证书与PKI

Public-Key Certificate and Public Key Infrastructure

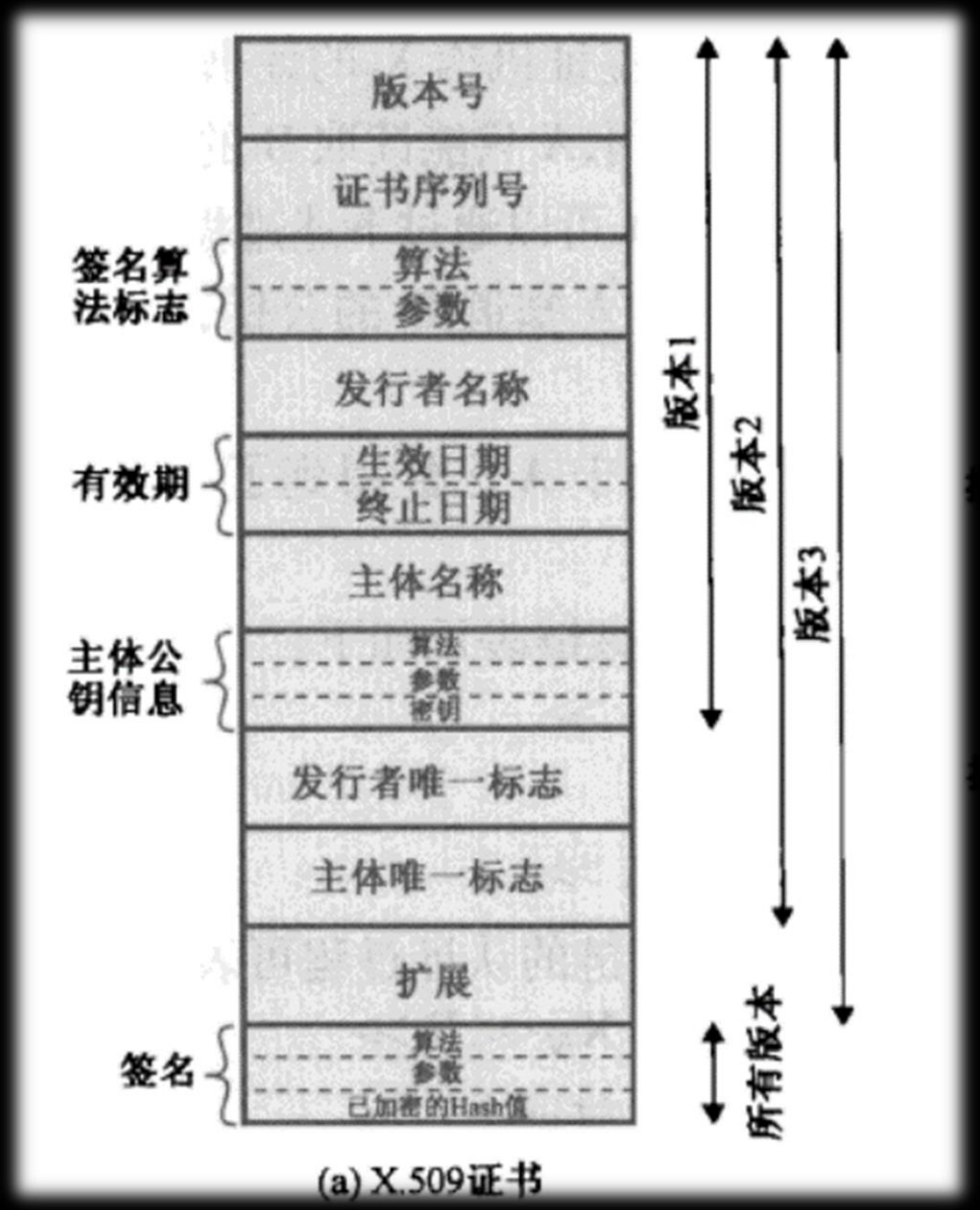
可厉害的土豆

- 什么是证书
- 证书的工作原理
- 什么是PKI
- PKI的组成
- PKI的工作原理
- 攻击方法

什么是证书

公钥证书(Public key certificate, PKC)：用来证明公开密钥拥有者的身份。此文件包含了公钥信息、拥有者身份信息（主体）、以及数字证书认证机构（CA）对这份文件的数字签名。通常简称为证书。

业界现行的标准是国际电信联盟电信标准化部门制定的X.509，并由IETF发行的RFC5280详细述明。


版本号
证书序列号
签名算法标志
算法
参数
发行者名称
有效期
生效日期
终止日期
主体名称
主体公钥信息
算法
参数
密钥
发行者唯一标志
主体唯一标志
扩展
签名
算法
参数
已加密的Hash值
版本1
版本2
版本3
所有版本

(a) X.509证书


证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
版本
V3
序列号
0279ac458bc1b245...
签名算法
sha256RSA
签名哈希算法
sha256
颁发者
DigiCert Global Roo...
有效期从
2017年11月27日 20:...
到
2027年11月27日 20:...
使用者
Encryption Everywh...
公钥
RSA (2048 Bits)

图片来源：[1]

证书的工作原理

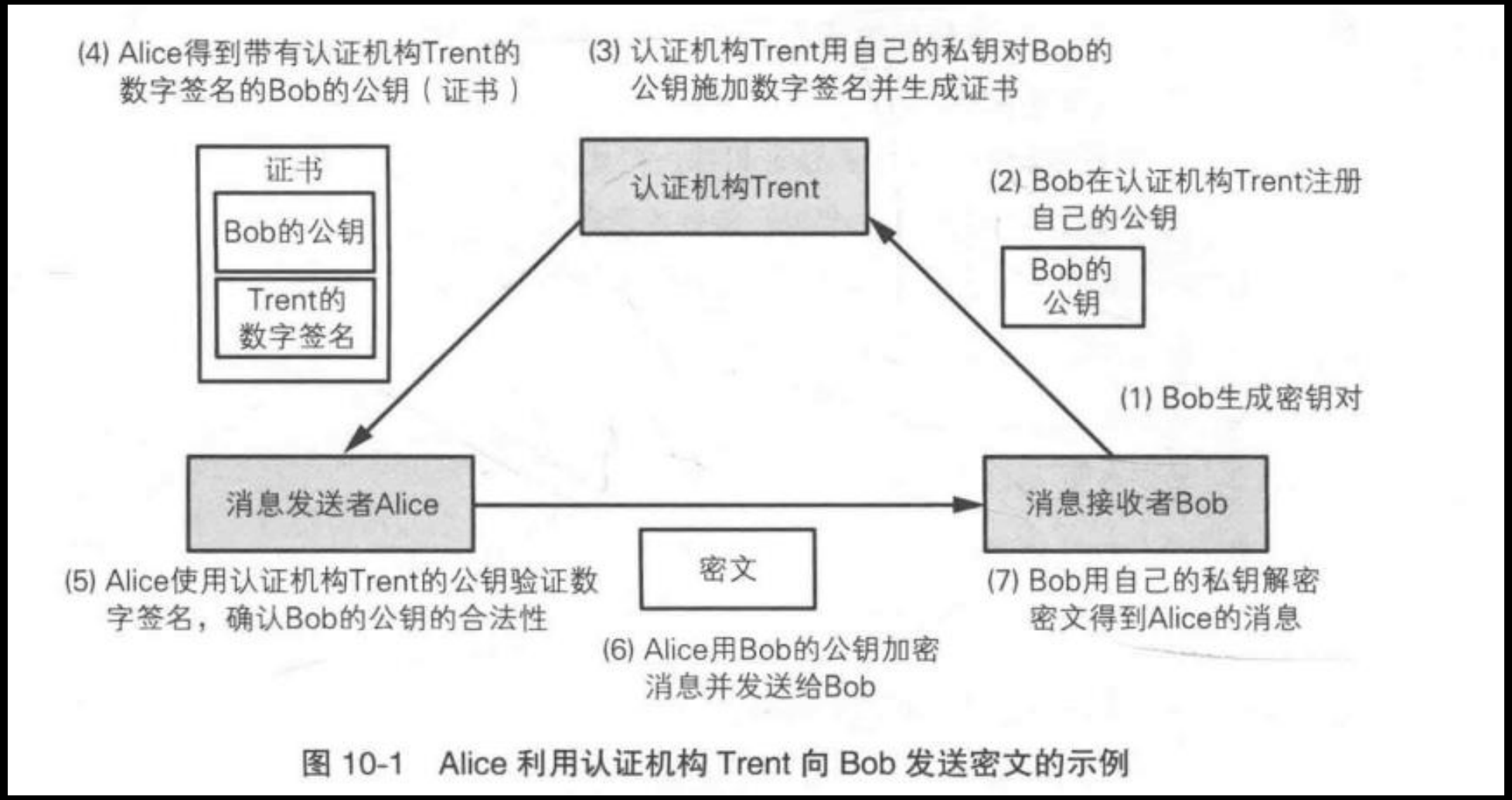


图 10-1　Alice 利用认证机构 Trent 向 Bob 发送密文的示例

什么是PKI

公钥基础设施 (Public-Key Infrastructure, PKI) 是为了能够更有效地要运用公钥而制定的一系列规范和规格的总称。

PKI只是一个总称，并非指某一个单独的规范或规格。

PKI的组成要素

- 终端实体——使用PKI的终端
- 注册中心 (Registration Authority , RA) ——身份验证和公钥注册
- 认证中心 (Certification Authority, CA) ——创建、发布、作废证书
- 证书存储库—— 存储证书和与PKI相关的信息

图片来源：[2]

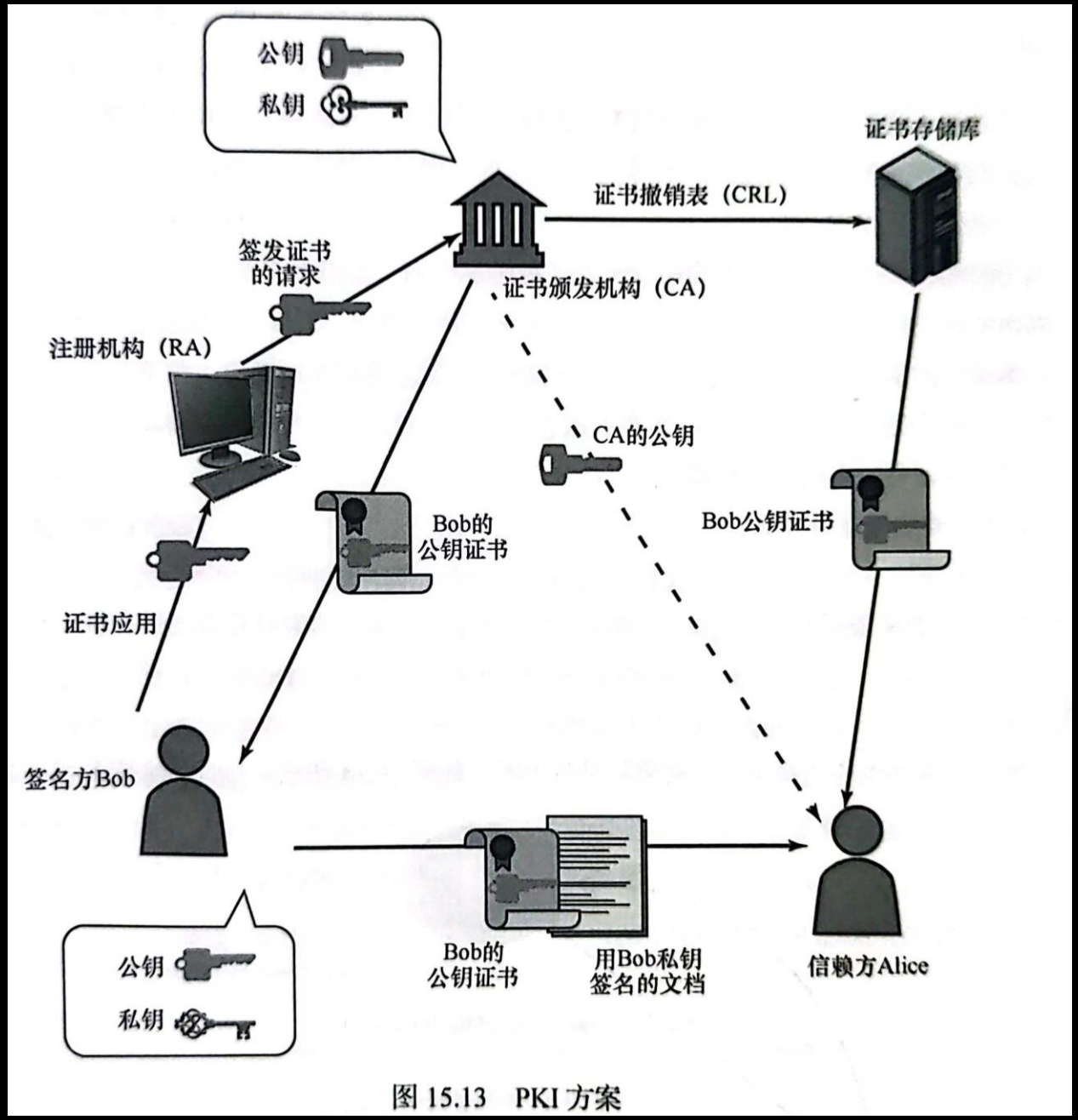


图 15.13　PKI 方案

证书作废清单CRL

- 当用户私钥丢失、被盗或更新等变更情况出现时，CA需要对证书进行作废。要作废证书，CA需要制作一张证书作废清单 (Certificate Revocation List, CRL)。清单内列举了已作废的证书序列号，并由认证机构加上数字签名，然后发布出来。

层级关系

- 认证机构的公钥可以由其他认证机构施加数字签名，从而对认证机构的公钥进行验证。
- 一个认证机构来验证另一个认证机构的公钥，这样的关系可以迭代好几层。
- 广受信任的根CA签署从属 CA的公钥证书。
- 所有的证书都可以追溯到最终的根CA。(根CA不唯一)

攻击方法

- 在公钥注册之前进行攻击
- 注册相似人名攻击
- 窃取认证机构CA的私钥进行攻击
- 伪装成认证机构进行攻击
- 利用CRL发布的时间差实现仿冒
- 利用CRL发布的时间差实现否认

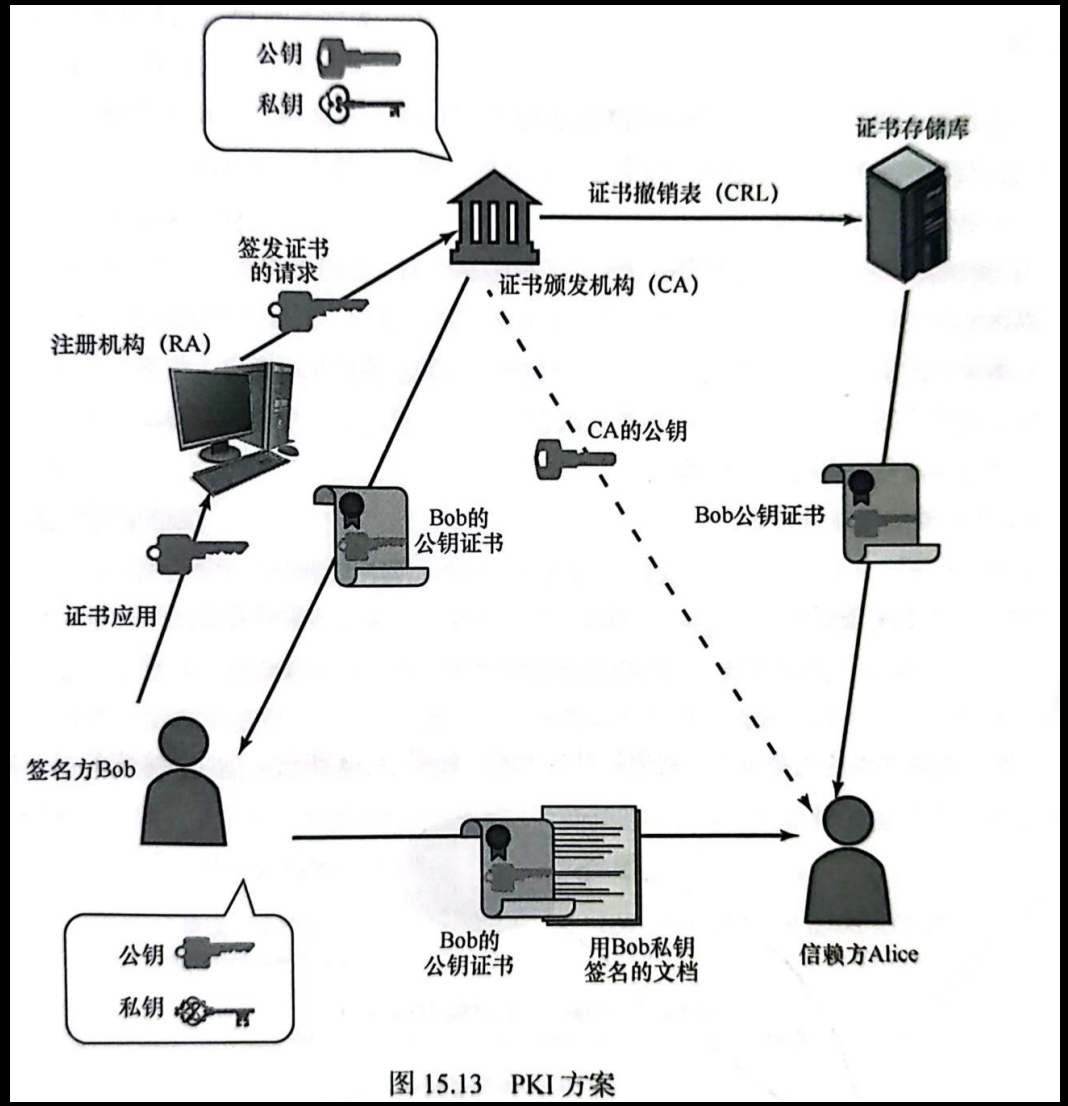


图 15.13　PKI 方案

参考资料

[1] [日] 结城浩. 图解密码技术(第3版)[M].周自恒,译.北京:人民邮电出版社, 2014.

[2] [美] William Stallings.密码编码学与网络安全：原理与实践(第8版)[M]. 陈晶, 译. 北京:电子工业出版社, 2021.

感谢观看

祝你

每顿饭都吃饱

每晚都睡好

身体健康

学业有成

工作顺利

天天开心

~O(∩_∩)O~

可厉害的土豆