pads were accepted for forms 8878 and 8879, which authorize an Electronic Return Originator (ERO)

continued on next page

to e-file tax returns to the IRS. In March 2014, new IRS rules allowed the forms to be signed by taxpayers electronically, making it easier for accountants and tax preparers to electronically file customers' tax returns.

E-signatures used for tax-related documents keep the IRS's e-filing system working toward its intended goal: to make tax processing quicker and more convenient for everyone involved in the preparation process.

Take it from Michael Miller, owner of Miller & Associates Tax Service Inc. in Winter Haven, Florida. This year, he's used e-signature technology to send tax forms and collect signatures from every out-of-town client, which represents about 20 percent of his business.

"Previously, I would have to print and mail the documents to them. They would sign them and fax them back to me," Miller said. "So, it's far more convenient for me to send the form to them with the attached tax return, and they can digitally sign and send everything right back to me. It's efficient, it's less stressful, and it even saves money."

But before you run out and sign up for an e-signature service, there is a critical component to be aware of: The technology must keep the personal and confidential data secure. Anyone who has kept track of recent news headlines knows that the information in tax documents is a sought-after commodity in the digital black market. Consider that **the IRS paid out $5.8 billion in bogus refunds** to identity thieves for tax year 2013, according to the US Government Accountability Office. In 2014, **2.7 million taxpayers** were identity theft victims.

IRS Mandates

The first step in selecting secure, reliable e-signature technology is an obvious one: Make sure it meets **IRS mandates** for e-signatures. For IRS documents, an e-signature service must do the following:

continued on next page

1. Identify the person who signed the document. E-signature providers must be able to calibrate their identity authentication processes to specifically meet IRS requirements, beginning with the basics: your personally identifiable information.

A signer must provide his name, Social Security number, address, and date of birth, and the information given must be consistent with information provided through record checks with credit bureaus or similar databases. E-signature technology must be able to record this information, too.

For a remote signer, the software must also use knowledge-based authentication (KBA) to further verify the taxpayer's identity. This process asks the signer a series of detailed questions generated from information found in public databases that is typically not known by anyone other than the signer (and isn't easily found in someone's wallet).

The software must record that a signer successfully passed this form of authentication, per National Institute of Standards and Technology requirements. And after three tries – you're out. If there are three failed KBA attempts, the signer must authorize the documents with a handwritten signature.

Finally, if there is more than one taxpayer for the electronic record, the signature process must be designed to **authenticate each taxpayer separately.**

2. Retain integrity of electronic records. Each e-signature must be linked to its respective electronic record, or there should be proof that the signature is a valid one. An e-signature should not be able to be removed, copied, or transferred to falsify a digital record.

Once signed, the document must be tamperproof, so the e-signature service must use techniques to **lock a document and prevent it from being modified.** Storage systems must also contain a retrieval system with an index and the ability to reproduce legible hard copies of electronic records.

continued on next page

3. Create a digital "paper trail." For IRS compliance, e-signature technology must record the digital image of the signed form, the date and time of the signature, the taxpayer's computer IP address, the taxpayer's login identification/user name, identity verification (the taxpayer's KBA results showing he passed), and an audit trail that reflects the completion of the process by the signer.

The ERO must keep this information on hand and be able to provide it to the IRS as requested, so it's important that the data trail be comprehensive and easily accessible.

Security, Defensibility Stretch Beyond Government Mandates

While the IRS provides a solid framework for an e-signature transaction, it doesn't answer questions of e-signature longevity. That is: "Will I be able to prove my e-signature's validity in the future?" With tax preparation, this isn't a question to dismiss. Audits on tax records could occur several years after filings take place, so e-signatures must remain defensible in court at least that long – and ideally forever.

The simplest way to dissect an e-signature's validity strength is to think about e-signatures in terms of their dependence on a vendor.

Dependent e-signatures require clicking a link to a vendor's server to access the legal evidence of a signature that proves it is valid. Dependent e-signatures may also use proprietary technology to retrieve validity information. This can be fine in the short term, but there will always be an element of the unknown that makes long-term validity nearly impossible to guarantee. For instance, what happens if a link breaks or your relationship changes with a vendor? The dependence on that link could end up compromising the e-signature's validity and, indeed, the entire process.

Independent e-signatures do not rely on a vendor's server or use proprietary technology. These are called "digital signatures," and they use public key infrastructure technology to permanently embed the legal evidence of a signature into a signed document. That means the e-signature exists independently of a vendor and an Internet connection,

continued on next page

and its validity can be accessed anywhere, anytime – online or offline. And if desired, independent e-signature vendors can even digitally shred their copies of signed documents from their servers with no impact on the available legal evidence.

Independent, digital signatures are also based on international, published standards for document management, which will always be discoverable. This, again, supports the long-term validity of signed documents.

E-Signature Opportunities

Widespread e-signature use for tax documents is still in its infancy, but the technology has the ability to drastically improve operations. With e-signatures, there's less paperwork to file, manage, and store; paper-related expenses drop; and tax documents can be safely emailed to clients. It's a value-added service, too: Taxpayers can sign forms anywhere, anytime – easing a process typically perceived to be anything but convenient.

With the right technology that is both compliant and defensible, the tax process can move another important step forward into the digital world.

About the author

Pem Guerry

Pem Guerry is the executive vice president at SIGNiX, an Independent E-Signature™ solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers an independently verifiable cloud-based digital signature solution, which combines workflow convenience with superior security.