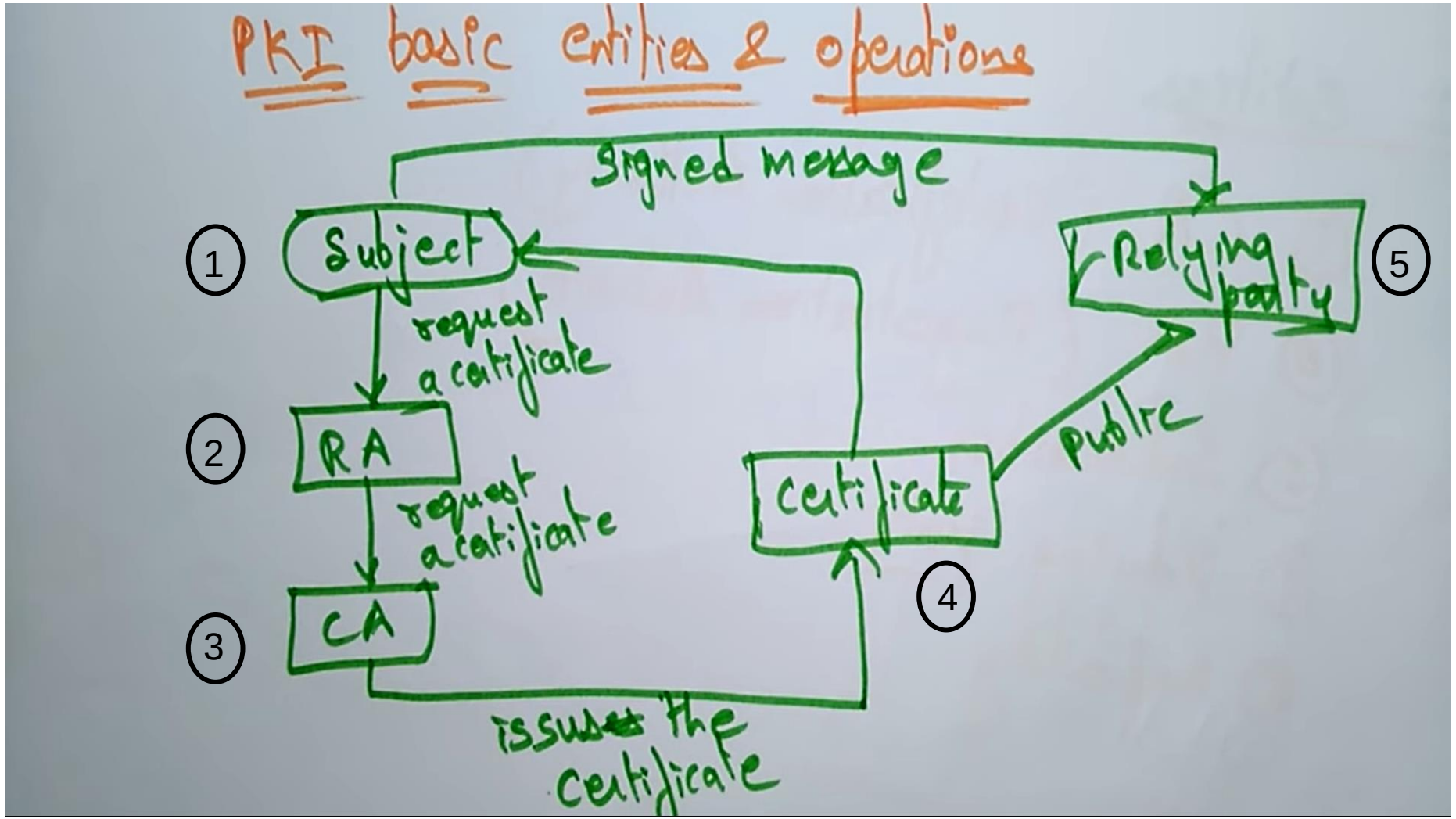
PKI vs KDC

	PKI	KDC
Abbreviation	Public Key Infrastructure	Key Distribution Center
Definition	It is a technology for authenticating users and devices in the digital world to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device.	It is a form of symmetric encryption that allows the access of two or more systems in a network by generating a unique ticket type key for establishing a secure connection over which data is shared and transferred.
Type of encryption	Asymmetric Encryption	Symmetric Encryption
Period	Long time period	During a limited time (also called session)

PKI Diagram


PKI basic entities & operations
Signed message
1
Subject
request a certificate
2
RA
request a certificate
3
CA
issues the certificate
Certificate
4
Public
Relying party
5

PROCESS TO GET DIGITAL CERTIFICAT

(1). The Subject who wants to receive the information register in RA (Registration Authority) in order to get a certificat

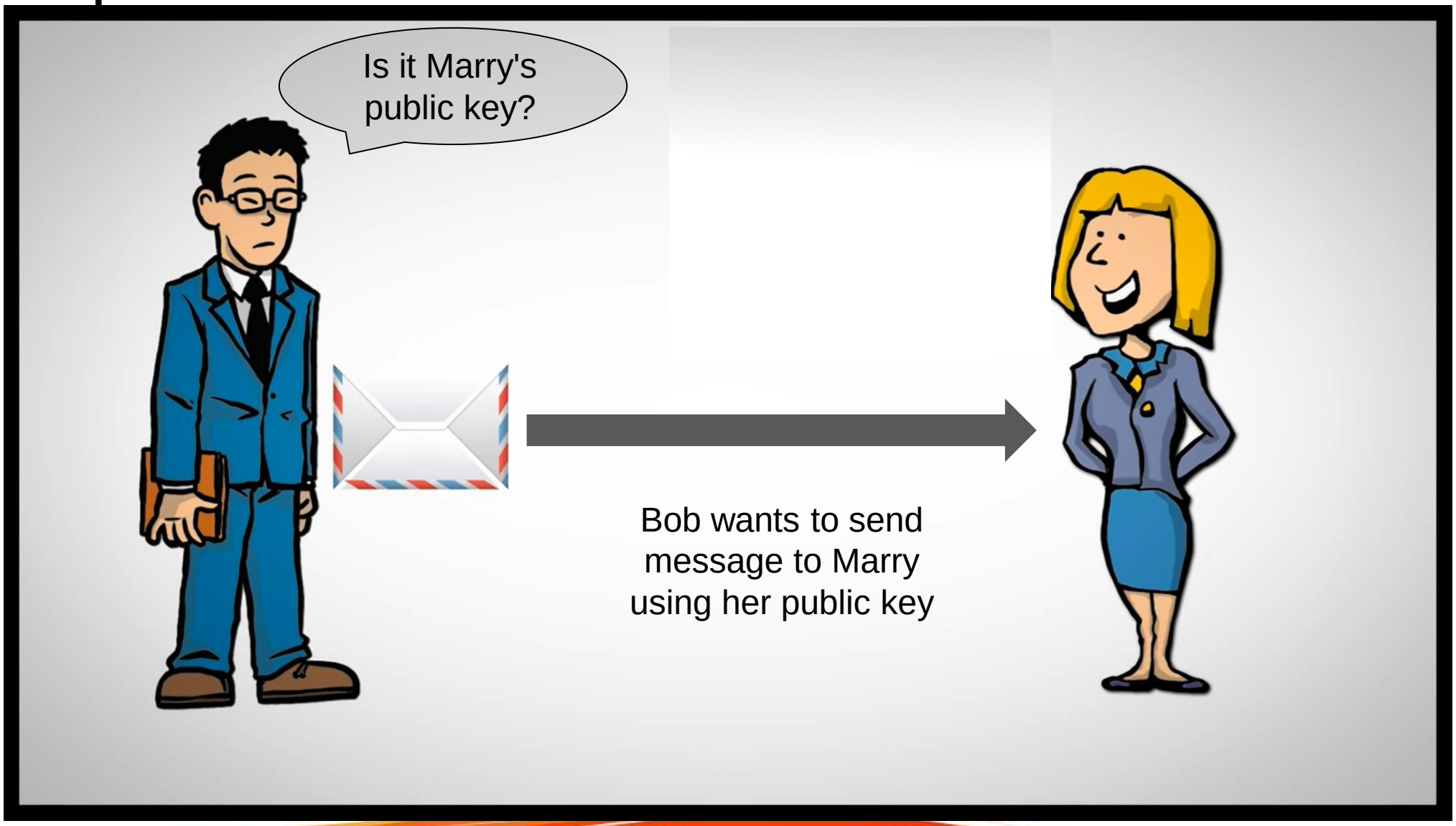
(2). The RA send the request to the CA (Certificate Authority) to issue the digital certificat

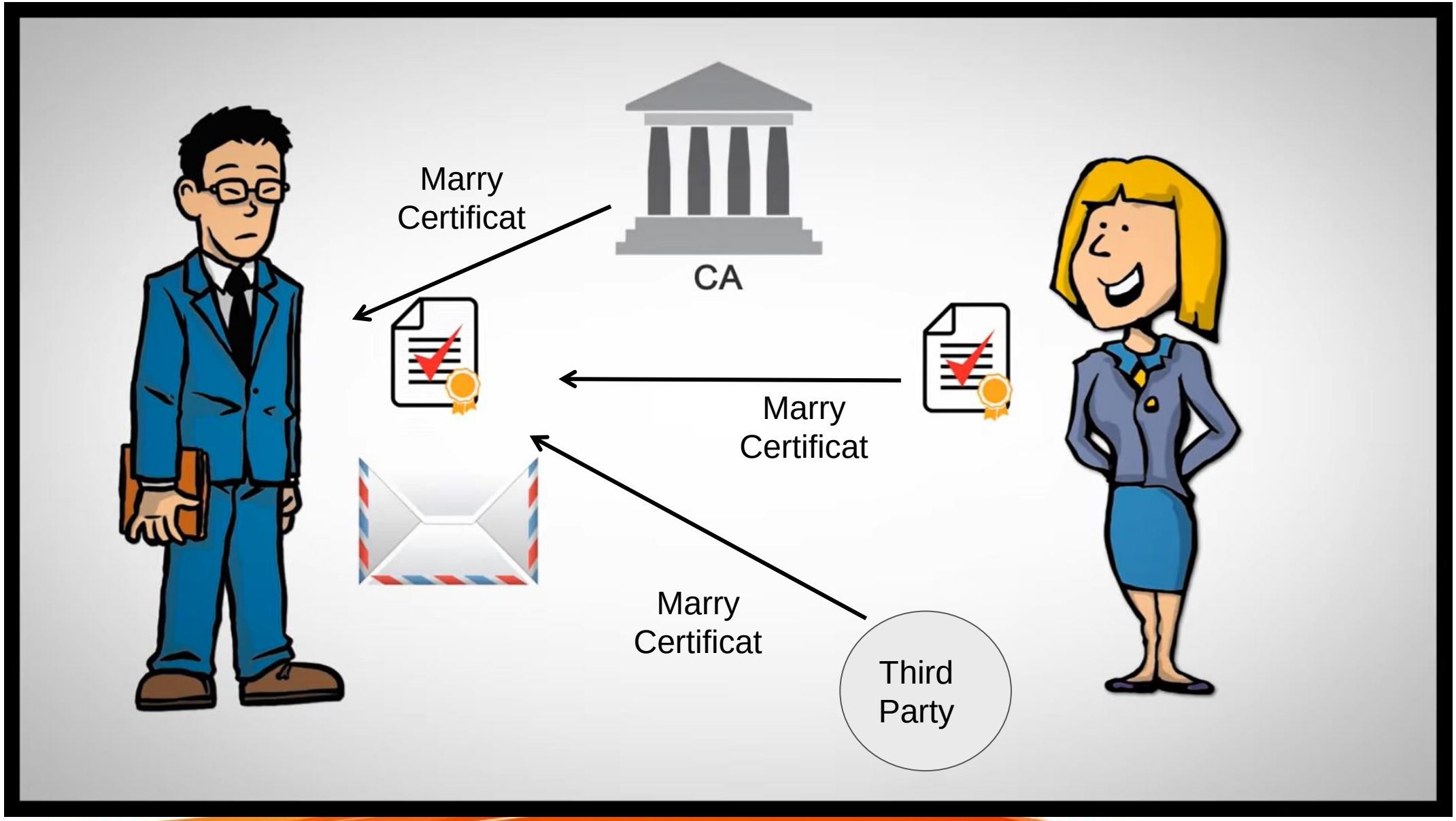
(3). The CA store and issue the certificat

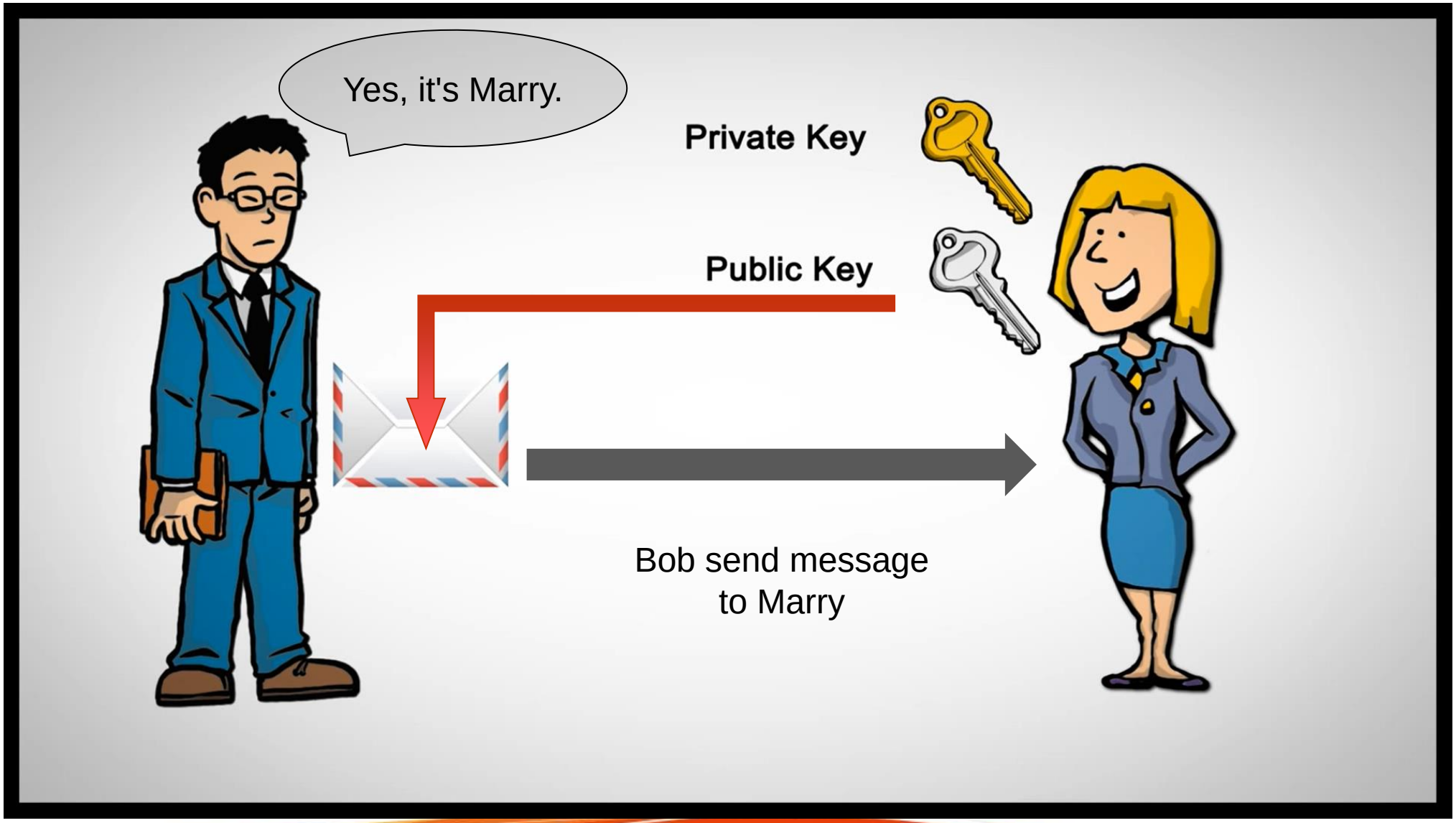
(4). The Certificat is send to the requestor and to a third party who will also store it.

(5). The third party can share the digital certificat to anyone who ask for it

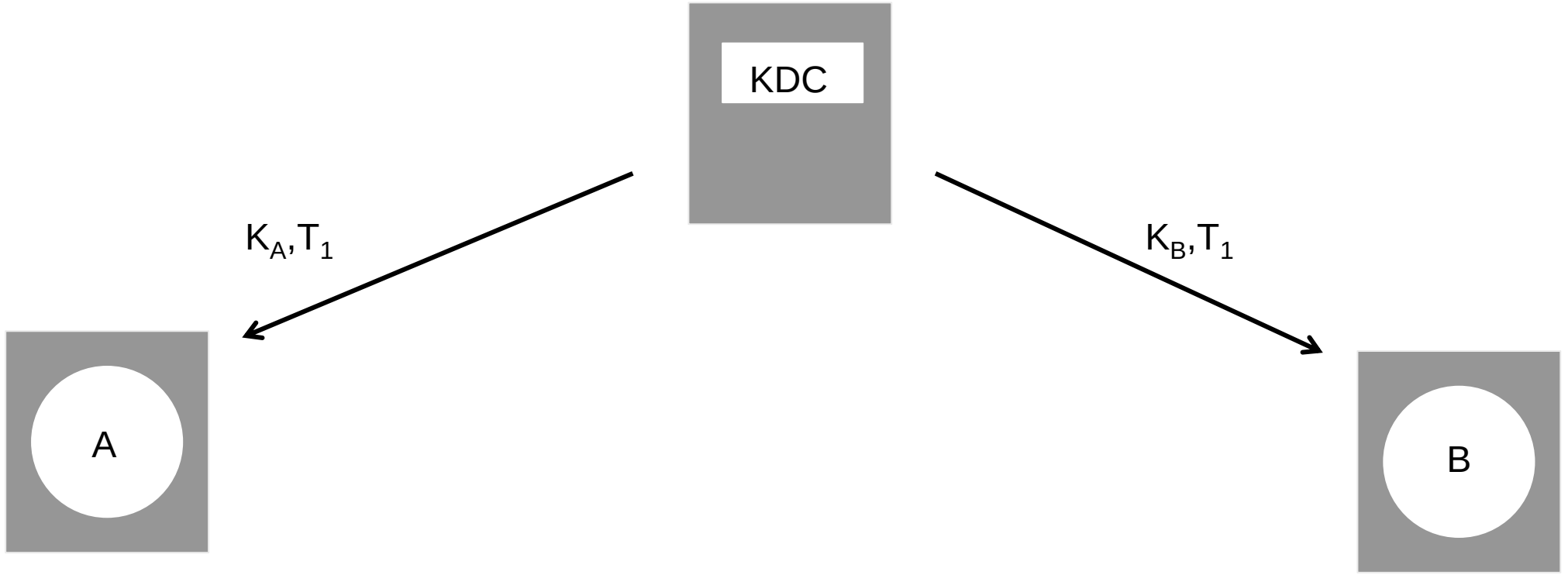
Example


Is it Marry's public key?
Bob wants to send message to Marry using her public key


Marry
Certificat
CA
Marry
Certificat
Marry
Certificat
Third
Party

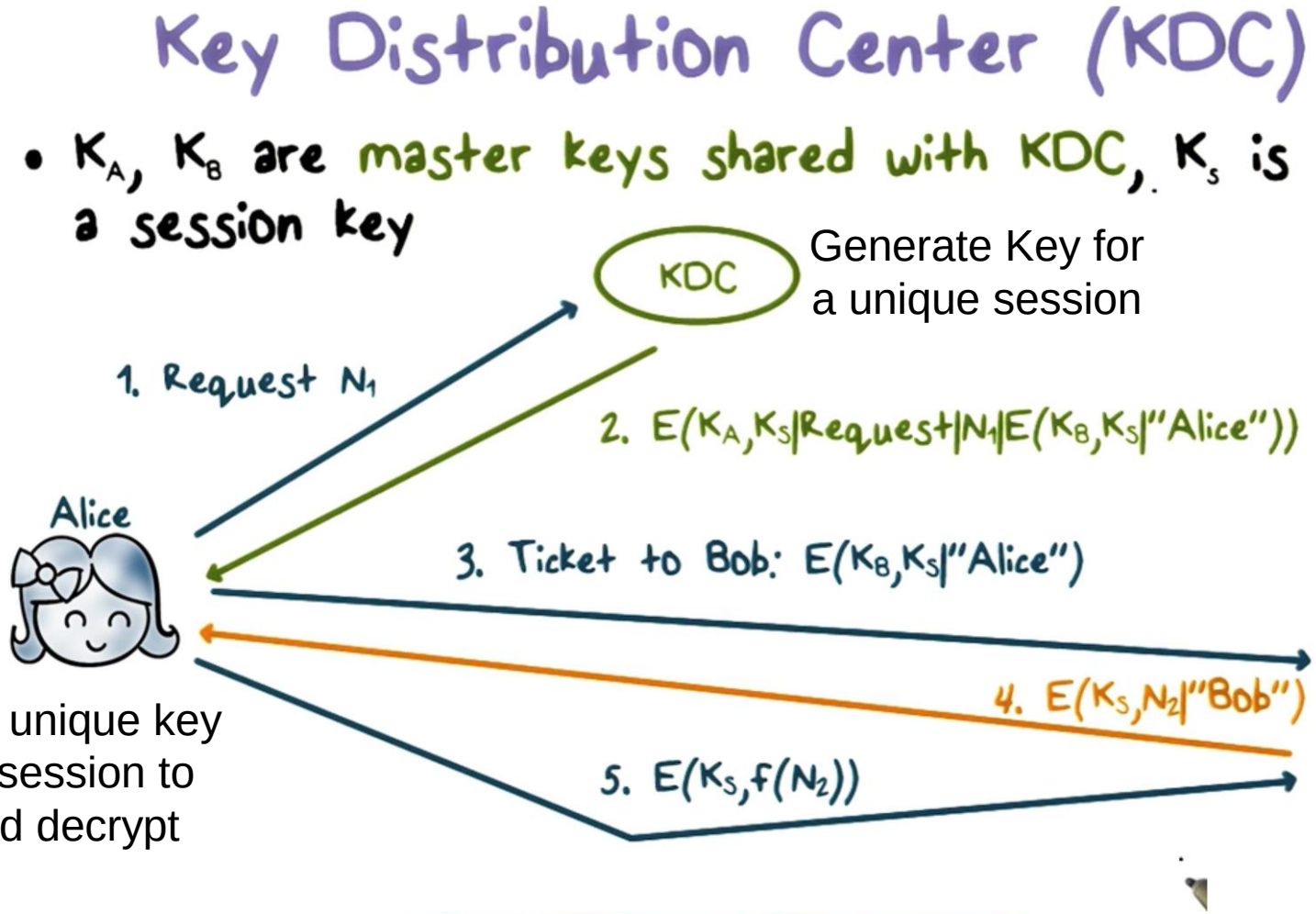

Yes, it's Marry.
Private Key
Public Key
Bob send message
to Marry

KDC Diagram



K_A: Key for encryption and decryption of A
K_B: Key for encryption and decryption of B
T_1: Session 1

Example



Alice has a unique key during this session to encrypt and decrypt message

Bob has also a unique key during this session to encrypt and decrypt message

- Alice and Bob have two different key, it means Alice cannot use Bob key to decrypt a message and vice versa.
- After one session, Alice and Bob loose their previous key. In order to communicate again, KDC will generate a new key for the new session.
- Alice and Bob cannot use their previous key in the new session.