# Digital Signatures & eSignatures in PDF

Jonathan D. Rhyne, esq.

Disclaimer: This talk does not constitute legal advice and does not establish an attorney-client relationship.

If you need legal advice, please contact an attorney directly.

# Overview

- Background on Signatures
- What is an eSignature?
- What is a Digital Signature?
- What is the current legal landscape?

# History of Signatures

# First Signatures

- Romans were known to use signatures during the reign of Valentinian III around 439 AD.
- However, it wasn’t until 1069 that the first signature from a well-known figure nobleman and military leader Rodrigo Diaz "El Cid" from Medieval Spain was recorded when making a donation to the Cathedral of Valencia.

ego ruderico

# An Act for Prevention of Frauds and Perjuries.

- In 1677, the English Parliament passed the Statute of Frauds act that required certain contracts to contain a signature shepherding in the era of signatures!
- Sale of Land, Agreements of Executor, Marriage Promises, Contracts Not to be Performed within One Year, and Promises to Pay Debt.

# An Act for Prevention of Frauds and Perjuries.

- In 1776, John Hancock, the President of the Continental Congress signs the Declaration of Independence.
- In 1954, the Uniform Commercial Code was drafted and proposed to add the Statute of Frauds to more types of contracts including the sale of anything over $500.

# Technology Changes

- In 1869, *Howley v. Whipple* established that an agreement made by telegram constituted a signed contract.
- By the 1980s, the rise of fax machines lead to many US courts deeming fax signed documents to be valid.
- In 1999, the Uniform Electronic Transactions Act (UETA) is proposed and begins to be adopted by the majority of States.

# The Electronic Signatures in Global and National Commerce Act

In 2000, President Bill Clinton signs into law the Electronic Signatures in Global and National Commerce (ESIGN) Act that facilitates the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

# What matters with a signature?

# Main Considerations

The two main considerations with signatures are

- (a) to show the signor’s intent to enter into a contract; and
- (b) that the signature was done in such a tangible medium that it could pass evidentiary standards.

# Verifying a Signature

- The most common way of verifying a wet ink signature is not a forgery is to employ the services of a qualified document examiner and have them testify in court.
- The most common forgery method of a wet ink signature occurs by tracing or copying a person's signature either through transmitted light, carbon intermediate or using pressure to ident the image.

# Verifying a Signature

A document examiner typically looks at the following when examining a signature:

- Speed and pressure of the signature
- Pen lifts or hesitation marks
- Tremor lines due to the signature being drawn slowly
- Thick starts and stops
- Whether the two signatures were a perfect match

# What is an eSignature?

# eSignature

- An electronic signature is defined as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign" (eIDAS Article 3).
- This is the broadest definition. From here there are further distinctions in jurisdictions for Advanced and Qualified eSignatures.

# Advanced eSignature

Common elements:

- The signatory can be uniquely identified and linked to the signature
- The signatory must have sole control of the private key that was used to create the electronic signature

# Advanced eSignature

Common elements, continued:

- The signature must be capable of identifying if its accompanying data has been tampered with
- In the event that the accompanying data has been changed, the signature must be invalidated

# What is a Digital Signature?

# Digital Signatures

- A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

# Digital Signatures

- Think of it as like a digital fingerprint.
- Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance.
- They are a specific technological implementation of electronic signatures.

# Current Legal Landscape

# US UETA & ESIGN Acts

Both laws sought to give electronic records & signatures the same legal effect of wet-ink signatures by providing the following:

- No contract, signature, or record shall be denied legal effect solely because it is in electronic form
- A contract relating to a transaction cannot be denied legal effect solely because an electronic signature or record was used in its formation

# US UETA & ESIGN Acts

Both Acts have four major requirements for an eSignature to be valid:

- Intent to Sign
- Consent to do business electronically
- Association of signature with the record
- Record retention

# US - Intent to Sign

- Like a wet-ink signature, both parties to the contract must intend to sign for the electronic signature to be valid.
- The US laws really focused on intent since often the objection in US courts was not to who or whether it was their actual signature but the validity of the instrument used.

# US - Consent

- The parties to the transaction must consent to do business electronically.
- Between a business to business transaction there is a lower standard and can be establish by analyzing the circumstances surrounding the transaction.

# US - Consent

Transactions involving consumers require that:

- the consumer has received the UETA Consumer Consent Disclosers
- Affirmatively agreed to use electronic records for the transaction
- Has not withdrawn their consent before signing

# US - Association of Signature

- In order for a signature to qualify as a valid eSignature then the system that captures the transaction must keep an associated record.
- The record must reflect the process by which the signature was created, or generate a textual or graphic statement that can then be added to the signed record, proving that it was executed with an electronic signature.

# US - Record Retention

- eSignature records must be capable of retention and accurate reproduction to all parties entitled to retain the contract or record.
- The best way to maintain retention and ensure accurate reproduction is via the PDF file type.

# US - Further Considerations

- These laws are the minimal requirements and depending on the industry, use case and associated state and federal regulations there might be additional requirements.
- As stated before, since the laws focused primarily around intent and validity to use an electronic medium they left a gap that can cause evidentiary issues.

# US - Further Considerations

- Most of these additional considerations, such as electronic records and signatures that are accepted by the Federal Drug Administration (FDA), revolve around resolving the evidentiary issues.
- These can include requirements that ensure accuracy, reliability, protection, the ability to limit access to only authorized individuals, and a secure electronic audit log of actions.

# EU - eIDAS Regulation

- eIDAS went into effect on July 1, 2016 and replaced the older eSignature Directive.
- eIDAS defined three types of eSignatures:
    - Simple
    - Advanced
    - Qualified

# EU - eIDAS Regulation

- eIDAS focused more on the technological process of verifying the identity of the signor, security around the process, and ensuring that the signature has not been tampered with.
- Purpose was again to allow the evidence of any of the three types of eSignatures to be admissible as evidence.

# EU Considerations

- Many member states in the European Union have specific transactions that cannot be electronically signed such as land transfers or certain corporate formation documents.
- Further, since it’s an evidentiary standard there’s always the case that the more a signature follows eIDAS the heavier weight the signature will be given.

# So how does this relate to PDF?

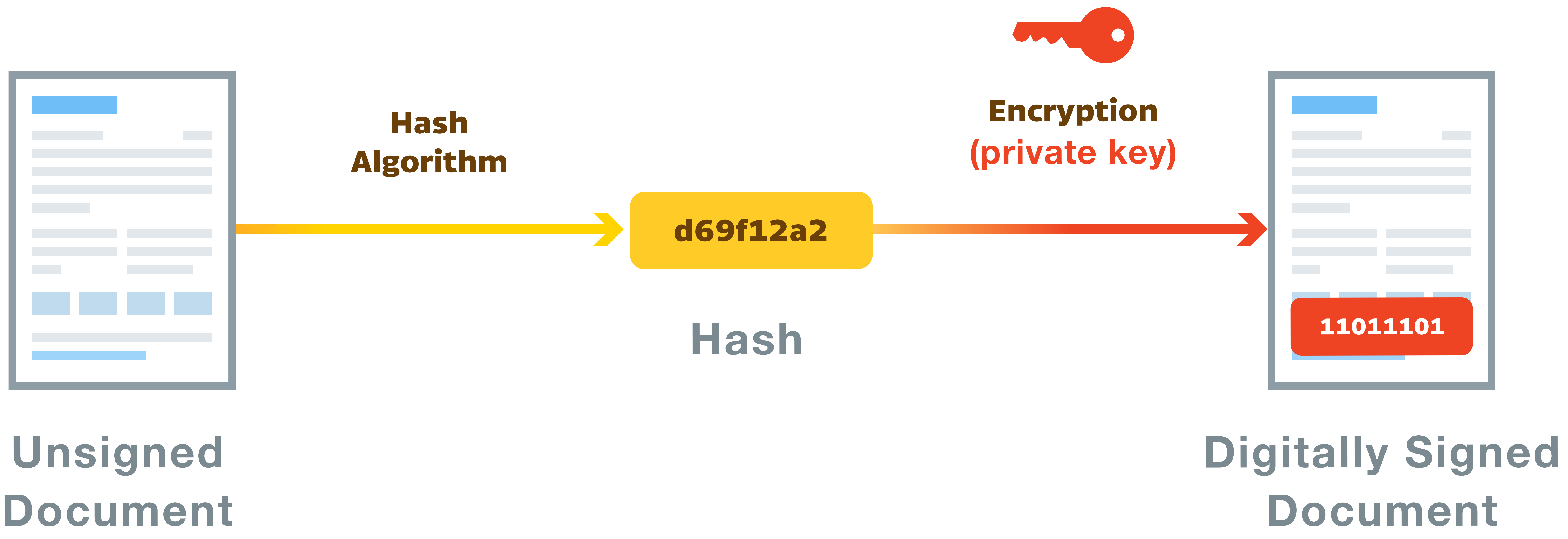
# Digital Signatures with PDF

- Through the PDF Spec, you can create and verify a cryptographically secure Digital Signature when signing a PDF using the public key infrastructure (PKI) protocol.
- The PKI protocol uses a mathematical algorithm to generate two long numbers, called keys. One key is public, and one key is private.

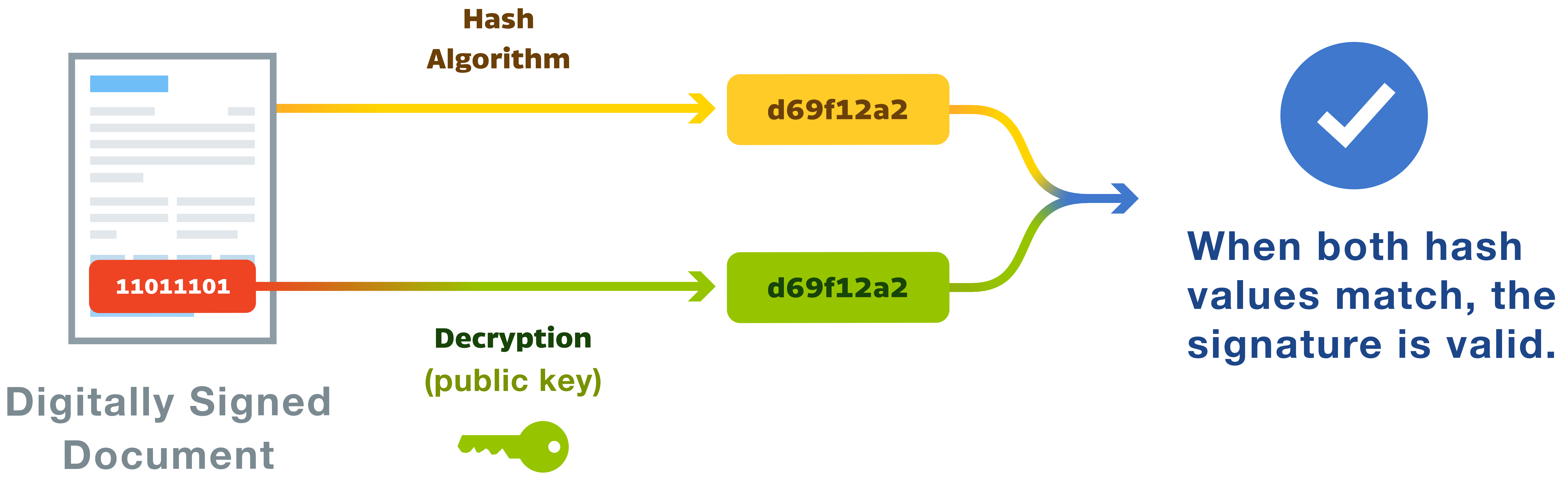
# Digital Signatures with PDF

- When a signer e-signs a PDF, the signature is created using the signer’s private key. The algorithm acts as a cipher, creating data called a hash and encrypting the hash matching the signed document. The resulting encrypted data is the digital signature.
- The digital signature can also be marked with other meta data, typically the time that the document was signed but also can include data such as pressure sensitivity, time and speed of signing, touch radius, and input method.

# Digitally Signing a Document



# Validating a Signature



When both hash values match, the signature is valid.

# Digital Signatures in PDF

- With Digital Signatures relying on public and private keys, parties want assurances that the document and keys are valid and were created securely to prevent forgery or malfeasance.
- Certificate Authorities are third-party organizations that have been widely accepted and/or vetted by regulatory bodies as being reliable for issuing the necessary digital certificates and ensuring key security.

# Digital Signatures in PDF

- A Digital Certificate contains the public key for a digital signature and the identity associated with the key. The certificate confirms the specific key belongs to the particular party and the Certificate Authority acts as the guarantor.
- Certificate are valid for a time limited period and must be issued by a trusted authority. Both the sender of the document and the signor have to agree to use a given Certificate Authority

# PaDES Standard

- PaDES - PDF Advanced Digital Electronic Signatures standard is an extension to the PDF and ISO 32000-2 spec that specifies precise profiles making it compliant with the European Union eIDAS regulation.
- PaDES introduced a number of adaptations and extensions to PDF that were proposed back into ISO and included in the latest release of the PDF standard, ISO 32000-2.

# PaDES Standard

- The major advantage of PaDES is the ability to keep a signatures long term validity by digitally time stamping when the PDF is signed as well as time stamping when the certificate was verified as valid and storing the data in the PDF.
- This ensures that after a certificate has expired or if later was revoked due to it being compromised that it is still possible to determine whether the signature was valid at the time of signing.

# Thank you!

## Questions?