WHITEPAPER

Guide to Electronic and Digital Signatures

This document is an overview of digital signatures in North America and provides concise insights into the evolving significance of digital signatures and highlights key global legislation supporting their adoption.

AEISHA VYAS

4Point

TABLE OF CONTENTS

Disclaimer

This document is based on opinions and legislation collected regarding digital signatures and their general applicability for public and private organizations. We are not lawyers and the opinions provided in this document are not intended as legal advice or counsel. Your legal representatives should use this information to help them develop the policies specific to your organization, your requirements and your regulations.

OVERVIEW

The increasing prevalence of online activities, coupled with organizational objectives to reduce costs and improve efficiency are driving a new chapter in digital transformation. This transformation requires more than just moving processes and documents online, it requires new ways of addressing the real needs of identification, authorization, non-repudiation, and data integrity.

The use of electronic or digital signatures for documents, contracts and agreements is a critical element to power this digital transformation. As organizations move more and more processes online, as they capture more information from partners and customers and as they deliver more information in an electronic form, digital signatures are crucial to ensure that documents are approved and protected.

This document provides background information about signatures, their purpose and how they are changing. But more importantly, this document identifies the key global legislation and regulations that make the use of digital signatures possible and desirable.

WHAT IS A SIGNATURE

A signature is a mark or sign made by an individual on a document to signify knowledge, approval, acceptance and obligation.

The term signature is generally understood as the signing of a document with one's own hand. Signatures may be typewritten, engraved, or stamped, and serves to tie the person signing a document to the terms of the document's contents.

A signature can obligate a party to terms of a contract or verify that a party intended to make a change in information or status [1]. Because of the importance of signatures, several countries have developed laws and rules that govern what constitutes a legally valid signature. Almost all states in the USA have passed laws that recognize the validity of electronic signatures, which will be discussed in detail in this document.

The Internet and other forms of telecommunication have created the need to transact legally binding agreements electronically. This has introduced different types of signatures and laws that recognize non-physical signatures as binding for the persons involved.

PURPOSE OF A SIGNATURE

A signature is needed where an oral agreement or handshake is insufficient due to involved legal or monetary risks. In the event of a conflict, it would be impossible to prove to a court that a handshake or oral agreement occurred.

In these situations, courts rely on the presence of the parties' signatures on a document to treat that document as legally valid and binding on those parties.

This lends immense trust and credibility to the contract. A signature is a tangible, preservable and visible way of a party signifying its commitment to a transaction – making it harder for the same party to backtrack from its commitments [13]. This also becomes an invaluable source of evidence.

There are two main purposes of a signature in a legal contract:

- Authorization and authentication

  - To identify the person who is a party to the contract.

- Non-repudiation and integrity

  - To show that the signing party has read the contents of the document, understands the contents, and consents to the stipulations of the document [14].

TYPES OF SIGNATURES

WET SIGNATURE

A wet signature is the most common type of signature. It is a physical mark on a document which can be in the form of a symbol or name. This type of signature is placed onto the document by hand and has not been embedded by digital means.

According to the U.S. Uniform Commercial Code "A signature may be made manually or by means of a device or machine, and by the use of any name, including a trade or assumed name, or by a word, mark, or symbol executed or adopted by a person with present intention to authenticate a writing."

In most cases a wet signature is writing your name in cursive on a piece of paper, document or contract, often with initials on each page indicating the extent of what is being accepted and acknowledged [4] [5].

"I AGREE" CHECKBOXES

Checkboxes can be used to signify the acceptance of terms of an agreement. In this case, the user must check the boxes associated with the terms of the agreement to indicate they agree. If a box is not checked that term is considered to not be accepted. This form of a signature is called a “clickwrap agreement.” The agreement is wrapped up in the deliberate action of clicking to signify acceptance of the terms or contract.

In general, courts uphold clickwrap agreements as legally binding and they can be used for order forms, contracts, and other agreements [6] [7] [8].

E-SIGNATURE

Any electronic process that signifies acceptance of an agreement or record is known as an electronic signature, or e-signature. This broad category includes most electronic signature systems in the U. S. Electronic signatures use a wide range of electronic authentication techniques, such as email, corporate ID, password protection, or a PIN issued to a mobile phone, to confirm the identity of the signee.

A secure procedure that includes an audit trail and a final tamper-evident digital certificate embedded into the finished signed document is used to demonstrate proof of signing.

E-signatures are more practical than a traditional signature since they may be used to remotely sign papers. The time and money efficiencies associated with e-signatures have made them become a necessity for many small organizations [9].

DIGITAL SIGNATURES

Digital Signatures use a combination of complex algorithms, certificate authorities (CAs) and trust service providers (TSPs) to authenticate the signee and the integrity of the document.

Users can be identified by a unique virtual fingerprint to protect information in digital messages or documents. Email content itself becomes a part of the digital signature in emails. Digital signatures are significantly more secure than other forms of electronic signatures [10].

DIGITAL SIGNATURE VS. E-SIGNATURES

The main difference between digital signatures and e-signatures is that digital signatures rely on PKIs and associated encryptions standards, therefore they are preferred over e-signatures as they are more secure and authentic. PKIs can be visualized as an electronic fingerprint which encrypts and identifies a person’s identity.

The table below shows a detailed comparison between the two [12].

E-SIGNATURES	DIGITAL SIGNATURES
An e-signature is a digital form of a wet signature that is legally binding and secure.	A digital signature is a secure signature that works with an e-signature and relies on public key infrastructure.
Can be a symbol, image, or process attached to the message or document to recognize the signer's identity and to give consent to it.	Can be visualized as an electronic fingerprint that encrypts and identifies a person's identity.
Used for verifying a document.	Used for securing a document.
The validation of e-signatures is not performed by any trusted certificate authorities or trust service providers.	The validation of digital signatures is performed by trusted certificate authorities or trust service providers.
Vulnerable to tampering.	Highly secure.
Not usually authorized.	Usually authorized.
Cannot be verified.	Can be verified.
Does not incorporate any coding or standards.	Comes with encryption standards.
Common types of e-signatures include verbal, electronic ticks, or scanned signatures.	Common types of digital signatures include Adobe and Microsoft.
Few security features.	Many security features.
When to use? E-signatures are widely used in contracts and agreements by many businesses. For example, your company may require clients to electronically sign loan applications and other financial commitments.	When to use? A digital signature uses a digital certificate to verify the signer's identity, making it a safe tool for sensitive data like financial records, HIPAA-compliant paperwork, and other private papers or contracts.

BENEFITS OF E-SIGNATURES

DECREASING STATIONARY COSTS

With digital signatures, the money-consuming process for printing, mailing, and storing documents is unnecessary. Automating the signature process helps reduce the costs associated with human errors like lost or incorrectly signed documents, which slow down the process and result in expenditure problems if left unnoticed [15].

LEGAL COMPLIANCE

The U.S. Electronic Signatures in Global and National Commerce (ESIGN) Act in 2000 legislated electronic signatures legal in every state and U.S. territory where federal law applies. In other industrialized countries, electronic signatures carry the same weight and legal efficiency as handwritten signatures and paper documents [16].

There is a more detailed description around e-signatures legal compliance and acceptability across USA in the section 9 of the document.

SAVE TIME

When documents don't need to be scanned, printed, and mailed on paper, such as in the case of electronically signing a document, procedures can be completed more quickly. [17].

DOCUMENT SECURITY

In cases of security breaches, the encryption of data makes it difficult to extract. This encryption also guarantees that the document cannot be modified after the signature, so there is no risk of a document being changed once the signer has agreed to the contents. [18].

REMOTE ACCESSIBILITY

Digital signatures can be created anywhere, at any time. Remote work has increased, so location independence is crucial to ensuring that documents can be signed remotely instead of the signers having to be physically present [19].

CUSTOMER EXPERIENCE

Our clients, business partners, and stakeholders will also benefit from digital signatures. They can sign on line on any device, and at their own leisure rather than travelling to your branch, office, or store.
In addition to resulting in quicker turnaround times, this provides a better experience and increases customer satisfaction and retention [20].

TRACK SIGNATURES

When several people need to sign a document, it can be difficult to know its status. With digital signatures, you can stay on top of that by tracking and managing the process [21].

AUTHENTICITY

Digitally signed documents can be tracked back to their original owner. A digital signature certificate ensures the e-signature is authenticated and provides legal legitimacy. It can stand in any court of law. Additionally, time stamping plus ability to track documents improve and simplify audit [22].

LEGALITY AND COMPLIANCE

More organizations are conducting business over the web and are moving away from paper. Electronic signatures are becoming more accepted and more prevalent for a wide range of documents, agreements and contracts. Most countries around the world now have laws in place to accept electronic or digital signatures as described in the following sections.

E-SIGNATURES IN THE US AND CANADA

The Electronic Signatures in Global and National Commerce Act (ESIGN Act)

Throughout the U. S., the ESIGN Act gives electronic signatures the same legal standing as handwritten ones, substantially streamlining and speeding up how businesses collect, track, and handle signatures and approvals on all kinds of agreements and documents. The definition of an electronic signature in the ESIGN Act is "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." In simple terms, electronic signatures are legally recognized as a viable method to indicate agreement to a contract.

As per the ESIGN Act

- Any law with a requirement for a signature may be satisfied by an electronic signature
- Allows electronically executed agreements to be presented as evidence in court
- Prevents denial of legal effect, validity, or enforceability of an electronically signed document solely because it is in electronic form.

Uniform Electronic Transactions Act (UETA)

In 1999, the Uniform Law Commission drafted the Uniform Electronic Transactions Act (UETA) to provide a legal framework for the use of electronic signatures in each state. UETA has since been adopted by 49 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. However, one state—New York—has not adopted UETA, but instead has passed Electronic Signatures and Records Act (ESRA), a similar law that makes electronic signatures legally binding.

The following fundamental principles are outlined in UETA:

- A record or signature can't be denied legal effect or enforceability simply because it's in electronic form.
- A contract can't be denied legal effect or enforceability simply because an electronic record was used in its formation.
- If a law requires a record to be in writing, an electronic record satisfies the law.
- If a law requires a signature, an electronic signature satisfies the law [25].

E-SIGNATURES IN CANADA PIPEDA (FEDERAL)

The Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA - Canadian federal law - provides a regime that defines an e-signature as "a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document." Essentially, an e-signature can be virtually any form of electronic representation that can be linked or attached to an electronic document or transaction, including:

- User authentication to an internal application to approve something, such as when a supervisor logs into an application to approve a leave request
- Using a stylus on a tablet touchscreen to write a signature by hand and capture it in electronic form

- A typed name or signature block in an email
- User authentication to access a website, coupled with a mouse click on some form of acknowledgment button to capture intent
- A scanned hand-written signature on an electronic document
- A sound such as a recorded voice command (for example, a verbal confirmation in response to a question)

PIPEDA also recommends how an e-signature must be applied in different scenarios based on the level of authentication required.

On a provincial level, legislation governing electronic transactions has been enacted in all the provinces and territories of Canada. The legislation of each province and territory (except for Quebec) is largely modelled on the Uniform Electronic Commerce Act of Canada ("UECA"), which is a piece of legislation rather than a binding piece of legislation. For example, Ontario has enacted the Electronic Commerce Act (2000) (the "Ontario Act"), British Columbia has enacted the Electronic Commerce Act (2000) (the "BC Act") and Alberta has enacted the Electronic Transactions Act (2001) (the "Alberta Act").

The Ontario Ministry of the Attorney General issued a Notice to the Public and Legal Profession on February 24, 2022 in regards to electronic signatures. It specifies acceptable formats of electronic signatures as:

- A certificate based digital signature
- A scan of a wet handwritten signature
- A non-wet handwritten signature generated by hand using electronic stylus, track pad, touchscreen, etc.

COURT CASINGS AND RULINGS INVOLVING SIGNATURES

Humphreys v. Houston Pizza Venture Rest. Grp.

Humphreys (plaintiff) twice worked as a delivery driver for Houston Pizza Venture Restaurant Group (defendant) at its Papa John's location in The Woodlands, Texas. Humphreys first began her employment with Houston Pizza in January 2015 and based on her payroll records she was terminated voluntarily in July 2015 and later returned in November 2015.

Humphreys alleged in this lawsuit that she was sexually harassed by a co-worker and that the defendants discriminated against her by ignoring her complaints. She also complained, due to her complaint's defendant revoked her promotion and raise which forced her to resign.

In response Houston Pizza alleged that as a standard "on boarding" process for a newly hired employee at their business, Humphreys had electronically signed for the Dispute Resolution Program ("DRP") that requires arbitration of employment-related disputes. To this Humphreys testified that she did not sign any application during the on boarding process.

By tracking back to find who and when signed the DRP it was found that Humphreys performed her on boarding process, including accessing the DRP screen, on January 16, 2015 at 2:10 p.m. from her portal to which she had a unique, personal password that was unknown to Houston Pizza or any of its employees.

As a conclusion, the court identified her e-signature as legally binding and quoted "A certified digital signature is a valid form of signature" [40]. This is an example of how usage of e-signature proved helpful to track back to verify the signee.

Klein v. Delbert Servs. Corp.

Around January 2012, Klein obtained a personal loan from CashCall, Inc. At the time he submitted his online loan application, Klein was provided with a document titled CashCall, Inc. Promissory Note and Disclosure Statement.

To execute the Note and receive his loan proceeds, Klein was required to check several consent boxes during the online application process which represented confirmation of having read and understood the arbitration provision and agreed to be bound to arbitration provision terms. Upon Klein's execution of the Note by way of electronic signature on January 11, 2012, CashCall funded his loan.

Around May 2014, CashCall engaged Delbert to perform collection activities on Klein's account. In response Klein filed a Complaint on January 30, 2015, alleging that Delbert used deceptive means in connection with the collection of a debt.

Delbert moved to compel arbitration, to which Klein had given his consent. But Klein argued by saying that Delbert has no admissible evidence that he voluntarily signed the Note or voluntarily checked the boxes. The court disagreed and declared that checkmarks are sufficient to establish Klein's acceptance of the terms of the Note and the arbitration provision, quoting "(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation" [41].

Mallia v. Drybar Holdings

Plaintiff Salvatore Mallia, Jr., ("Mallia") alleged that he was terminated by Defendant Drybar Holdings, LLC ("Drybar") due to discrimination which he experienced while in Drybar's employ. Defendants claimed Mallia signed a binding arbitration agreement when Drybar first hired him.

Drybar maintains all job-related paperwork online, including "New Hire Paperwork" through a program called "My Staffing Pro," which allows employees to sign and acknowledge any job-related paperwork through "eSign" and documents provided by Drybar indicated that Mallia, Jr. electronically signed the Arbitration Agreement on August 30, 2017. As a result, the court dismissed all the claims under this action.

Armstead v. Starbucks Corp.

Plaintiff Ebony Armstead alleged that defendant Starbucks Corporation required her to work approximately 9.5 uncompensated hours each week and failed to pay overtime for hours worked more than 40 per week, which is in violation of the Fair Labor Standards Act.

In response Starbucks claimed that Armstead had electronically signed an arbitration agreement (the "Arbitration Agreement") that requires her claims to be decided by an arbitrator during the hiring process.
Armstead asserted that she did not knowingly consent to the Arbitration Agreement. According to her, the Agreement was "hidden" and "buried" by Starbucks as part of a complicated, multi-step application process that was misleadingly presented as a mere formality.

Further Starbucks stated that Armstead could not have electronically signed the Arbitration Agreement without first clicking a "View" button that opened a copy of the agreement and as per Starbucks records it was found,

- Armstead electronically signed the Arbitration Agreement at 9:43 a.m. on May 18, 2015
- She received an automatically generated e-mail which was sent to her e-mail address, with an attached copy of the Arbitration Agreement.

As a result, Defendant's motion to compel arbitration was granted by the court.

CANADA COURT RULINGS

City of London v. Caza

In September 2009 London Police Service implemented a new technology which allows for the issuance of electronically based Provincial Offence Notices, to replace the traditional paper ticket. To issue an e-ticket a police officer must log into their secured portal, fill in required details and apply a signature before printing a copy.

On November 18th, 2009, in the course of his regular duties, Constable Cory Rowsell personally served electronically signed e-tickets upon Brian Caza, Michael Gorlick and Chelsea O'Donoghue (the respondents) for various offences. On January 5th, 2010, His Worship Justice of the Peace J. Bruinewood examined the tickets to determine if they were complete and regular on their face but proceeded to annul the tickets as they were e-signed rather than with pen-and-ink.

Later on, this issue was put before the Superior Court of Justice, who acknowledged the electronic signature of the policer officer affixed to the tickets in accordance with the regulation and validated the standing of the three tickets.

Elementary Teachers' Federation of Ontario v Grand Erie District School Board

On June 25, 2020 voting was held where all the occasional/casual Designated Early Childhood Educators in the employ of the Grand Erie District School Board were required to vote to indicate whether they wish to be a member of Elementary Teachers' Federation of Ontario. Three days before the voting day, Elementary Teachers' Federation of Ontario (the Applicant) submitted an electronic membership evidence, which was electronically signed by the members using Adobe sign, to the Ontario Labour Relations Board.

Due to the nature of the membership evidence, the Board demanded for a detailed explanation of security and verification measures that were taken by the applicant to ensure the authenticity of the electronic signature. However, next day the applicant responded with a submission describing all the necessary details like

- When the member opened the hyperlink sent to them by the organizer (the applicant), which directed them to the blank membership webpage.
- When the member signed the membership form using the Adobe "draw" function.
- The date and time that the document was filled in by the applicant for membership, as well as the IP address of the device which the document was filled out on.

Due to the availability of detailed data and audit trail Board was satisfied and accepted the electronic membership evidence.

Alberta Union of Provincial Employees v Masterpiece Retirement

In October 2020 Alberta Union of Provincial Employees (the Union) applied to become the certified bargaining agent for employees at Masterpiece Southland Meadows (Masterpiece Retirement) and submitted electronic support petition which was electronically signed, using Adobe Sign, by the employees and by the Union's organizer for verification.

In response, the respondent challenged the authenticity of the submitted petition as it was electronically signed by the Union and its bargaining unit. To support it's evidence the Union submitted

- an Audit Report with details like, who signed the document, date and time when the petition was electronically signed, IP address of the device, who viewed the signed document and when, etc.
- and a detailed testimony on how Adobe Sign functioned to certificate of authenticity.

After reviewing the details above, the Board was satisfied and accepted the electronic petition, in addition to this the Board also quoted, "In general, we expect the use of electronic membership or petition evidence will become more frequent in Alberta. An applicant seeking to use such technology should be prepared to provide the Board with a detailed explanation of the security and verification measures that have been taken to ensure the authenticity and integrity of electronic evidence."

E-SIGNATURE INCENTIVES

STATE OF UTAH

Spencer J. Cox, Lieutenant Governor of Utah introduced eSign as part of the New Workplace Teleworking Initiative, which utilizes Adobe Acrobat Sign. The primary purpose of the initiative is to improve government efficiency, enabling employees to work remotely.

Utah officials could not have possibly known how important it would become to provide telework capability. While the State had contingency plans in place in case of natural disasters, no one could have predicted for Utah to be simultaneously struck by a 5.7 earthquake and the growing threat of the COVID-19 pandemic. Fortunately, the employees working for the State of Utah had a digital solution in place to keep vital services running even while impacted. Almost immediately, residents were able to access these much-needed government services.

COLORADO DEPARTMENT OF TRANSPORTATION

The Colorado Department of Transportation (CDOT) transformed its operations by moving to Adobe Acrobat Sign to manage its complex documents that can stretch up to 3,000 or more pages which involves sign from dozens of professional engineers who need to sign multiple pages, sometimes even requiring multiple seals on the same page, along with integration to their existing ProjectWise system.

According to Tom Bovee, CDOT ProjectWise Program Manager “Using Adobe Acrobat Sign for electronic routing and signing, we’re projecting a reduction in signature turnaround times by 85 to 90 percent. Plus, we estimate we’ll be saving more than $100,000 in labor, printing, shipping, scanning, and document storage costs.”

STATE OF HAWAII

The State of Hawaii has seen dramatic changes since the deployment of the Adobe Sign, while it once took two weeks or longer to route a document for signature, now a contract can make its way up the chain of approvals and to the governor’s desk in just a few hours. To date, the state has processed more than 400,000 documents through Adobe Sign, including travel forms, approval forms, expense claims, accounting forms, and payslip confirmations for 40,000 people in each pay cycle. It has also helped government employees who used to spend two hours on their first day filling out onboarding papers, can now fill out online forms at home before even setting foot in the office.

David Ige Governor, State of Hawaii remarks “Our eSign Services initiative helped kick off a digital transformation throughout the state government that encourages us to be more agile and responsive so that we can deliver better and more valuable services for our citizens.”

APPENDICES

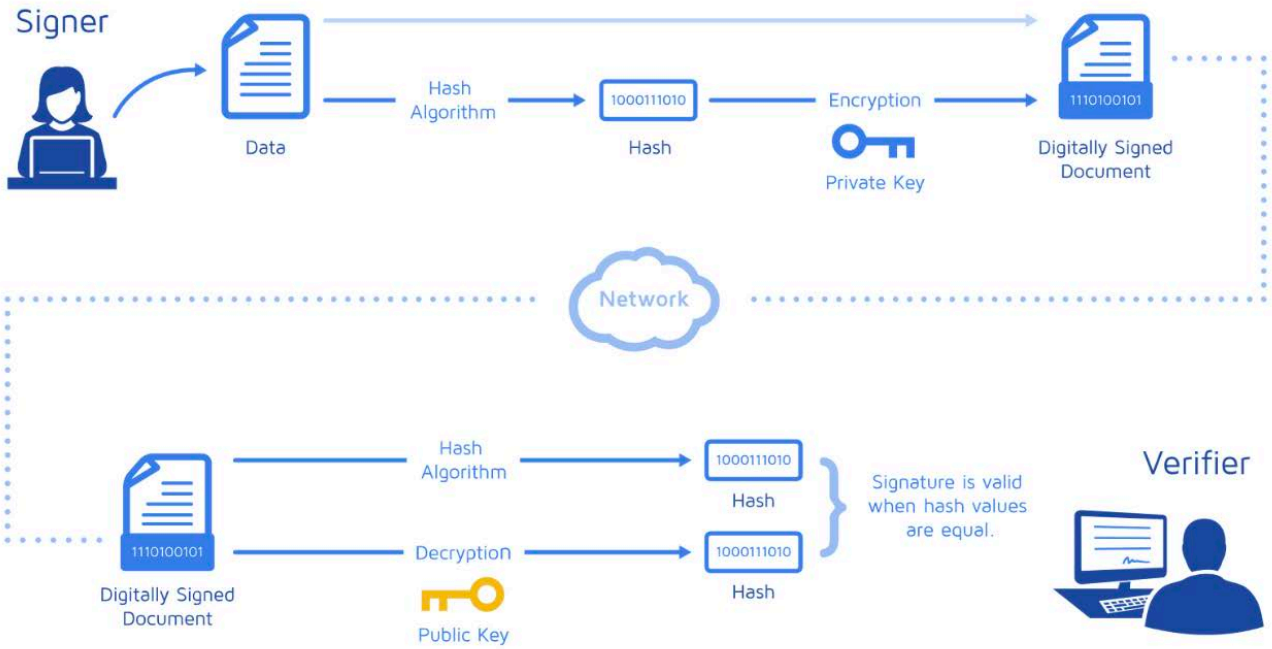
HOW DO DIGITAL SIGNATURES WORK

Like wet signatures, a digital signature is unique to the signee. Digital signatures use a protocol called PKI (Public Key Infrastructure). PKI demands that the provider of the document(?) create two long numbers, called keys, using a mathematical algorithm. One key is private, and the other is public. In most normal operations all of this is automated and provided by the digital signature tool or provider.

When a signee digitally signs a document, their private key, which was generated when they registered with or created an account with a digital signature provider, is used to create the signature. The algorithm creates a hash of the signed document, The hash of the document is a string of characters generated from the document. It is effectively a digital fingerprint of the document since chances of any two documents producing the same hash output is extremely small. The generated hash is then encrypted using the private key generated for this signee. The resulting encrypted hash is the digital signature. The date and time when the signature was made are also noted. The encrypted hash allows to check the signee's identity and original document in the following ways:

- The identity of the signer can be verified by using their public key to decrypt the signature and checking the hash against the document. If the hash does not decrypt properly then this is not the right person

- If the hash decrypts, but the hash does not match the hash for the document in its current state then it is clear that the document has been modified
  Let's look at it with an example, where Alice digitally signs a document and sends it to Bob. Alice uses her private key to sign a contract to sell a product. The document is sent to the buyer (Bob) who also receives a copy of Alice's public key. If the public key can't decrypt the signature, it suggests the signature isn't Alice's, or has been changed since it was signed. The signature is then considered invalid [11].



REMOTE ONLINE NOTARIZATION

Notarization is the final seal on many crucial documents, from business agreements to closing a real estate sale. However, finding a notary and getting to them in person is becoming more of a challenge. It can get even more complicated when you need to notarize a document in a hurry. A convenient solution is to use an electronic notary service.

An electronic notary works like a traditional notary, except they are online. An electronic notary service connects you with a secretary of state-certified professional notary through a video conference call. During the session, you'll prove your identity and authenticate your document, before signing and certifying it digitally [23] [24].

There is a detailed description around the legality and acceptance of remote online notarization in USA and Washington under section 9.3.

E-SIGNATURES IN OTHER COUNTRIES

European Union: eIDAS (Except in Switzerland)

Electronic Identification, Authentication and Trust Services (eIDAS)

EIDAS stands for "Electronic Identification, Authentication and Trust Services," and is the commonly used name for the EU regulation 910/2014 governing electronic identification and trust services for European Union Member States.

All public services in the Member States must recognize national electronic identification schemes (eIDs). eIDAS defines the standards across the EU for electronic identification (eID), electronic signatures, time stamps, electronic seals, and other proof of authentication that give electronic transactions legal validity equivalent to paper documents. The eIDAS regulation has been enforceable across the EU since 2016 July 01 [28] [29].

Some of the trust services it governs include:

- Advanced and Qualified Electronic Signatures associated to a legal or natural person
- Advanced and Qualified electronic seals associated to a legal entity
- Electronic identification (eIDs) - currently not provided by DigiCert
- Qualified timestamping
- Qualified Web Certificate for Authentication (QWAC)
- Electronic Registered Delivery Services (ERDS) - currently not provided by DigiCert
- Validation Services - currently not provided by DigiCert

Australia: Electronic Transactions Act

The Australian Government is working to make it easier and more reliable to use electronic communications in business and personal transactions. This includes a commitment to provide government services online wherever possible.

The Electronic Transactions Act 1999 ensures that a transaction under an Australian Commonwealth law will not be invalid simply because it was conducted through electronic communication [30] [31].

If an Australian Commonwealth law requires you to:

- give information in writing;
- provide a handwritten signature;
- produce a document in material form; or
- record or retain information

The Electronic Transactions Act means you can do these things electronically.

According to the Electronic Transactions Act an e-signature can be used legally to show the person's intention in relation to the information communicated.

New Zealand: Electronic Transactions Act

The Electronic Transactions Act 2002 helps businesses, individuals, and the government to manage commercial transactions electronically. It gives certain electronic information the same legal status as paper-based information, making certain electronic communications valid. Specifically, you can generally meet a requirement by electronic means when there is a legal need for the information:

- to be in writing;
- to be given in writing; or
- recorded in writing

This is significant because it allows individuals, businesses, and the New Zealand Government to exchange and accept information online [32] [33] [34].

DEFINITIONS

- Certificate authority (CA) – A CA is a trusted third party that validates a person's identity and either generates a public/private key pair on their behalf or associates an existing public key provided by the person to that person. Once a CA validates someone's identity, they issue a digital certificate that is digitally signed by the CA. The digital certificate can then be used to verify a person associated with a public key when requested.

- Trust service providers (TSPs) - A trust service provider (TSP) is a person or legal entity providing and preserving digital certificates to create and validate electronic signatures and to authenticate their signatories as well as websites in general.

- Protocol – Protocol is an established set of rules that determine how data is transmitted between different devices in the same network.

- Encrypt - To change electronic information or signals into a secret code (= system of letters, numbers, or symbols) that people cannot understand or use on normal equipment.

- Decrypt - To change electronic information or signals that were stored, written, or sent in the form of a secret code (= a system of letters, numbers, or symbols) back into a form that you can understand and use normally.

- Hash function – A hash function (also called a "hash") is a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function— a computed hash cannot be reversed to find other files that may generate the same hash value.

- Public key cryptography – Public key cryptography (also known as asymmetric encryption) is a cryptographic method that uses a key pair system. One key, called the public key, encrypts the data. The other key, called the private key, decrypts the data. Public key cryptography can be used several ways to ensure confidentiality, integrity, and authenticity.

- Public key infrastructure (PKI) – PKI consists of the policies, standards, people, and systems that support the distribution of public keys and the identity validation of individuals or entities with digital certificates and a certificate authority.

- Digital certificates – Digital certificates are analogous to driver licenses in that their purpose is to identify the holder of a certificate. Digital certificates contain the public key of the individual or organization and are digitally signed by a CA. Other information about the organization, individual, and CA can be included in the certificate as well.

- Pretty Good Privacy (PGP)/OpenPGP – PGP/OpenPGP is an alternative to PKI. With PGP/OpenPGP, users "trust" other users by signing certificates of people with verifiable identities. The more interconnected these signatures are, the higher the likelihood of verifying a particular user on the internet. This concept is called the "Web of Trust."

- Electronic Signatures in Global and National Commerce (ESIGN) Act - ESIGN Act gives electronic signatures the same legal standing as handwritten ones, substantially streamlining and speeding up how businesses collect, track, and handle signatures and approvals on all kinds of agreements and documents.
- HIPAA - HIPAA is an acronym for the Health Insurance Portability and Accountability Act. The Act led to the establishment of federal standards for safeguarding patients´ “Protected Health Information” (PHI) and ensuring the confidentiality, integrity, and availability of PHI created, maintained, processed, transmitted, or received electronically (ePHI).
- Contact claims - Contract claims are court cases that result from a breach of contract. When a party breaches a contract, and another party files a claim, the injured party will have access to a variety of remedies, including monetary damages and enforcement of the contract.
- Plaintiff - the party who initiates a lawsuit by filing a complaint with the clerk of the court against the defendant(s) demanding damages, performance and/or court determination of rights.
- Defendant - The person defending or denying; the party against whom relief or recovery is sought in an action or suit, or the accused in a criminal case.
- Respondent - The party who answers a bill or other proceeding in equity. The party against whom an appeal or motion, an application for a court order, is instituted and who is required to answer in order to protect his or her interests.
- Petitioner - One who presents a formal, written application to a court, officer, or legislative body that requests action on a certain matter. In legal proceedings initiated by a petition
- Arbitration - The submission of a dispute to an unbiased third person designated by the parties to the controversy, who agree in advance to comply with the award—a decision to be issued after a hearing at which both parties have an opportunity to be heard.

REFERENCES

[1] [Online]. Available: https://legal-dictionary.thefreedictionary.com/signature.

[2] [Online]. Available: https://www.forbes.com/advisor/business/electronic-signature/.

[3] [Online]. Available: https://usefulpdf.com/blog/types-of-signatures/.

[4] [Online]. Available: https://realyst.com/digital-transaction-management/different-types-of-signatures/.

[5] [Online]. Available: https://help.macquarie.com.au/adviser/s/article/What-are-the-different-types-of-signatures.

[6] [Online]. Available: https://www.termsfeed.com/blog/i-agree-checkbox/.

[7] [Online]. Available: https://incorporated.zone/by-signing-this-agreement-you-agree/.

[8] [Online]. Available: https://luxsci.com/blog/is-a-click-here-to-agree-checkbox-really-legally-binding.html.

[9] [Online]. Available: https://helpx.adobe.com/sign/using/legality-united-states.html.

[10] [Online]. Available: https:/www.cisa.gov/uscert/ncas/tips/ST04-018.

[11] [Online]. Available: https:/www.cisa.gov/uscert/ncas/tips/ST04-018.

[12] [Online]. Available: https:/www.geeksforgeeks.org/difference-between-electronic-signature-and-digital-signature/.

[13] [Online]. Available: https://www.lawdepot.com/blog/signing-legal-contracts-does-a-signature-need-to-be-in-cursive/#:~:text=There%20are%20two%20main%20purposes,the%20stipulations%20of%20the%20contract.

[14] [Online]. Available: https://www.leegality.com/blog/whats-a-signature.

[15] [Online]. Available: https://www.adobe.com/sign/hub/features/how-to-solve-esignature-challenges-docx.

[16] [Online]. Available: https://blog.waiverforever.com/electronic-signatures-legally-binding/.

[17] [Online]. Available: https://www.adobe.com/sign/hub/features/how-to-solve-esignature-challenges-docx.

[18] [Online]. Available: https:/www.investglass.com/what-are-the-top-5-advantages-of-digital-signatures-with-rpa/.

[19] [Online]. Available: https://dvv.fi/en/benefits-of-electronic-signature.

[20] [Online]. Available: https://penneo.com/blog/7-advantages-digital-signatures/.

[21] [Online]. Available: https://penneo.com/blog/7-advantages-digital-signatures/.

[22] [Online]. Available: https://www.adobe.com/sign/hub/features/how-to-solve-esignature-challenges-docx.

[23] [Online]. Available: https://www.expertbells.com/blog-detail/top-10-benefits-of-digital-signature-certificate.

[24] [Online]. Available: https://www.adobe.com/documentcloud/integrations/notarize.html.

[25] [Online]. Available: https://www.adobe.com/sign/hub/how-to/how-to-notarize-electronically.

[26] [Online]. Available: https://helpx.adobe.com/sign/using/legality-united-states.html.

[27] [Online]. Available: https://securiti.ai/canada-pipeda/.

[28] [Online]. Available: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html#toc1.

[29] [Online]. Available: https://www.eid.as/.

[30] [Online]. Available: https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-eidas.

[31] [Online]. Available: https://www.ag.gov.au/rights-and-protections/e-commerce#:~:text=The%20Electronic%20Transactions%20Act%201999,provide%20a%20handwritten%20signature.

[32] [Online]. Available: https://www.legislation.act.gov.au/a/2001-10.

[33] [Online]. Available: https://www.legislation.govt.nz/act/public/2002/0035/latest/DLM154185.html#DLM154823.

[34] [Online]. Available: https://legalvision.co.nz/commercial-contracts/electronic-transactions-act/#:~:text=The%20Electronic%20Transactions%20Act%202002,status%20as%20paper%2Dbased%20information.

[35] [Online]. Available: https://blog.waiverforever.com/electronic-signatures-legally-binding/.

[36] [Online]. Available: https://www.usfn.org/blogpost/1296766/354058/Some-Good-News-in-Pandemic-Times-Washington-State-s-Electronic-Signature-and-Notary-Laws-Are-Effective.

[37] [Online]. Available: https://app.leg.wa.gov/RCW/dispo.aspx?cite=19.360.030.

[38] [Online]. Available: https://ocio.wa.gov/sites/default/files/public/Electronic_Signature_Guidelines_FINAL.pdf.

[39] [Online]. Available: https://www.limitlesslaw.com/2020/11/02/washington-state-now-has-virtual-remote-notaries.

[40] [Online]. Available: https://casetext.com/case/humphreys-v-houston-pizza-venture-rest-grp?p=1&q=digital%20signature%20is%20valid&sort=relevance&type=case&ssr=false&scrollTo=true.

[41] [Online]. Available: https://casetext.com/case/klein-v-delbert-servs-corp?resultsNav=false#p8.

OTHER USEFUL MATERIAL

https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
https://www.dol.wa.gov/business/notary/nremote.html
WA State Licensing (DOL) Official Site: Laws, rules, and rulemaking activity for notaries public
https://app.leg.wa.gov/RCW/default.aspx?cite=42.45.280
https://www.docusign.com/sites/default/files/resource_event_files/Court%20Support_WPHM071519LEGPUBUS%20%281%29.pdf
https://aboutssl.org/what-is-digital-signature-how-does-it-work/
https://blog.adobe.com/en/2020/04/27/the-state-of-utah-uses-adobe-sign-to-accelerate-telework-during-crisis
https://blog.adobe.com/en/2020/01/13/cdot-saves-time-and-money-paving-the-way-to-digital-with-adobe-sign
https://business.adobe.com/customer-success-stories/state-of-hawaii-case-study.html#:~:text=Since%20deploying%20Adobe%20Sign%2C%20the,setting%20foot%20in%20the%20office.
https://static.carahsoft.com/concrete/files/5815/9838/0532/Adobe_Sign_Government_Solution_Brief1.pdf
https://news.adobe.com/news/news-details/2021/Adobe-Partners-With-All-50-US-States-to-Modernize-Digital-Experiences-for-Citizens/default.aspx
Mallia v. Drybar Holdings, Case No. 2:19-cv-00179-RFB-DJA | Casetext
Armstead v. Starbucks Corp, 17-cv-1163 (PKC) | Casetext
https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html
https://helpx.adobe.com/sign/using/legality-canada.html
https://www.canlii.org/en/on/onsc/doc/2010/2010onsc1548/2010onsc1548.html#cited
https://www.canlii.org/en/on/onlrb/doc/2020/2020canlii43116/2020canlii43116.html#document
https://www.canlii.org/en/on/onlrb/doc/2020/2020canlii43102/2020canlii43102.html
https://www.canlii.org/en/ab/ablrb/doc/2020/2020canlii74263/2020canlii74263.html?searchUrlHash=AAAAAQALZS1zaWduYXR1cmUAAAAAAQ&resultIndex=13
http://ontariocourtforms.on.ca/static/media/uploads/courtforms/civil/notices/csd_notice_to_public_and_profession_regarding_e-signatures_and_submissions_through_the_online_filing_portals_(final).pdf

ABOUT 4POINT

4Point is the global leader in documents and forms. We have helped customers move from paper to digital for decades. This unmatched experience makes us experts in digital transformation. Our incomparable knowledge facilitates successful transformations from paper to digital, giving organizations limitless opportunities to save money, increase efficiencies, and enhance end-user experiences.

4Point is an Adobe Gold Solution Partner that specializes in Adobe Experience Manager Sites and Adobe Experience Manager Forms. Our team is certified and trained by Adobe. This combination of Adobe training and our unmatched experience allows us to transform organizations' processes from paper to digital around the world.

In 2003, the founding members of 4Point combined their expertise in software consulting, project management and sales to develop and support leading-edge solutions based on Adobe enterprise technology. As the company grew, 4Point added decades of experience in documents and forms. As it stands today, 4Point employs many of the original architects of the Adobe forms technology used by major global organizations. This gives them unmatched experience in the application of these technologies to your business problems.

Our expertise and focus in Adobe-based enterprise level document and form solutions helps your organization meet modern business challenges through the transformation from paper to digital. 4Point gives organizations limitless opportunities to save money, increase efficiencies, and enhance end-user experiences.

As Adobe technology has evolved, so has 4Point. We've progressed from building solutions around document output to delivering online forms and workflow applications that are beyond compare. With changing technologies, 4Point continues to build smart solutions, rooted in exceptional user experiences for your business and customers.