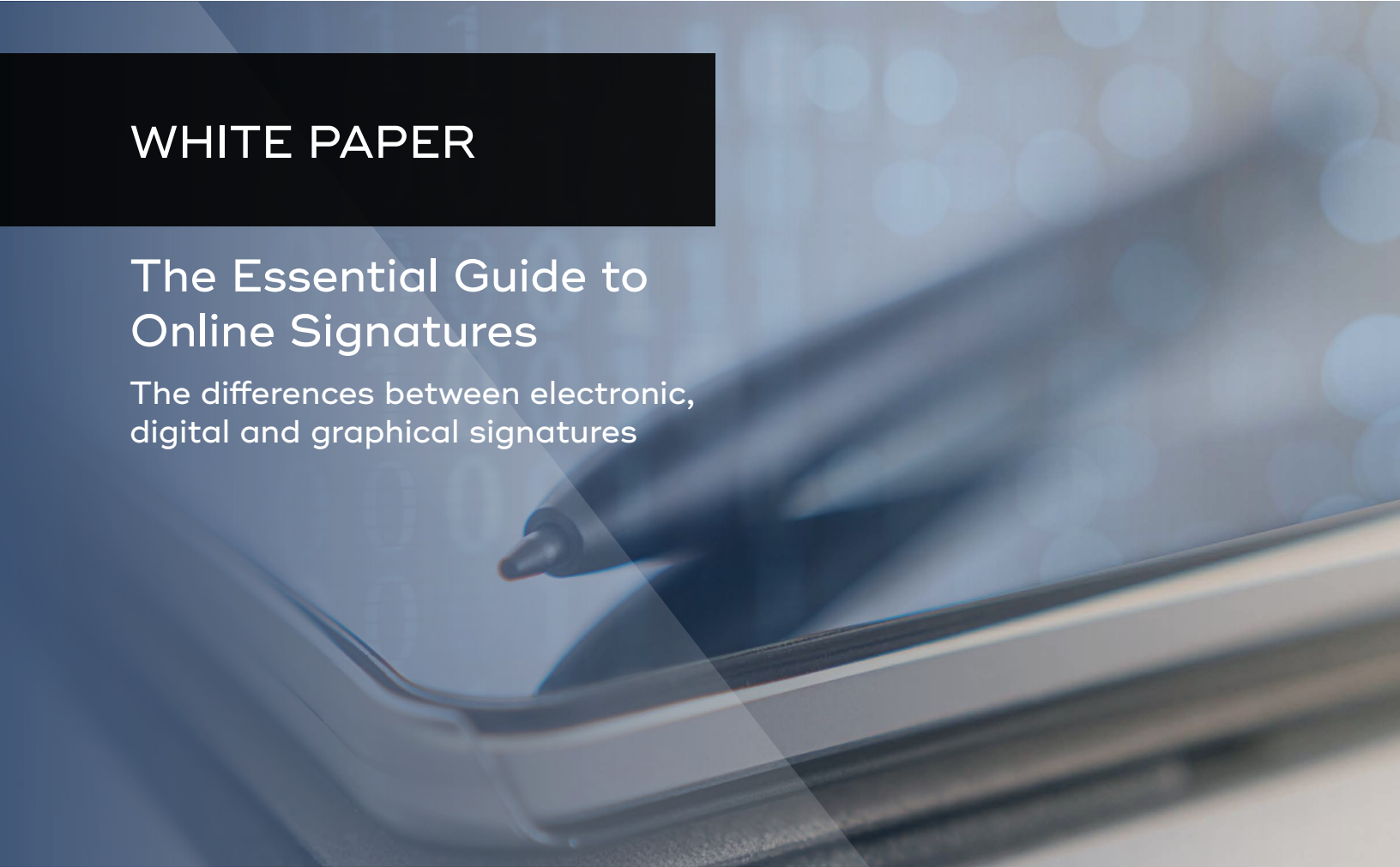



WHITE PAPER

The Essential Guide to Online Signatures

The differences between electronic,
digital and graphical signatures





As companies rely ever more on digital processes, the traditional tools for transacting business are also becoming more automated. Around the world, organizations are replacing paper-based processes with more efficient, digital equivalents. As a result, the traditional way of using pen and paper to sign documents is rapidly changing.

When it comes to digitizing signing processes there are three types of signatures that are commonly used within organizations - electronic, digital and graphical. Do you know exactly what each of these is and how they differ from one another? If not, then rest assured that you are not alone. Read on and find out more.

In this whitepaper we will examine the purposes, regulations and use-cases underlying each type of signature. By the end of this document you should be able to clearly define the difference between an electronic, digital and graphical signature and know which apply to your specific business scenarios.

Electronic Signatures

What is an electronic signature?

An electronic signature is first and foremost a legal concept. According to the U.S Electronic Signatures in Global and National Commerce Act, an electronic signature is an “electronic sound, symbol, or process attached to, or associated with, a contract or other record and adopted by a person with the intent to sign a record.” In layman’s terms, an electronic signature provides a secure and accurate identification method for the signatory to complete a seamless electronic transaction.

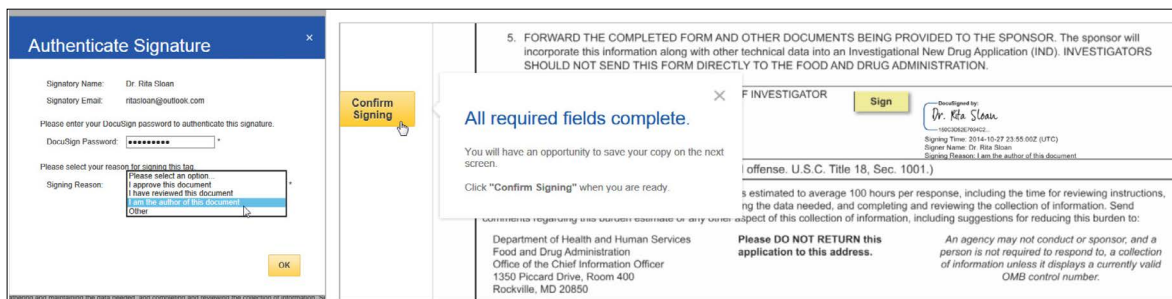
Electronic signatures contain information about who signed the electronic document, the processes they followed to do it, and their intent to act based on that agreement. Typically, an electronic signature consists of four major components:

1. a method of signing
2. data authentication
3. user authentication
4. statement of intent

Without requiring the complexity of a digital signature, electronic signatures make it much simpler and easier for users to sign agreements and complete other online transactions. The signing information can be stored externally to the signed document as long as there is traceability.

Regulations surrounding electronic signatures

Around the world there are numerous legal acts and regulations covering the area of electronic signatures. These include PIPEDA (Canada), E-SIGN Act Sec 106 (US), eIDAS (European Union), Electronic Transactions Act 1999 (Australia), and Electronic Communications Act 2000 (UK) to name but a few. Within the realms of the life science industry, electronic signatures are typically defined by US FDA regulation 21 CFR Part 11 - the regulation defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.



courtesy of docusign.com

Electronic signature usage scenarios

Electronic signatures are commonly used by drug producers, medical device manufacturers, bio-tech companies, biologics developers, CROs, and other FDA-regulated industries. Beyond the basic signature, regulations specify that the signing process requires an audit trail in order to comply. As an example, when a pharmaceutical company files an eCTD submission with the FDA, all documents that require a signature need to be signed electronically.

Digital Signatures

What is a digital signature?

Digital signatures are essentially a digital version of a “notarized signature”. It’s a cryptographic implementation of electronic signatures. They are used as both a proof of authenticity and data integrity. Digital signatures are often used as part of an electronic signature implementation, but the key thing to remember is that not all electronic signatures use digital signatures.

A digital signature essentially creates a “fingerprint” of the document at the time of signing and links it with an identity credential (a digital certificate). The resulting encrypted signature is then permanently embedded into the document. A digital signature explicitly proves integrity by clearly showing when a document has been changed or tampered with. The signature also uniquely identifies the signer and can provide additional information about the time of signing, providing significant non-repudiation.

Because digital signatures travel with the document and are based on industry and international standards, they can be verified independently without requiring the document check back with a central server. As a legal form of agreement, digital signatures are also more widely accepted internationally than electronic signatures.

A digital signature typically consists of three algorithms:

1. **A key generation algorithm** that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
2. **A signing algorithm** that, given a message and a private key, produces a signature.
3. **A signature verifying algorithm** that, given the message, public key and signature, either accepts or rejects the message’s claim to authenticity.

The main complexity behind the digital signature approach is the infrastructure required to create and manage these authenticated certificates and keys. The process of digital signing requires that the signature generated by both the fixed message and private key can then be authenticated by an accompanying public key. Using these cryptographic algorithms, the user’s signature cannot be replicated without having access to their private key.



courtesy of cpaperless.com

Digital signature standards

Digital signatures form a vital element within the ISO 32000 standard – aka. PDF files. The standard specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed.

It is intended for the developer of software that creates PDF files (conforming writers), software that reads existing PDF files and interprets their contents for display and interaction (conforming readers) and PDF products that read and/or write PDF files for a variety of other purposes (conforming products).

Digital signature usage scenarios

As organizations move away from paper documents with ink signatures and authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. Digital signatures are deployed across various organizations both in the public and private sectors. For example, the United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities such as the University of Chicago and Stanford are publishing electronic student transcripts with digital signatures etc.

Graphical Signatures

What is a graphical signature?

Graphical signatures are the format that most closely resembles the traditional paper-based ink signature. A graphical signature has a designated location within a document and is typically accompanied by additional information regarding the signee (e.g. name, title, etc.) There may or may not be an audit trail.

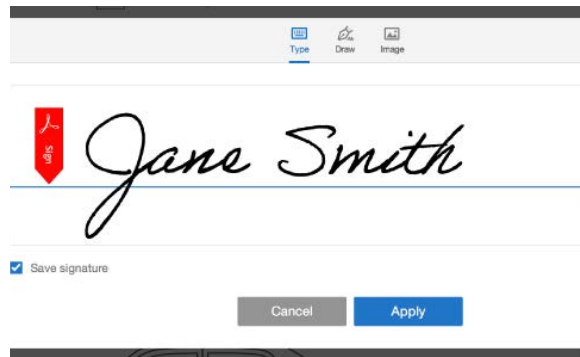
In many organizations, graphical signatures are widely used for internal business processes that don't require third party authentication.

The legality of graphical signatures

Graphical signatures are not regulated by any particular governmental regulations. Drawing a comparison to the traditional paper-based signing process - using a graphical signature is like an individual signing a document without a notary. That doesn't mean that it isn't a valid signature, it only means that it wasn't subject to any third party authentication.

Graphical signature usage scenarios

Graphical signatures are deployed in almost every organization that uses electronic document management systems. While systems vary from provider to provider, the general idea behind them is the same. You upload a document—Word, PDF, or even an image file—to an online service, then



courtesy of adobe.com

tag it with annotations to indicate where signatures eventually need to be placed. The service sends the marked-up file to the specified recipient, who then signs it with a few clicks, usually either with stock cursive fonts or with a scrawl they draw using their mouse (or a finger, using a tablet) on the fly.

How do signatures affect business processes?

Many document-based business processes require signatures, such as the approval of contracts, invoices and employee evaluation forms. Wet signatures (print out the document, sign it, scan it, and put it back into the business process) tend to slow these processes down because of their dependence on the physical exchange of paper, thus electronic, digital and graphical signatures enable the streamlining of such processes.

Depending on your organization's needs, incorporating one or more of the above mentioned signatures in an automated business process enables organizations to operate at peak efficiency.



GCI POWERTOOLS ELECTRONIC SIGNATURES

Is your organization required to assemble and electronically sign collections of documents in compliance with regulations such as the FDA's 21 CFR Part 11?

The need to **sign multiple documents within a single Content Server workflow** is something we commonly hear. GCI PowerTools for OpenText Electronic Signatures™ provides an effective solution to this challenge. Its powerful workflow enhancements enable the development of electronic signing processes that allow the simultaneous signing of multiple documents and the creation of workflows that more closely align to existing business procedures.

More about GCI PowerTools for OpenText Electronic Signatures



GCI POWERTOOLS DOCUMENTS

Is your organization in need of automated document production processes that allow you to integrate metadata, merge documents, convert content to PDF, and digitally sign documents within OpenText Content Server?

GCI PowerTools for Documents is a powerful and intuitive solution for constructing professional documents within Content Server. Its automated approach simplifies the production of complex documents. Once assembled, documents can be attached to Content Server workflows ready for review and approval, then finally sent for electronic, graphical or digital signing. **PowerTools for Documents supports the signing of Word and PDF documents through Windows Certificate Authority, GlobalSign, and DocuSign, CoSign, as well as YubiKey two-factor authentication.**

More about GCI PowerTools for Documents

