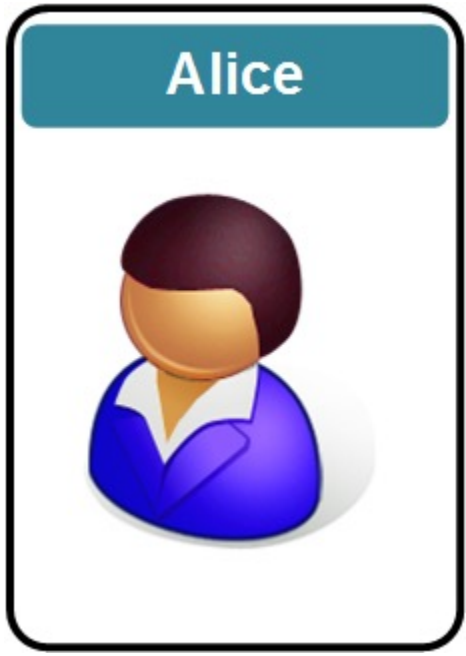
AWS KMS

Prof Bill Buchanan OBE, Blockpass ID Lab

http://asecuritysite.com

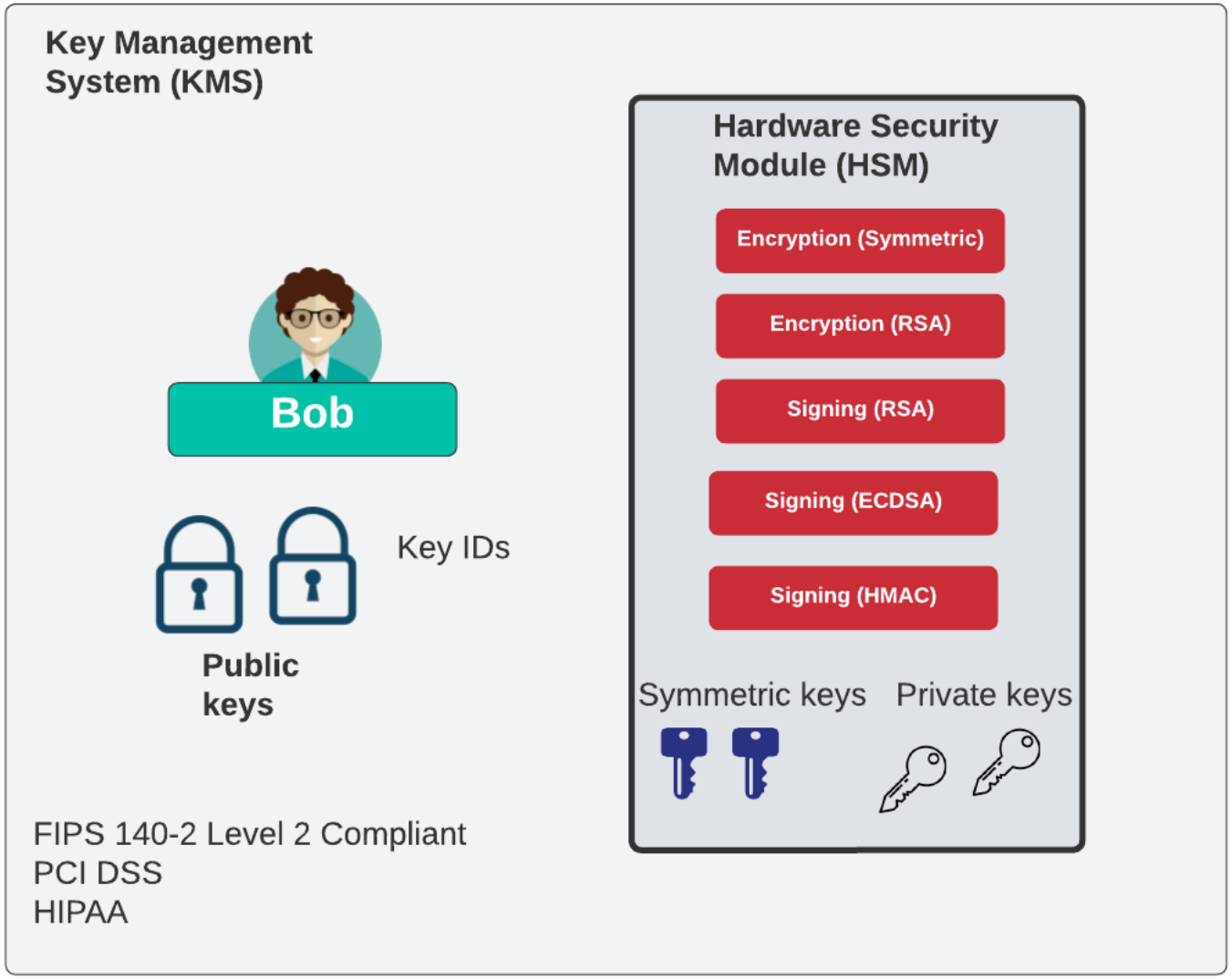


BLOCKPASS
IDENTITY
LAB

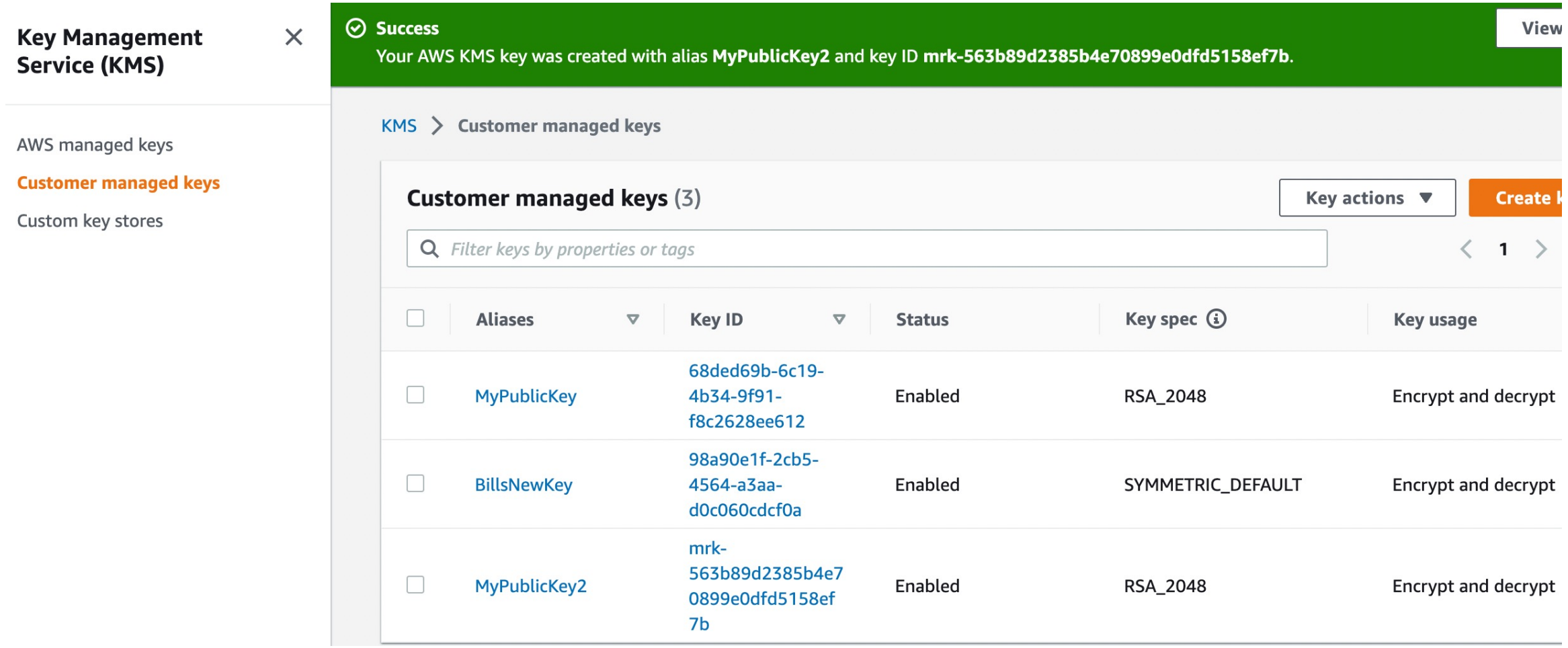
World-leading Collaboration between
Blockpass IDN and Edinburgh Napier University

KMS

- Symmetric Key Encryption [here].
- Public Key Encryption [here].
- Public Key Signing (ECDSA) [here].
- Public Key Signing (RSA) [here].
- HMAC [here].
- Secrets Store [here].
- Envelope Encryption [here].



KMS


Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
Success
Your AWS KMS key was created with alias MyPublicKey2 and key ID mrk-563b89d2385b4e70899e0dfd5158ef7b.
View
KMS > Customer managed keys
Customer managed keys (3)
Key actions
Create k
Filter keys by properties or tags
1
Aliases
Key ID
Status
Key spec
Key usage
MyPublicKey
68ded69b-6c19-4b34-9f91-f8c2628ee612
Enabled
RSA_2048
Encrypt and decrypt
BillsNewKey
98a90e1f-2cb5-4564-a3aa-d0c060cdcf0a
Enabled
SYMMETRIC_DEFAULT
Encrypt and decrypt
MyPublicKey2
mrk-563b89d2385b4e70899e0dfd5158ef7b
Enabled
RSA_2048
Encrypt and decrypt

KMS

Configure key

Key type Help me choose

- (●) **Symmetric**
  A single key used for encrypting and decrypting data or generating and verifying HMAC codes.
- ( ) **Asymmetric**
  A public and private key pair used for encrypting and decrypting data or signing and verifying messages.

Key usage Help me choose

- (●) **Encrypt and decrypt**
  Use the key only to encrypt and decrypt data.
- ( ) **Generate and verify MAC**
  Use the key only to generate and verify hash-based message authentication codes (HMAC).

▸ Advanced options

Cancel Next

View

Create k

1

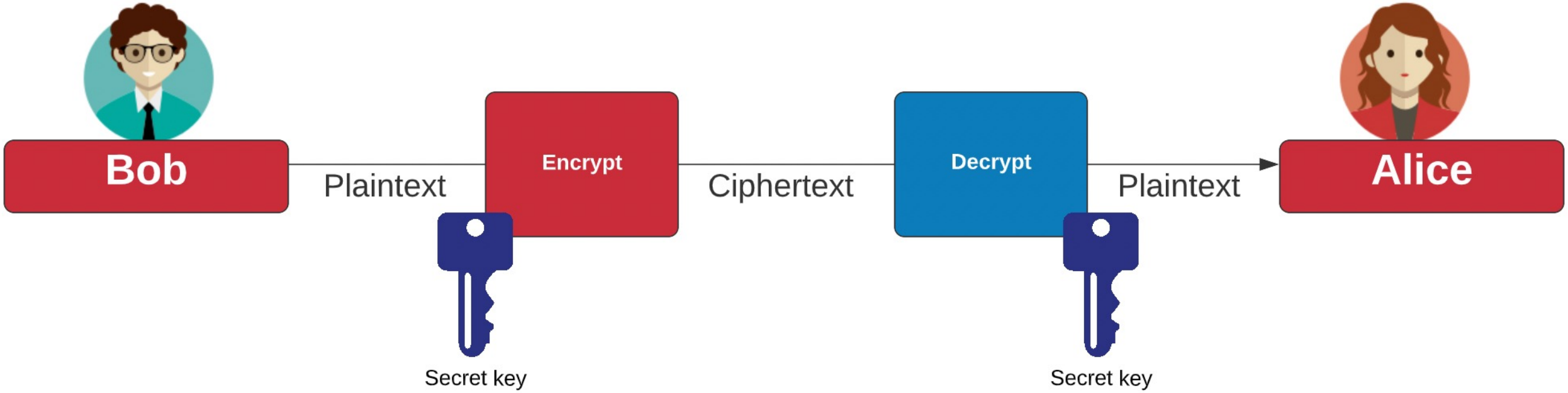
Key usage

Encrypt and decrypt

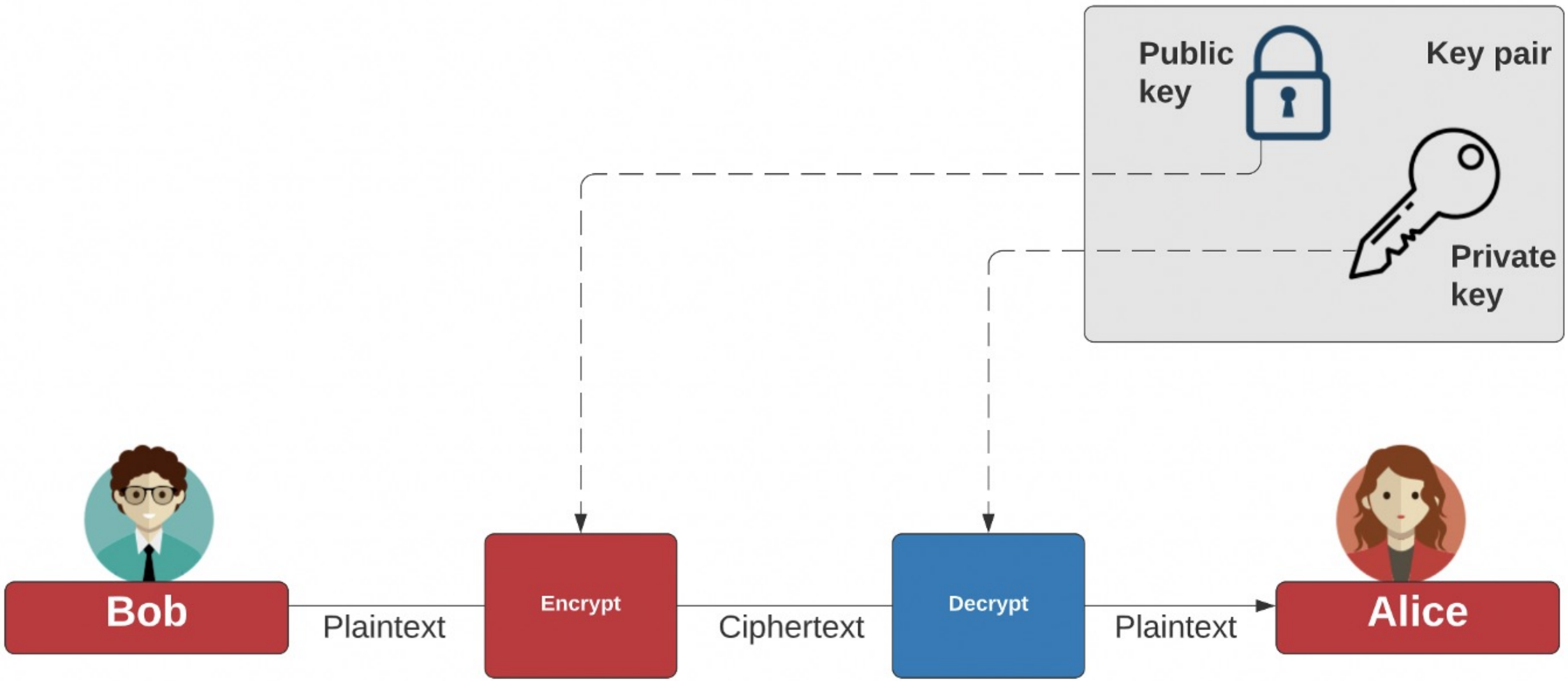
Encrypt and decrypt

Encrypt and decrypt

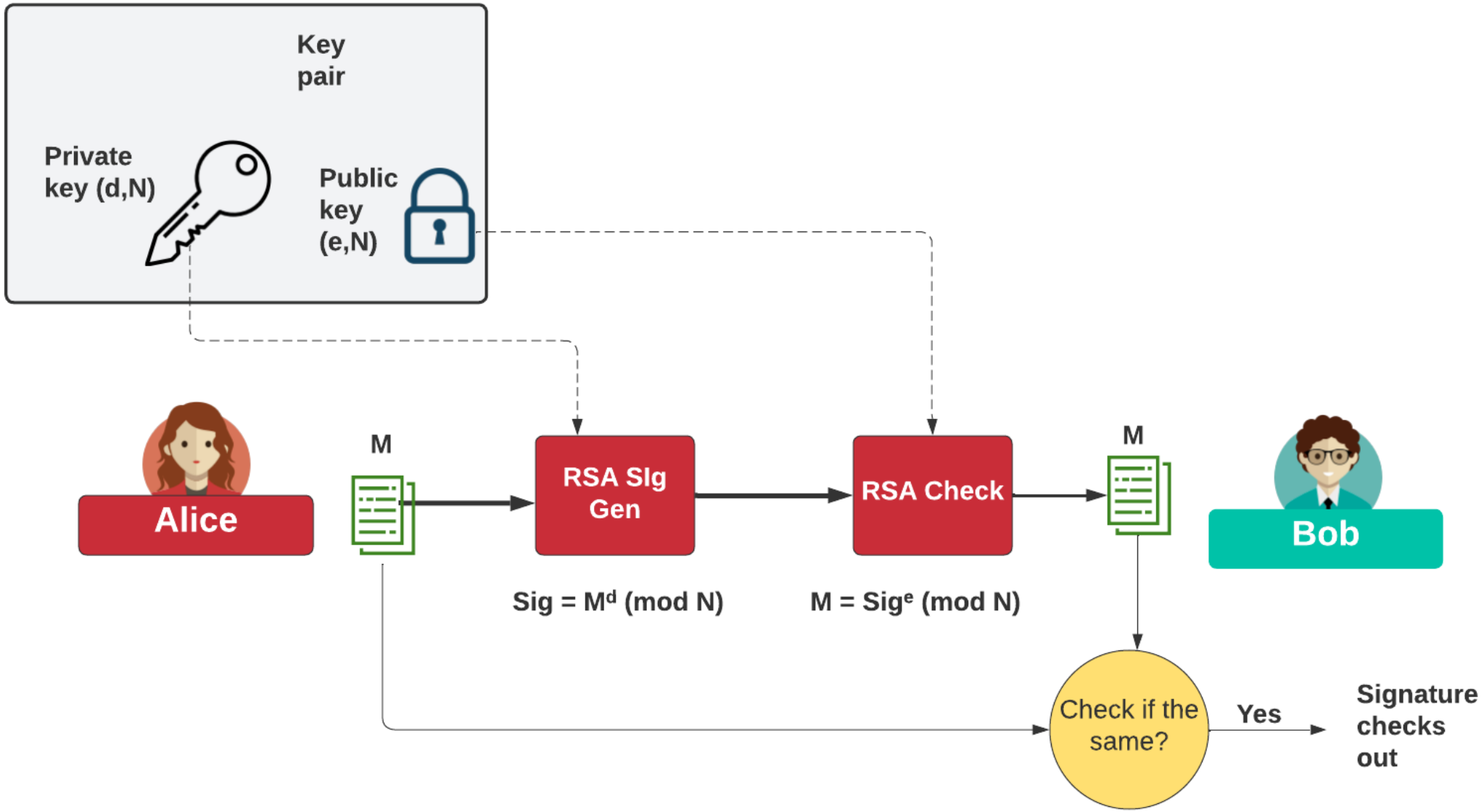
Symmetric Key



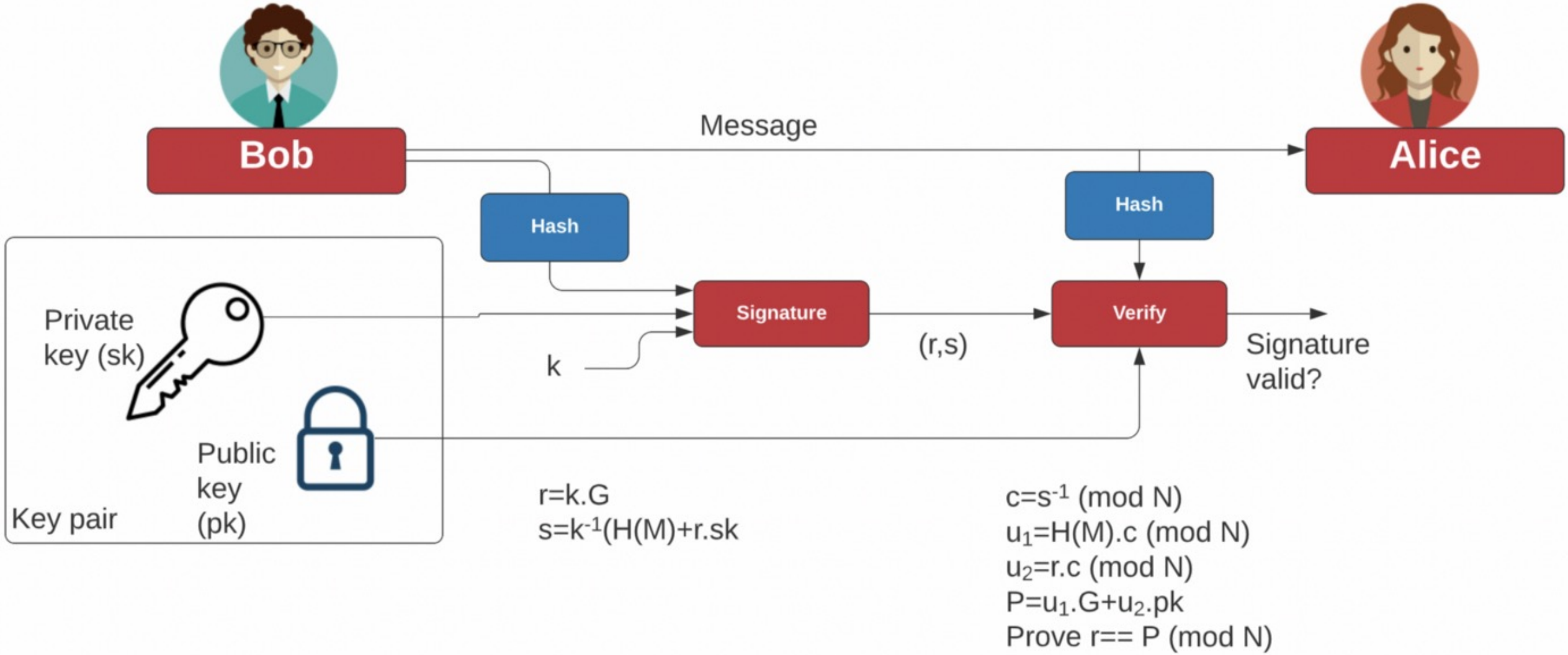
Public Key Encryption (RSA)



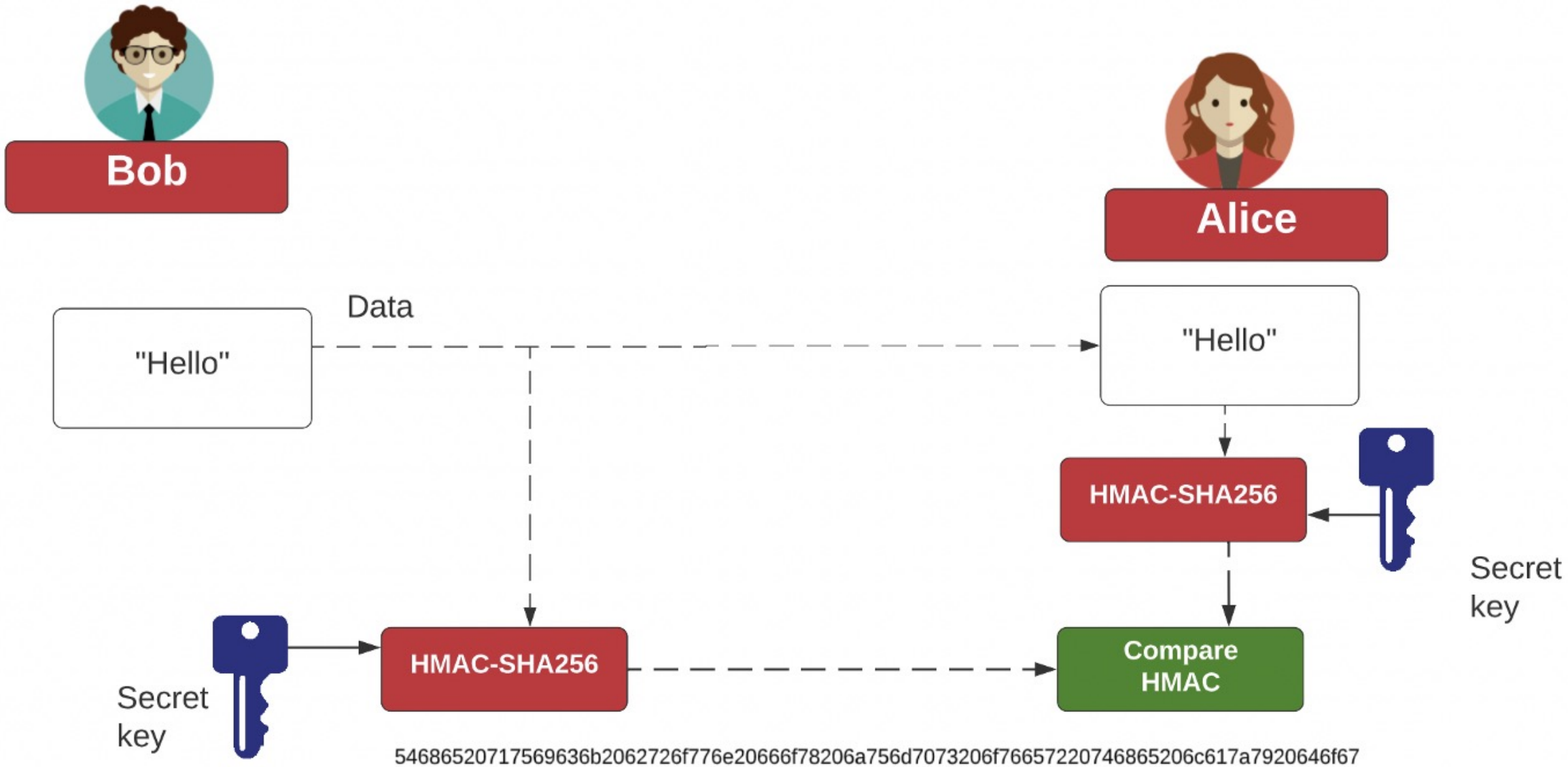
Public Key Signing (RSA)



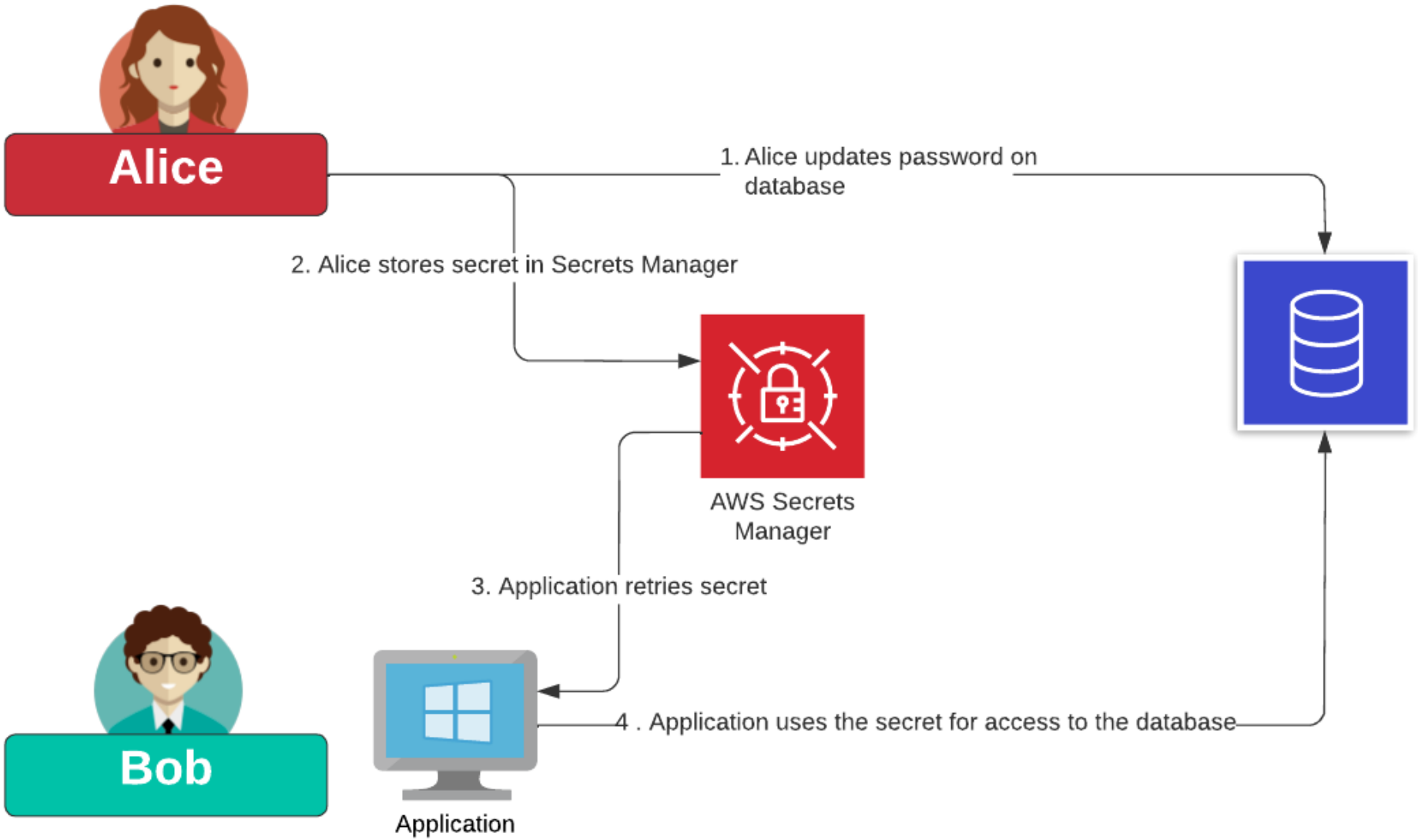
Public Key Signing (RSA)



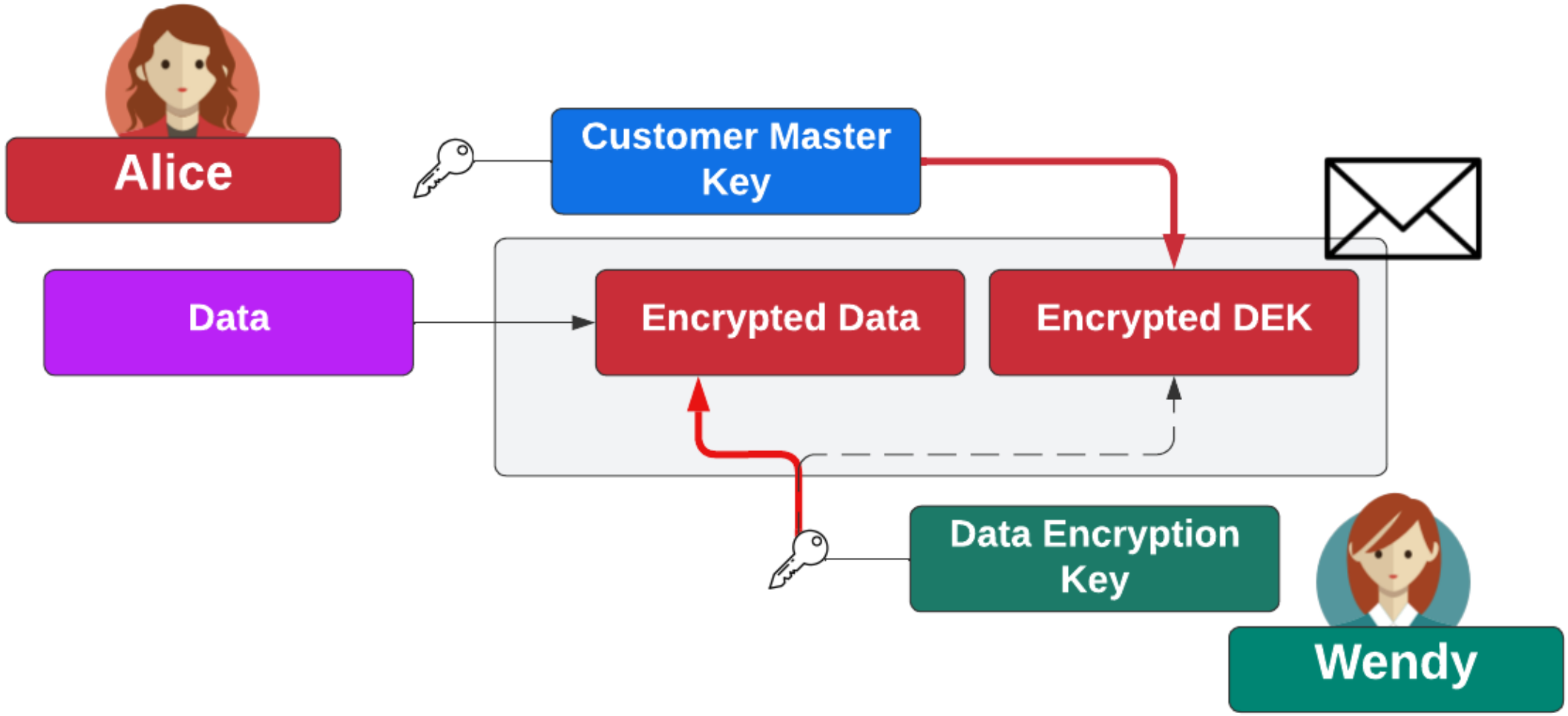
HMAC


Bob
Alice
Data
"Hello"
"Hello"
HMAC-SHA256
Secret
key
HMAC-SHA256
Compare
HMAC
Secret
key
54686520717569636b2062726f776e20666f78206a756d7073206f766572207468652065206c617a7920646f67

Secrets Store



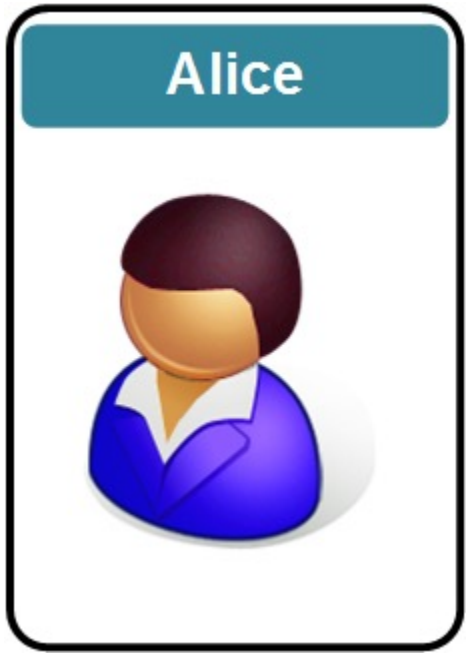
Envelope Encryption



AWS KMS

Prof Bill Buchanan OBE, Blockpass ID Lab

http://asecuritysite.com



BLOCKPASS
IDENTITY
LAB

World-leading Collaboration between
Blockpass IDN and Edinburgh Napier University