

5. 密钥分发和证书

5.1 可信赖中介

对称密钥问题:

相互通信的实体如何分享对称式的密钥

解决办法:

trusted key distribution center (KDC) 在实体之间扮演可信赖中介的角色

公共密钥问题:

当Alice获得Bob的公钥(from web site, e-mail,diskette), 她如何知道就是Bob的public key, 而不是Trudy的?

解决办法:

可信赖的certification authority (CA)

5.2 KDC Key Distribution Center

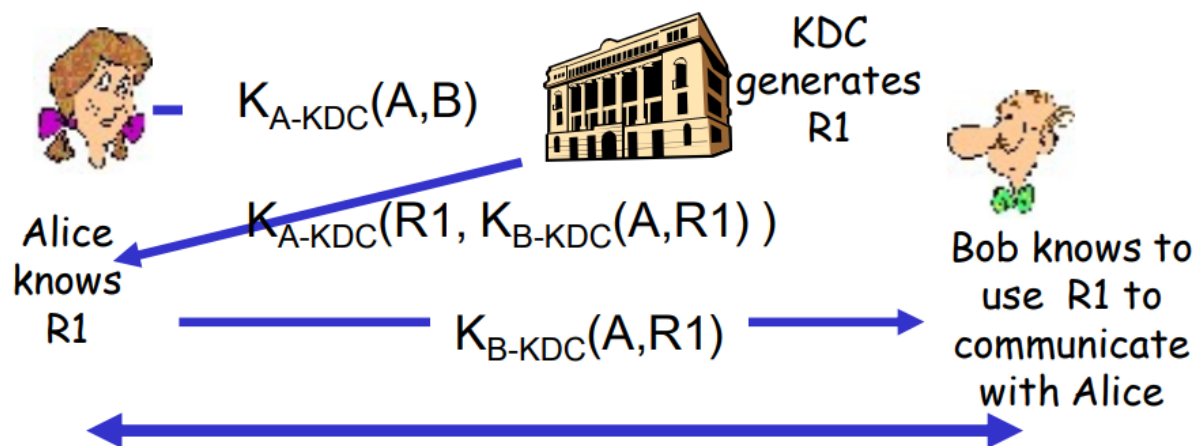
Alice, Bob 需要分享对称式密钥.

KDC: 服务器和每一个注册用户都分享一个对称式的密钥(many users)

Alice, Bob在和KDC通信的时候, 知道他们自己的对称式密钥 KA-KDC KB-KDC.

Key Distribution Center (KDC)

Q: KDC如何使得 Bob和Alice在和对方通信前, 就对称式会话密钥达成一致?



Alice 与Bob通信: 使用R1作为对称式的会话密钥

5.3 CA Certification Authorities

将每一个注册实体E和他的公钥捆绑

E (person, router) 到CA那里注册他的公钥.

E 提供给CA, 自己身份的证据 "proof of identity"

CA创建一个证书, 捆绑了 实体信息和他的公钥.

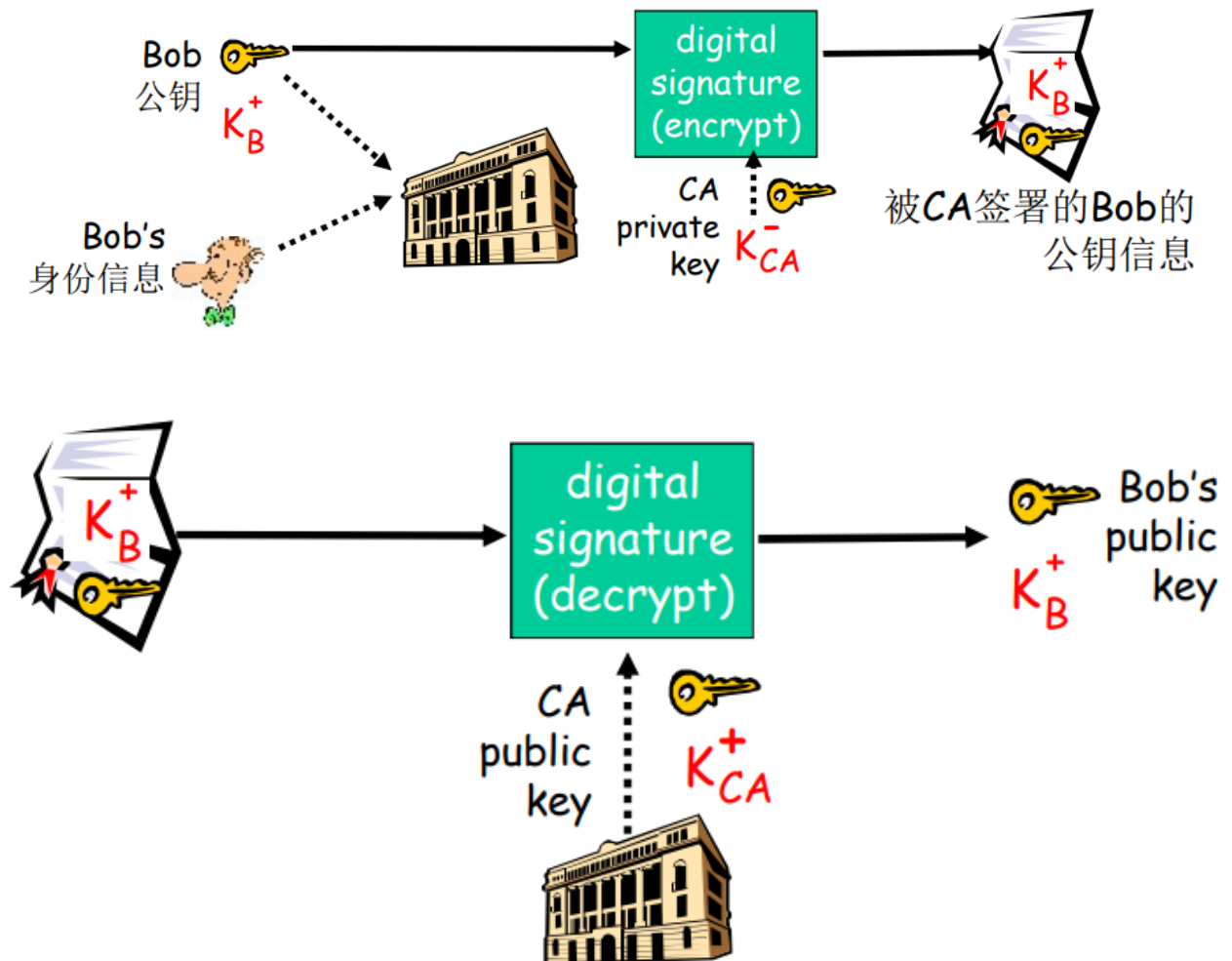
Certificate包括了E的公钥, 而且是被CA签署的 (被CA用自己的私钥加了的) - CA说 "this is E's"

public key”

当Alice需要拿到Bob公钥

获得Bob的证书certificate (从Bob或者其他地方).

对Bob的证书, 使用CA的公钥来验证



5.4 证书

串号: 证书发行者唯一

证书拥有者信息, 包括算法和密钥值本身 (不显示出来)

证书发行者信息

有效信息

颁发者签名

