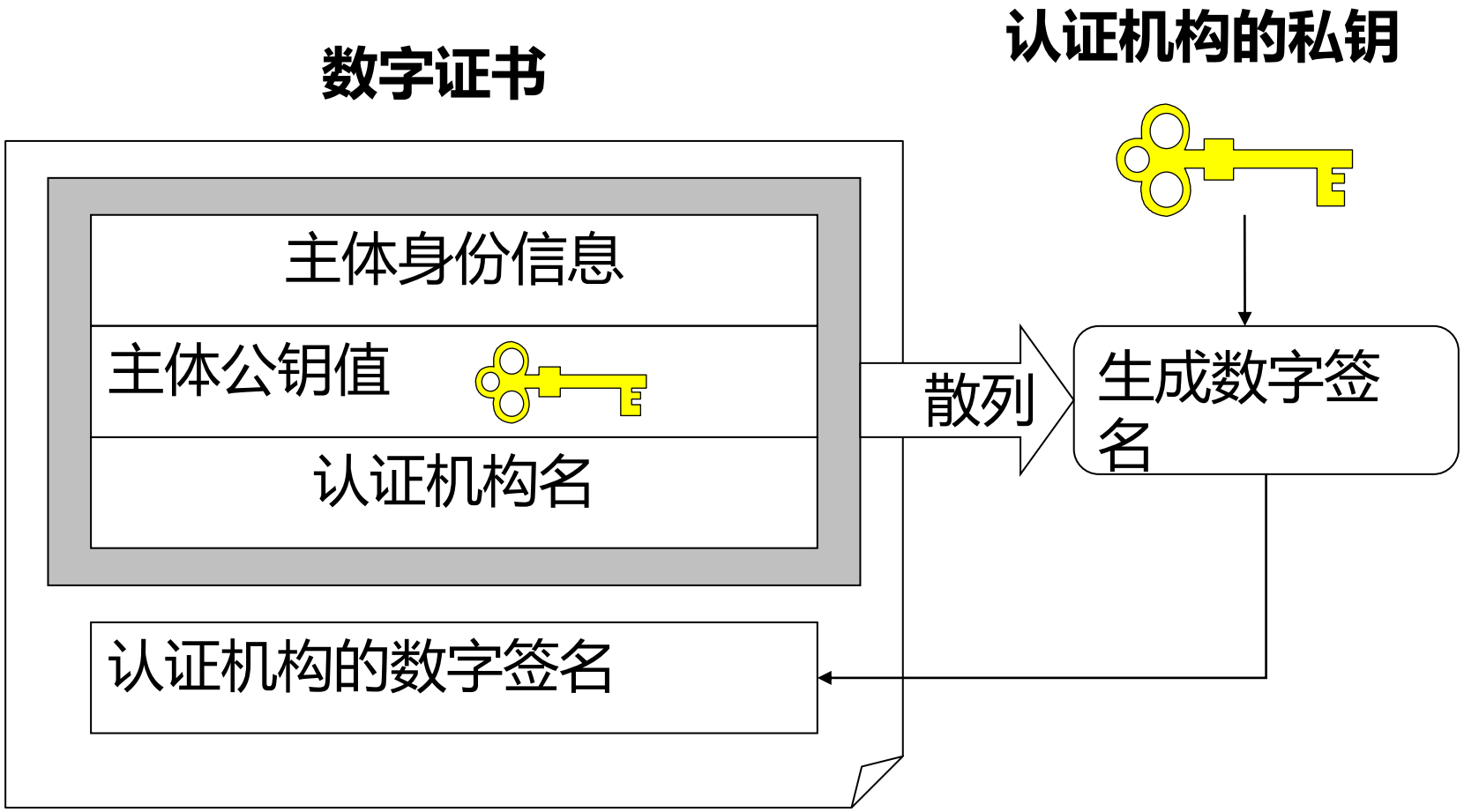
公钥基础设施

李琦
清华大学网研院

公钥基础设施PKI的核心组件: 数字证书



注意：

- 虽然证书只包含了公钥，但必须与对应私钥配合使用
- 数字证书和私钥的关系有点像锁和钥匙的关系。虽然锁里面没有包含钥匙，但是锁必须和钥匙配合使用

公钥基础设施PKI（Public Key Infrastructure）

CA（Certificate Authority）：可信赖的第三方权威机构，负责给网络实体颁发身份证明书，将用户所持有的公开密钥与其身份信息结合在一起

PKI（Public Key Infrastructure）：由CA，数字证书等组成的公钥与身份验证体系

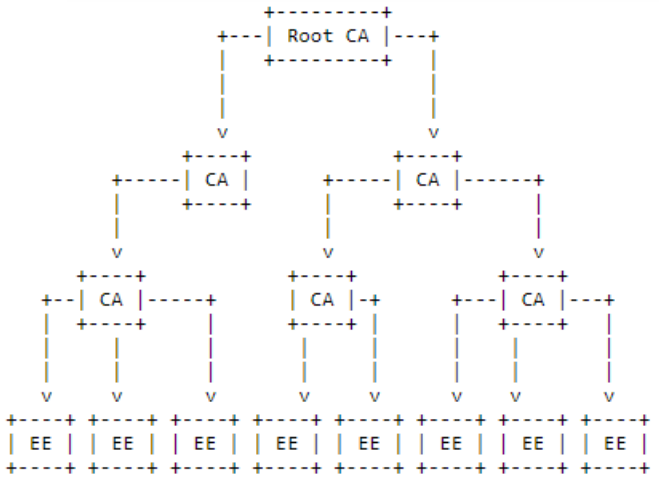


Figure 1 - Sample Hierarchical PKI

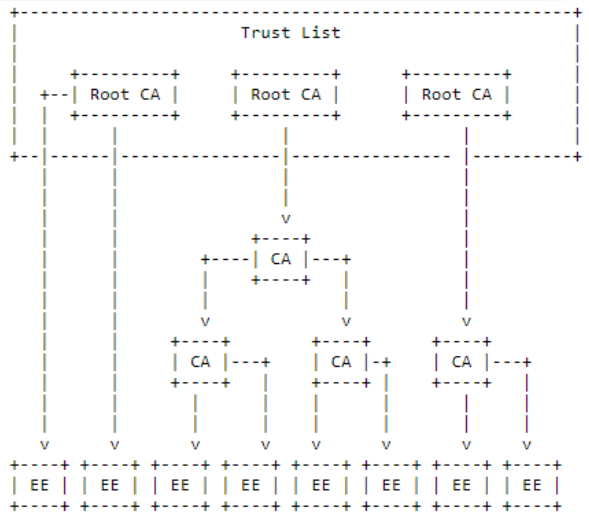


Figure 2 - Multi-Rooted Hierarchical PKI

讨论

畅所欲言

你认为 公钥基础设施本身是否存在安全问题?

PKI的作用及存在问题

用户可以利用PKI提供的服务进行安全通信，但PKI仍然存在安全问题

01 认证机关是否可信?

02 证书颁发与维护过程是否存在风险?

PKI的作用及存在问题

保障公钥基础设施安全性并不是一个很容易解决的问题

PKI: an ideal solution or source of the problem?

PKI Issues - 10 things I wish they warned me about PKI

PKI has been reviewed as a technical infrastructure by a number of security experts. In this paper we look at a number of pratical organizational issues that pure PKI suppliers often fail to mention.

4 fatal problems with PKI

The Web's security runs on complicated PKI deployments, few of which are implemented correctly, and all of which will soon be at the mercy of Moore's Law

本章的内容组织

第一节
PKI概述

- 数字证书
- PKI组成体系结构
- CA的信任关系

什么是PKI?
PKI的存在意义?

第二节
PKI安全问题的由来

- 数字证书颁发过程中的安全问题
- 数字证书维护过程中的安全问题

PKI有什么安全问题?

第三节
PKI安全问题的解决思路

- 建立监督机制
- 建立证书状态日志

如何解决PKI安全问题?

第四节
PKI主要应用场景

- 加密数据传输
- HTTPS协议
- VPN
- RPKI

PKI有哪些应用场景?

PKI的存在意义及
如何构建安全的PKI

如何利用PKI提升
网络空间安全能力

第1节 PKI概述

- 数字证书
- PKI组成体系结构
- CA的信任关系

证书

- 证书是由机关、学校、团体等发的证明资格或权力的文件，是表明（或帮助断定）事理的凭证
- 常见的证书有：身份证、毕业证、荣誉证书、党员证、出生证、学生证、驾驶证、记者证等等
- 现实中的证书是拥有唯一编号的凭证

数字证书

- Kohnfelder于1978年提出数字证书概念
- 数字证书是包含用户身份信息、公钥以及CA数字签名的数据文件

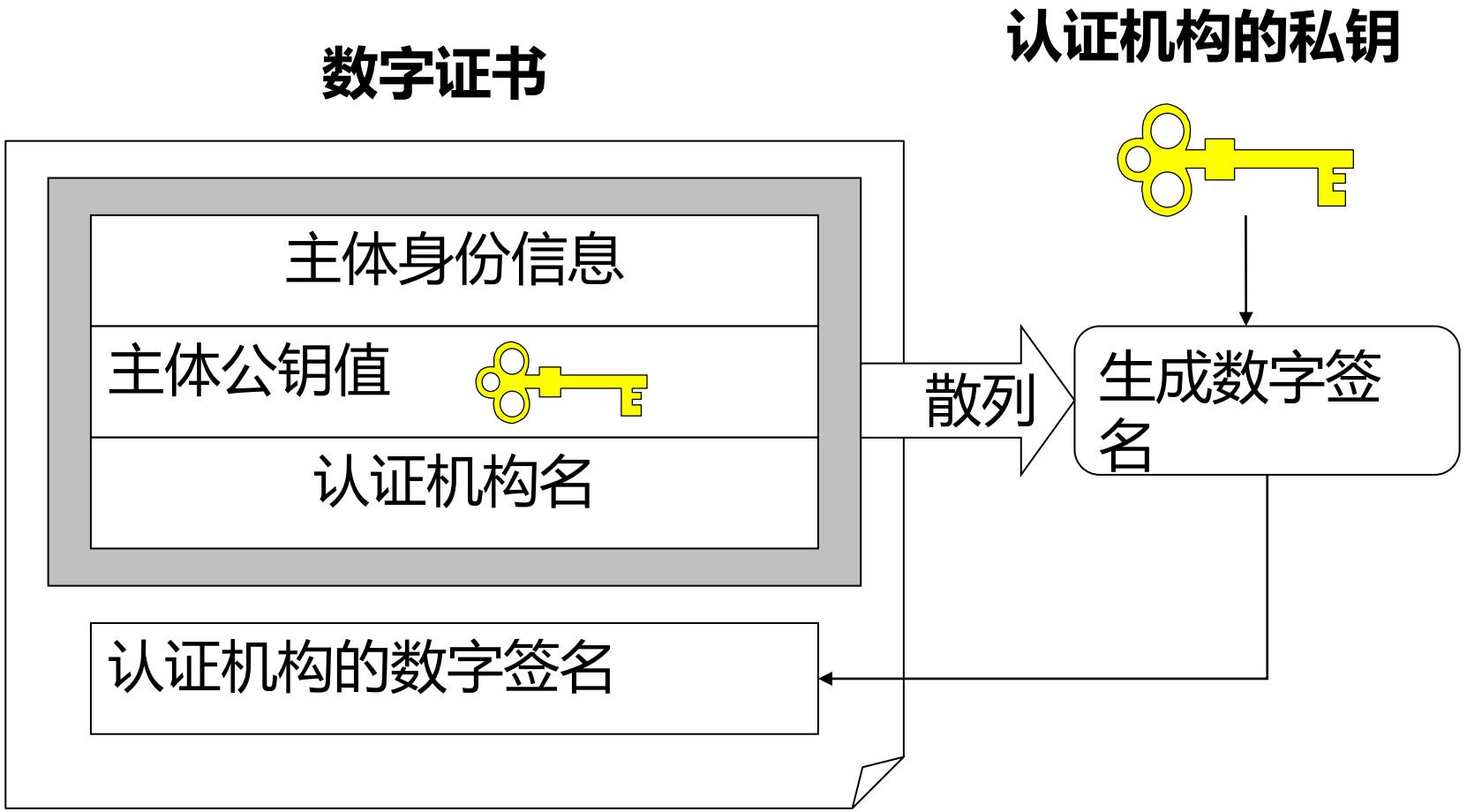
tang.cer

```
sava@sava:~$ cat tang.cer
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIUHTT7rzuoDXEFdcZrC6Xb5EONA0UwDQYJKoZIhvcNAQEL
BQAwcjELMAkGA1UEBhMCdXMxCzAJBgNVBAgMAmRjMQwwCgYDVQQHDANuZXcxEzAR
BgNVBAoMCnVuaXZlcnNpdHkxCzAJBgNVBAsMAkhWMQswCQYDVQQDDAJYdTEZMBcG
CSqGSIb3DQEJARYKMTIzQGFzZC51czAeFw0yMTAzMDIwMjAwMzRaFw0yMjAzMDIw
MjAwMzRaMHIxCzAJBgNVBAYTAnVzMQswCQYDVQQIDAJkYzEMMAoGA1UEBwwDbmV3
MRMwEQYDVQQKDAp1bml2ZXJzaXR5MQswCQYDVQQLDAJIVjELMAkGA1UEAwwCWHUx
GTAXBgkqhkiG9w0BCQEWCjEyM0Bhc2QudXMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC/BaJe7CCEoLtzvhhk8LtFNHp2bYpKPor96kQUMynSUtVxiynv
FY27mpOhFPzrpUwzDFfcI1bF3FVmC9mcbZQvyU9FYQ6Lw8xe8yAoGy/FmwF1w5Ev
DmLqVlcB8uwyMBFqoXr6y/zRVtsC58iuxoV9Q3jHEZkXoZwnlVGl9xr6fNZ6AO90
f5C3+GF6t4IEMKtVJUxP5mDbweq1qCzGx0ILSi3gjf7g3rlbvOXWMXYghaP6w67g
IbzbteC2fvorWyLEB3LThhzYEI4IEZiTavJlbaS9uGOl/LtGRij/Hb+whETcq0IC
9Q4I6r66YO0HipfLEe4VS1DXTDEVkIQyyeBpAgMBAAGjUzBRMB0GA1UdDgQWBBSC
EYpL0Alf7fwN1z8TVh1Q99UkgzAfBgNVHSMEGDAWgBSCEYpL0Alf7fwN1z8TVh1Q
99UkgzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCoySPDeWPJ
OjYG6uzQ77Q9bGEUm2t4d/4n/aIquheblTtahf2XPDunjL56woaGBDntOOZaTJOU
lg6N7scfmn+wh0Ew+iTkNISANzgdEMqepD3aTllLdzAiM4ct7IGTFwVZCMZA1jFm
6KTcPHAf7houqrtYOw64ag7qyokTg4tIaNSEaKhQ04OCRIGl84Z88dixHAxlhiIo
eqk85lvuPIxz6nMkg58+HVuUkh2yj72ES8YaXqKVri3pTdtePF9LHdSmrepCgC/4
VQsge1TdHKTRybQVFxWW6wLVcyvhQa4C7YQcOtMyERW9We2AJGZeh6IVJvBmAq6f
vTzmtiH9xrAx
-----END CERTIFICATE-----
sava@sava:~$
```

数字证书

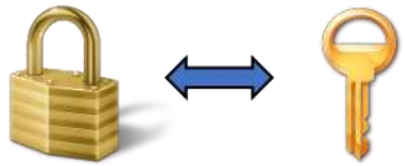
主体将其身份信息和公钥以提交给CA认证中心，CA用自己的私钥对主体公钥和身份ID进行签名，生成由公钥、身份ID和CA签名三部分组成的证书

数字证书



注意：

- 虽然证书只包含了公钥，但必须与对应私钥配合使用
- 数字证书和私钥的关系有点像锁和钥匙的关系。虽然锁里面没有包含钥匙，但是锁必须和钥匙配合使用



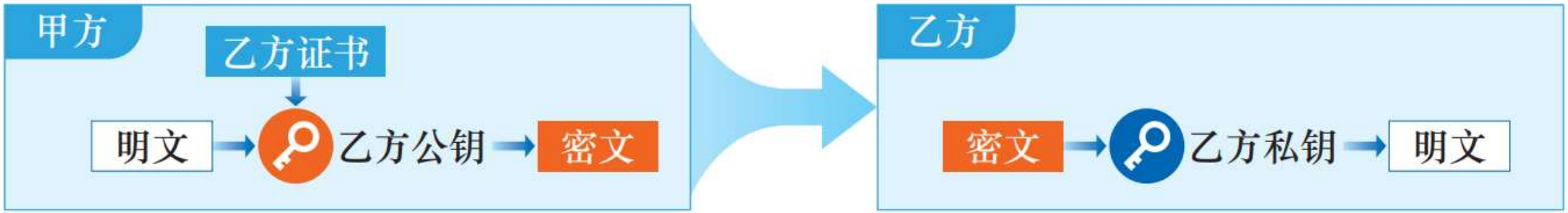
利用数字证书进行加密

① 甲方准备好要传送给乙方的信息（明文）

② 甲获取乙的数字证书，并验证该证书有效后，用乙方证书中的公钥加密信息（密文）

③ 乙方收到加密的信息后，用自己证书对应的私钥解密密文，得到明文信息。

明文数据量很大时可以结合数字信封的方式加密



利用数字证书进行签名

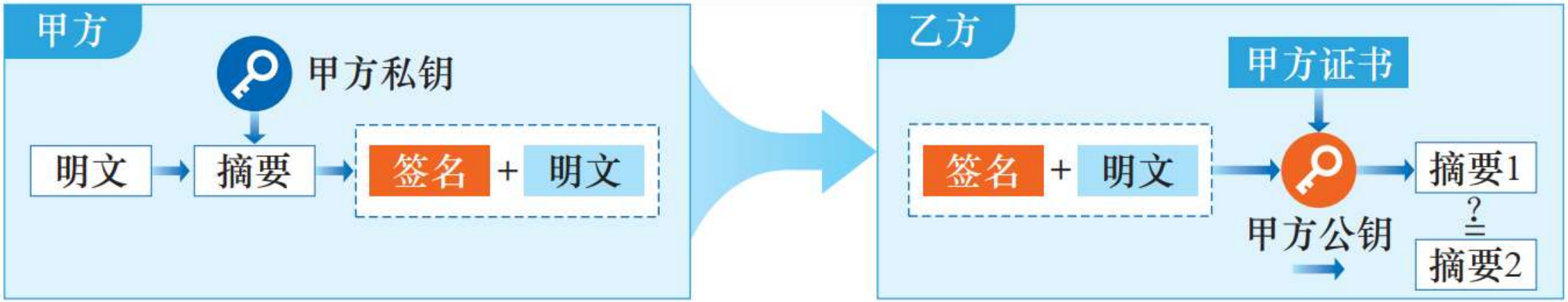
① 甲方准备好要传送给乙方的信息（明文）

② 甲计算该信息的消息摘要

③ 甲用自己证书对应私钥对消息摘要加密得到数字签名，并将其附在信息后

④ 甲方将附带有数字签名的信息传送给乙方

⑤ 乙方验证甲方数字证书后用证书中的公钥解密数字签名



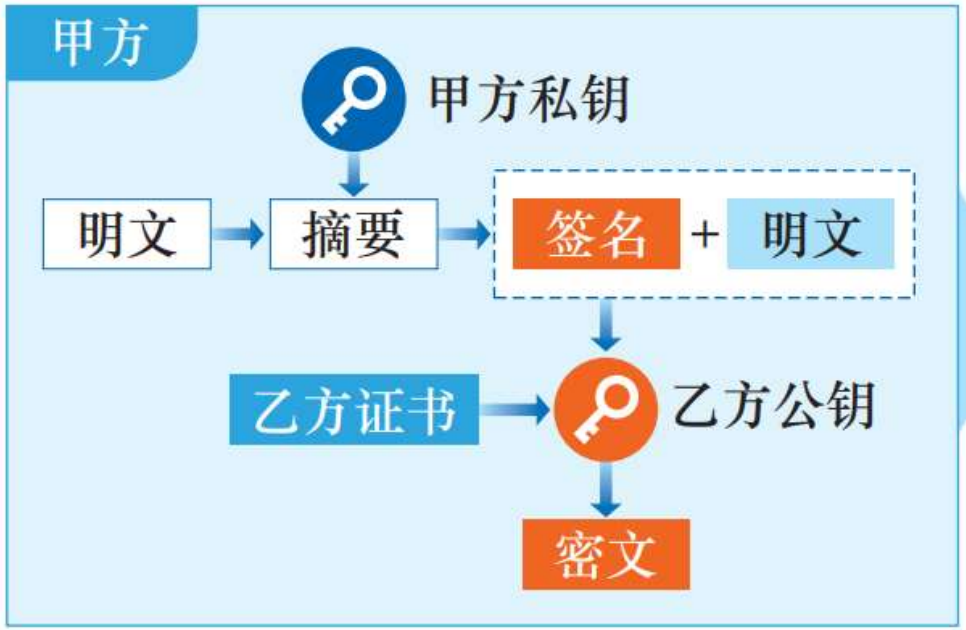
利用数字证书同时进行签名和加密

① 甲方准备好要传送给乙方的信息（明文）

② 甲计算该信息的消息摘要

③ 甲用自己证书对应的私钥对消息摘要进行加密得到甲的数字签名，并将其附在信息后

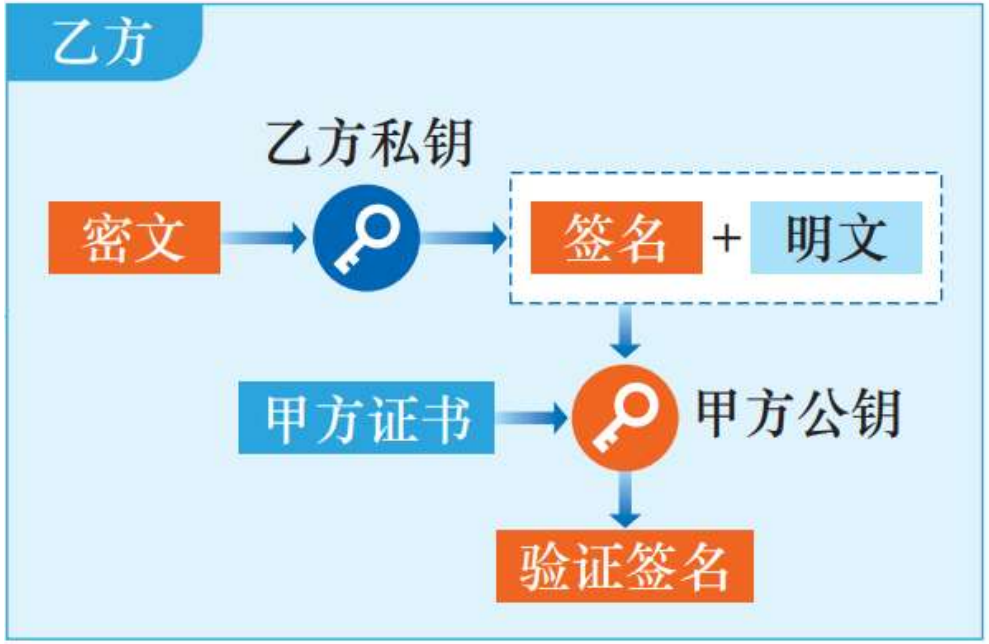
④ 甲用乙方证书中的公钥加密信息和签名的混合体



利用数字证书同时进行签名和加密

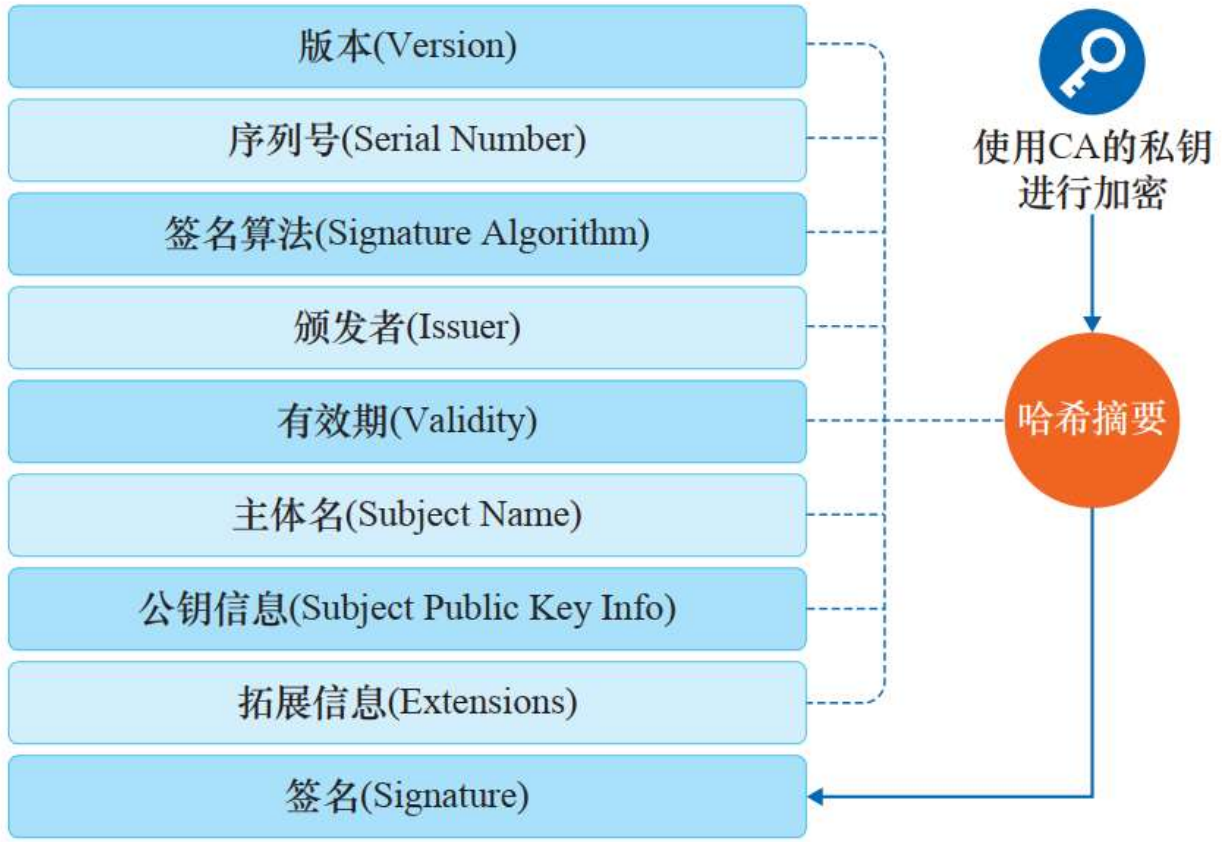
⑤ 乙方收到加密数据，用自己证书对应私钥解密密文，得到信息和数字签名的混合体

⑥ 乙方验证甲方证书有效后，用甲方证书中公钥解密数字签名，得到消息摘要，验证签名



X.509证书格式

- 现实中有各种各样的数字证书，如PGP、SET、IPSec
- 目前应用最广泛的证书格式是国际电信联盟ITU提出的X.509版本
- X.509于1988年颁布，1993和1995年两次修改
- IETF针对X . 509在Internet环境的应用，颁布了RFC2459



X.509证书实例子

CFCA是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一

CFCA
中国金融认证中心

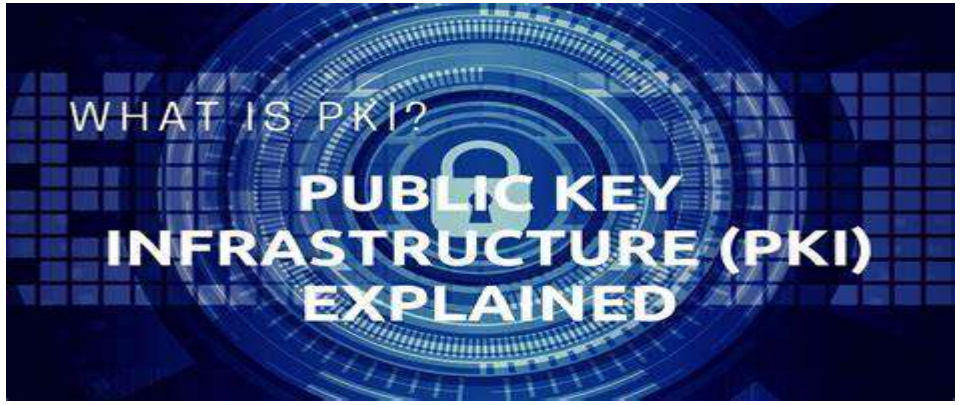
保证公钥的真实性

- 公钥的分发虽然不需要保密，但需要保证公钥的真实性
- 就好像银行的客服电话，虽然不需要保密，但需要保证真实性

- 数字证书和公钥基础设施PKI就是为了实现在公钥分发过程中确保公钥真实性

PKI的作用

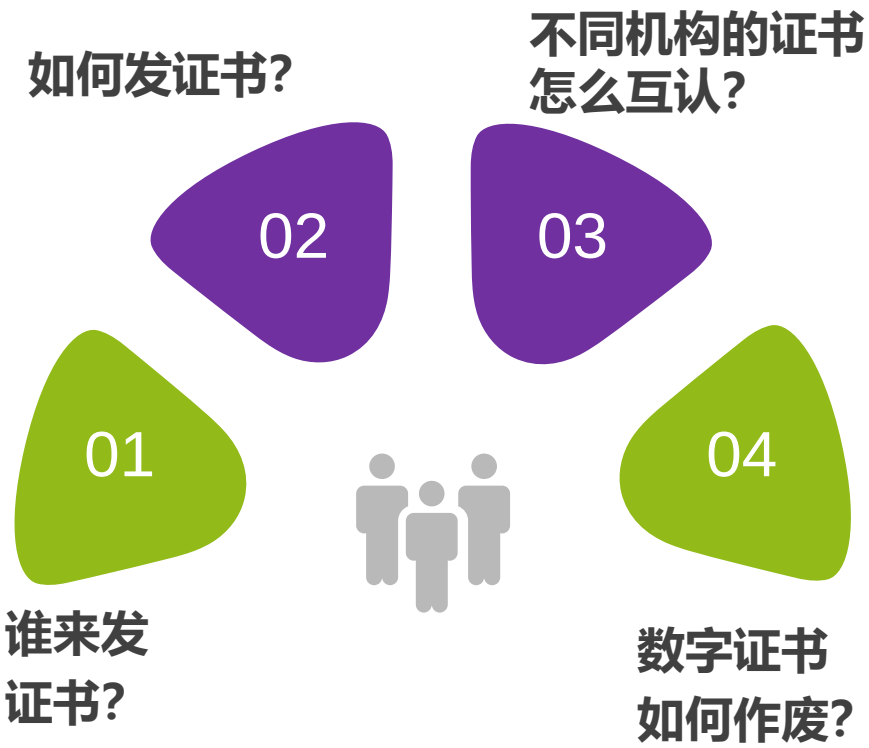
- 公钥基础设施（Public Key Infrastructure）以公钥技术为基础，提供具有普适性安全服务的基础设施
- PKI 旨在从技术上解决网上身份认证、信息的完整性和不可抵赖性等安全问题



例如：

1. 在WEB服务器和浏览器之间的通信
2. 电子邮件
3. 电子数据内部交换
4. 在Internet上的信用卡交易
5. 虚拟专用网VPN

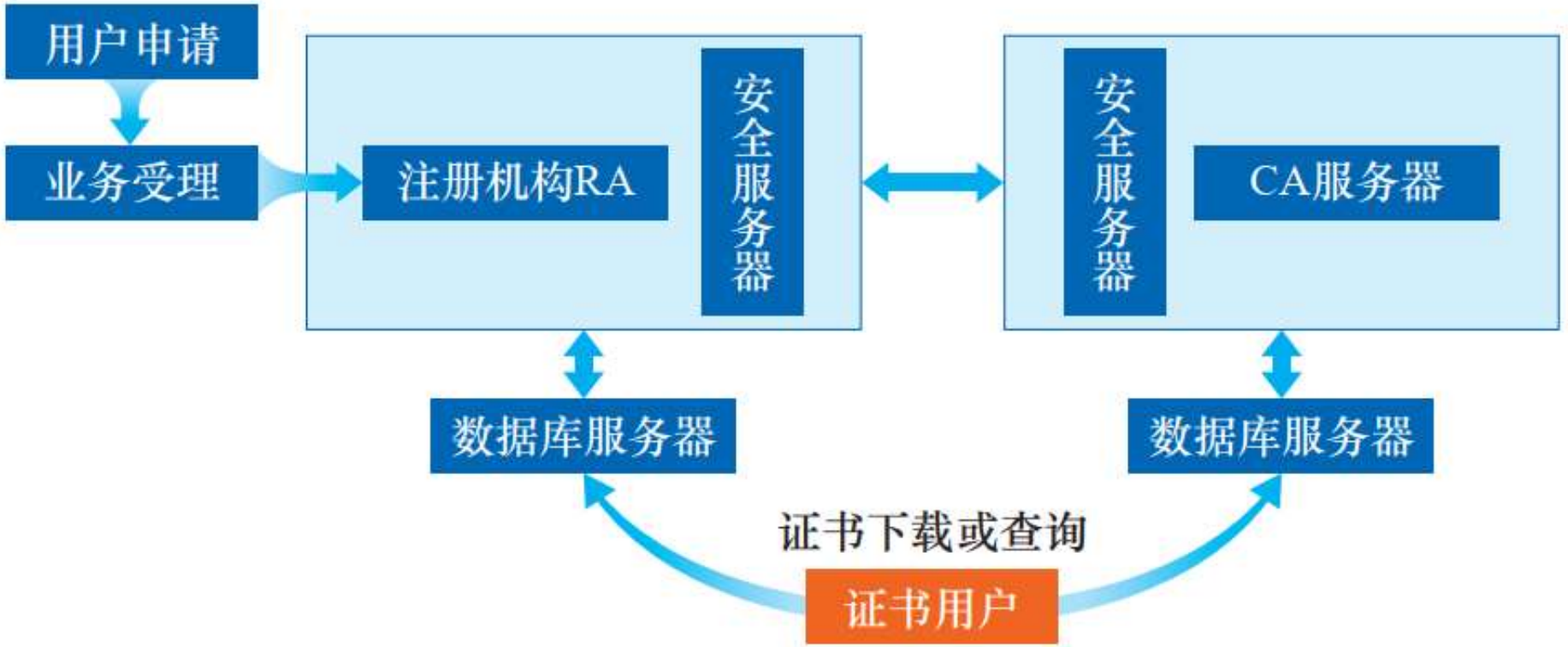
PKI基本功能



- 用户注册
- 证书申请
- 密钥产生
- 密钥更新
- 密钥备份
- 密钥恢复
- 证书作废
- 证书归档

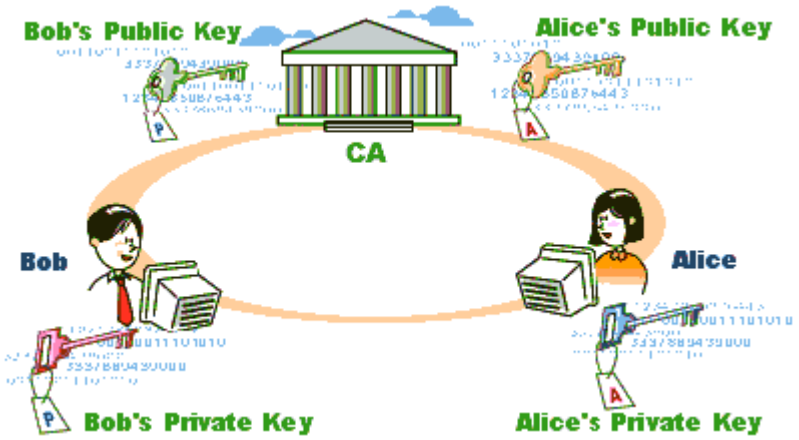
PKI 体系架构

PKI体系通常由终端实体用户、证书认证机构(CA)、证书注册机构(RA)和证书数据库，以及安全服务器组成



CA（Certification Authority）

- 证书机制是目前被广泛采用的一种安全机制，使用证书机制的前提是建立认证中心(CA)以及配套的注册中心(RA)系统
- 证书依靠一个可靠的第三方机构验证，CA专门提供这种服务



CA的职能

- 产生自身证书并传输给安全服务器
- 验证用户的身份，产生、分配并管理PKI结构下的所有用户的证书
- 核心功能就是发放和管理数字证书
- 负责用户证书的黑名单登记和发布

CA的组成

01 **注册服务器**

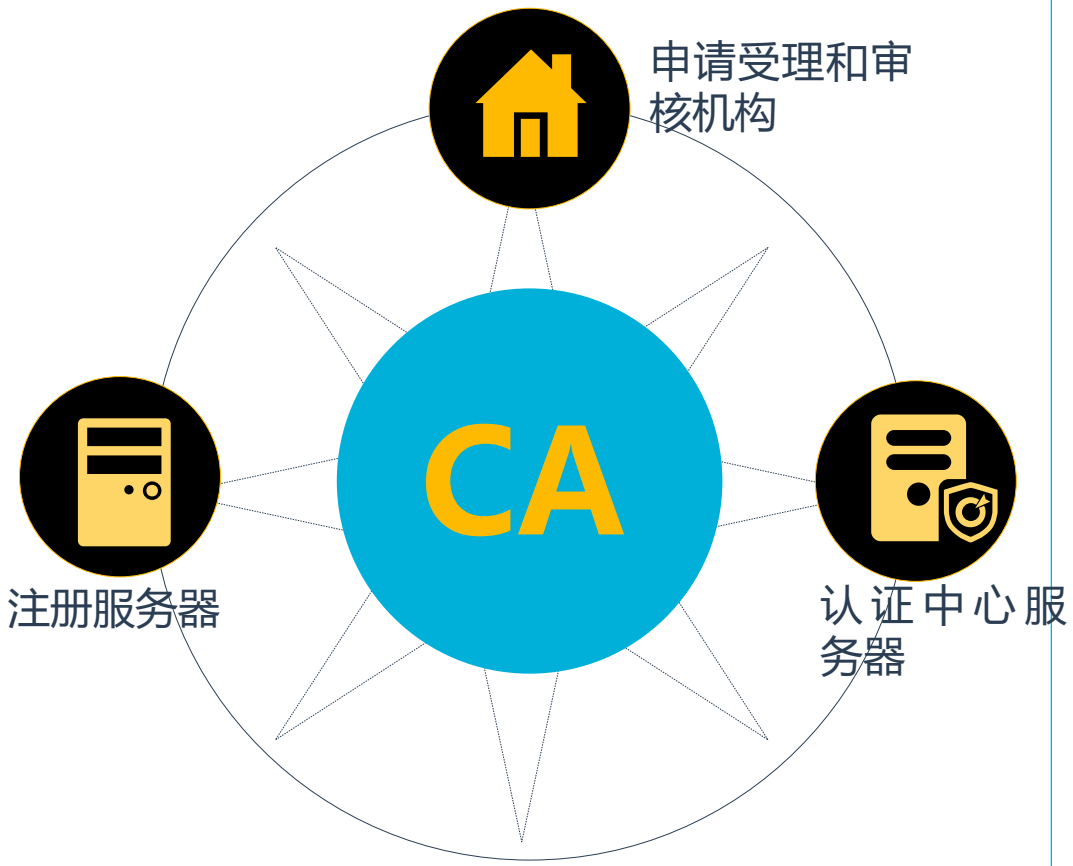
通过 Web Server 建立的站点

02 **证书申请受理和审核机构**

负责证书的申请和审核

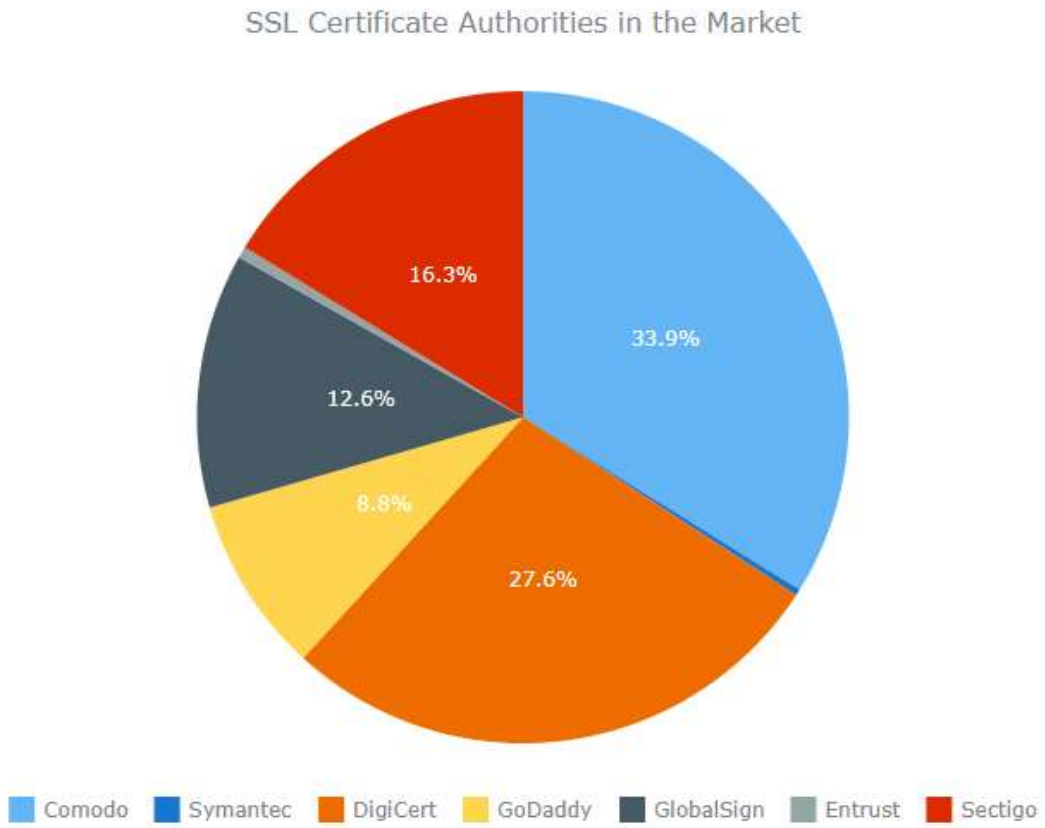
03 **认证中心服务器**

数字证书生成、发放的运行实体



国际主要的CA

全球SSL市场上大约有50个CA，只有少数真正占有一席之地



- Comodo with 42.6%
- Symantec 15.3%
- GoDaddy with 7.7%
- GlobalSign with 4.9%
- Digicert with 2.3%
- StartCom with 0.9%
- Entrust with 0.4%
- Certum with 0.5%

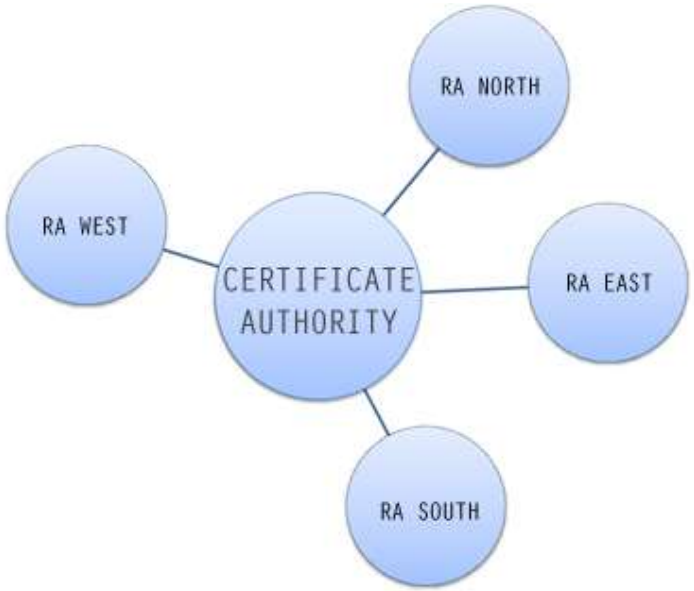
国内主要的CA

我国目前有40多家 CA

- 如: 中国电信CA安全认证体系（CTCA）、
  上海电子商务CA认证中心（SHECA）、
  中国金融认证中心（CFCA）等

RA (Registration Authority)

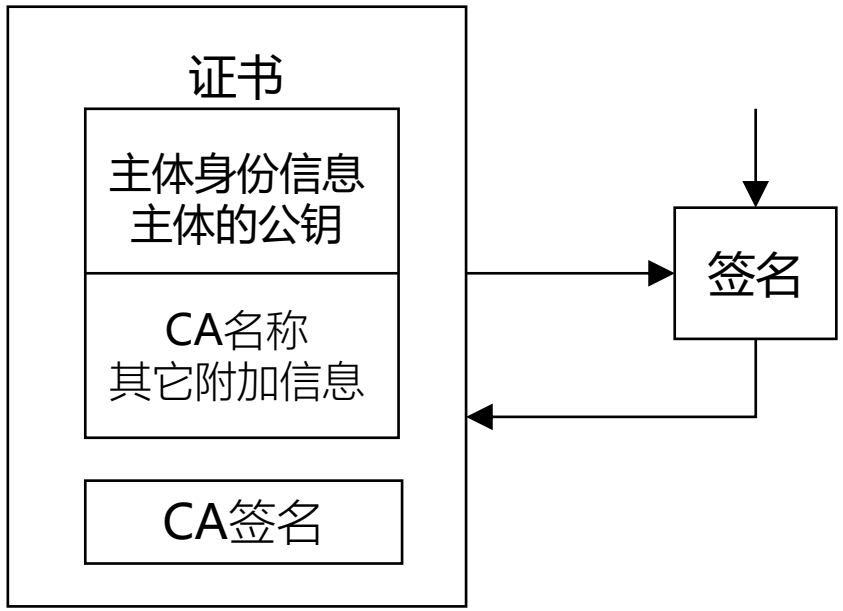
注册中心RA系统负责证书申请者的信息录入、审核以及证书发放等工作；对发放的证书完成相应管理功能



What is a Registration Authority?

"The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation"

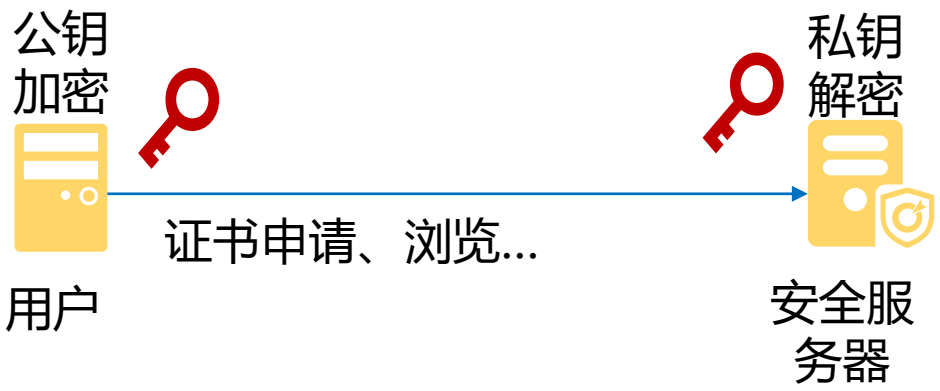
证书库



证书库

- 证书集中存放地，用户可以从此处获得其他用户的证书和公钥
- 证书数据库服务器用于认证机构中数据（如密钥和用户信息等）、日志和统计信息的存储和管理

安全服务器



- 安全服务器面向普通用户，提供证书申请、浏览、撤销列表及证书下载等安全服务
- 用户首先得到安全服务器证书（CA颁发），然后用户与服务器之间的所有通信均以安全服务器的密钥进行加密传输，通过安全服务器的私钥解密得到明文，保证了证书申请和传输过程中的信息安全性

密钥备份及恢复系统

- 为防止用户丢失密钥或密钥被破坏，PKI提供解密密钥的备份和恢复的机制
- 解密密钥的备份和恢复由CA、专用备份服务器等可信机构完成
- 用于签名和校验的密钥对不可备份

证书撤销列表

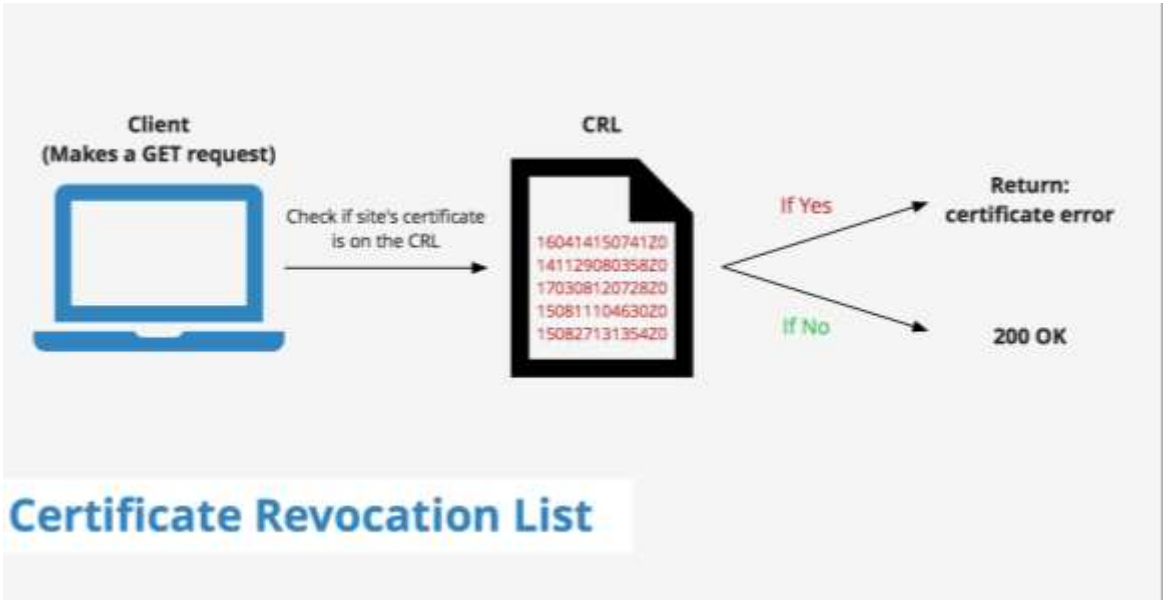
- 私钥泄露、密钥更换、用户变化等情况，证书需要被注销，PKI中通过CA维护一个证书撤销列表（Certificate Revocation List，CRL）
- 检查CRL的URL应该内嵌在用户的证书中，可通过安全途径（SSL）访问URL，返回注销状态信息

证书撤销三种策略

01 作废一个或多个主体的证书

02 作废由某一对密钥签发的所有证书

03 作废由某CA签发的所有证书

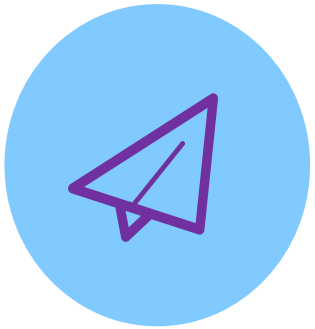


PKI应用接口系统

PKI需要良好的应用接口系统，确保所建立起来的网络环境可信性，降低管理维护成本，向应用系统屏蔽密钥管理细节，提供证书验证及备份恢复

证书验证

完成证书的验证工作，为所有应用以一致、可信的方式使用公钥证书提供支持



备份恢复

以安全、一致的方式与PKI的密钥备份与恢复系统交互，为应用提供统一的密钥备份与恢复支持

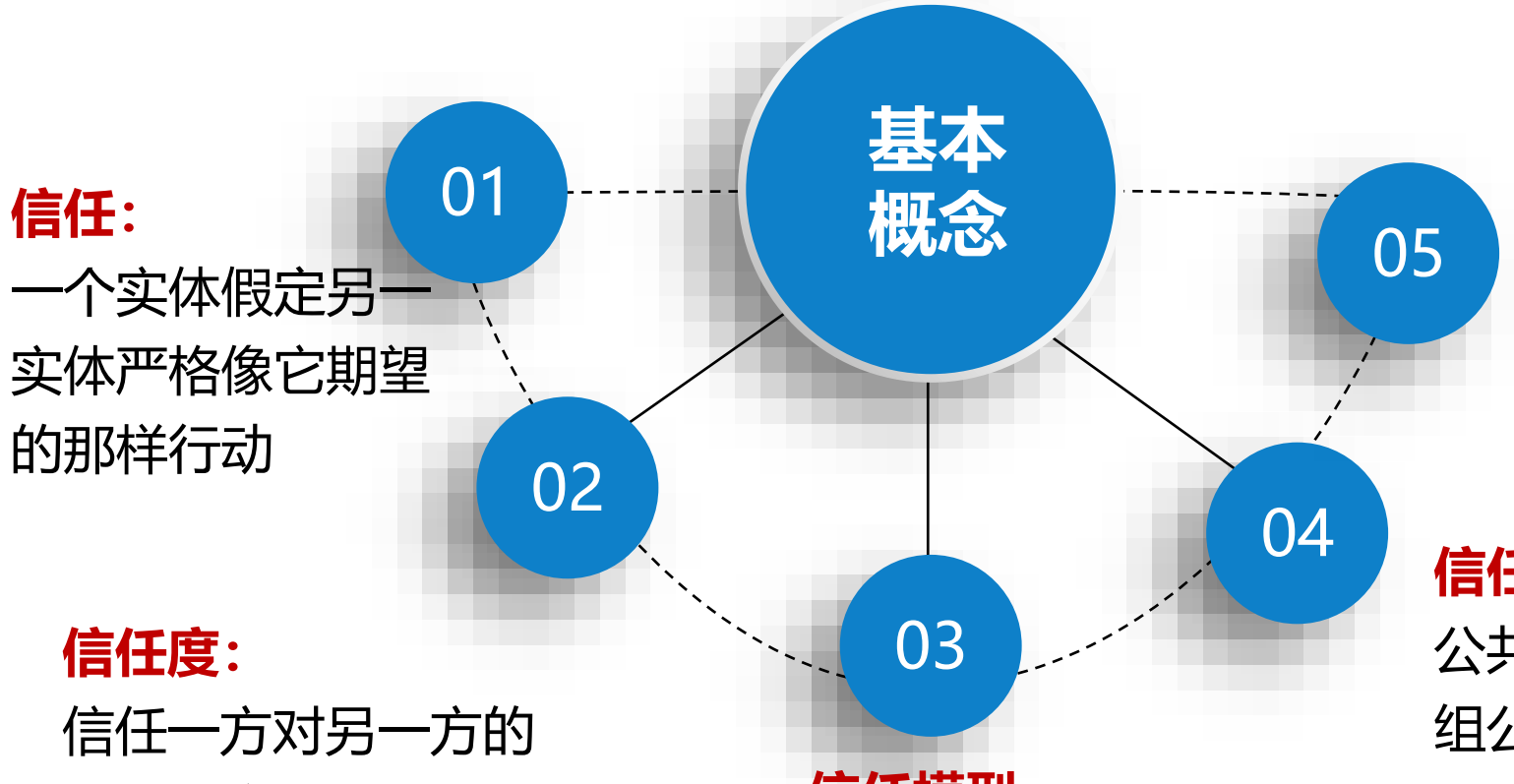
透明性

可扩展性

多种用户

互操作性

CA的信任关系



信任：
一个实体假定另一实体严格像它期望的那样行动

信任锚：
信任体系的起点

信任域：
公共控制下或服从于一组公共策略的系统集

信任度：
信任一方对另一方的信任程度

信任模型：
规定最初信任的建立

PKI信任模型

PKI信任模型：证书用户、证书主体、各CA间的证书认证关系称为PKI信任模型

用户的信任起点在何处

01

信任在系统中如何被传递

02

解决两个问题

01

各国都建立自己的PKI，内部建立不同行业地区PKI

02

不同的PKI之间的互联互通和相互信任

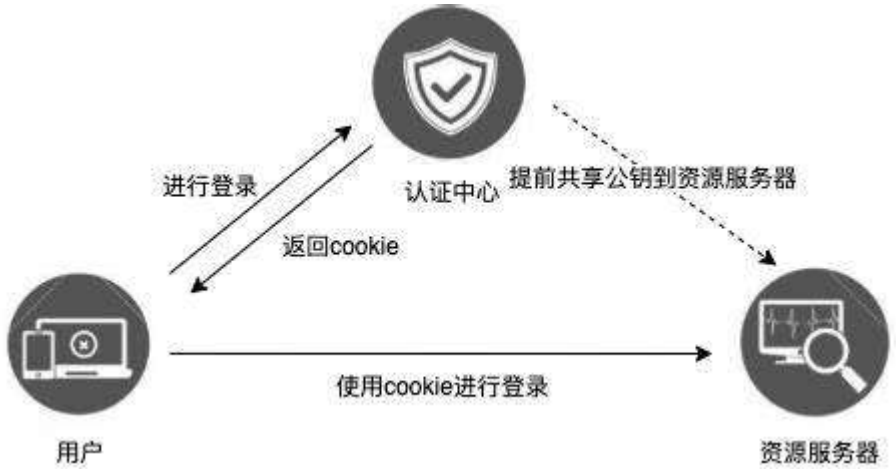
建立形式

PKI信任模型

信任模型提供了建立和管理信任关系的框架，

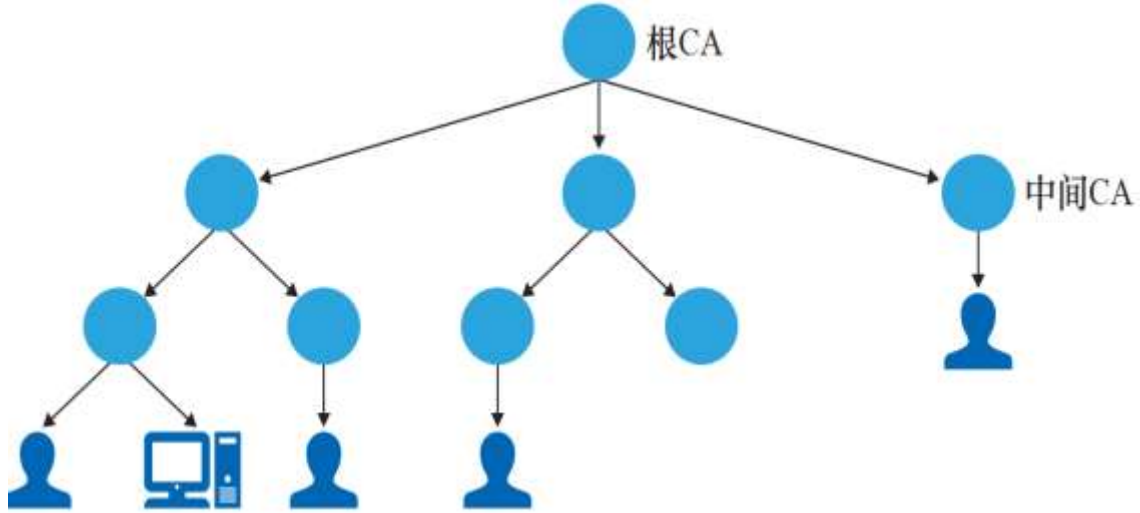
按照有无第三方可信机构参与，信任可划分为直接信任和第三方信任

第三方信任是指两个实体以前没有建立起信任关系，第三方为两者的可信任性进行了担保，是目前网络安全中普遍采用的信任模式



CA的层次结构

- 对于大型权威机构，签发证书的工作不能仅仅由一个CA来完成，可建立一个CA层次结构
- 一个CA一般为一个安全域（security domain）的有限群体发放证书
- 每个CA覆盖一定作用范围，不同用户群体往往拥有不同的CA

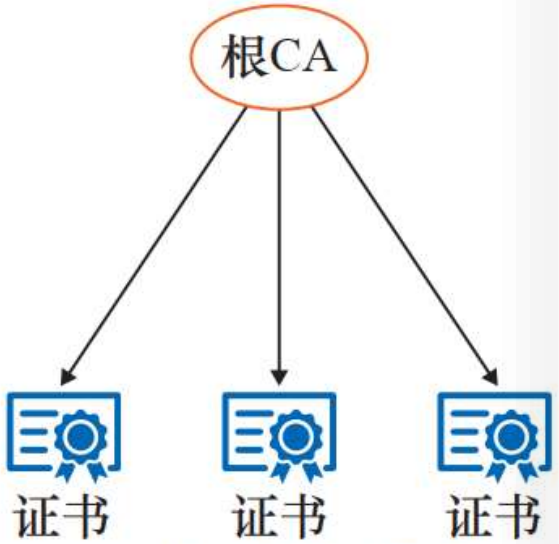


CA的信任模型

A

单CA信任模型：

基本信任模型

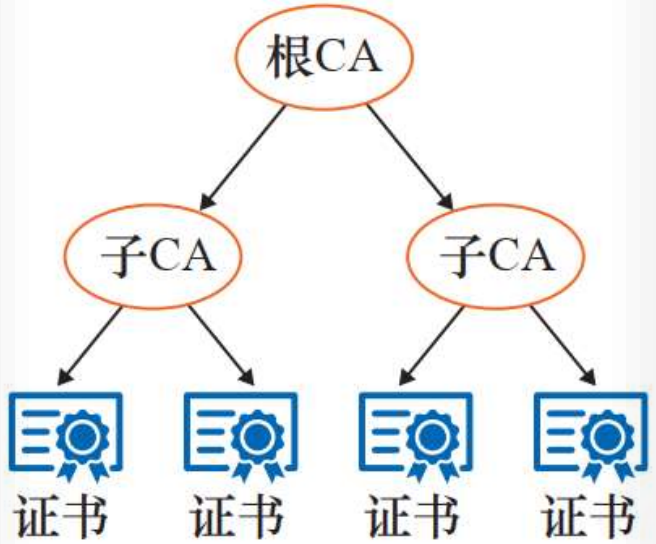


(a)单CA信任模型

B

层次信任模型：

主、从CA建立分级结构

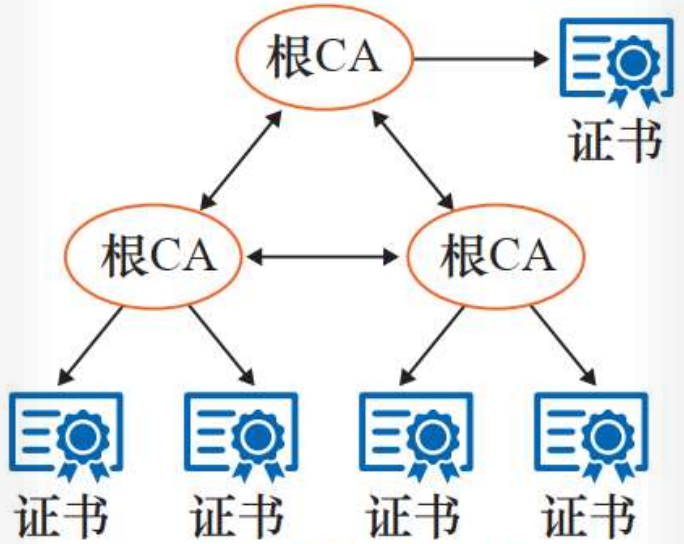


(b)层次信任模型

C

分布式信任模型：

CA间存在交叉认证



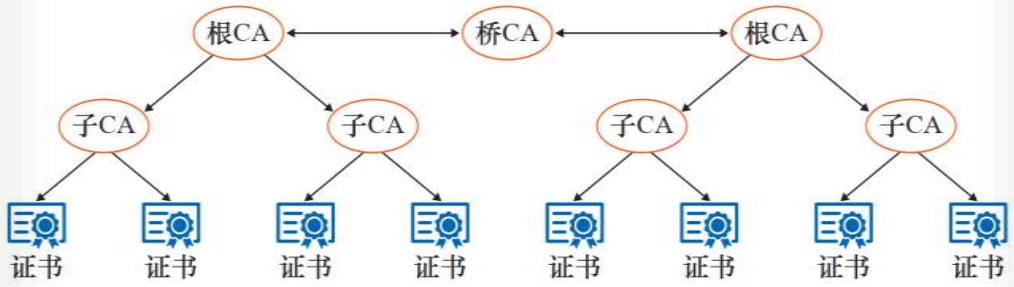
(c)分布式信任模型

CA的信任模型

D

桥CA信任模型：

中心辐射式信任模型

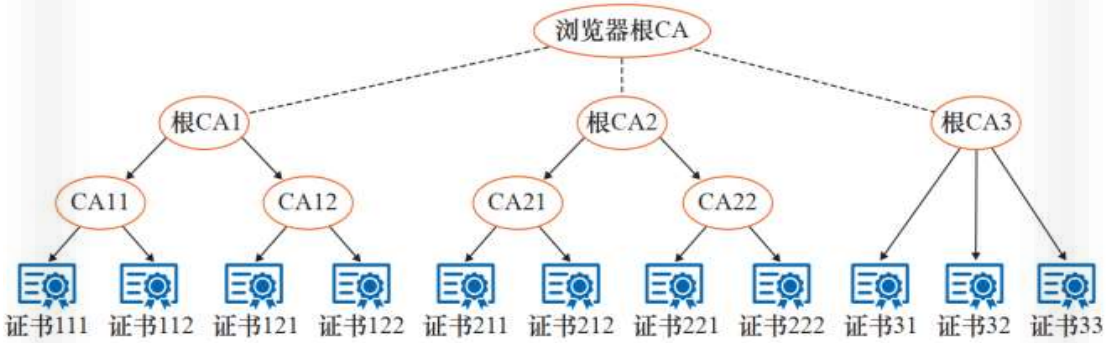


(D)桥CA信任模型

E

WEB信任模型：

构建在Web浏览器基础上

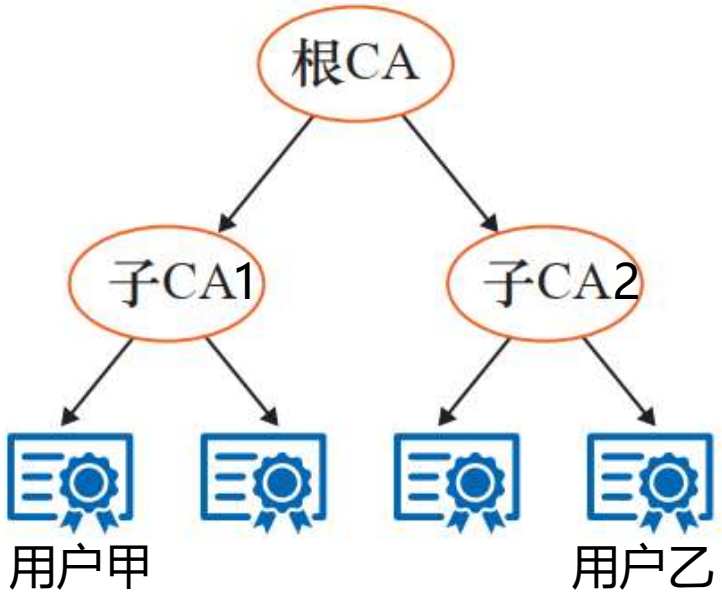


(E) WEB信任模型

严格层次结构模型

CA的严格层次结构可描绘为一颗倒挂的树，根代表整个系统信任起始点，是整个系统的信任锚,根CA下面的分支节点代表中间CA，被称作子CA，叶子节点代表终端用户

- 认证过程：用户甲沿着CA的信任路径验证用户乙证书的数字签名，证书路径长度平均只有层次树高的一半
- 缺点：小规模群体容易对公共根CA达成一致信任，全局范围难以达成一致信任



甲拥有根CA的公钥，可验证子CA2的证书，提取公钥K2，再用K2验证乙的证书

CA层次结构的建立

A 根CA具有一个自签名的证书

B 根CA依次对下面的CA签名

C 叶子节点上的CA用于对个体签名

D 个体仅需信任根，个体证书由底层CA签发

节点CA保存两种证书：

（1）其他CA发给它的certs

（2）它发给其它CA的certs

CA层次结构中证书的验证

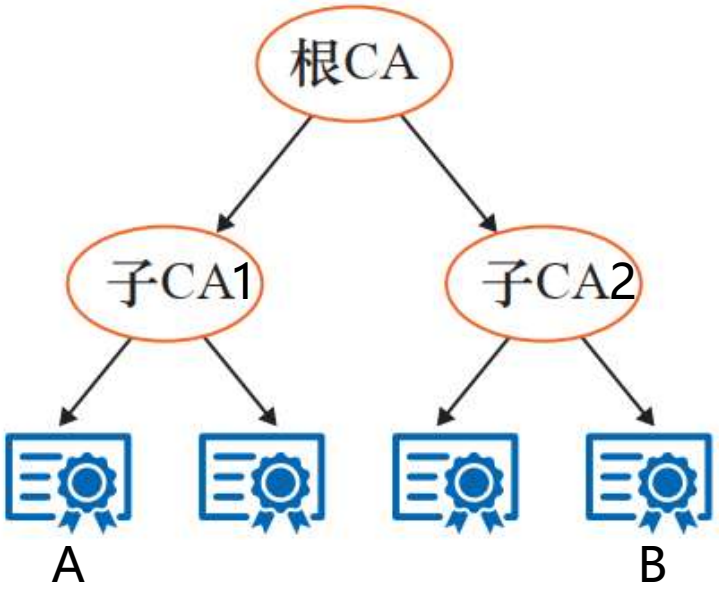
假设个体A看到B的一个证书，B的证书中含有签发该证书的CA的信息，沿着层次树往上找，可以构成一条证书链，直到找到根证书

验证过程

从根证书开始，依次往下验证每一个证书中的签名，一直到验证B的证书中的签名

信任条件

如所有签名验证通过，A可以确定所有证书正确，如果他信任根CA，则相信B的证书和公钥



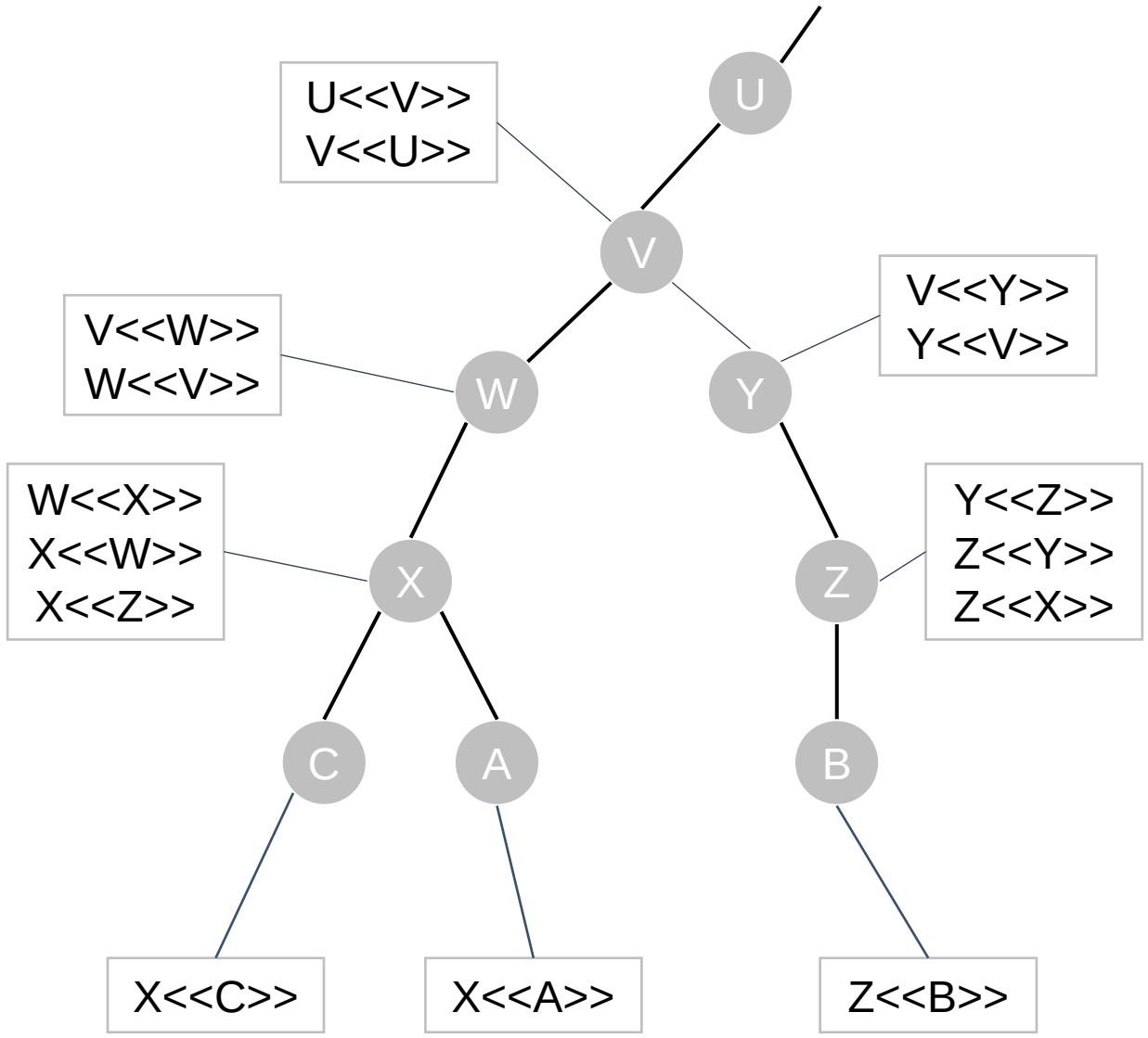
CA层次结构中证书的验证

- A建立通往B的证书路径

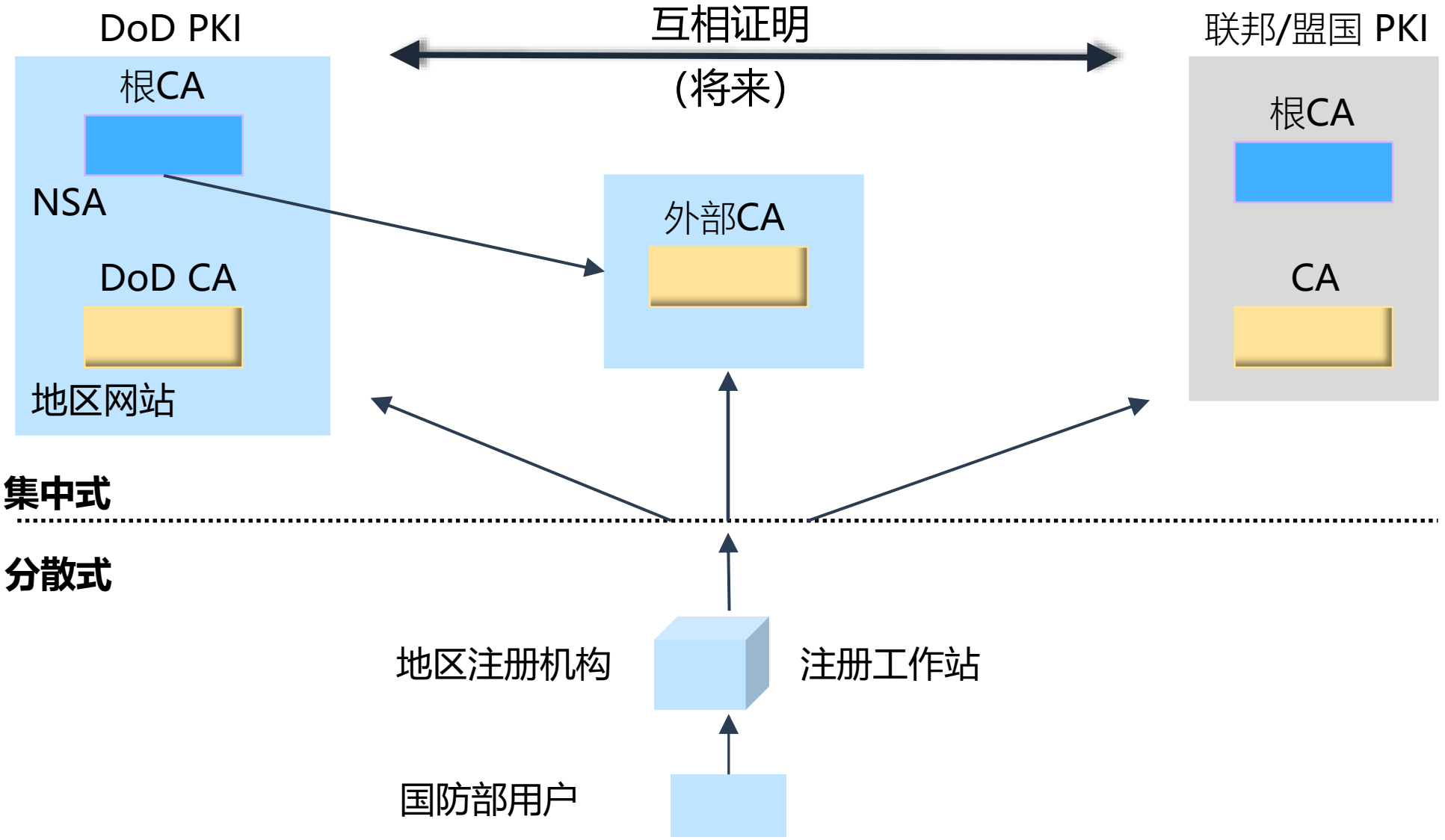
X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>

- B获得A的公开密钥

Z<<Y>>Y<<V>>V<<W>>W<<X>>X<<A>>



层次结构应用：美国防部PKI



层次模型的优缺点

优点

- 管理开销小
- 可扩展性好
- 与组织内部结构比较吻合
- 公共信任锚简化CA证书分发
- 实体到信任锚的路径固定

缺点

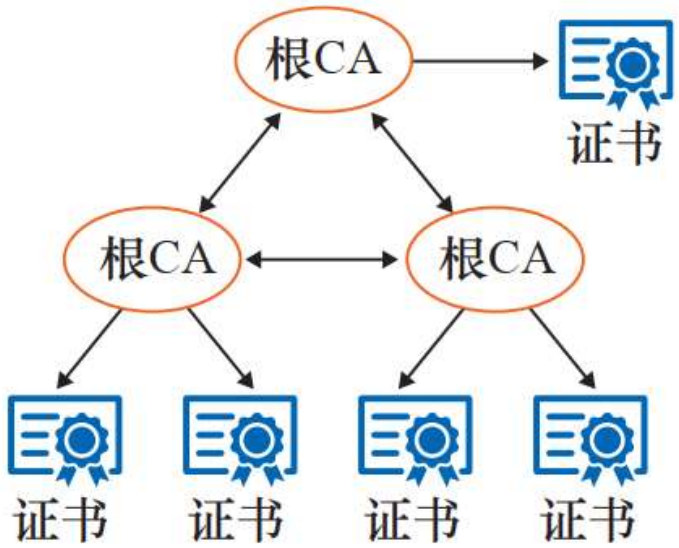
- 只存在一个根CA作为公共信任锚，世界范围内不可能只有单个根CA
- 商业和贸易等信任关系不必采用层次型结构
- 根CA私钥的泄露的后果非常严重

分布式信任模型

01 分布式信任模型是一种“对等模型”，建立信任的两个认证机构是对等关系

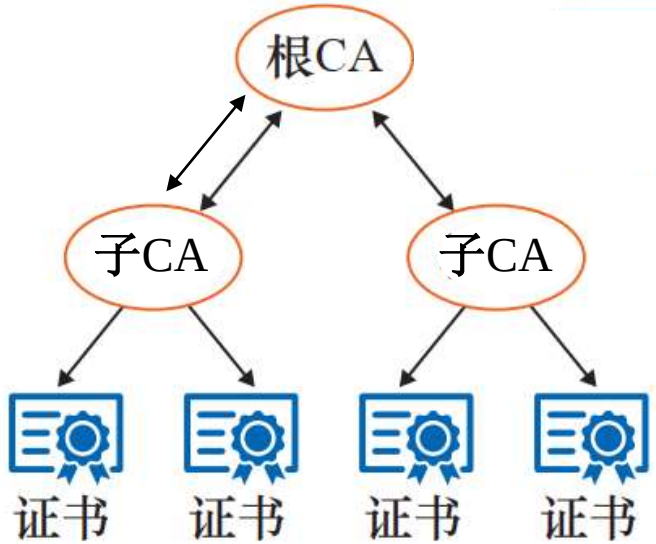
02 模型中CA间存在着交叉认证

03 信任锚分散到两个或更多根CA，单CA安全性削弱不会影响整个PKI

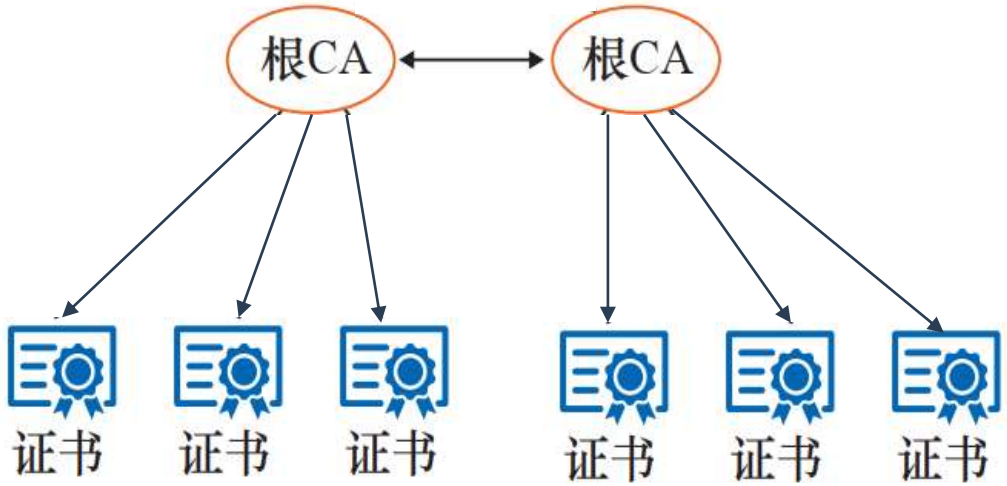


交叉认证

交叉认证：是一种将以前无关的CA连接在一起的机制，认证主体和颁发者都是CA，根据CA是否属于同一信任域，分为域内交叉认证和域间交叉认证



域内交叉认证



域间交叉认证

交叉认证

优点

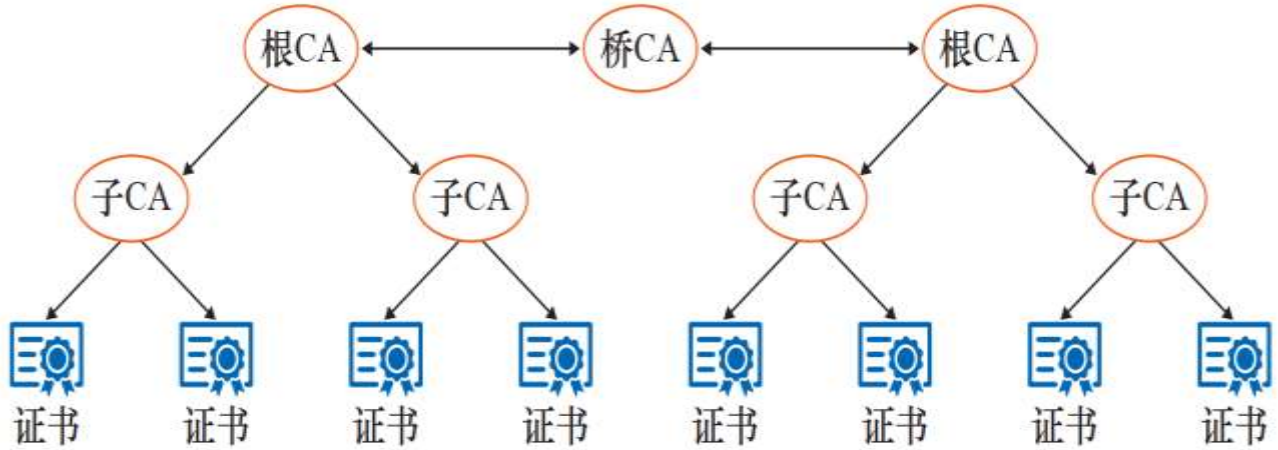
- 灵活，便于建立特殊信任关系，符合商贸中双边信任关系
- 合理，PKI用户至少要信任其证书颁发CA
- 高效，频繁通信的CA间直接认证，降低认证路径处理量
- 可靠，CA私钥泄露仅涉及到该CA的证书用户

缺点

- 认证路径搜索策略可能很复杂
- 用户仅提供单个认证路径不能保证PKI的所有用户能验证他的签名

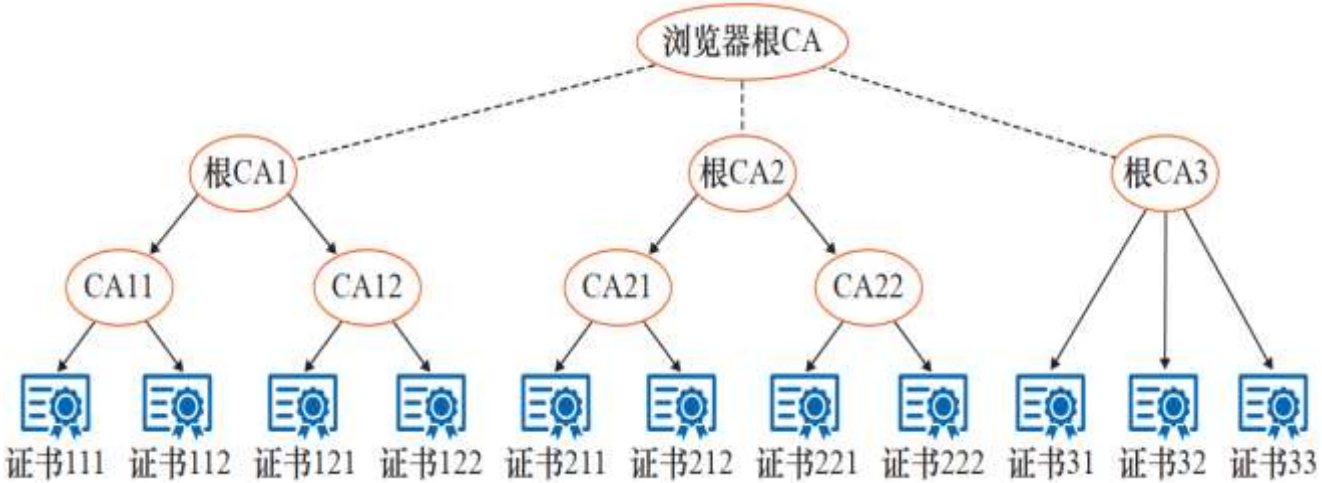
桥CA信任模型

- 中心辐射式信任模型
- 克服层次信任模型和分布式信任模型的缺点，连接不同的PKI系统

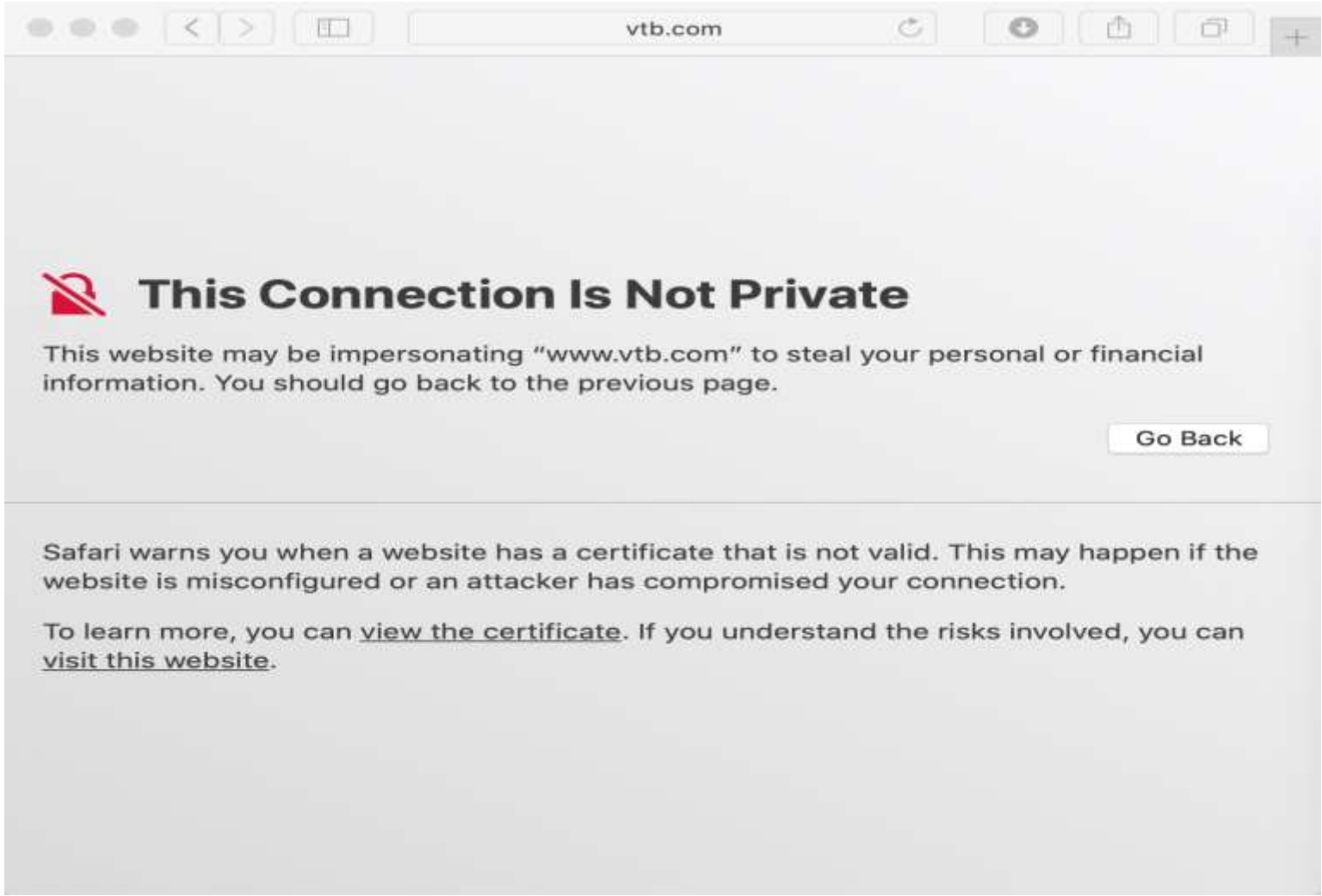


Web 信任模型

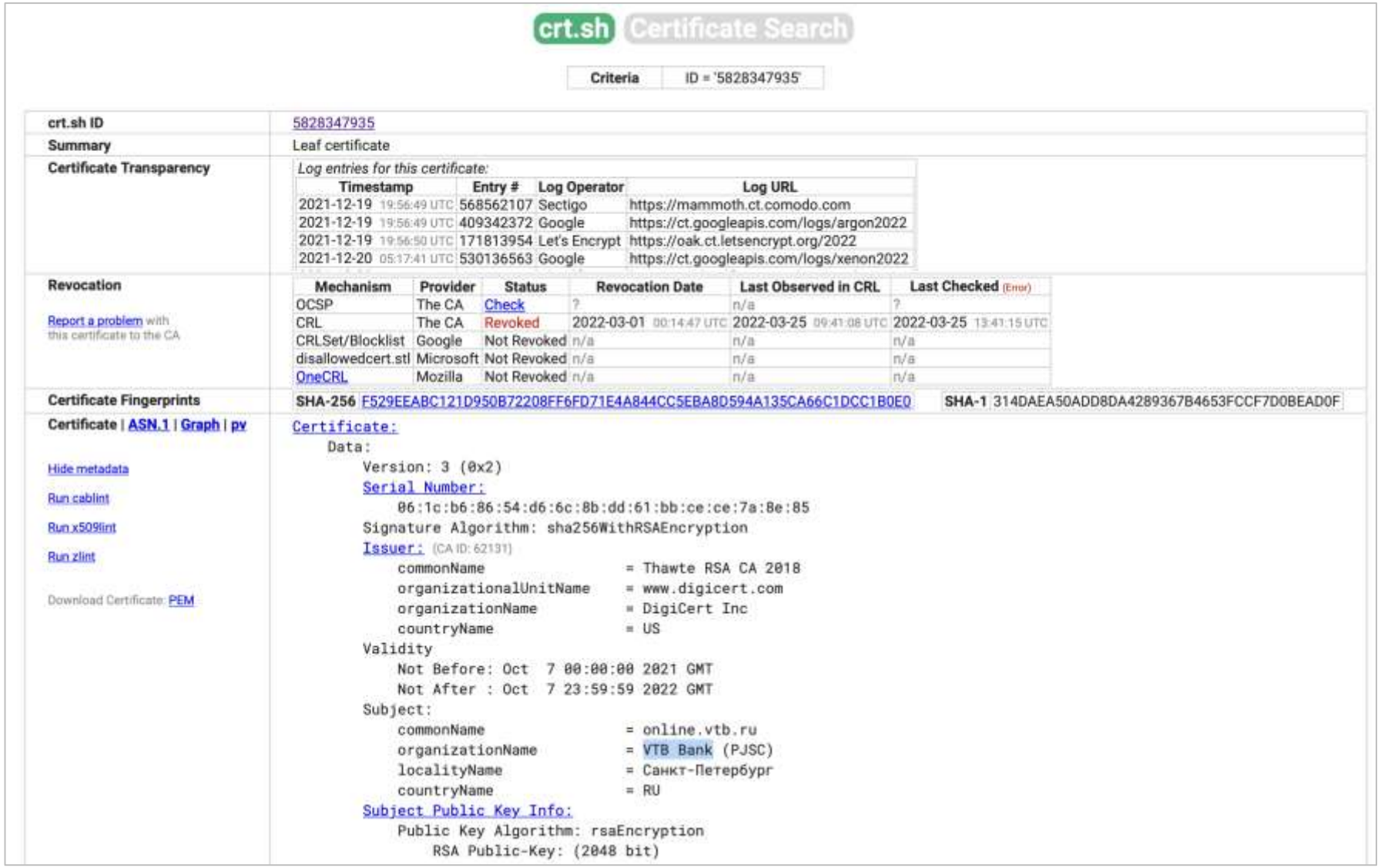
- Web信任模型构建在Web浏览器的基础上，浏览器中内置多个根CA
- 根CA间是平行的，浏览器用户同时信任多个根CA并把这些根CA作为自己的信任锚



Web 信任实例：俄罗斯外贸银行证书 (1)



Web 信任实例：俄罗斯外贸银行证书 (2)



crt.sh Certificate Search

Criteria: ID = '5828347935'

crt.sh ID	5828347935
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2021-12-19 19:56:49 UTC	568562107	Sectigo	https://mammoth.ct.comodo.com
2021-12-19 19:56:49 UTC	409342372	Google	https://ct.googleapis.com/logs/argon2022
2021-12-19 19:56:50 UTC	171813954	Let's Encrypt	https://oak.ct.letsencrypt.org/2022
2021-12-20 05:17:41 UTC	530136563	Google	https://ct.googleapis.com/logs/xenon2022

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Revoked	2022-03-01 00:14:47 UTC	2022-03-25 09:41:08 UTC	2022-03-25 13:41:15 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256 F529EEABC121D950B72208FF6FD71E4A844CC5EBA8D594A135CA66C1DCC1B0E0

SHA-1 314DAEA50ADD8DA4289367B4653FCCF7D0BEAD0F

Certificate | ASN.1 | Graph | pv

Hide metadata

Run cablint

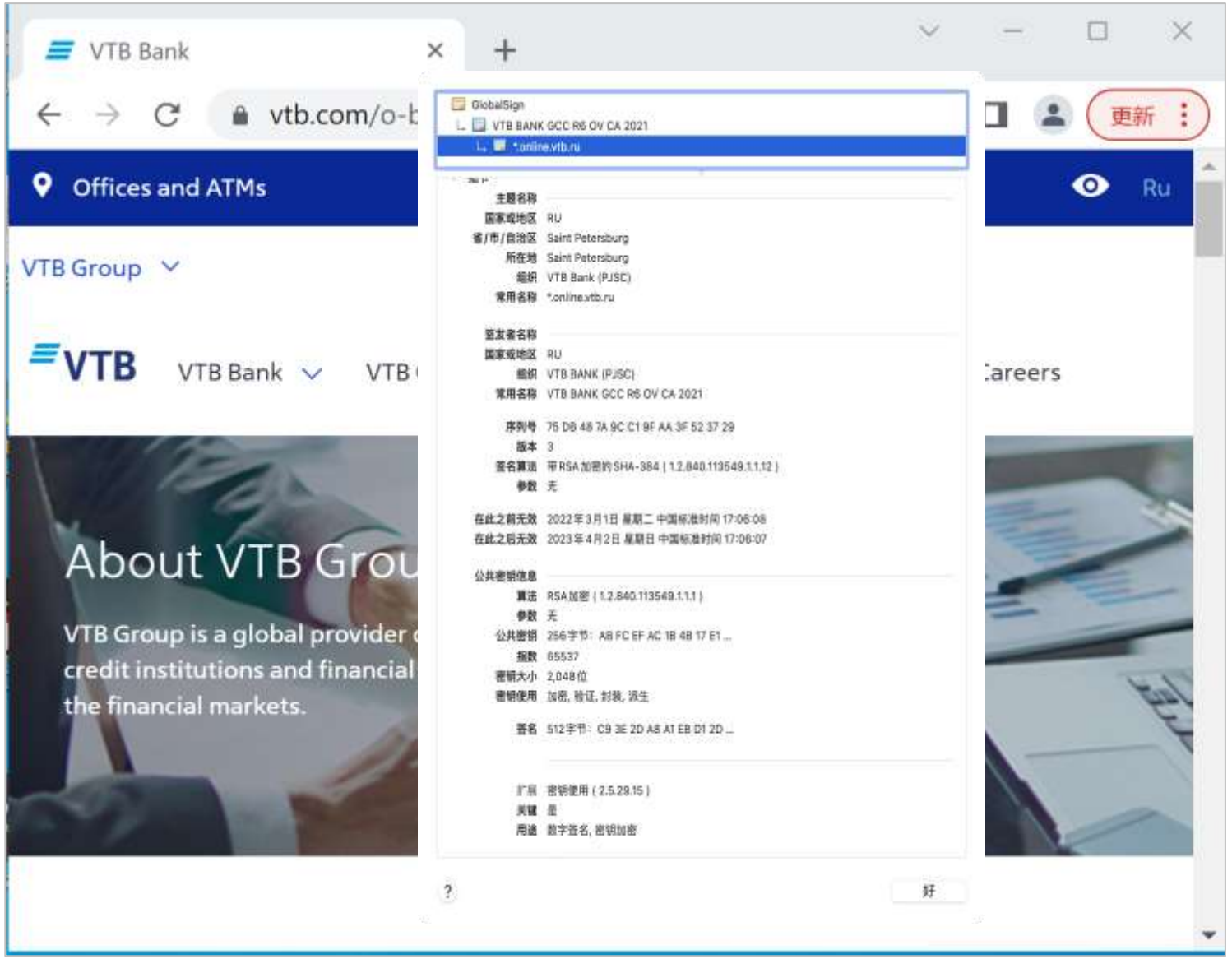
Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            06:1c:b6:86:54:d6:6c:8b:dd:61:bb:ce:ce:7a:8e:85
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 62131)
            commonName               = Thawte RSA CA 2018
            organizationalUnitName   = www.digicert.com
            organizationName         = DigiCert Inc
            countryName              = US
        Validity
            Not Before: Oct  7 00:00:00 2021 GMT
            Not After : Oct  7 23:59:59 2022 GMT
        Subject:
            commonName               = online.vtb.ru
            organizationName         = VTB Bank (PJSC)
            localityName             = Санкт-Петербург
            countryName              = RU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

Web 信任实例：俄罗斯外贸银行证书 (3)



Web 信任模型

实现方式

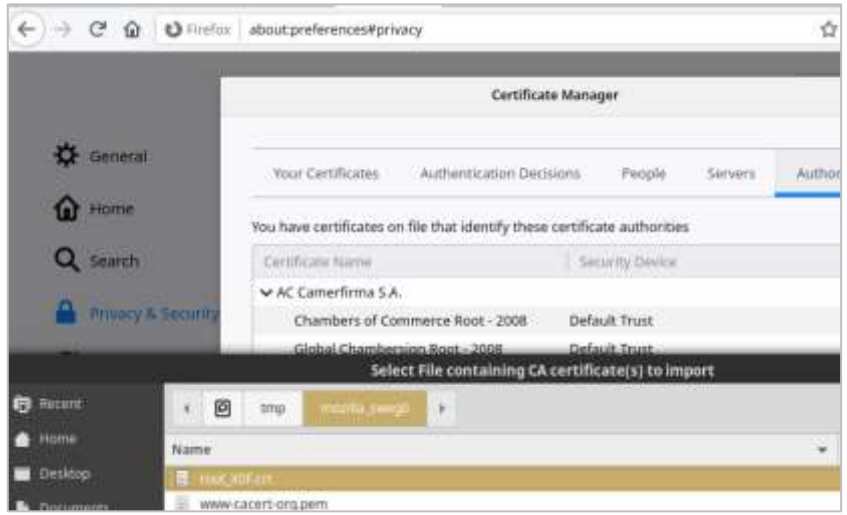
Web信任模型通过与相关域进行互连而不是扩大现有的主体群来使用户实体成为在浏览器中所给出的所有域的依托方

模型特点

具有分布式信任结构模型的特点，但根本上更类似于认证机构的严格层次结构模型

认证形式

浏览器厂商起到了根CA的作用，而与被嵌入的密钥相对应的CA就是它所认证的CA

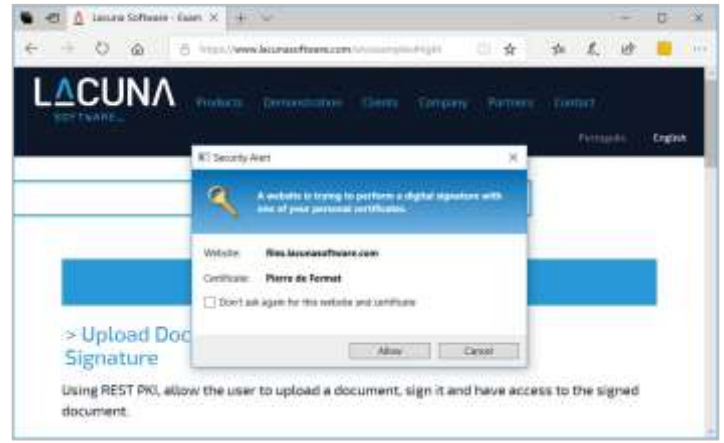


Web 信任模型的安全隐患

01

预装公钥信任问题

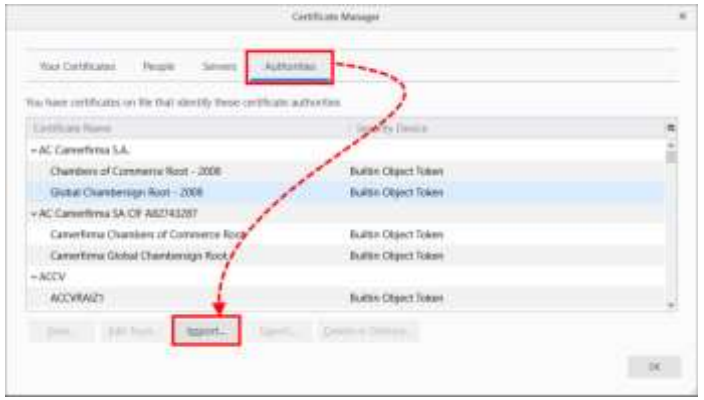
用户自动地信任预装公钥，即使这些 CA 中有一个是从没有认真核实被认证的实体，这时安全性将被完全破坏



02

缺乏根密钥撤销机制

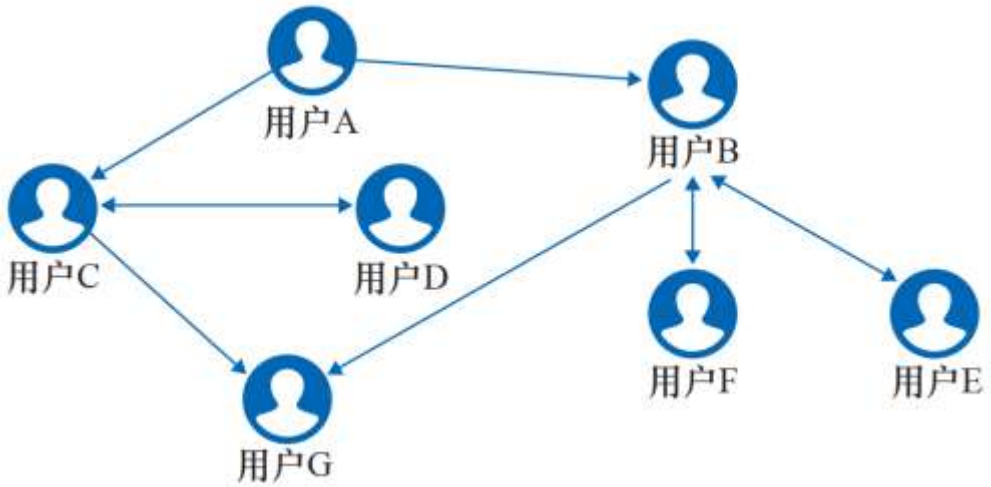
没有实用的机制来撤销嵌入到浏览器中的根密钥



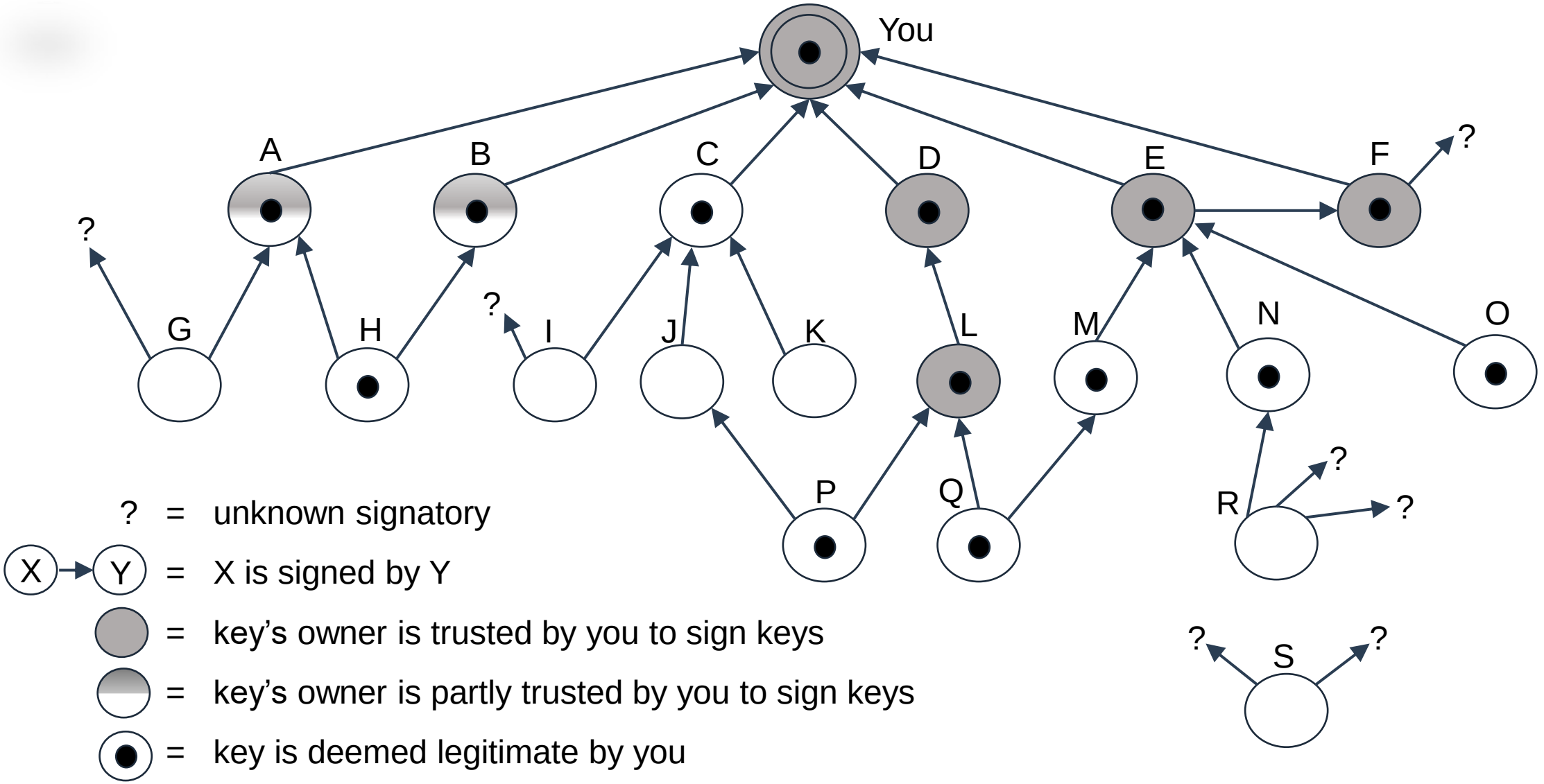
以用户为中心的信任模型--PGP

由每个用户自己决定信任哪些证书

- Pretty Good Privacy (PGP) 中，用户通过担当CA（签署其他实体的公钥）和使其公钥被其他人认证建立 “信任网（Web of Trust)
- 当 A 收到一个属于 B 的证书时，发现这个证书由不认识的 D 签署的，但是 D 的证书是由 A 认识且信任的 C 签署，于是 A 决定信任 B 的密钥，也可决定不接受 B 的密钥



以用户为中心的信任模型--PGP



PGP实例，用户决定是否采信

第2节 PKI安全问题的由来

- 数字证书颁发过程中的安全问题
- 数字证书维护过程中的安全问题

PKI安全问题

数字证书颁发过程中的安全问题

- 误发证书
- 恶意颁发证书
- 钓鱼网站证书

数字证书维护过程中的安全问题

- 证书过期
- 证书撤销

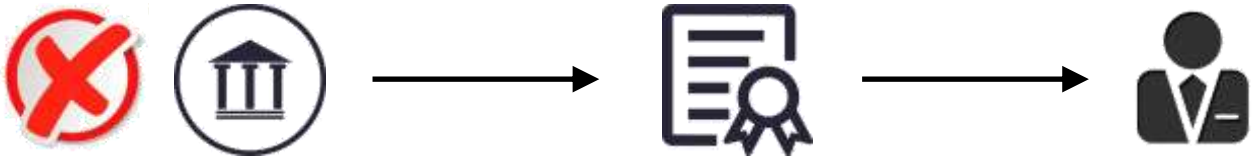
数字证书颁发过程中的安全问题

证书的合法性难以保证

误发证书

恶意颁发证书

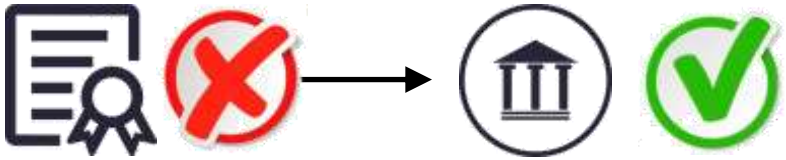
钓鱼网站证书



数字证书维护过程中的安全问题

证书的有效性难以验证

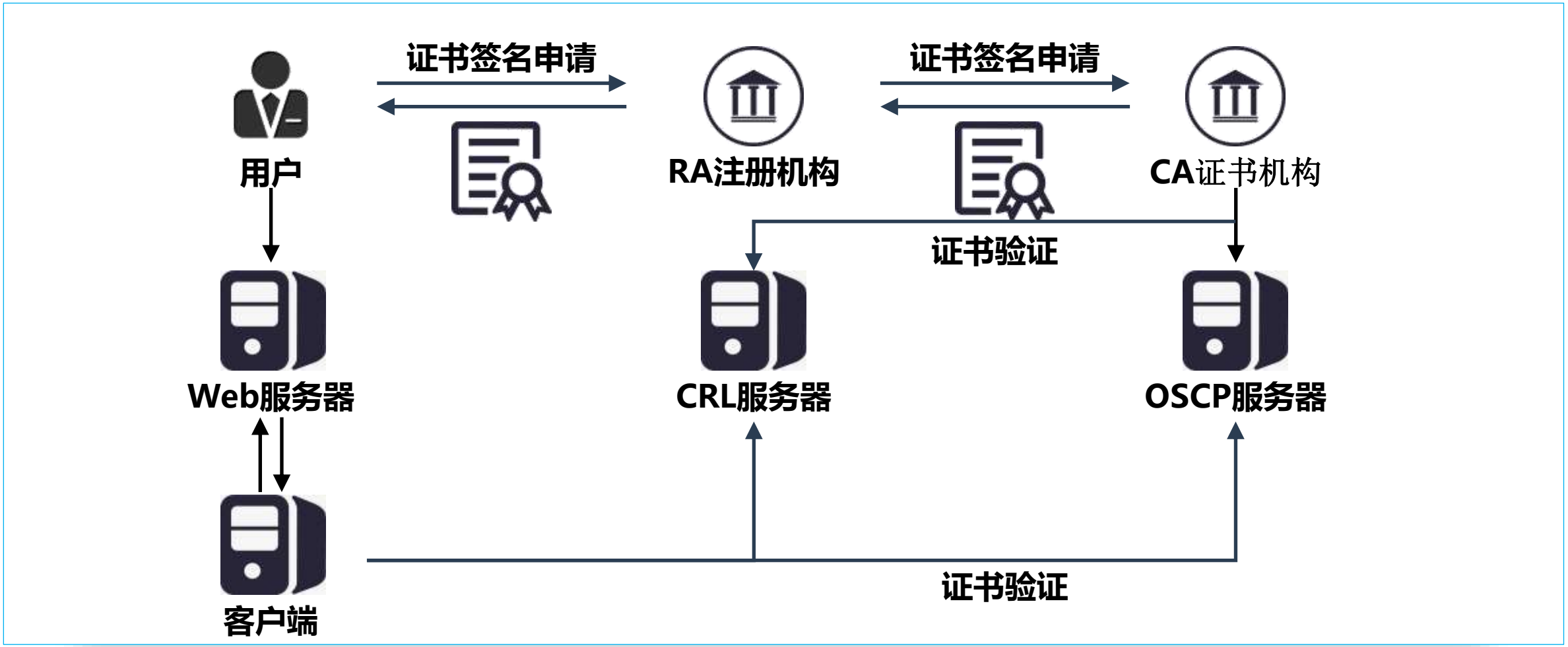
证书过期



证书撤销

数字证书维护过程中的安全问题

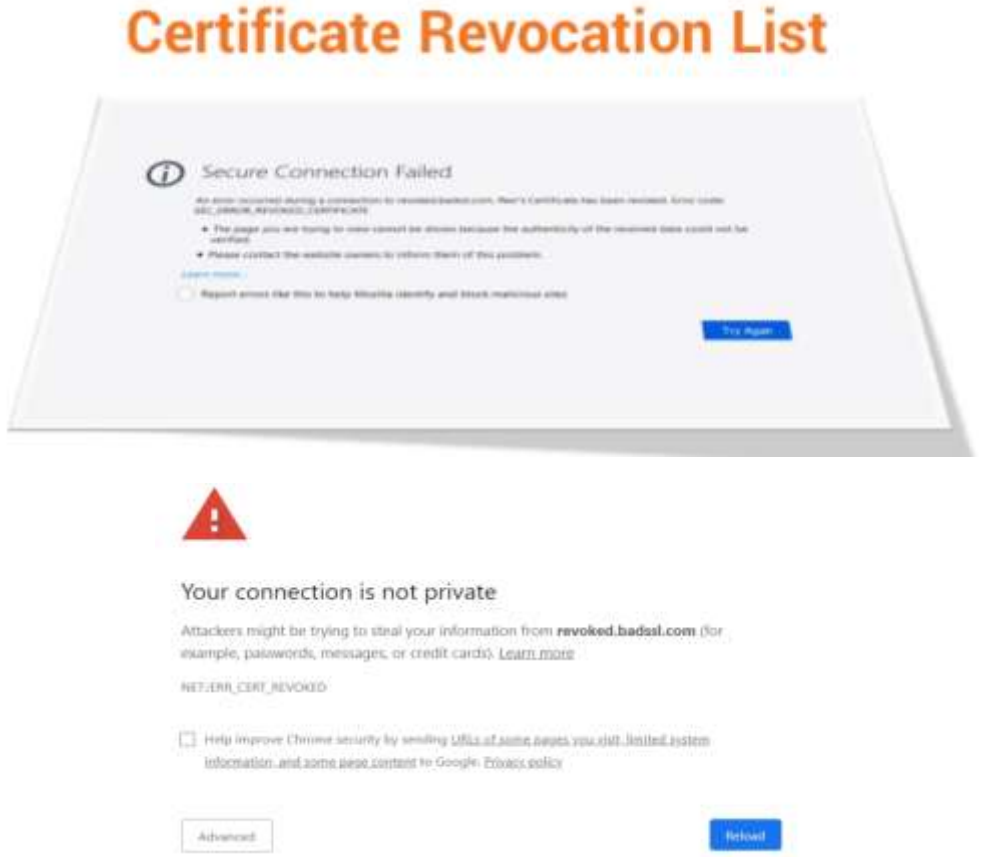
PKI证书生命周期



数字证书维护过程中的安全问题

PKI证书撤销

- 私钥泄露、密钥更换、用户变化时，需要撤销证书
- CA 维 护 CRL （ Certificate Revocation List），未到期但已撤销证书列表
- 检查CRL的URL内嵌在用户证书，浏览器安全访问URL查询证书状态，确定是否被CA撤销
- 在 线 证 书 状 态 协 议 OCSP (online certificate status protocol)是CRL之外维护PKI证书安全的另一个协议



数字证书维护过程中的安全问题

中心化监管带来的问题

- 证书的所有操作权利均归CA所有，在CA受到攻击后会带来严重的安全威胁
- 中心化监管导致PKI面临中心节点的安全脆弱性和信任链失效

真实案例

2011年7月, 荷兰著名CA DigiNotar的8台服务器被黑客攻破，至少531个虚假证书被发布，波及荷兰金融、科技、制造等各个行业，影响巨大

DigiNotar® A VASCO COMPANY

Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

第3节 PKI安全问题的解决思路

- 建立监督机制
- 建立证书状态日志

PKI安全问题解决思路

监督机制

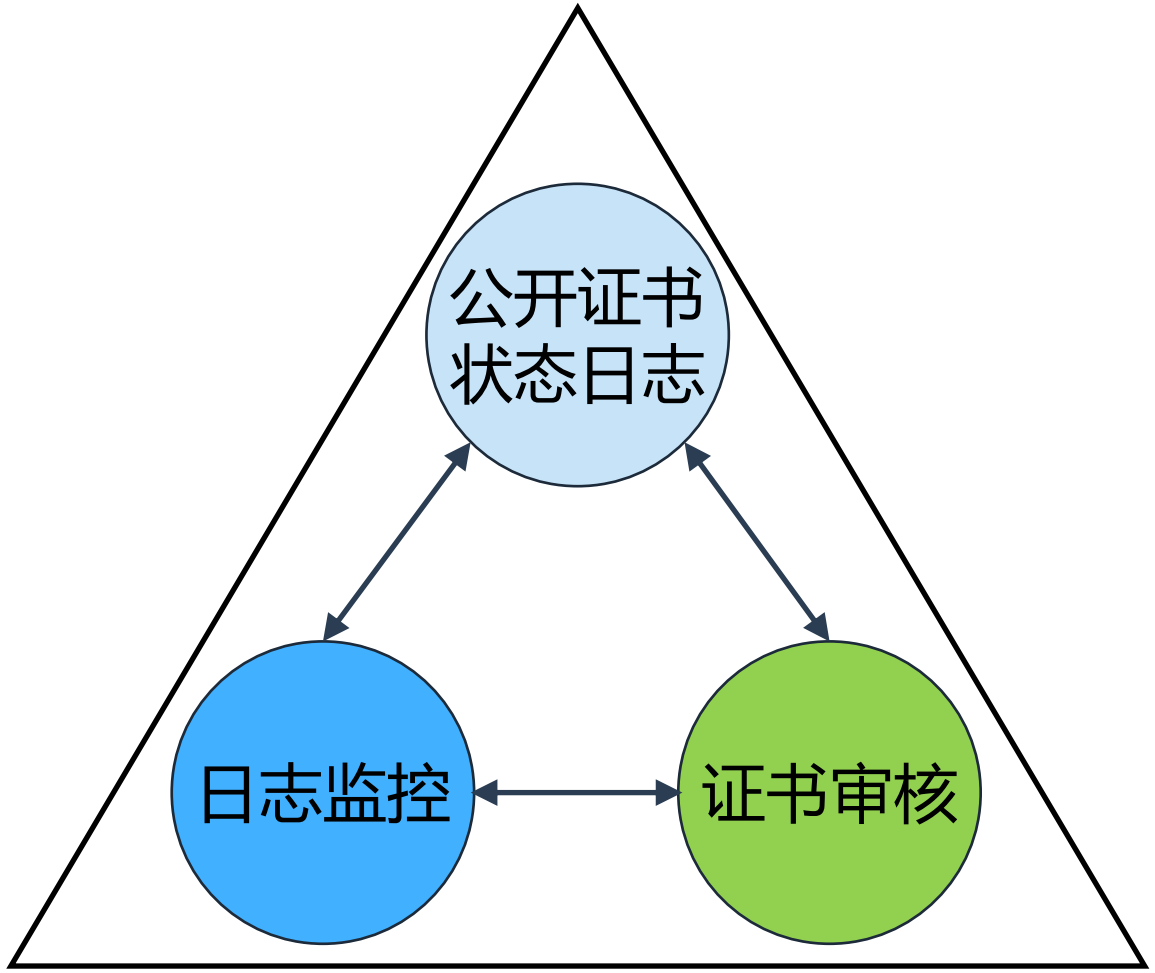
- 证书透明机制
- 经济激励机制

建立证书状态日志

- 证书撤销列表
- 在线证书状态
- 证书区块链

建立监督机制

证书透明机制（Certificate Transparency，CT）



- 利用公开的证书状态日志来记录证书签发，撤销情况
- CT服务器存储所有注册证书供第三方审计
- 解决证书合法性、有效性验证问题
- 容灾性较差，主要用于事后检测，提供追责证据

建立监督机制

经济激励机制

监督CA恶意证书的发布，检测者检查并上报，成功发现后扣除CA保证金奖励检测者/赔偿受害用户

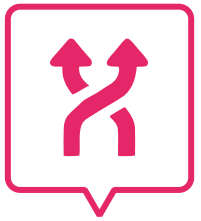
建立证书状态日志

证书撤销列表

每个CA维护一个证书撤销列表（Certificate Revocation List，CRL）记录被撤销证书

在线证书状态

用户通过CA指定在线证书状态服务器来查询证书的撤销状态信息

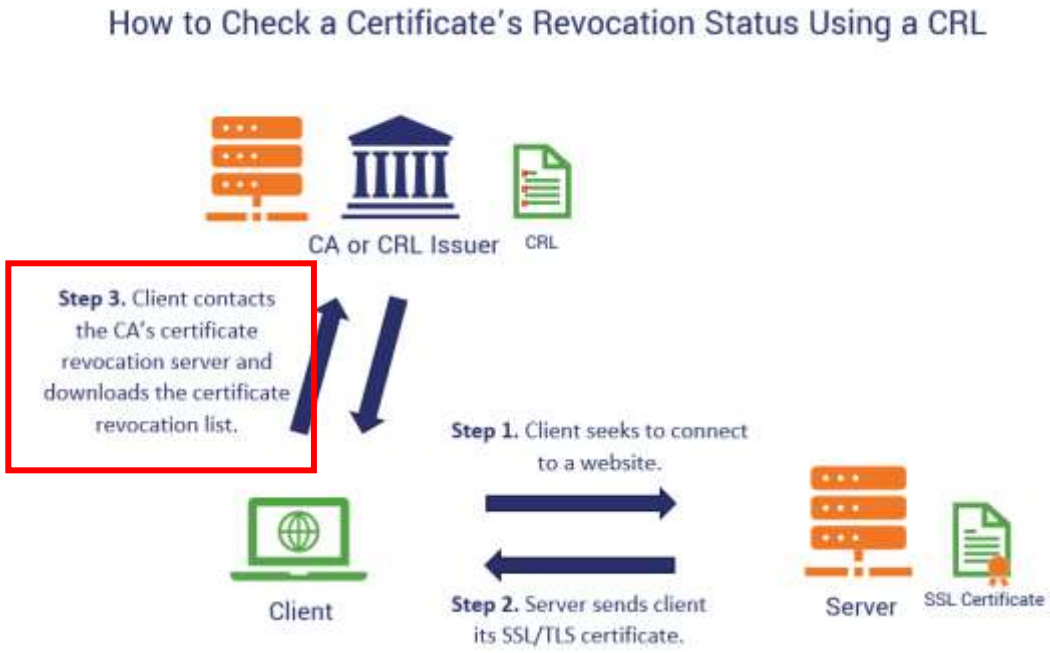


证书区块链

基于区块链记录证书的操作记录，维护最新的证书状态信息

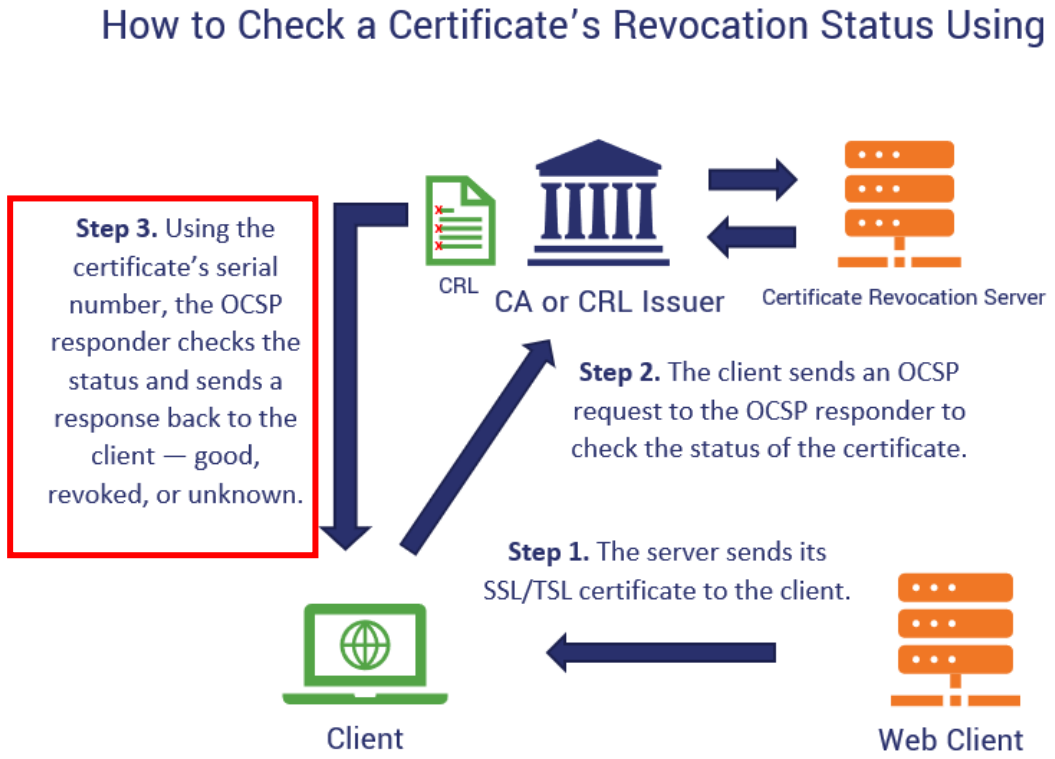
证书撤销列表

- 由CA 维护，包含被撤销的证书序列号和吊销时间
- 浏览器定期下载CRL列表用于校验证书是否已被撤销
- CRL会越来越大，查询检验效率低
- CRL实时性较差，证书被吊销后，服务器在更新 CRL 前依然信任证书



在线证书状态

- 在线证书状态协议（Online Certificate Status Protocol，OCSP），通过建立一个可实时响应的机制，CA服务器实时响应验证证书
- OCSP要求浏览器直接请求第三方CA以确认证书的有效性，因此会损害隐私
- 客户端会在SSL中实时查询OCSP接口，获得查询结果前阻塞后续流程，降低HTTPS性能



使用区块链技术

利用去中心化技术，实现资源的可信保障，避免中心化带来的安全隐患，保证基础设施的安全可信

系统安全性强

单一节点受到攻击不影响其他节点工作，不危害系统安全，扛外部攻击能力强

信息可信性高

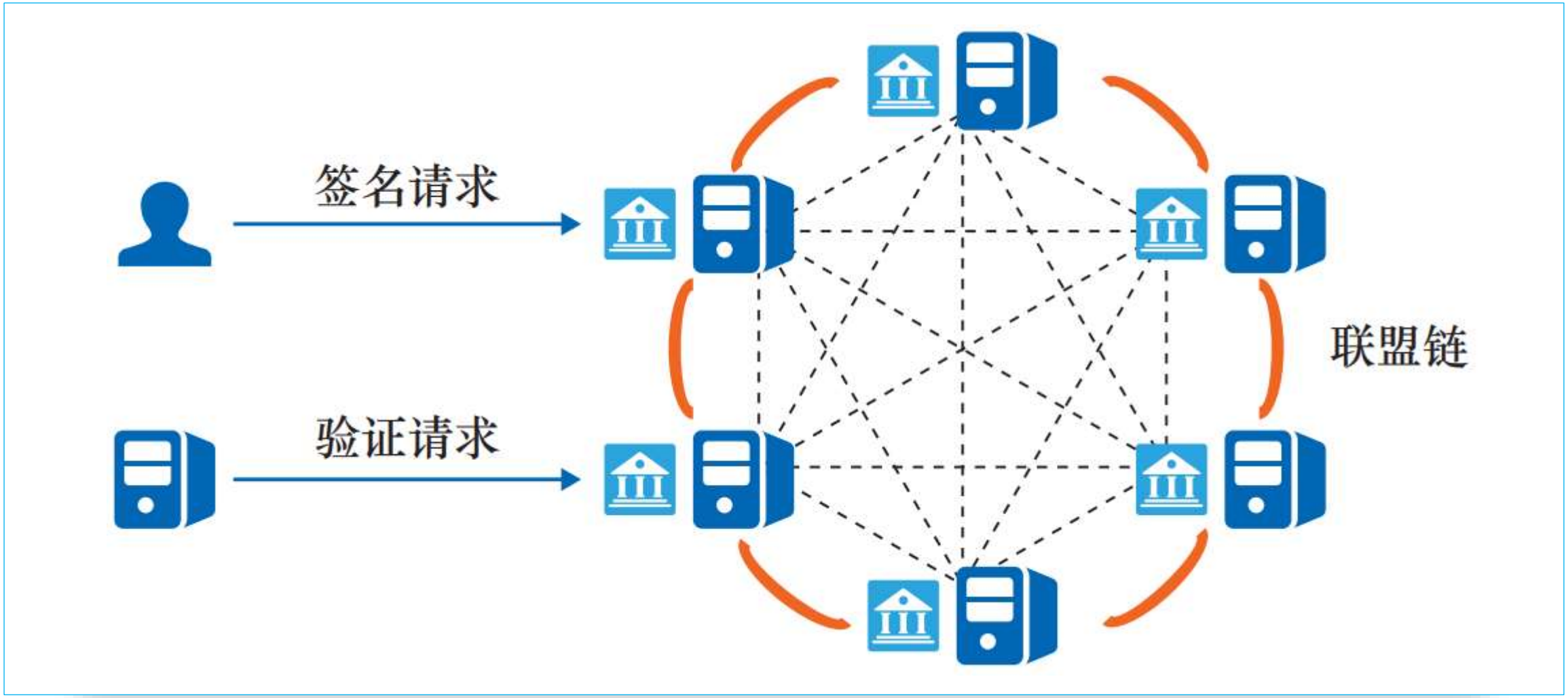
分布式信任模型通过P2P形式的节点间交叉认证，避免内部节点恶意行为

权力公平性好

与中心化监管相比，无权力层级结构，节点间关系对等，避免权力滥用与垄断效应

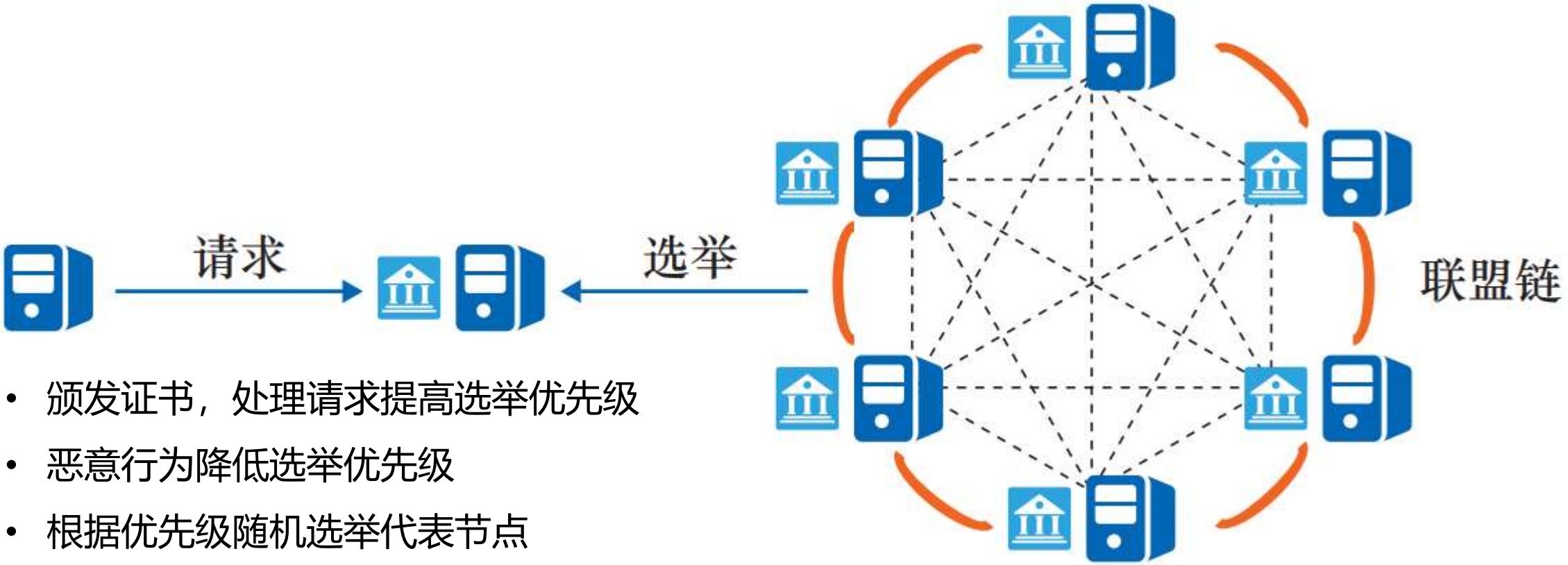
使用区块链技术

证书区块链



使用区块链技术

共识与激励机制

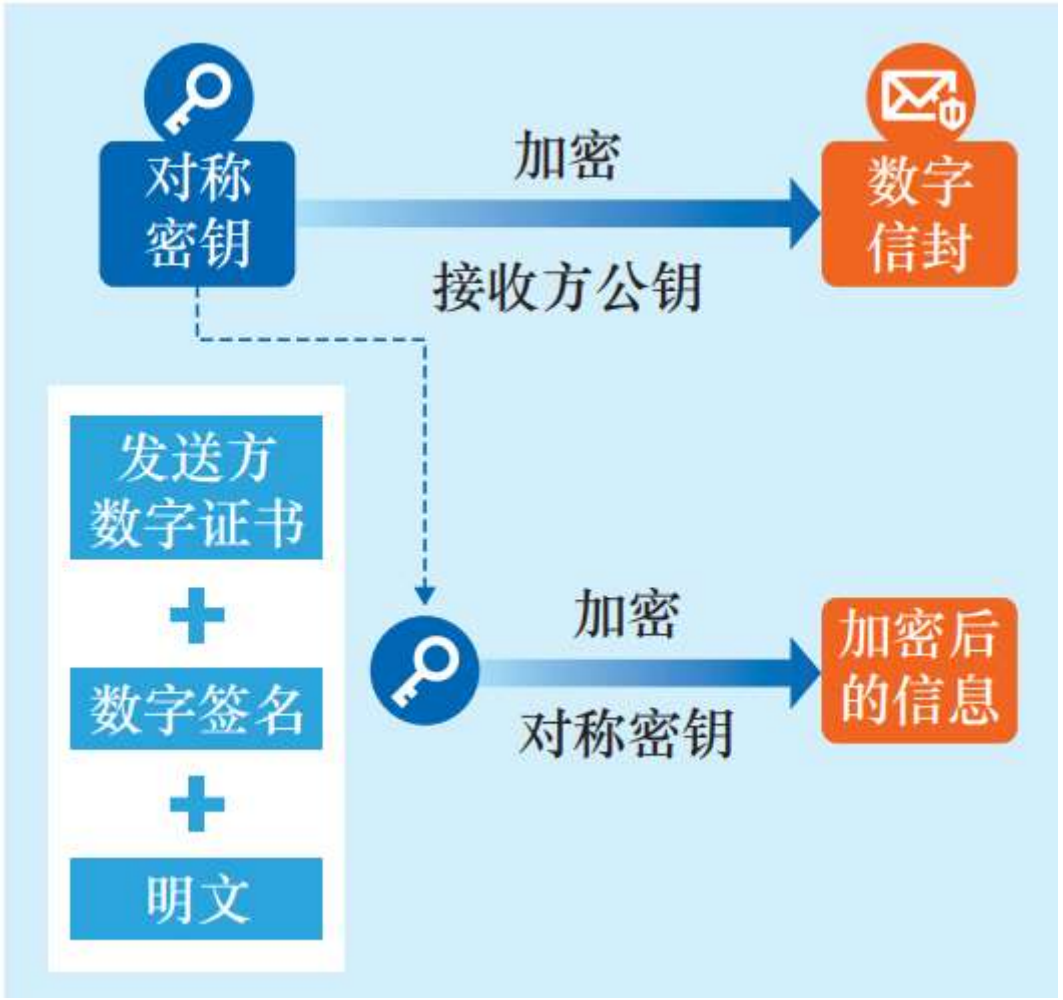


- 颁发证书，处理请求提高选举优先级
- 恶意行为降低选举优先级
- 根据优先级随机选举代表节点
- 代表节点处理请求，获取经济激励

第4节 PKI主要应用场景

- 加密数据传输
- HTTPS协议
- VPN
- RPKI

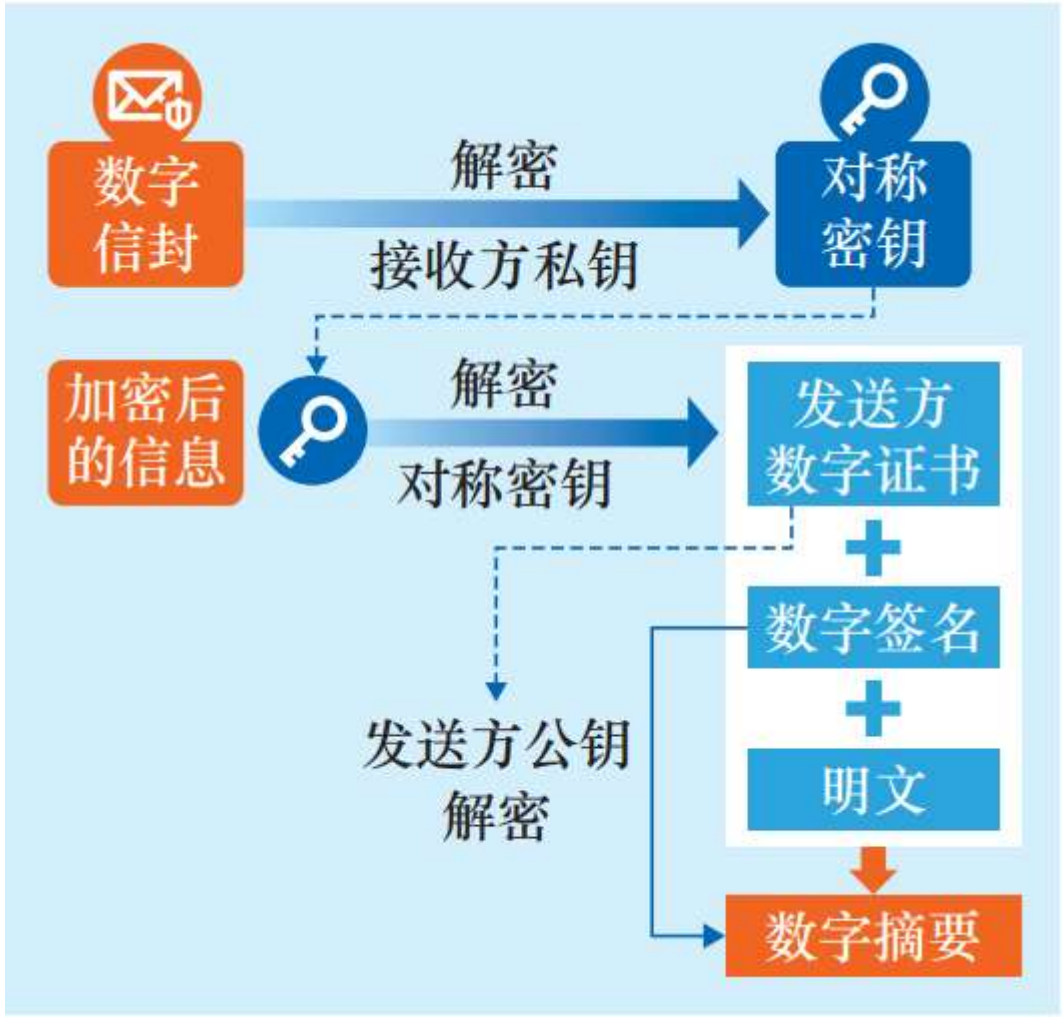
数字证书使用-发送方



数据加密传输

- 发送方产生对称密钥
- 使用对称密钥加密敏感数据
- 发送方使用接收方的公钥加密对称密钥

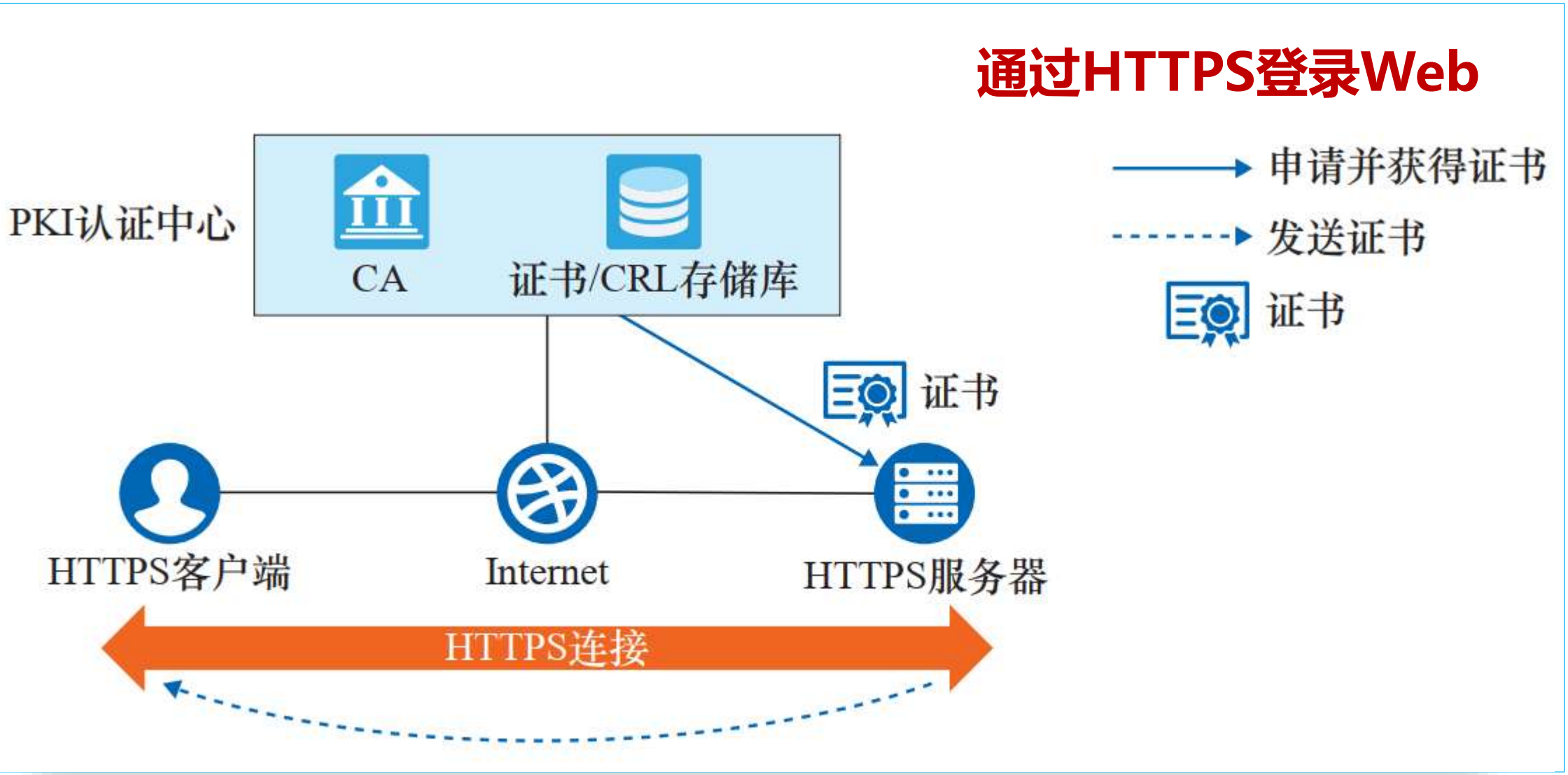
数字证书使用-接受方



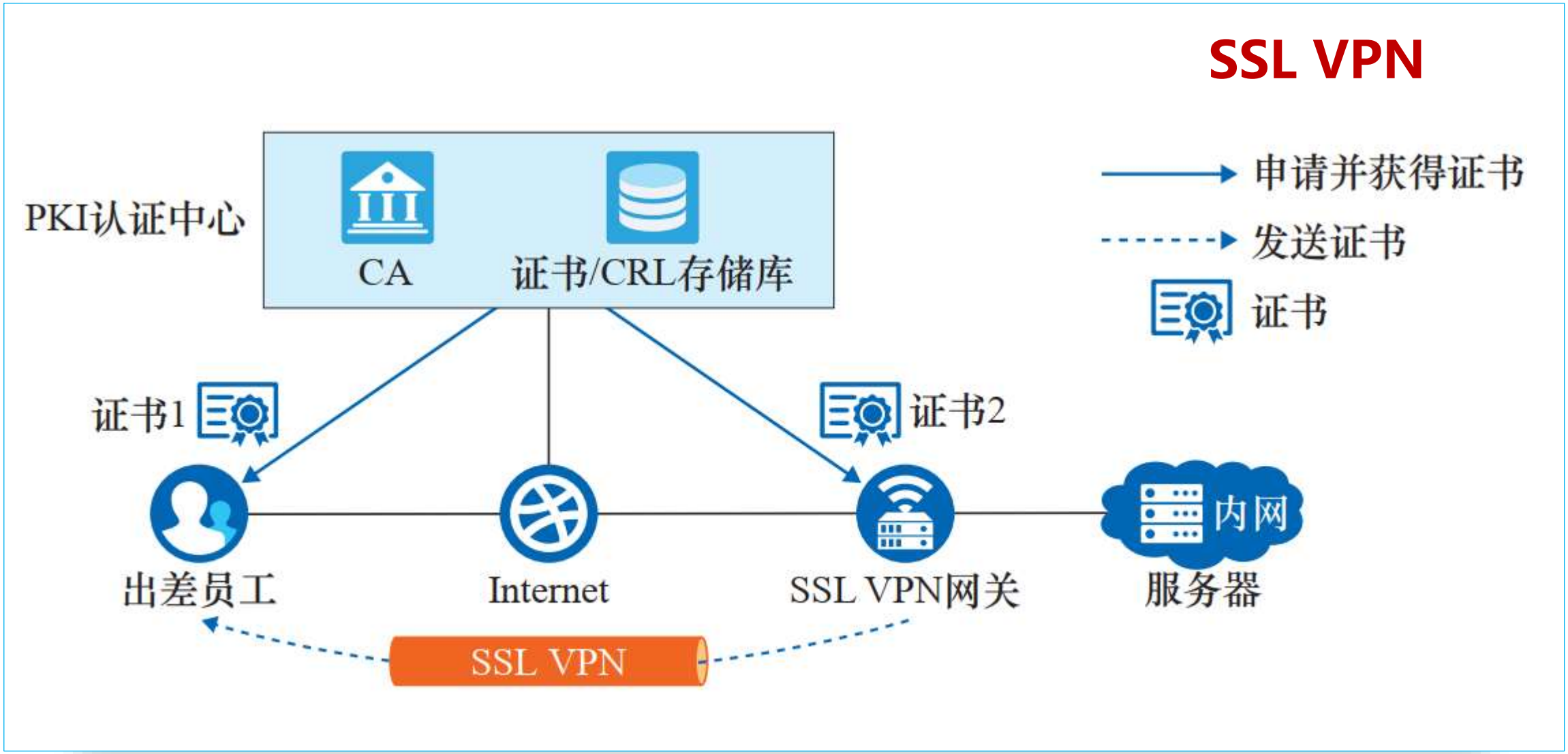
数据加密传输

- 接受方使用私钥拆开“数字信封”
- 使用得到的对称密钥解密敏感数据
- 使用发送方公钥验证数字签名

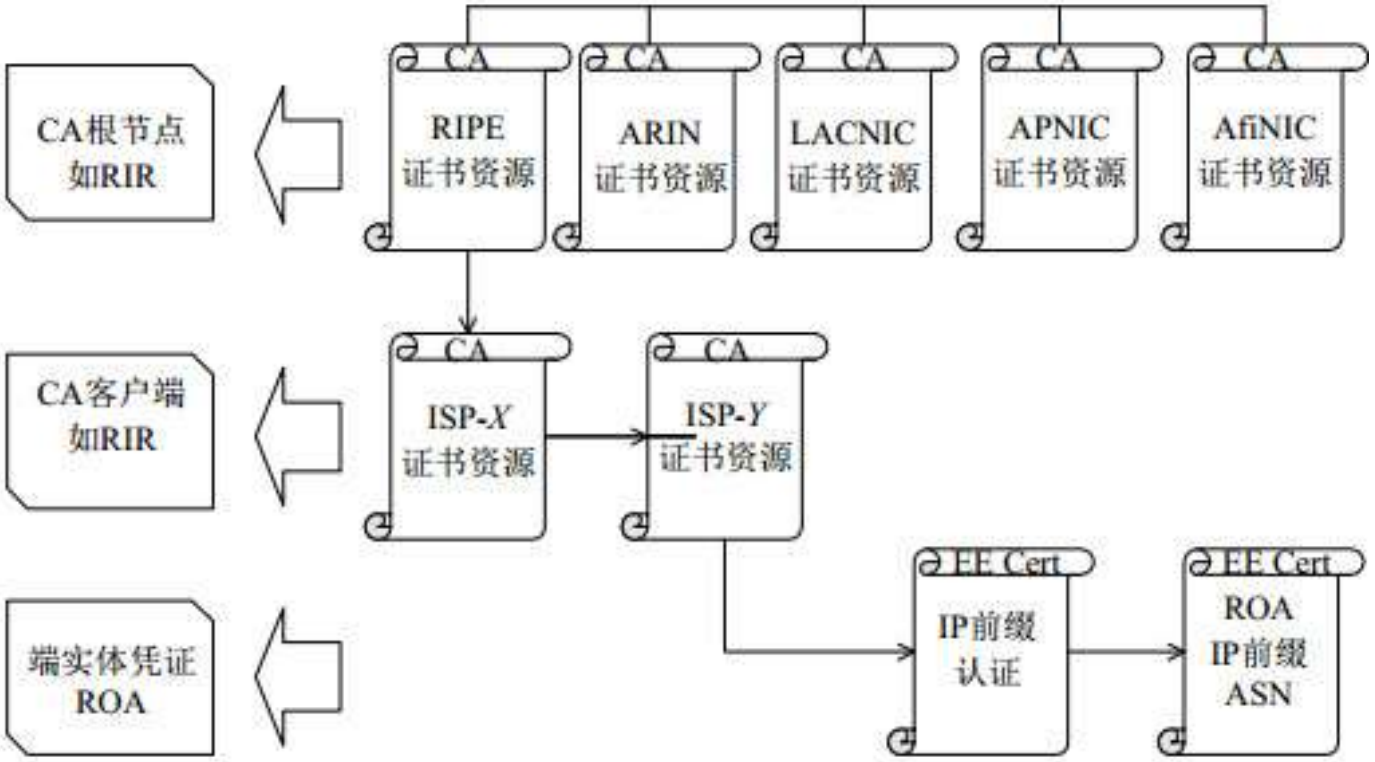
数字证书应用场景- HTTPS



数字证书应用场景- SSL VPN



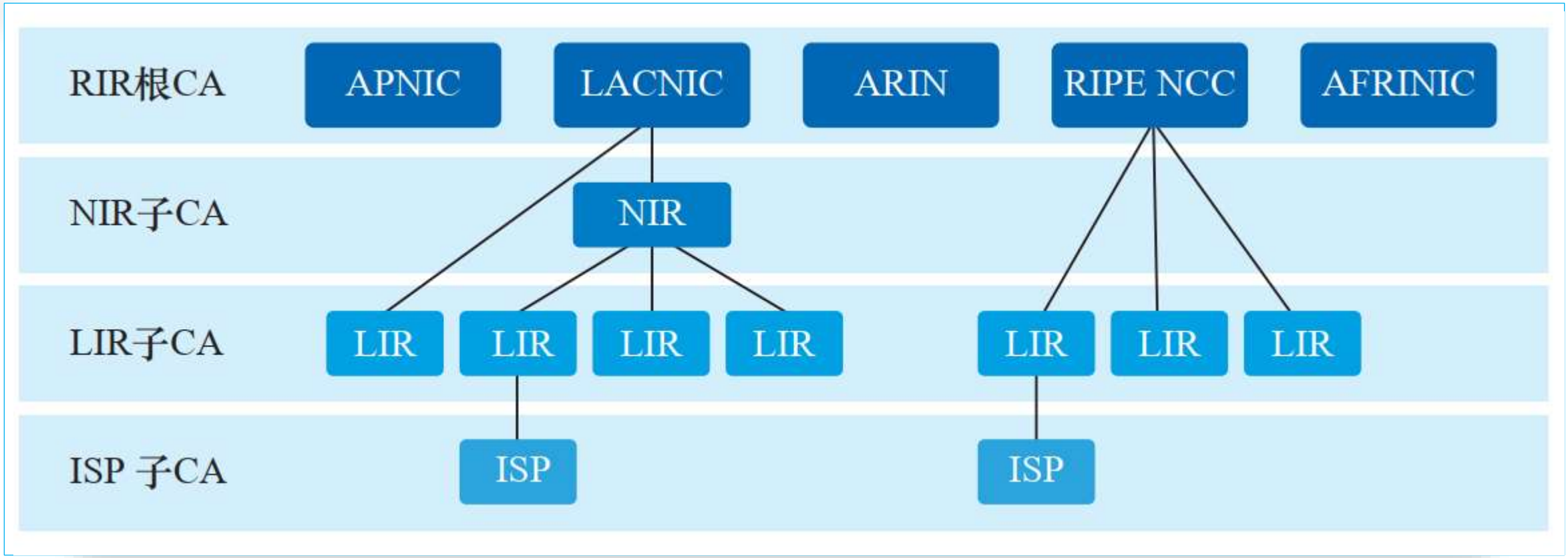
数字证书应用场景- RPKI



RPKI

- 路由源认证(Route Origin Authorization，ROA)将IP前缀和路由源AS ASN绑定
- 5个RIR作为根信任证书颁发机构CA，形成从根CA到某AS或ISP的信任链
- CA负责签发包含IP地址块和ASN的数字证书
- 终端实体传递中转IP地址块间授权

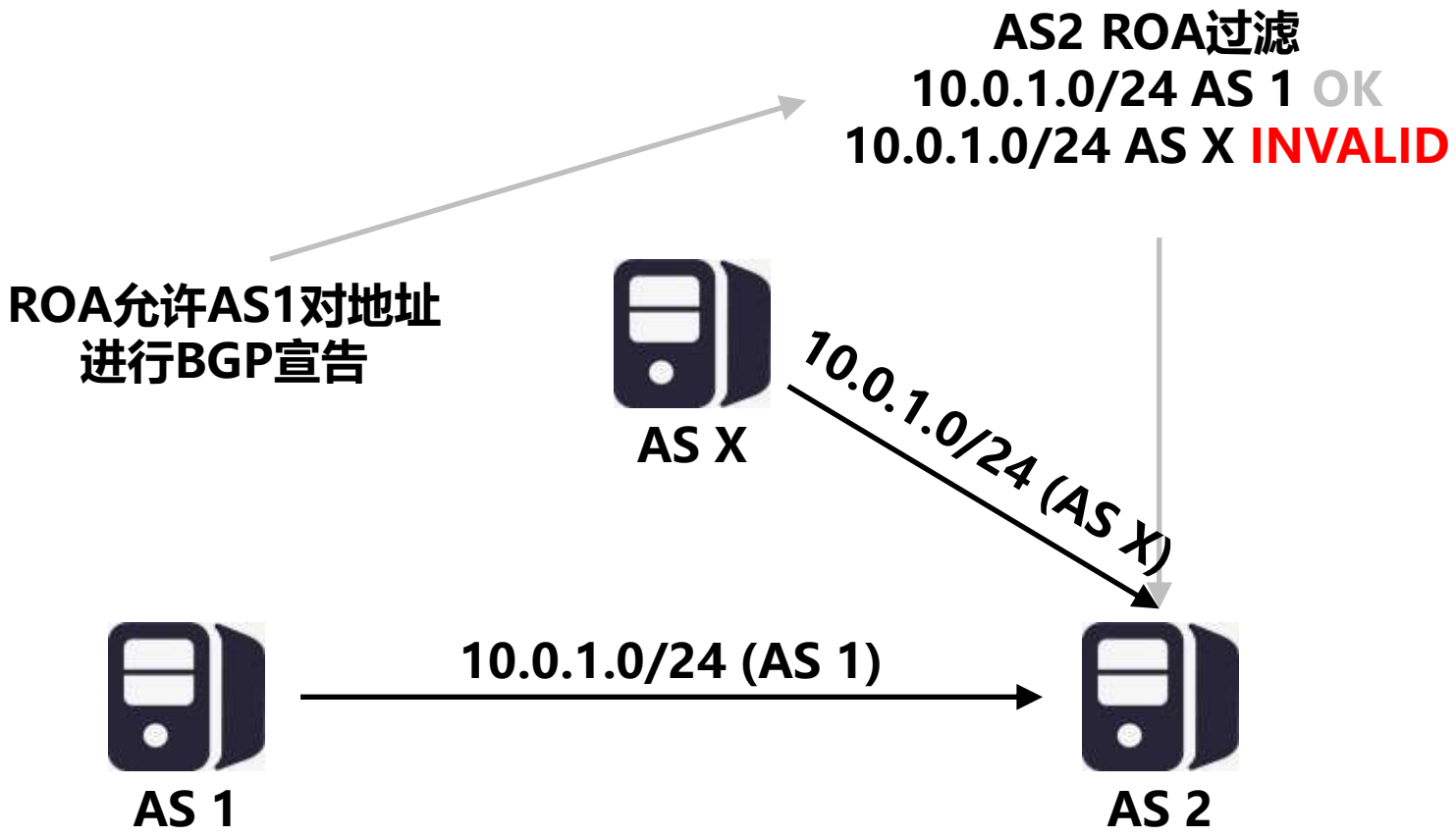
数字证书应用场景- RPKI



RPKI层级结构

- 提供基于RC证书的验证能力
- 使用RC证明地址所有权
- RC严格依赖于地址分配过程

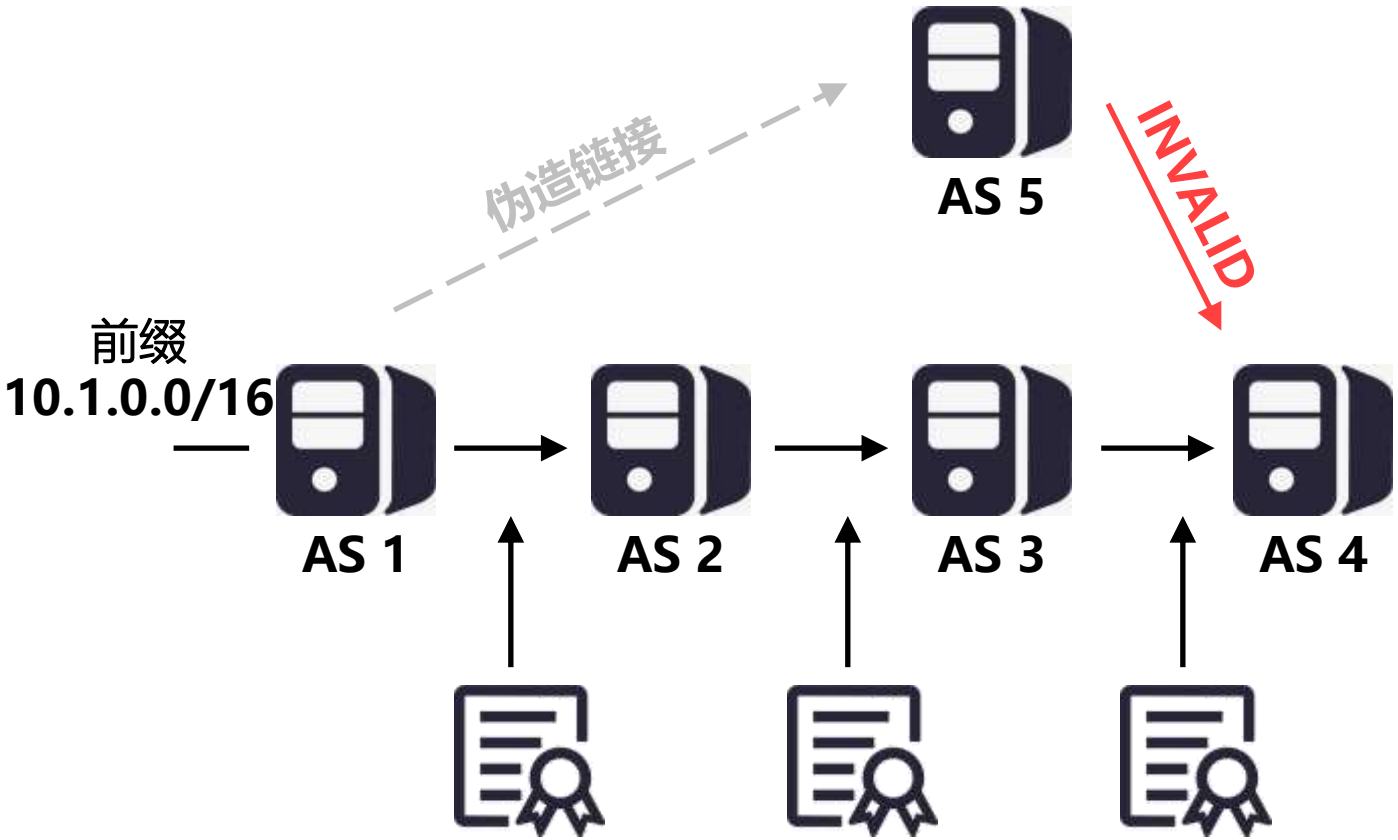
数字证书应用场景- RPKI



BGP源验证

- 根据RC证书链来验证ROA合法性
- 通过ROA来验证BGP宣告的合法性

数字证书应用场景- RPKI



BGP路径验证

- 通过RC证书链来验证签名公钥的合法性
- 逐个AS对路径信息进行签名

第5节 总结和展望

公钥基础设施安全

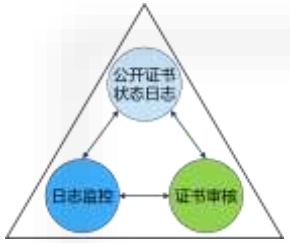
你认为 公钥基础设施本身是否存在安全问题?

数字证书颁发过程中的安全问题

- 误发证书
- 恶意颁发证书
- 钓鱼网站证书

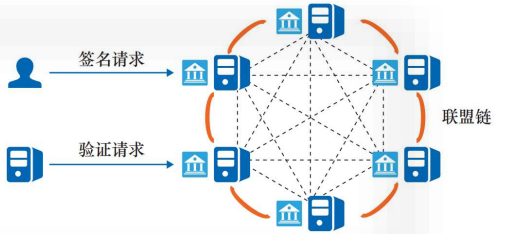
数字证书维护过程中的安全问题

- 证书过期
- 证书撤销



监督机制、证书状态日志及区块链等技术

可以提升公钥基础设施自身的安全能力



总结

介绍了什么是PKI，如何构建安全的PKI，总结了PKI的主要应用场景，探讨了如何利用PKI提升网络空间安全能力

第一节
PKI概述

- 数字证书
- PKI组成体系结构
- CA的信任关系

解决网上身份认证、信息完整性和不可抵赖性等安全问题

第二节
PKI安全问题的由来

- 数字证书颁发过程中的安全问题
- 数字证书维护过程中的问题

数字证书颁发与维护存在安全隐患

第三节
PKI安全问题的解决思路

- 建立监督机制
- 建立证书状态日志

颁发过程可监督
维护过程可追溯

第四节
PKI主要应用场景

- 加密数据传输
- HTTPS协议
- VPN
- RPKI

按不同安全需求提供安全服务

展望

PKI 为互联网提供了经由“官方”验证对方身份的机制

但证书颁发与维护过程存在影响PKI真实可信度的风险

How Will Blockchain Affect PKI?

- 互联网的安全离不开PKI建设， PKI建设也需要考虑自身安全问题，为互联网用户提供可靠的信任基础
- 区块链等去中心化技术为PKI安全注入新动力