Digital Signatures

Supervised By
DR. Basheer Abdel Fatah Youssef

Prepared By

Mootaz Medhat Ezzat Abdelwahab
mootazmwahab@gmail.com

Presenters

Name	ID
Dalia Gamal Abdelhamed	20206023
Mootaz Medhat Ezzat Abdelwahab	20206074

Outlines

- What are Signatures?
- What are Electronic Signatures?
- Different Types of Electronic Signatures.
- What are Digital Signatures?
- What makes up a Digital Signature?
- How does a Digital Signature work?
- Benefits of using Digital Signature

What are Signatures?

Traditional Pen-and-Paper Signatures

Traditional Pen-and-Paper Signatures

- Signatures, in a broad sense, are marks or symbols that represent the identity of a person or entity. They are used to **authenticate** documents, contracts, agreements, or transactions.

- In its simplest form, a signature is a handwritten mark made by an individual on paper document. It serves as proof of consent, agreement, or **authorization**. For instance**:**
  - **Signing** a rental agreement for your new apartment or a contract with a new employer.
  - **Signing** a check at the bank or a delivery receipt upon receiving a package.




- Signatures are essential for establishing the **authenticity** and **integrity** of documents, ensuring **accountability**, and preventing **fraud** or **tampering**.

Authorization & Authentication

Authorization

- Signatures serve as proof of authorization because they signify consent, agreement, or permission granted by the signer to carry out the actions or terms outlined in a document.

Authentication

- Signatures are used for authentication because they confirm the identity of the signer, thus validating the legitimacy of a document or transaction.
- They ensure that the individual or entity is what they claim to be.

" Your signature on a document authorizes a transaction or agreement (indicates your consent or agreement to the contents of the document), while the authentication of signatures verifies the validity (verifies your identity) and legitimacy of the document. "

With The Advent of Digital Technologies,

Have Evolved Into

Traditional Pen-and-Paper Signatures

Electronic & Digital Signatures

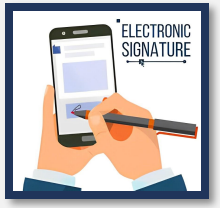
Providing More Efficient and Secure Means of Authentication in The Digital World

What are Electronic Signatures?

E-Signatures

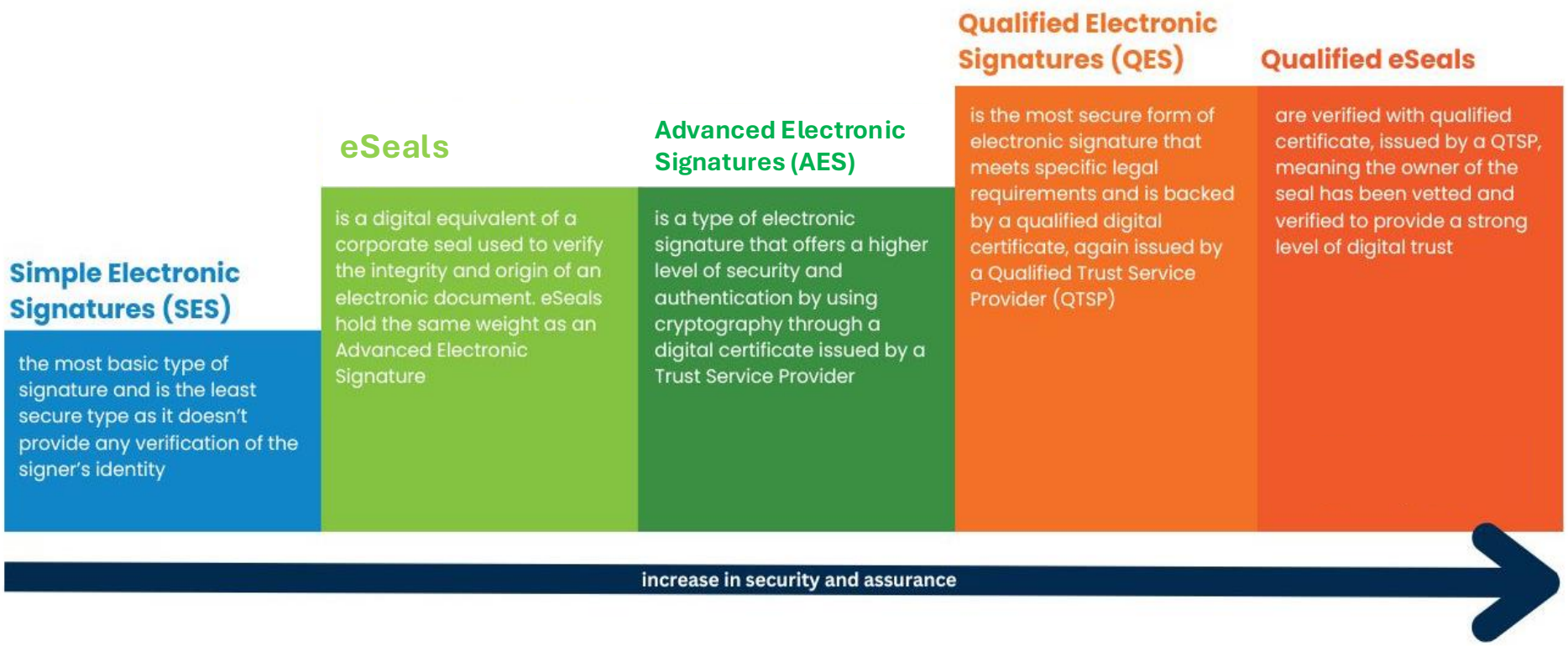
Electronic Signatures (E-Signatures)

- Electronic signatures are **digital versions** of traditional handwritten signatures.
- Electronic signatures can take various forms for **digitally signing** messages, including emails, digital documents, contracts, agreements, forms, and approvals. **(online without the need to print them)**
- **These various forms of the e-signatures include:**
  - Uploading a scanned image of your handwritten signature.
  - Drawing a signature on a digital device using a stylus or mouse.
  - Typing your name at the signature portion of an online form.
  - Clicking on "I agree" to terms and conditions button on a website.



- **There are five different types of electronic signatures, each allowing users to sign documents digitally, offering some degree of identity authentication and message integrity.**

Types of Electronic Signatures



Authenticity & Integrity

Identity Verification (Authenticity)

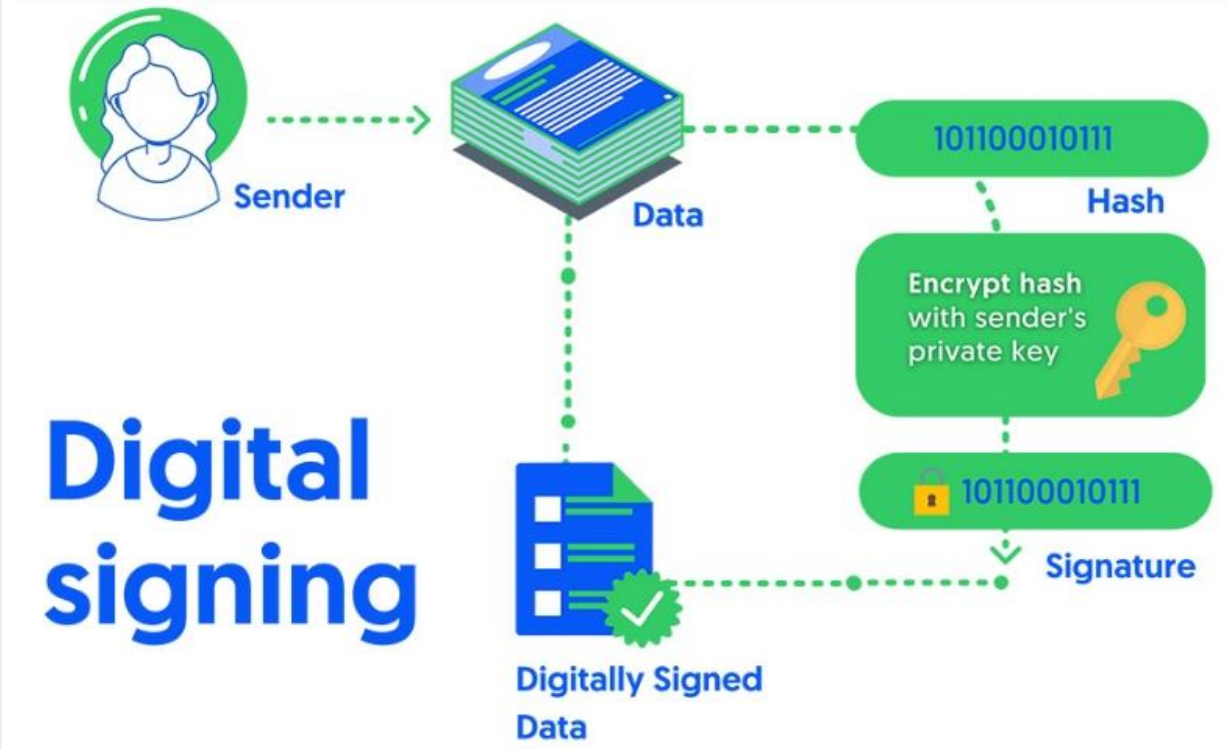
Not all electronic signature types provide definitive proof of the **signer's identity**, as they can be easily **copied** or **forged**. This lack of **identity verification** raises concerns about the **authenticity** of the **signature** and the signer's intentions.

Tamper Detection (Integrity)

Not all electronic signature types can detect if someone **tampers** with the document after it is signed. This poses a risk to the **integrity** and **authenticity** of the document, as it may be **altered without detection**.

What are Digital Signatures?

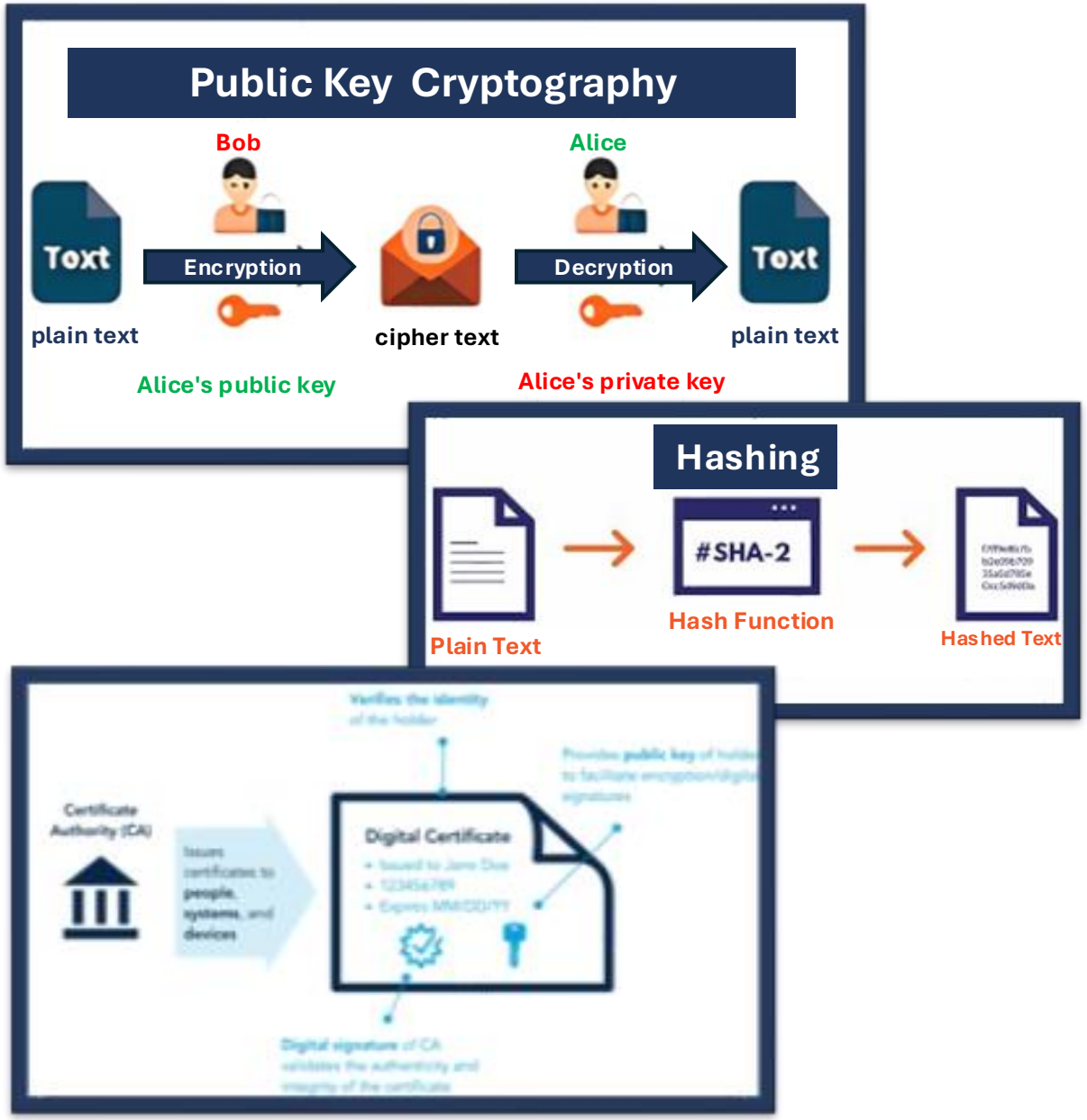
PKI-based digital certificate



Digital Signatures

- Digital signatures are one of electronic signature types and are the most secure type available.
- Digital signatures specifically utilize advanced cryptographic techniques to add an extra layer of security and authentication to the signed messages.
- Digital signatures use public key infrastructure **(PKI)**, which is considered the gold standard for digital identity authentication and encryption.
- Digital signatures create a digital fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. (In emails, the email content itself becomes part of the digital signature)
- **Digital signatures assure that:**
  - The message is authentic and comes from a verified source.
  - Identities have been verified by a publicly trusted organization **(the CA)**.
  - The message has not been tampered with since being digitally signed as the signature would be displayed as invalid if changes were made.

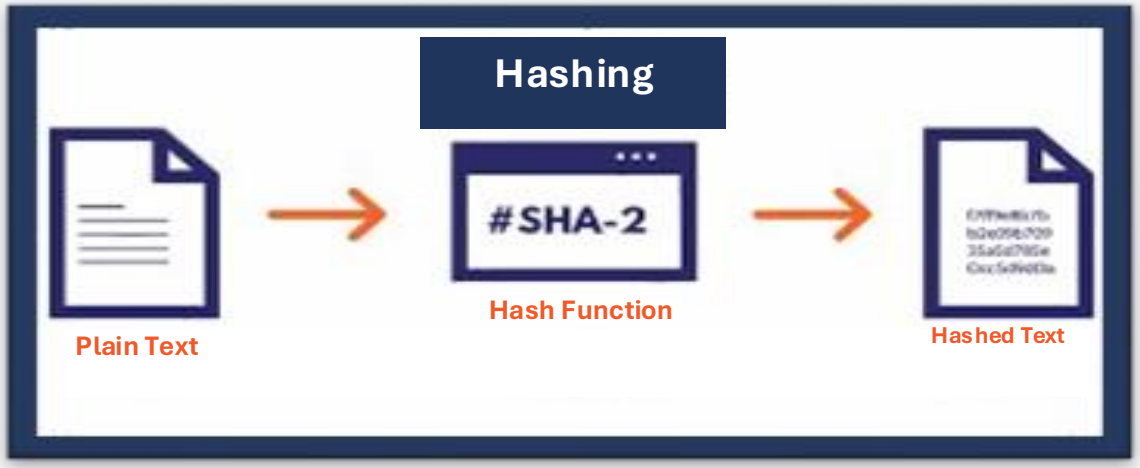
What makes up a Digital Signature?



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**.

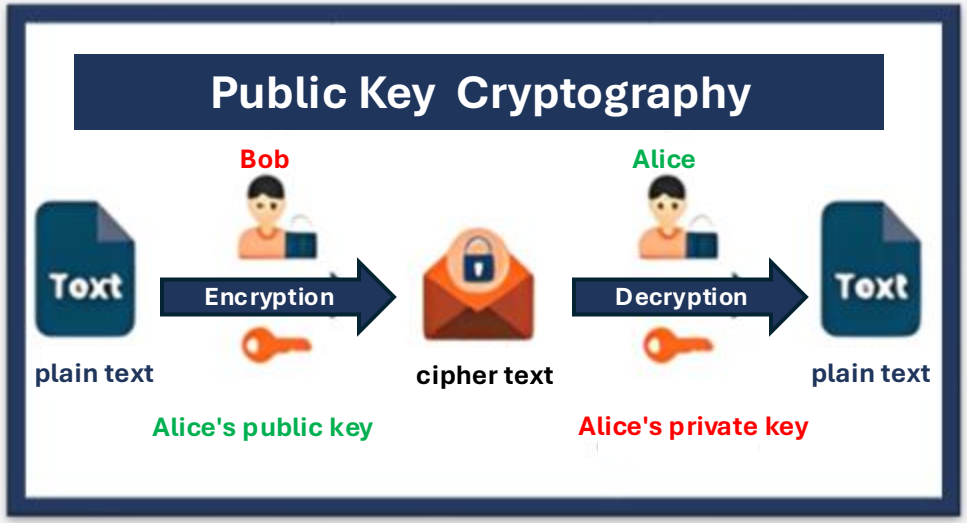
- This generated string is unique to the file being hashed and is a one-way function **(a computed hash cannot be reversed to find other files that may generate the same hash value)**



- **Some of the more popular hashing algorithms in use today are:**
  - Secure Hash Algorithm-1 **(SHA-1)**
  - Secure Hashing Algorithm-2 family **(SHA-2 and SHA-256)**
  - Message Digest 5 **(MD5)**

Public key Cryptography (Asymmetric Encryption)

- Public key cryptography 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**.

Certificate Authority (CA) & Digital Certificates

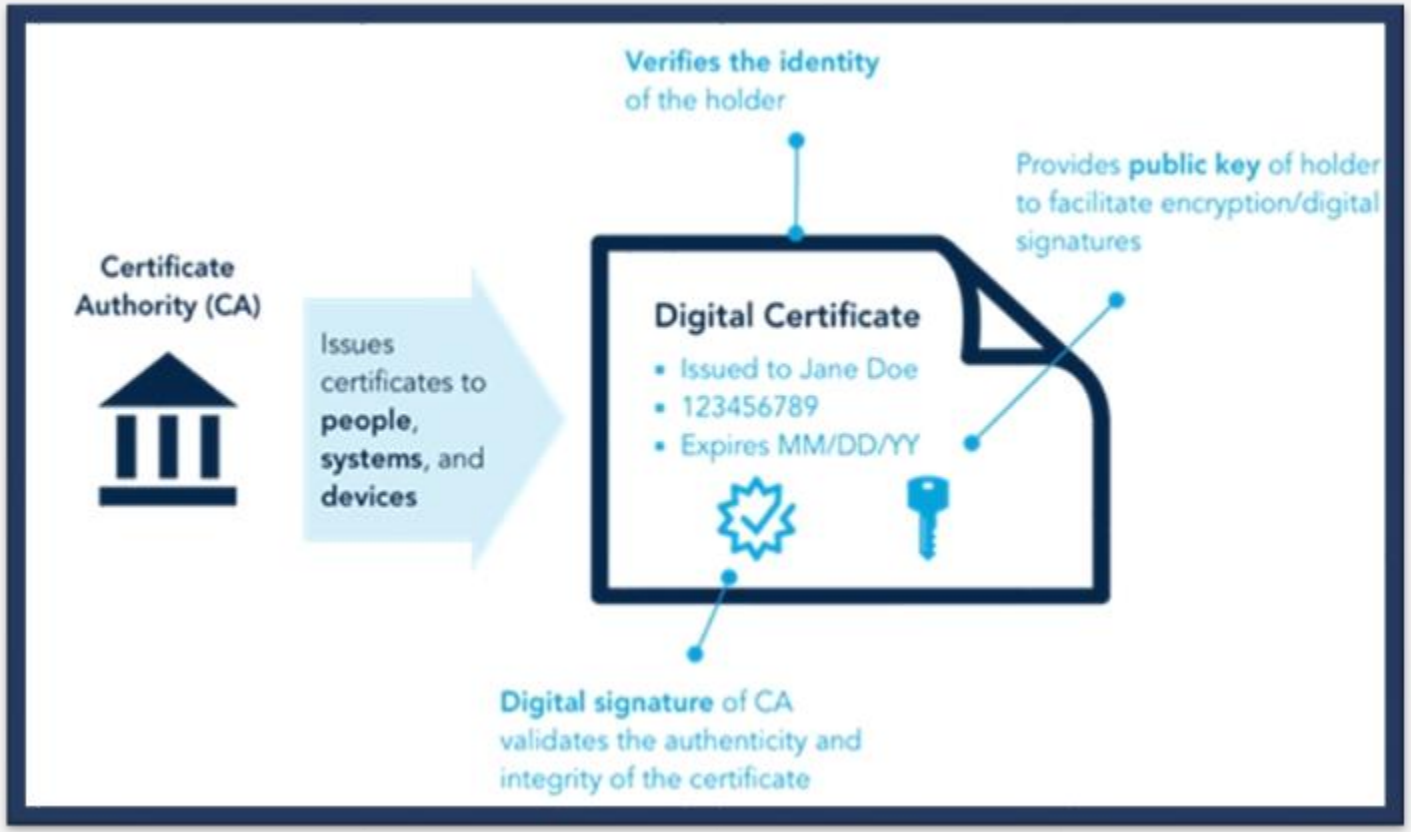
Certificate Authority

- 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.

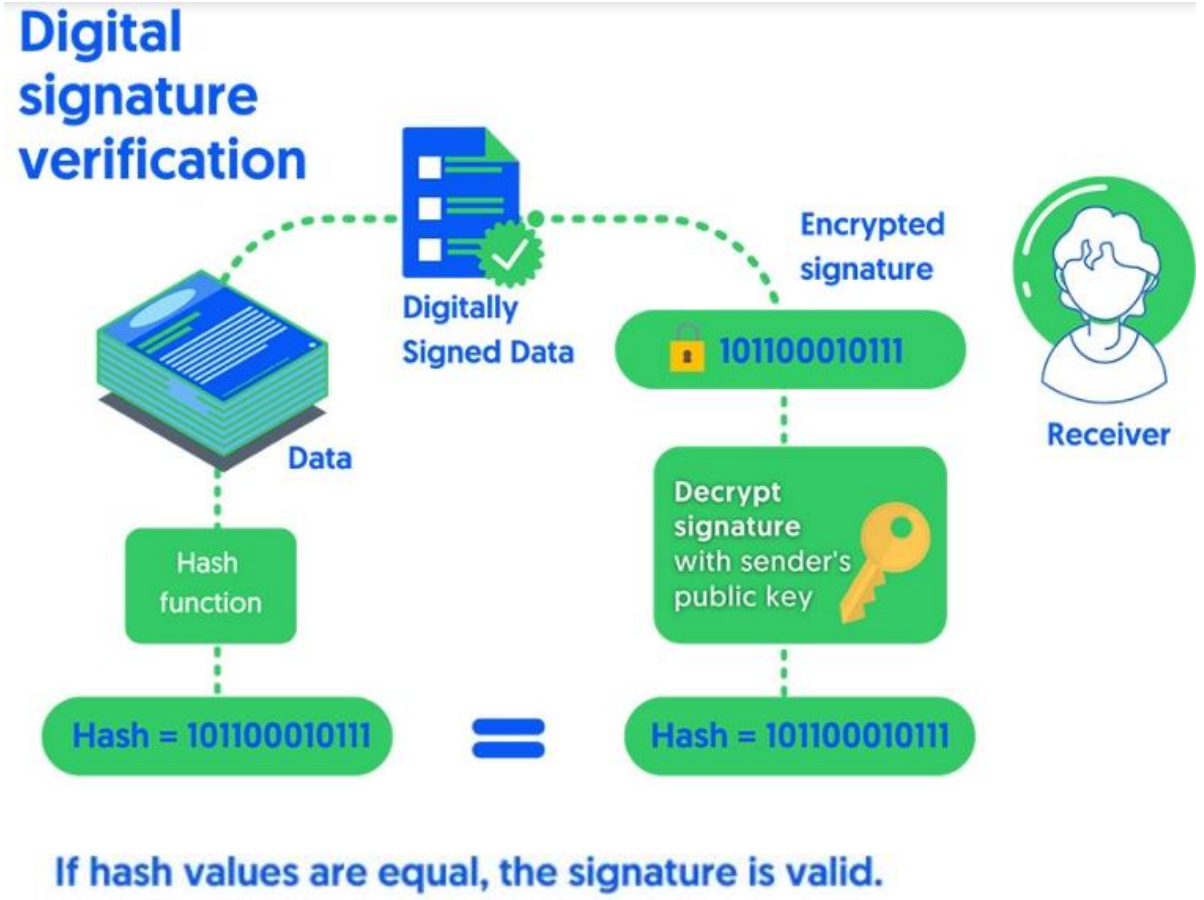
Digital Certificates

- Digital certificates are similar 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.

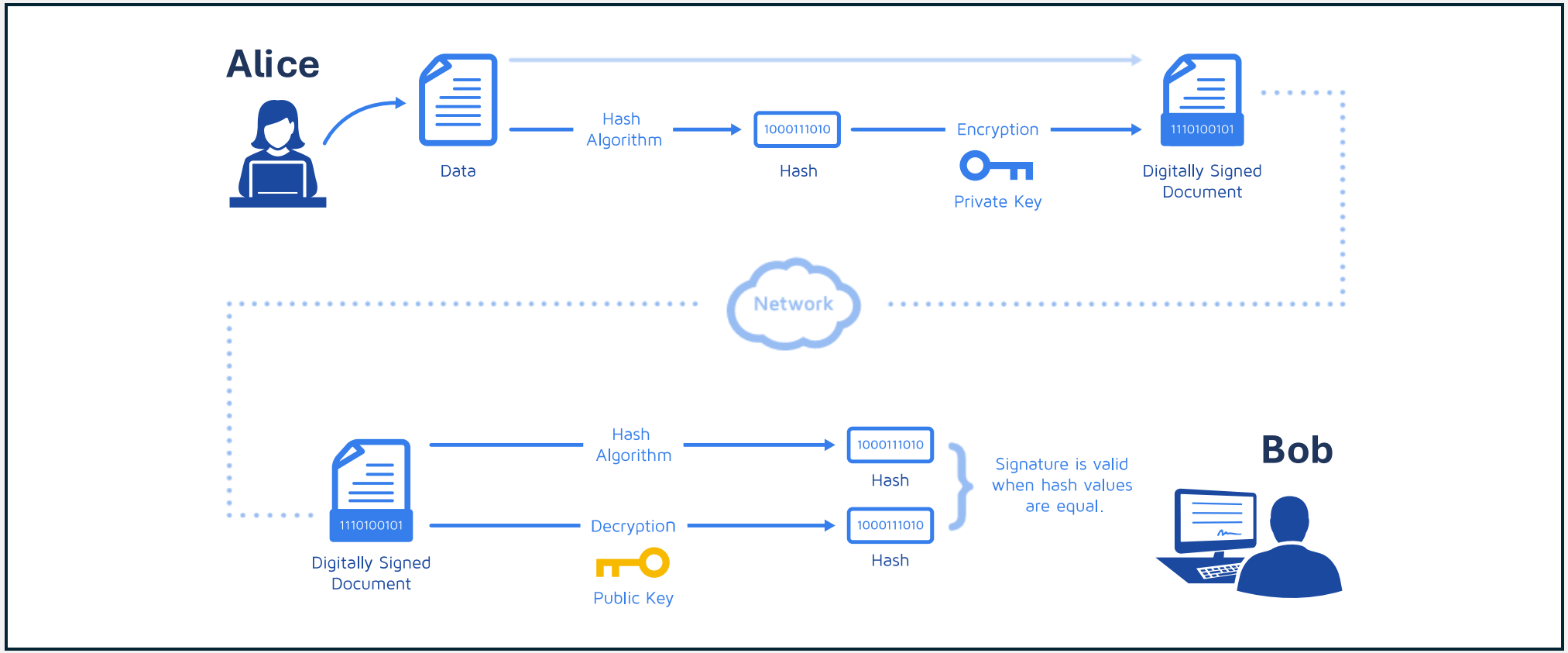
Certificate Authority (CA) & Digital Certificates



How does a Digital Signature work?



Alice Wants to Send a Digitally Signed Message to Bob



1) Alice Obtains a Digital Certificate from a CA

Alice

Alice generates a public-private key pair

Alice submits her public key and identity information to a CA, requesting a digital certificate

The CA verifies Alice's identity (checking government databases, contacting Alice's employer)

Once Alice's identity is verified, the CA creates a digital certificate. This certificate includes Alice's public key, Alice's identity information, the CA's identity, and a digital signature from the CA

2) Alice Digitally Signs the Message

Alice

Alice writes her message, let's say "Hello, Bob!"

Alice uses a hashing algorithm (e.g., SHA-256) to generate a hash of the message
This is a fixed-size string that uniquely represents the message content

```
hash("Hello, Bob!") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
```

Alice encrypts the hash using her private key, producing the digital signature

```
Digital Signature = Encrypt(hash("Hello, Bob!"), Alice's Private Key)
```

Alice sends the original message "Hello, Bob!" attached with the digital signature, and her digital certificate to Bob

3) Bob Verifies the Digital Signature

Bob verifies that the digital certificate is valid and has been issued by a trusted CA

Assuming the certificate is valid, Bob extracts Alice's public key from it.

Bob uses the same hashing algorithm (e.g., SHA-256) to generate a hash of the received message "Hello, Bob!".

```
hash("Hello, Bob!") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
```

3) Bob Verifies the Digital Signature

Bob

Bob decrypts the digital signature using Alice's public key, which should give him the hash that Alice originally generated.

```
Decrypted Hash = Decrypt(Digital Signature, Alice's Public Key)
```

Bob compares the hash he generated from the message with the decrypted hash

```
if Decrypted Hash == hash("Hello, Bob!") then
    Message is verified and authentic
else
    Message verification failed
```

Here are the 6 most important benefits:

Integrity

- Hashing algorithms will throw up different hash values for the same document if anyone tempers with the document.

Authenticity

- Digital signatures use both public keys and private keys to encrypt a document making it near impossible for the wrong person to sign the document.
- Also, certified authorities ensure that the public key belongs to the claimed sender.

Enhanced security

- Digital signatures use cryptography to authenticate and verify the content of a document. Cryptography makes it very hard for an imposter to replicate a digital signature and it also makes the content of the documents almost impossible to tamper with.

Here are the 6 most important benefits:

Time-Saving

- Digital signatures allow multiple parties to sign a document without having to be physically present in the same location. It also allows signatories to sign documents at any time of the day from a preferred device.

Cost-Effective

- You spend less money printing papers, and transporting to the signing venue when you sign digitally.

Eco-Friendly

- Papers are harmful to the environment but digital signatures reduce the use of paper to sign documents.

Thank You
Any Questions ?