GVHD: Ngô Huy Biên

Proof of Concept

VT Sign - Ký kết văn bản trực tuyến

Mục lục

1. Xác định Proof of Concept

Ký kết văn bản/hợp đồng giữa các bên với nhau thông qua internet điều quan trọng là tính định danh của chữ ký điện tử.

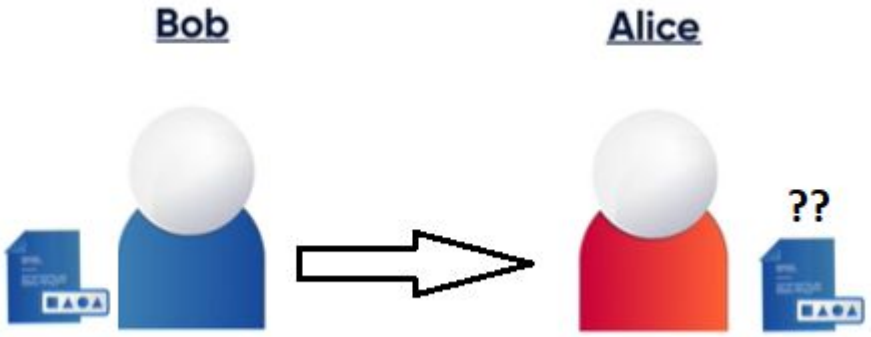
⇒ Proof of concept là: Độ tin cậy của chữ ký trên văn bản.

2. Vấn đề

*Bob ký vào **Tài liệu** và gửi cho Alice*

01 | Tài liệu có bị thay đổi khi gửi?

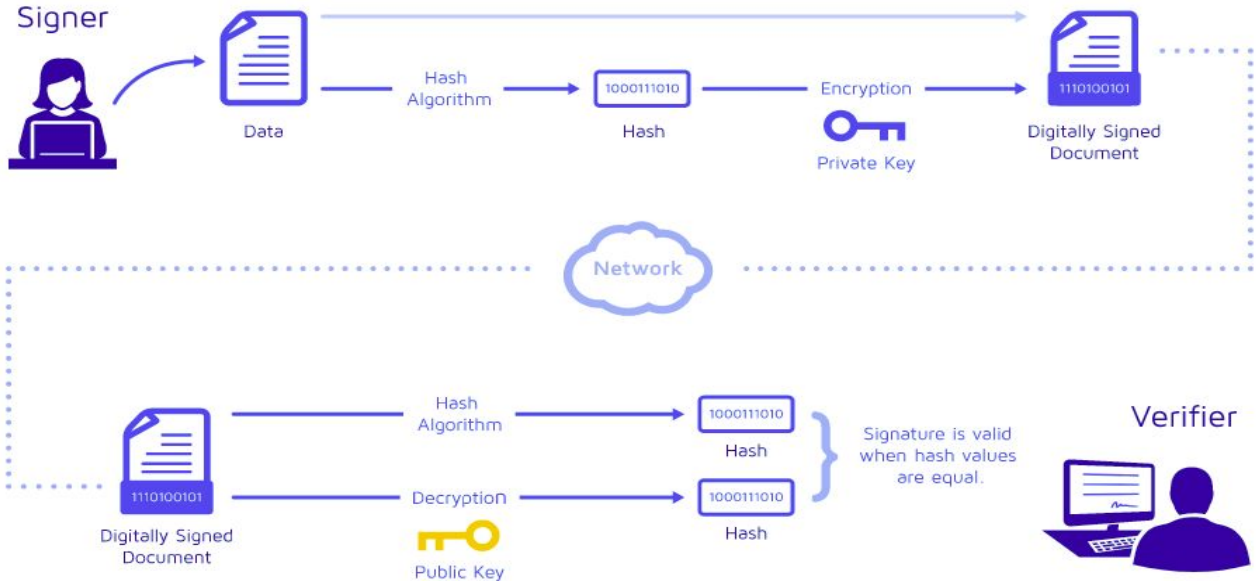
02 | Người gửi có chắc là Bob?



3. Giải pháp

- **Public Key & Private key:**
  - Private key: được giữ bí mật và dùng để mã hóa data (tài liệu)
  - Public key: chỉ được cung cấp bởi chủ tài khoản và dùng để xác thực người gửi.
- **Thuật toán phát sinh key:** RSA
- **Thuật toán mã hóa:** RSA
- **Chuẩn hash:** SHA256

3. Giải pháp


Signer
Data
Hash Algorithm
1000111010
Hash
Encryption
Private Key
1110100101
Digitally Signed Document
Network
Hash Algorithm
1000111010
Hash
Signature is valid when hash values are equal.
Verifier
1110100101
Digitally Signed Document
Decryption
Public Key
1000111010
Hash

3. Giải pháp

Quy trình thực hiện:

1. Hệ thống tạo ra keypair cho từng tài khoản của người sử dụng.
2. Người gửi sẽ ký và upload tài liệu lên hệ thống
3. Hệ thống sử dụng thuật toán SHA256 để mã hóa tài liệu thành digest
4. Hệ thống tiếp tục dùng digest và private key của người gửi để tiến hành tạo thành chữ ký số (digital signature)

5. Người nhận xác nhận danh tính với hệ thống để nhận được tài liệu + public key + digital signature của người gửi.
6. Hệ thống xác giải mã chữ ký điện tử của người nhận cung cấp bằng public key → digest 1 (nếu ko giải mã được thì chữ ký điện tử này là giả mạo)
7. Hệ thống cũng mã hóa tài liệu của người gửi → digest 2
8. Hệ thống so sánh 2 bản digest 1 và 2 để chứng thực.

3. Mã nguồn thực hiện giải pháp

Mã nguồn chi tiết tại: https://github.com/vtsign/PoC

Xin cảm ơn!