WHAT ARE DIGITAL SIGNATURES[1]?

In a nutshell, digital signatures are like electronic "fingerprints." Thanks to special coding, digital signatures securely associate a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance.

ELECTRONIC SIGNATURE VS. DIGITAL SIGNATURE

The terms "electronic signature" and "digital signature" are often used interchangeably.

An **electronic signature** captures the information about who signed what, when, where and how through an audit trail. Electronic signatures are purely electronic image of a signature (without a digital certificate).

A **digital signature** captures all the same information as the electronic signature but also confirms, through authentication, that the signer is who they claim to be. Digital signatures embed a unique digital certificate into a document (like a fingerprint) making it difficult to alter.

DIGITAL SIGNATURE REQUIREMENTS

In order to guarantee the reliability and the integrity of the document and its signature, **we must use the digital signature[2].** Without digital signatures, it may be difficult to prove the legitimacy of an electronic transaction, putting you and the University at risk in the event of litigation.

In order for the digital signature to be authentic and reliable, it must meet the following requirement:

- Be unique to each individual,
- Be created under the sole control of each individual,
- Confirm the individual's identity,
- Prove the signature was created with the intent to sign the document,
- Be linked/associated to the document in question in a reliable way,
- Have audit trail capabilities, and
- Protect against tampering or un-authorized changes.

BENEFITS OF DIGITAL SIGNATURE

- **Added security.** The digital signature offers more security than an electronic signature. The unique identifying "fingerprint" in a digital signature remains embedded within a document. Any signs that someone has tampered with or altered a document after signing it can be easily detected.
- **Quality**. Currently, paper signatures can produce a low quality document in the end, as a result of the re-printing/ re-scanning when multiple signatures are required.
- **User experience**. Digital signatures are easy to use. They provide alerts, notifications and better workflow visibility.
- **Intuitive interface**. No training is required for signatories. This ensures a high adoption rate.
- **Streamlined processes.**

---

[1] https://www.docusign.ca/how-it-works/electronic-signature/digital-signature/digital-signature-faq

[2] For more information, please consult the Information Management Best Practice on Digital Signatures.

- **Mobile access**. Web-based. Documents can be accessed and signed from any mobile devices.
- **Integration**. Can be easily connected with other technologies making the process even more efficient.

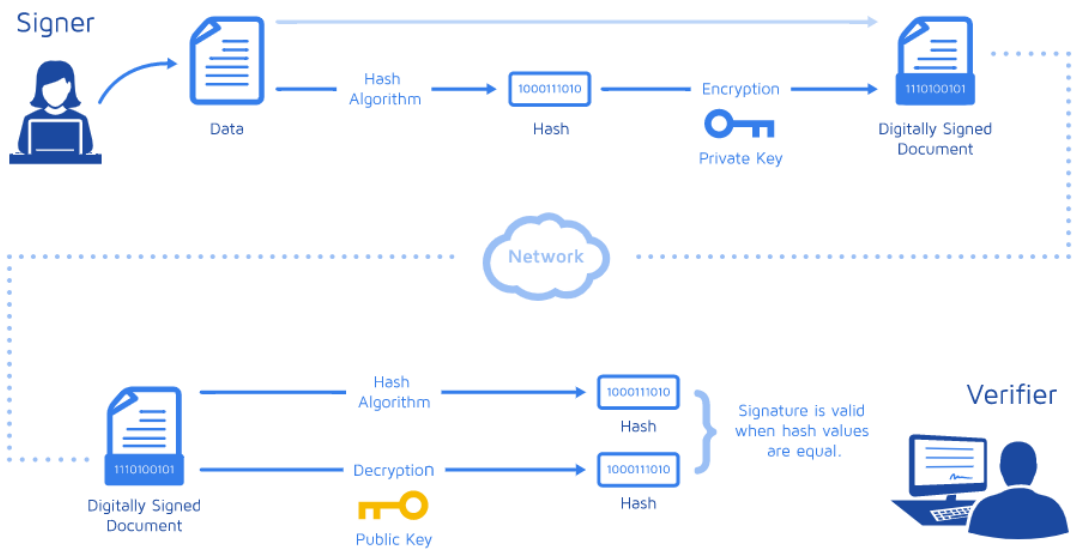
HOW DOES DIGITAL SIGNATURES WORK[3]?

Digital signatures, like handwritten signatures, are unique to each signer. Digital signature solution providers, such as DocuSign, follow a specific protocol that requires the provider to use a mathematical algorithm to generate two long numbers, called "keys". One key is public, and one key is private.

When a signer electronically signs a document, the signature is created using the signer's private key, which is always securely kept by the signer. The mathematical algorithm acts like a cipher, creating data matching the signed document, called a hash, and encrypting that data. The resulting encrypted data is the digital signature. The signature is also marked with the time that the document was signed. If the document changes after signing, the digital signature is invalidated.

As an example, Jane signs an agreement to sell a timeshare using her private key. The buyer receives the document. The buyer who receives the document also receives a copy of Jane's public key. If the public key can't decrypt the signature (via the cipher from which the keys were created), it means the signature isn't Jane's, or has been changed since it was signed. The signature is then considered invalid.

To protect the integrity of the signature, PKI requires that the keys be created, conducted, and saved in a secure manner, and often requires the services of a reliable Certificate Authority (CA). Digital signature providers, like DocuSign, meet PKI requirements for safe digital signing.



[3] https://www.docusign.ca/how-it-works/electronic-signature/digital-signature/digital-signature-faq

DOCUSIGN[4]

The University has chosen DocuSign as its solution for Digital Signatures.

Docusign is an industry leading solution in Digital Signatures. Their platform is cloud based, meaning that you can process digital signatures "real-time" from any device with an internet connection (including phones and tablets) offering you improved user experience and greater efficiency than paper signatures.

Easily send documents for electronic signature

Step 1: Upload your document.

Simply upload a Microsoft Word, PDF, or other common document format from your computer.

Step 2: Indicate who needs to sign.

Add the names and email addresses of your signers and other recipients, and specify the order in which they should sign.

Step 3: Place fields and send.

Drag and drop DocuSign fields to indicate where you need a signature, initial, or date. Then click Send. DocuSign emails a link to each recipient which they can use to access the document. Once the document is complete, everyone involved will receive a confirmation e-mail with the executed PDF. You can then save the document on your shared repository.

Easily sign documents

STEP 1: Click the link in email.

With one click, access the document and start the document signing process on any internet-enabled device.

Step 2: Follow the DocuSign tabs.

Tabs and simple instructions will guide you through the signing process.

Step 3: Finish, and you're done.

Once you're done signing, click Finish. That's it!

Readily check a document's status, send reminders and view audit trails

You can access your DocuSign dashboard anytime to check the status of a document, run reports, and see audit trails. You can always see where your document is in the signing process--and even set automatic reminders and receive notifications as needed.

[4] https://www.docusign.ca/products/electronic-signature

WHEN SHOULD A DIGITAL SIGNATURE BE USED?

The following are types of documents that should require a digital signature. However, it should be noted that faculties and services should perform their own assessments in the context of their business needs and requirements.

Digital signature must be used:

- based on the importance of your document and the likelihood of legal challenges of the signature.
- where a law or policy specifies the requirement for a digital signature.
- for legally binding documents such as contracts, agreements, etc.

Examples include, but are not limited to:

- **Student forms or applications:** admissions, housing, financial aid,
- **HR forms:** new hire paperwork, agreements
- **Registrar:** transcription request forms, internship proposal
- **Campus life:** parking forms, incident reports, health forms
- **Procurement documents:** Vendor contracts, non-disclosure agreements (NDA), letters of understanding
- **Finance documents:** Invoice processing, expense processing, capitalization management, audit sign-off
- **Research documents:** Grant applications
- **External relations:** donation requests, fundraising forms
- **Real estate contracts:** requirements sign off, lease agreements

In the absence of specified legal or policy requirements and when requirements for implementing a digital signature is not specified or is unclear, please send a request to the IT Service Desk.

HOW WILL DIGITAL SIGNATURES BE IMPLEMENTED AT THE UNIVERSITY OF OTTAWA?

WHO REQUIRES A LICENCE?

Only the person initiating the digital signature process requires a licenses. Signers **DO NOT** require a license.

HOW DO I GET A LICENCE?

To request Docusign licenses for your team please follow these steps:

1. Obtain the approval of your head of unit. Although the cost of licenses are centrally covered, we do have a limited allocation of transactions per year. We must ensure we are using these wisely.
2. Send a request to the IT Service Desk and specify:
    a. The type of documents you will send for signature.
    b. Your group's estimated number of transactions (to sign per year).
    c. The name of your group's administrator (this person that will manage licenses within your group).
3. Once approved, the group's administrator will add the e-mail address of all team members needing a license.

For clarity, a team that has been approved for Digital Signatures, does not need to create a new request whenever a new member joins the team. The group's administrator can grant them a license directly.

WHAT ABOUT TRAINING?

Once your license is setup, you will be able to log on to Docusign University**,** a virtual learning platform that will help you get familiar with the tool.

Depending on your role, we recommend you start with a **learning plan** for administrator or sender.

If you want to learn more about the tool, we invite you to visit DocuSign University for additional trainings. There are many 60-minute complimentary webinars available to satisfy your training needs (try this one first).

NEED HELP?

Please send a request to the IT Service Desk.