Key Distribution and Management

Key Distribution and Management

- Secret key distribution
- Public key distribution
- Secret key distribution using public key encryption

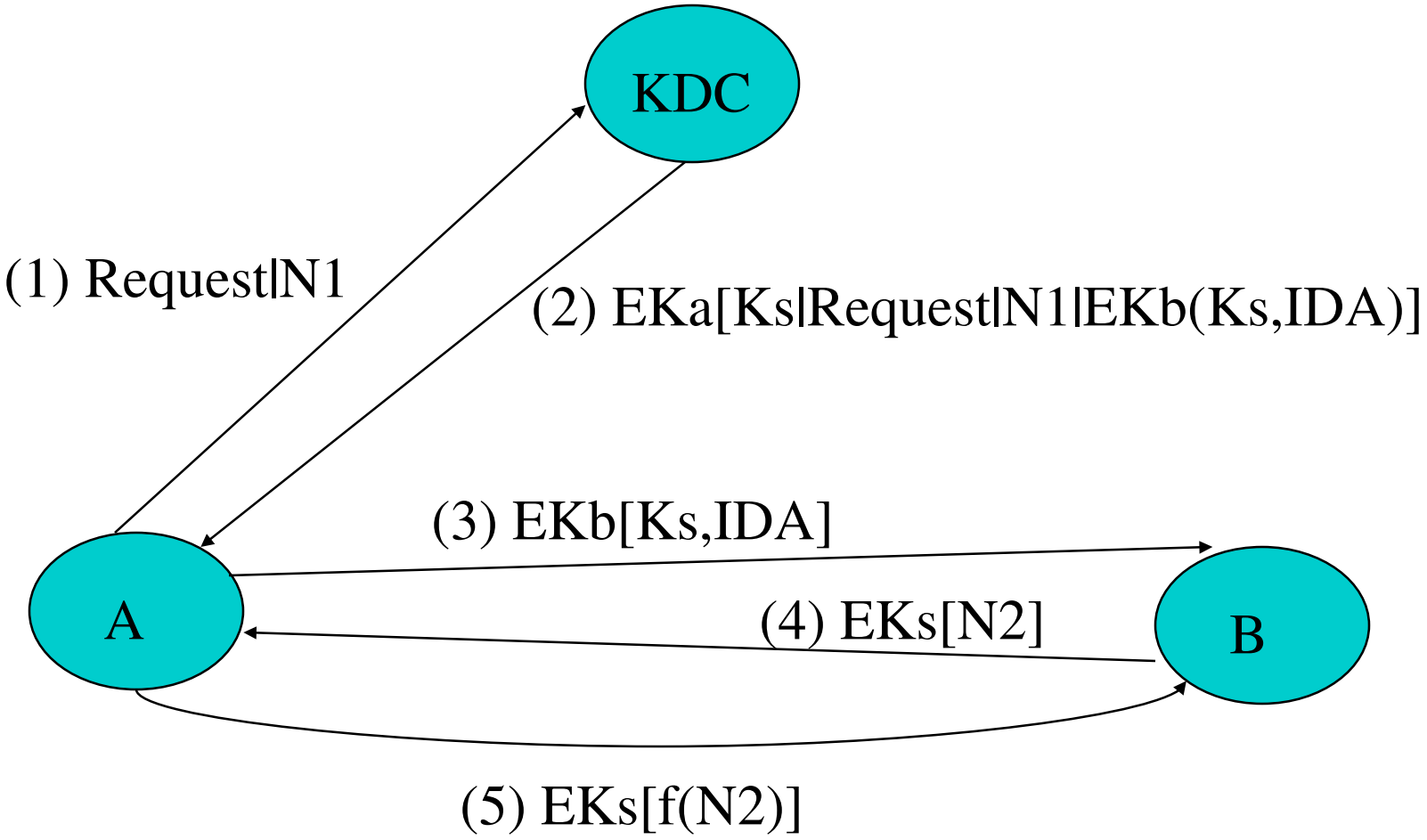
Secret Key Distribution

- A and B can establish a secret key by:
  - Manual delivery.
  - Selection and delivery by a trusted third party.
  - Using a previous key to encrypt the new key.
  - Using encrypted links to a third party to relay.
- Problem:
  - Need to scale up: need for each pair of hosts/applications ...

Key Distribution Center (KDC)

- Responsible for distributing keys to pairs of users (hosts, processes, applications)
- Each user must share a unique key, the *master* key, with the KDC
  - Use the master key to communicate with KDC to get a temporary *session* key for establishing a secure "session" with another user
  - Master keys are distributed in some *non-cryptographic* ways

A Typical Key Distribution Scenario

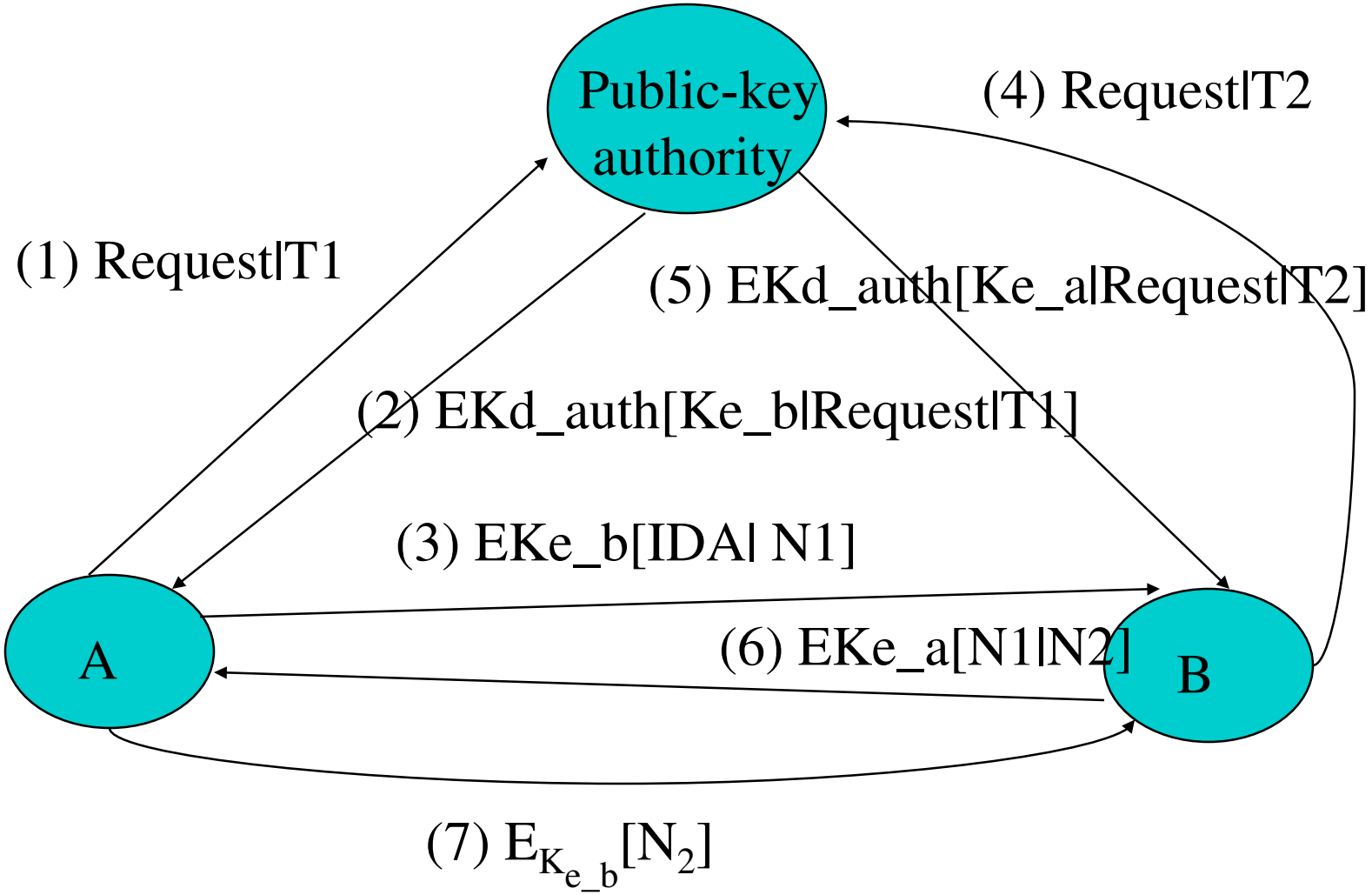


Ka, Kb are master keys, Ks is a session key

Public Key Distribution

- General schemes:
  - Public announcement
    - Can be forged
  - Publicly available directory
    - Can be tempered
  - Public-key authority
  - Public-key certificates

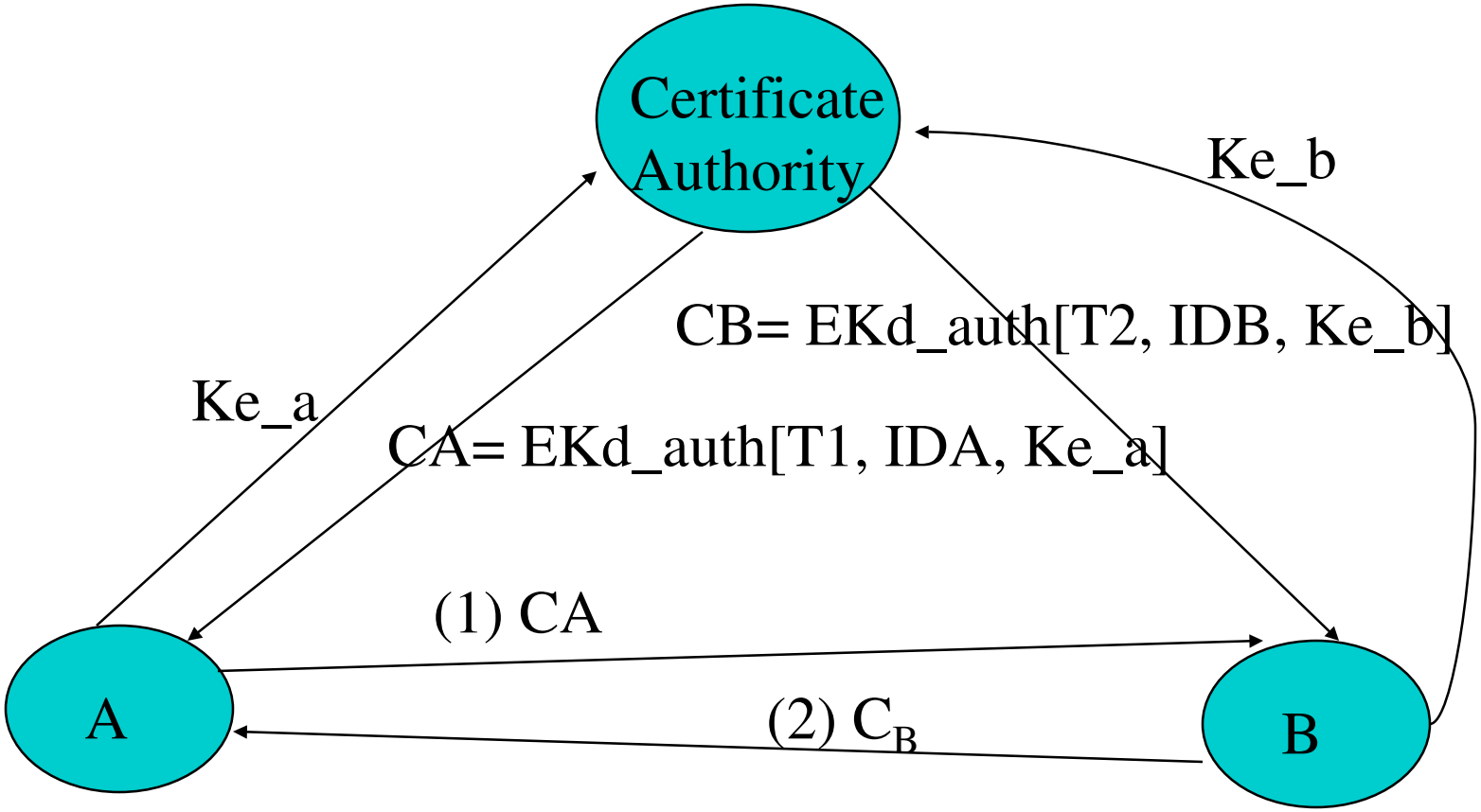
Public-key Authority



Public-key Certificates

- A certificate contains a public key and other information
  - Created by a certificate authority
  - Given to the participant with the matching private key
- A participant transmits its certificate to convey its key information
  - Other participants can verify that the certificate was created by the authority
    - All nodes are pre-configured with the public key of the certificate authority (CA)

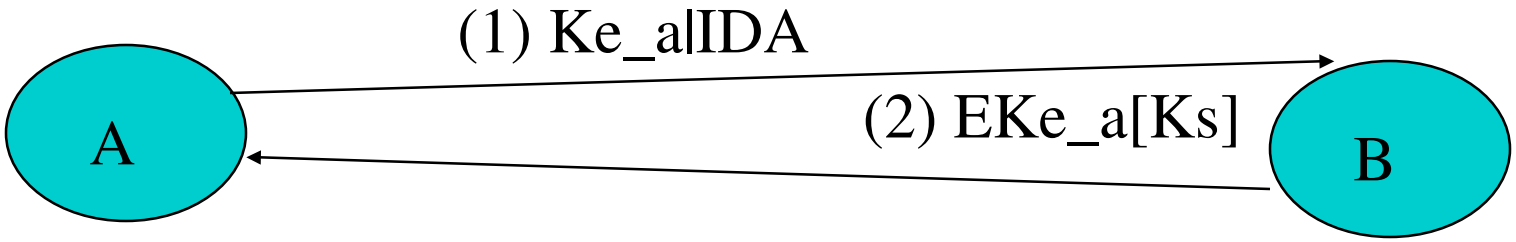
Exchange of Public-key Certificates



B does: $D_{K_{e\_auth}}(C_A) = D_{K_{e\_auth}}(E_{K_{d\_auth}}[T_1, ID_A, K_{e\_a}]) =$
(T_1, ID_A, K_{e_a}), hence gets the public key of A

Public-key Distribution of Secret Keys

Simple Secret Key Distribution



Vulnerable to an active attack: a bad guy can intervene in the communication channel and get a copy of K_s.

Secret Key Distribution With Confidentiality and Authentication