



Web



Digital signatures



WEB &gt; GUIDES &gt; PSPDFKIT SERVER &gt; DIGITAL SIGNATURES

# Understanding digital signatures and their importance



PSPDFKit Server has been deprecated and replaced by [Document Engine](#). To migrate to Document Engine and unlock advanced document processing capabilities, refer to our [migration guide](#). Learn more about these enhancements on our [blog](#).

In today's world, where online communication and transactions are prevalent, ensuring data integrity and authentication is of the utmost importance. Digital signatures play a pivotal role in verifying the authenticity and integrity of digital content. This section will describe the basics of digital signatures and the underlying foundation of public key cryptography.

## What is a digital signature?

Imagine having an important document that holds legal significance. Such a document may contain vital information about rights and obligations, warranting the need for assurance regarding its legitimacy. Furthermore, this document is likely to be circulated, accessed, and stored by different parties at various stages. Throughout this process, the document is susceptible to changes, whether intentional (such as adding an extra signature) or unintentional (due to transmission errors), and there's also the risk of deliberate forgery.

For centuries, we've relied on the traditional practice of using physical ink signatures on paper to tackle this challenge. However, in contemporary times, we have the advantage of employing digital signatures to achieve the following objectives:



ASK AI

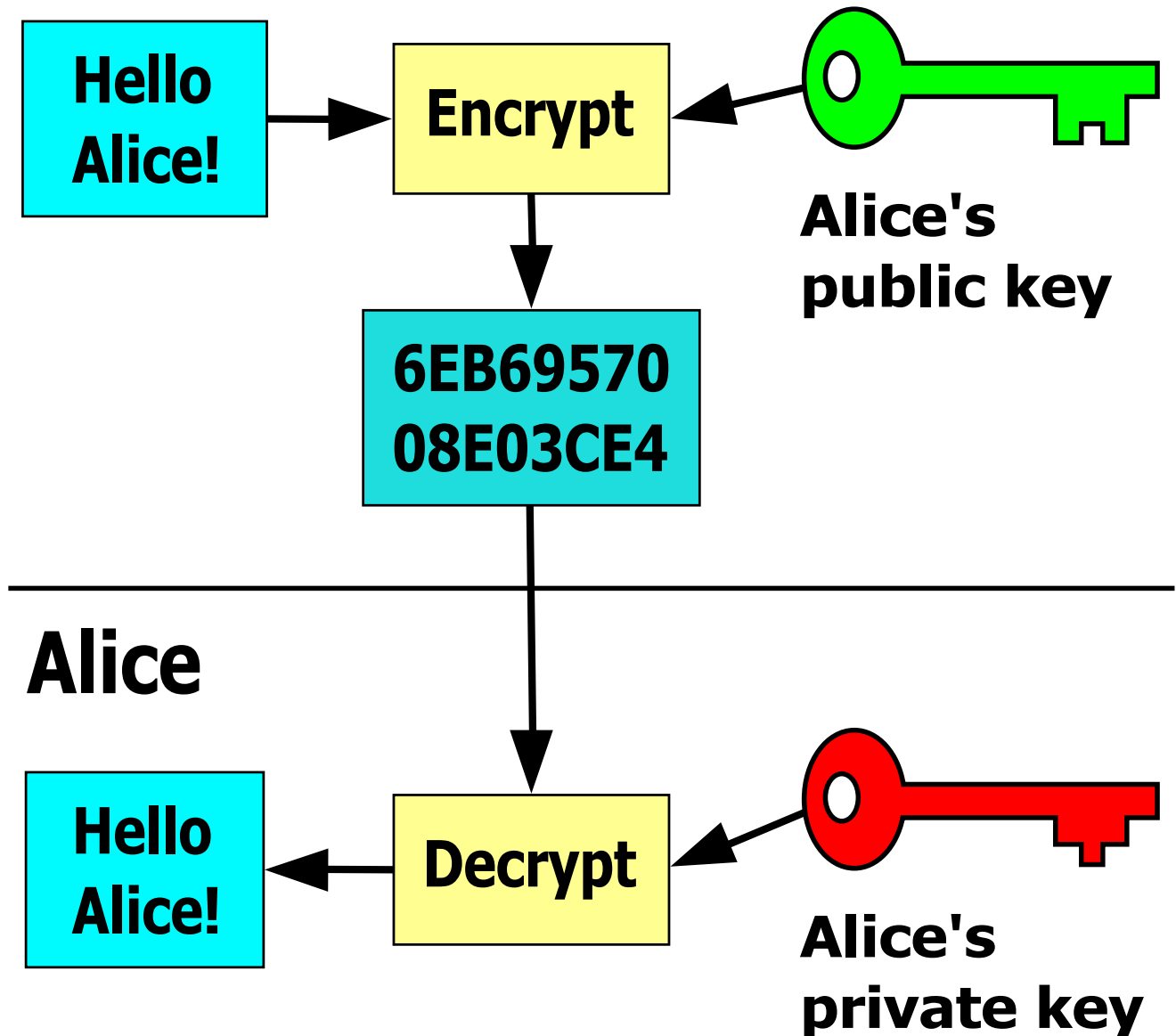
- **Document integrity** — Ensuring a document remains unaltered throughout an entire workflow, without any unauthorized modifications.
- **Document authenticity** — Establishing the true identity of a document's author, guaranteeing that it's indeed that of the expected individual rather than an imposter.
- **Non-repudiation** — Providing concrete evidence that a document's author cannot later deny their involvement or disown their responsibility.

By using mathematical algorithms, a digital signature algorithm generates a unique signature that can only be created by the original signer and ensures that the content hasn't been tampered with during transit.

## What is public key cryptography?

Digital signatures rely on the principles of public key cryptography. At its core, public key cryptography involves using a pair of mathematically related cryptographic keys: a public key and a private key. The public key is readily shared with the world, while the private key remains confidential and known only to the owner. Public key cryptography allows encryption with the public key and decryption with the corresponding private key. The following image shows the concept of public key encryption.

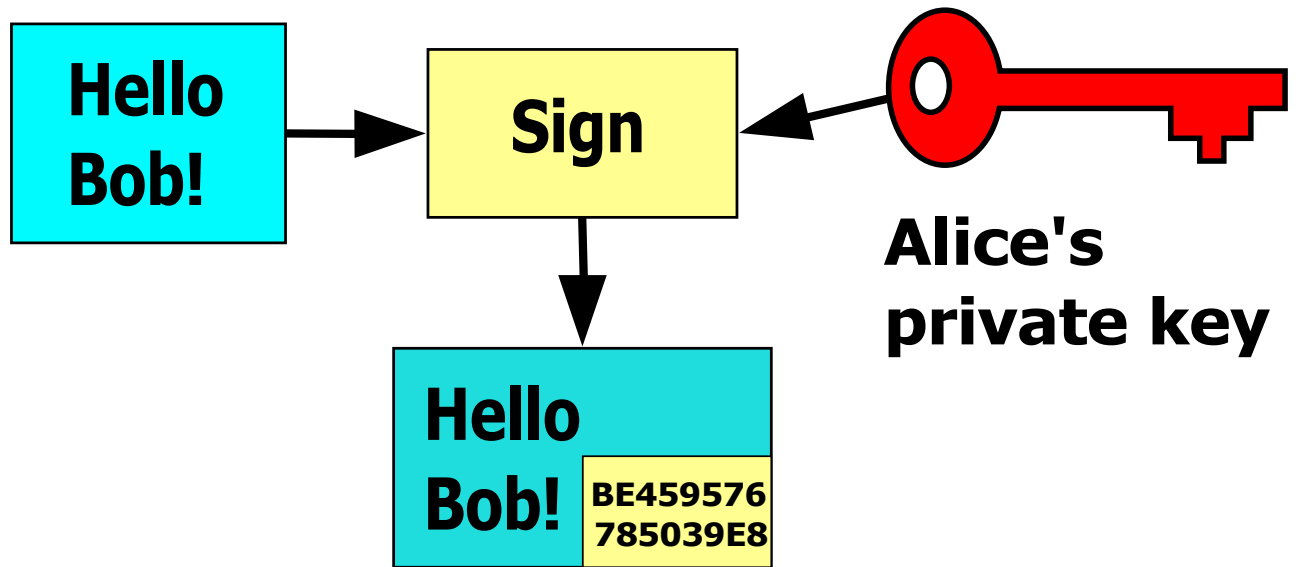
# Bob



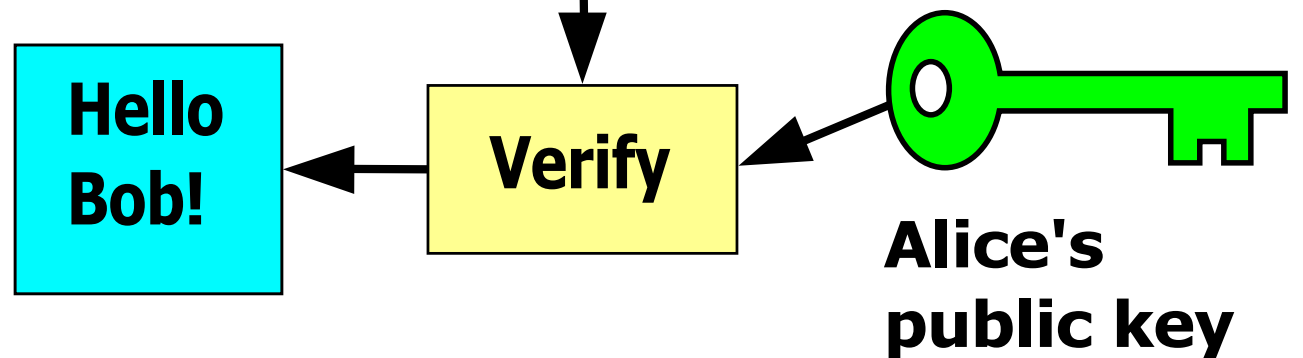
(Source: [Davidgothberg](#))

Public key cryptography also enables a party to create a digital signature. The sender generates a unique hash (a fixed-size string) of the message or document being signed. Then, the sender creates a digital signature by applying the private key to this unique hash. When a recipient receives the signed message, they can validate the signature using the sender's public key. The recipient applies the public key to the digital signature and compares it to the computed hash of the received content, ensuring its authenticity and integrity. The following image shows the concept of public key digital signing.

# Alice



# Bob



(Source: [FlippyFlink](#))

Was this helpful?

✓ YES

✗ NO

