走进PKI的神秘世界

PKI培训小组（吴凡、马超、闫雪娟）

课程目标

CFCA

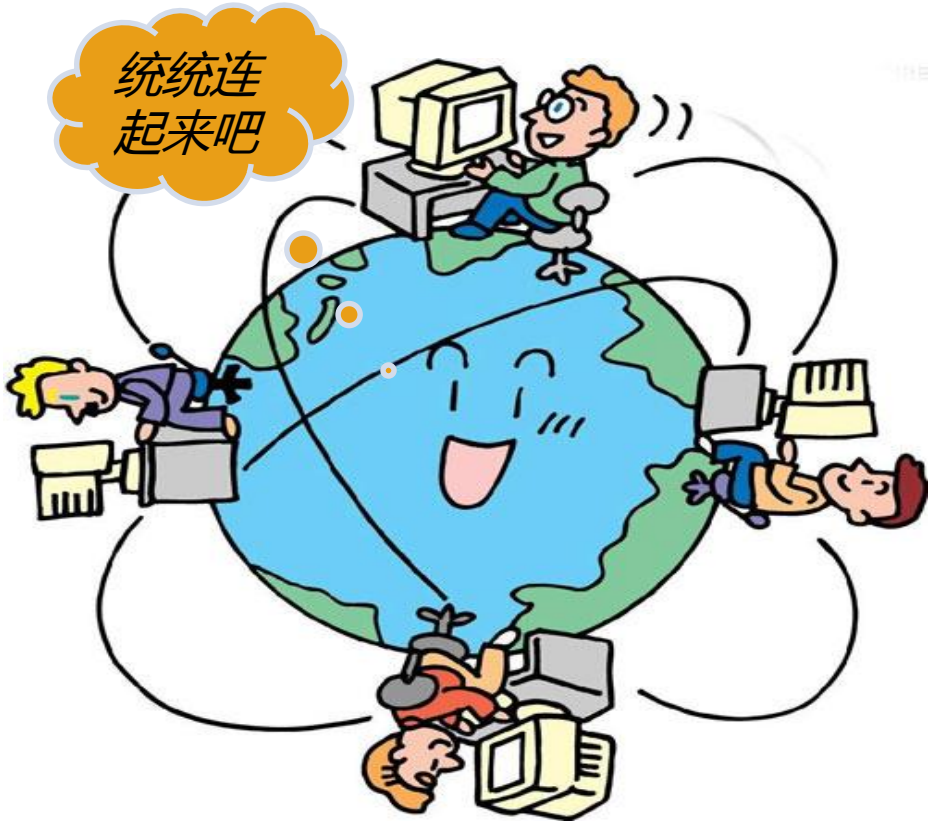
1、了解密码学及PKI基本概念

2、了解PKI如何使得网络更安全

3、通过课程测试

网络时代

CFCA



网上购物

网上银行

安全隐患

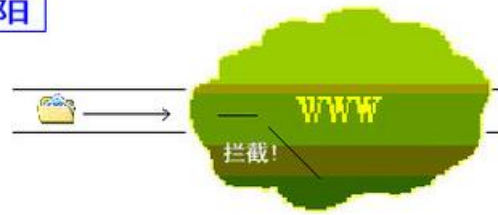
CFCA

窃听

伪造

截获 篡改

浔阳



东京

蔡九

嘿嘿，被我拦截

蔡京

梁山

吴用

网络安全要素

CFCA

传输的原始数据不被第三方获取	保密性
数据在传输过程中不被篡改	完整性
防止事件发起者事后抵赖，避免法律纠纷	不可抵赖性
相互通信时（交换敏感信息时）确认对方的真实身份	身份确定性

课程内容

CFCA

01 密码学基础

PKI基本概念 02

03 数字证书原理

目录页

CONTENTS PAGE

密码学基础-基本术语

CFCA

明文(Plaintext)：　被保护的原始数据，也叫消息(Message)

加密(Encryption)：用某种方法伪装消息，隐藏原始内容的过程

密文(Cipher text)：被加密的消息

解密(Decryption)：将密文转换为明文的过程

会话(Session)：　　一次网络通信的过程

密码学基础-基本术语

CFCA

密码算法: 加密及解密过程使用的数学函数（运算方法）

密钥(key): 使用加密算法加密或者解密过程中，需要使用的控制参数；
分为加密密钥和解密密钥

密钥加密密钥(Key Encrypting Key): 保护密钥的密钥

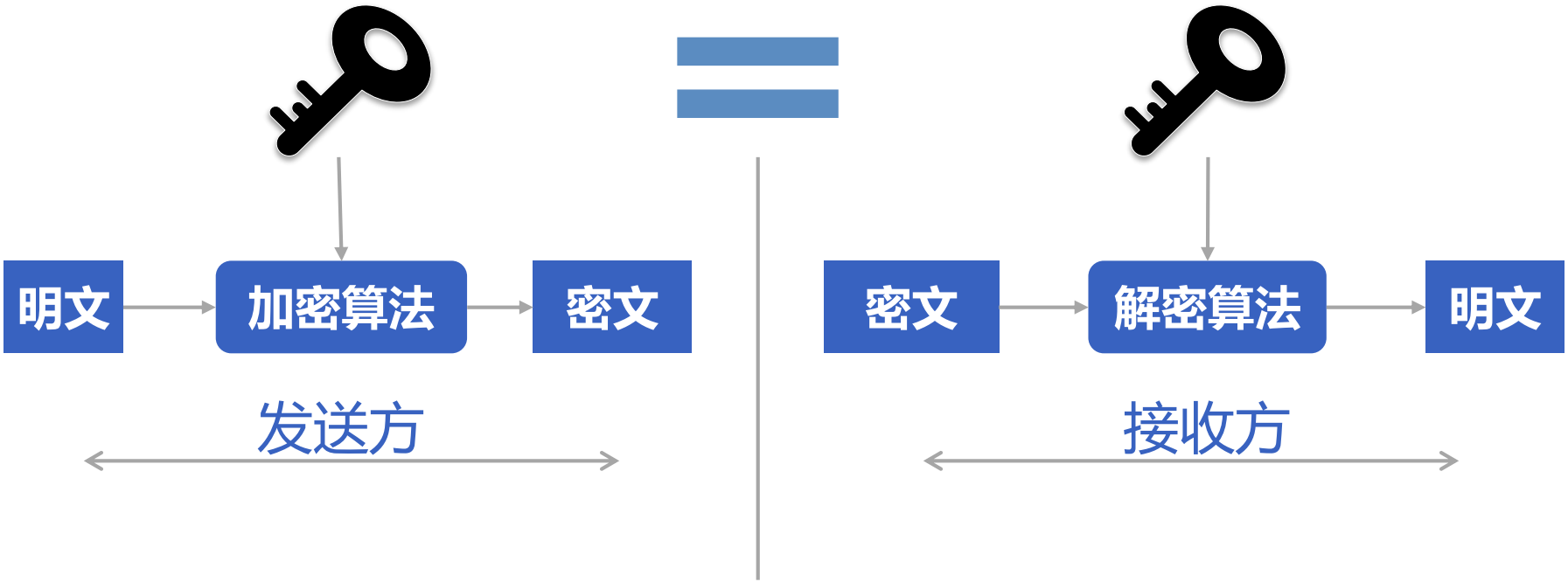
密码体制: 由所有可能的明文M、密文C、密钥K以及加密算法E和解密算法D，组成的系统
五元组{P, C, K, E, D}

目录页

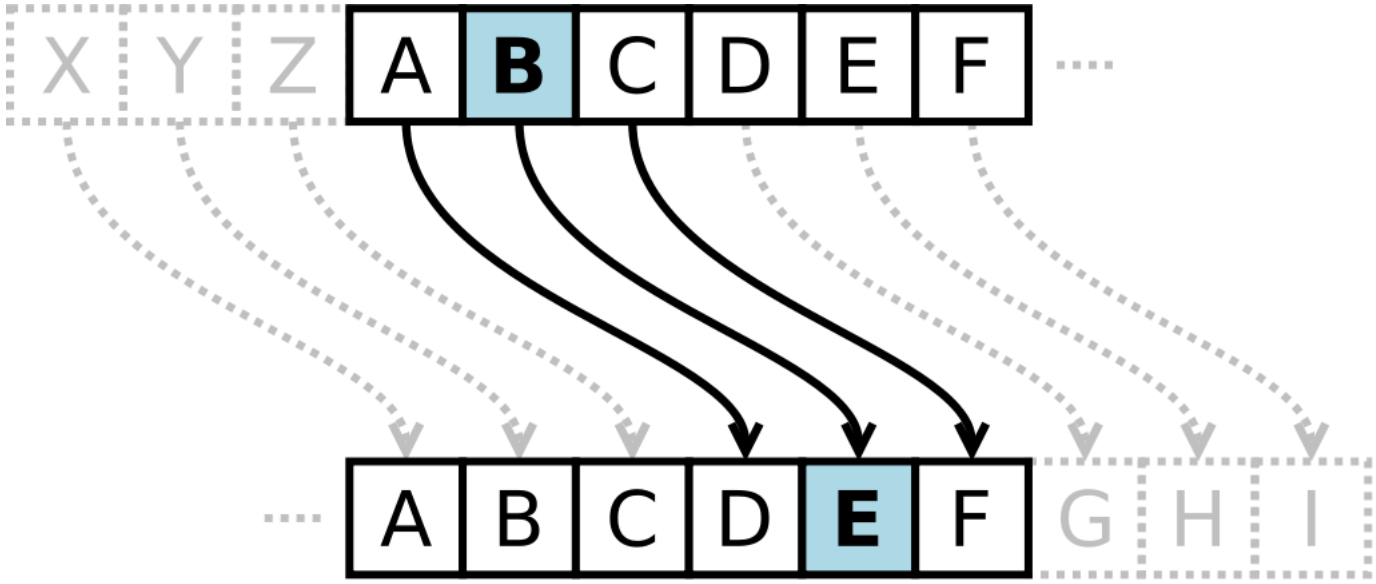
CONTENTS PAGE

密码学基础-对称密码体制

CFCA



密码学基础-凯撒密码



明文 Hello

H	e	l	l	o

密文 Khoor

K	h	o	o	r

密码学基础-凯撒密码五元组

CFCA

加密算法 E	C = P + 3(mod 26)
解密算法 D	P = C - 3(mod 26)
密钥 K	3
所有可能的明文P	ABCDEDFHIJKLMNOPQRSTUVWXYZ
所有可能的密文C	DEDFHIJKLMNOPQRSTUVWXYZABC

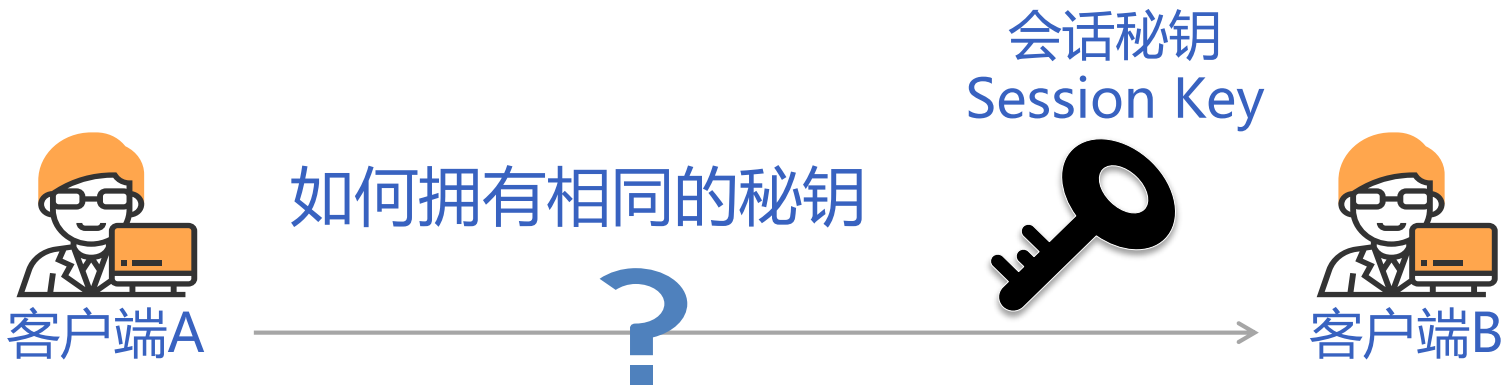
?

密码学基础-现代密码系统

CFCA

名称	全称	密钥长度(bit)	破解难度
DES	Data Encryption Standard	64	中
3DES		192	难
AES	Advanced Encryption Standard	128 192 256	难 难 难
SM4		128	难
RC4	Rivest Cipher		中
…			

密码学基础-对称密码系统的秘钥分配



密码学基础-对称密码系统的秘钥分配

CFCA

1976年之前

①密钥由A选取并通过物理手段发送给B
②密钥由第三方选取并通过物理手段发送给A和B

③如果 A、B事先已有一密钥，则其中一方选取新密钥后用已有的密钥加密新密钥并发送给另一方

④如果 A和B与第三方C分别有一保密信道，则C为A、B选取密钥后，分别在两个保密信道上发送给 A、B

密码学基础-对称密码系统的秘钥分配

CFCA

① ②物理手段缺点
- 速度慢
- 会话密钥个数：n(n-1)/2

③缺点
- 初始密钥分配困难
- 安全性低

密码学基础

CFCA

Key Distribution Center

n个密钥加密密钥

n(n-1)/2个会话密钥

KDC

1,Request || N1

2, $E_{K_A}[K_s \| Request \| N_1 \| E_{K_B}(K_s \| ID_A)]$

3, $E_{K_B}[K_s \| ID_A]$

4, $E_{K_S}[N_2]$

5, $E_{K_S}[f(N_2)]$

客户端A

客户端B

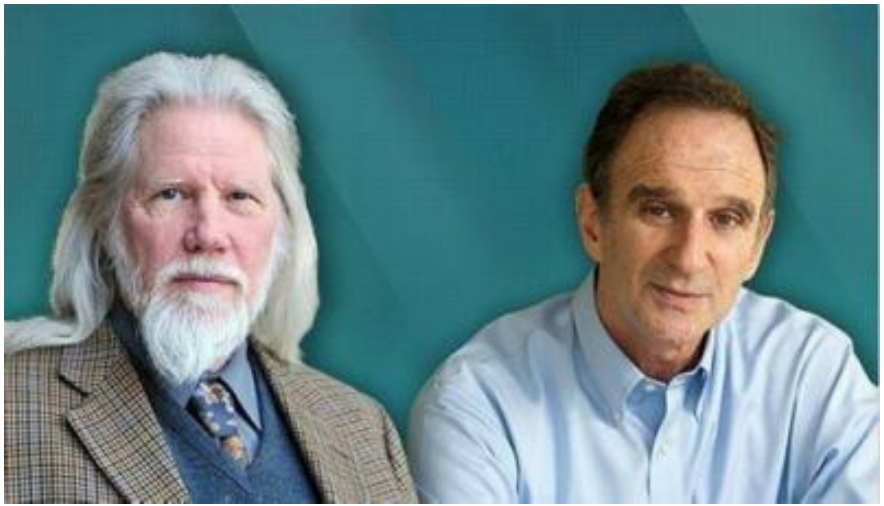
目录页

CONTENTS PAGE

密码学基础-非对称密码系统

CFCA

1976 New Directions in Cryptography



菲尔德·迪菲(Whitfield Diffie)

马丁·赫尔曼(Martin Hellman)

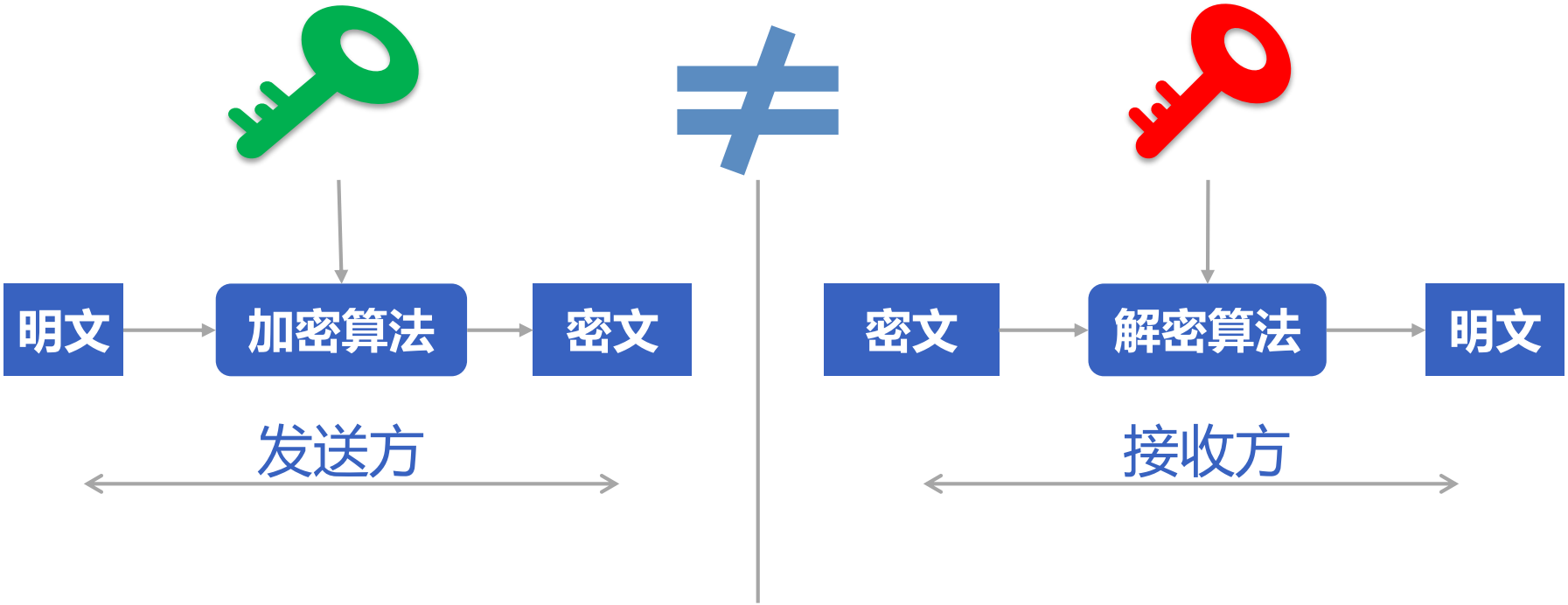
非对称密钥对
- 公钥(Public Key)
- 私钥

加密和解密通过数学运算完成

Diffie-Hellman Key Exchange

密码学基础-非对称密码体制

CFCA

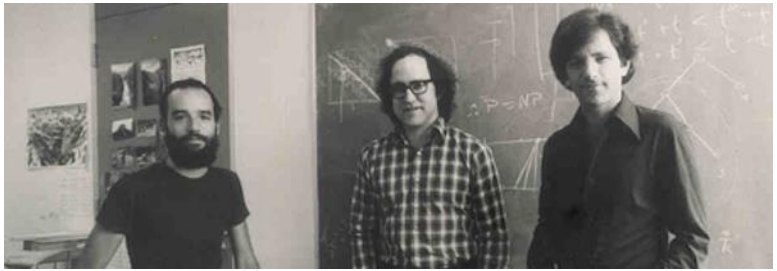


密码学基础-非对称密码体制

CFCA

名称	密钥长度(bit)	破解难度
RSA	1024 2048 4096	中 难 难
SM2	256	难
ECC		难
…		

1978 RSA



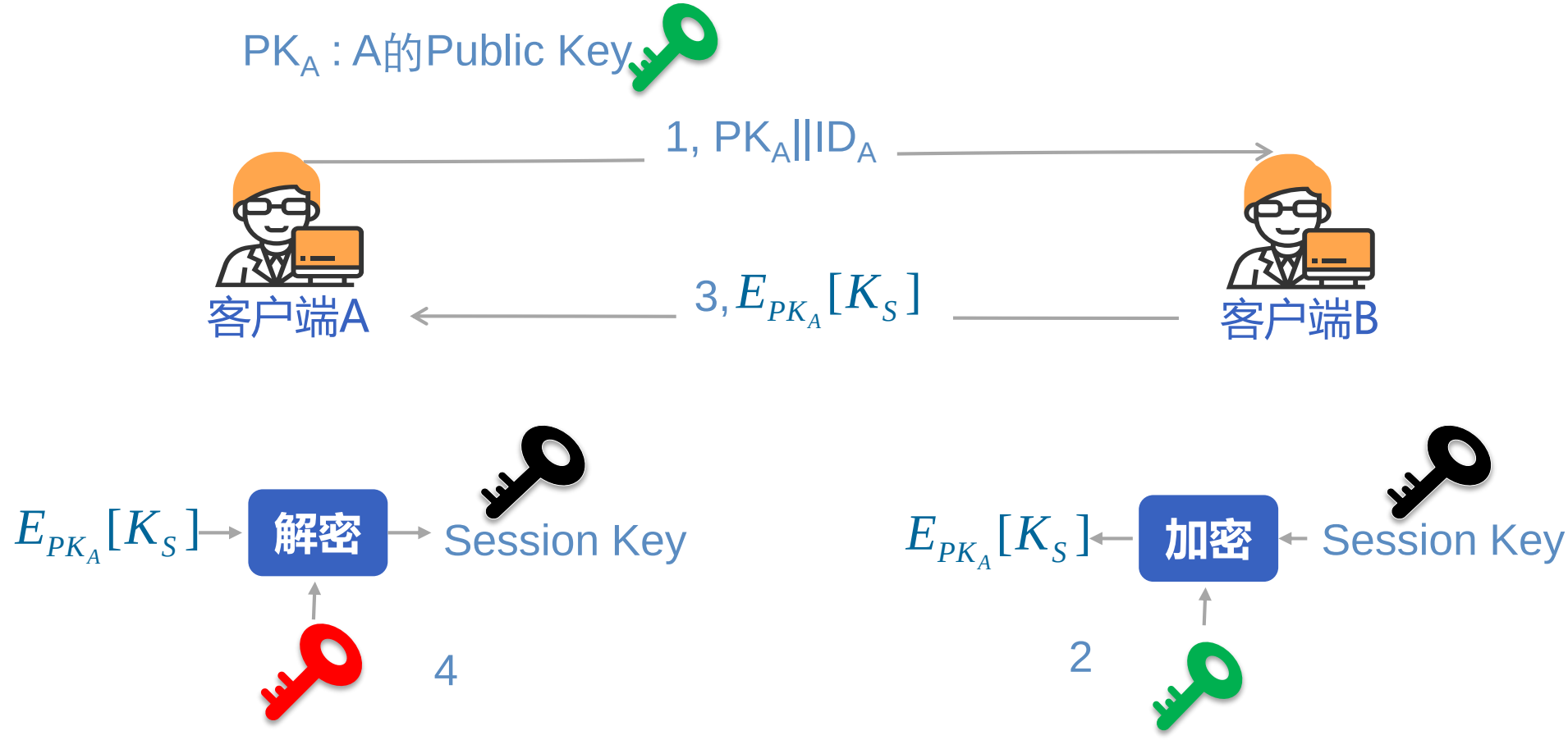
罗纳德·李维斯特 (Ron Rivest)

阿迪·萨莫尔 (Adi Shamir)

伦纳德·阿德曼(Leonard Adleman)

密码学基础-非对称密码体制密钥分配

CFCA



密码学基础-对称密码与非对称密码对比

CFCA

	效率	运算量	密钥管理	密钥分配	签名认证
对称密钥	高	小	困难	困难	不支持
非对称密钥	低	大	简单	简单	支持

密码学基础-非对称密码强度分析

CFCA

RSA公钥
- 参数 n = p * q
- p、q 为素数

n = 143

11 * 13

n = 1403

23 * 61

密码学基础-非对称密钥强度分析

CFCA

n =

CFCA 官网 2048

bf970e05bc502b468f345b9b586d415b8f547e8db874e3ff25f667ebc87ae925
2e9ae3d99895d602da1493a74ca963947bece06a32f7e823b4dfb881c231e557
c8761b9f5a2eb122f31b2b517779aadadb142f759632b66a5cbeee1c17bb0853
43f73a0595e674374f94c59c6f05c79109972b8b79a060bf6ffca654286032e3
185efab54298b181b79760c9c073479e3cb0d57a6a58c34344931b38177e2d6d
e74331e66a279a406c60a5576f827d4ec676e4a200bea182d31adc7419934d5f
7f2a7f9df82f8177cc4bd1d586007f30bffe80ead7d07ff401bb3123ce25b62d
dfd3bb3e485c37d350da1a88e6b2053516a689b5859867b7780e522afd32dc63

对RSA 密钥的攻击

- 1994年，通过分布式计算，历时8个月 428 bit的公钥被破解
- 1999年，使用高性能计算机，历时5个月512bit的公钥被破解
- 2009年12月，768bit的公钥被破解，计算时长超过2年
- 1024 bit的破解难度是 768 bit 难度的1000 倍，预计需要100万美元及1年以上的时间

目录页

CONTENTS PAGE

密码学基础-哈希

CFCA

哈希：将任意长度的数据作为输入，通过特定运算得到固定长度输出的过程。输出结果叫哈希值、数字摘要、数字指纹。

- 确定性，相同消息的输入总是产生相同的摘要
- 快速性，可以快速计算任何给定消息的摘要
- 不可逆，不能从摘要推出原始消息
- 雪崩效应，即使细小的更改也会导致摘要发生巨大的变化
- 唯一性，不能找到具有相同摘要的两个不同数据

密码学基础-哈希

CFCA

使用场景
- 完整性验证
- 数字签名

名称	输出长度(bit)
MD5	128
SHA1	160
SHA256	256
SM3	256
…	

hello → 5D41402ABC4B2A76B9719D911017C592

hcllo → 1B0DBB128BF46D916FF38CAE0AB6F4CB

CFCA

数字签名

数字签名是使用一组规则和一组参数计算出的, 可以验证签名者身份、数据完整性的数据。(Digital Signature Standard)

密码学基础-数字签名特性

- 依赖性
- 唯一性
- 可验证性
- 不可伪造
- 可用性

规则、法规和法令），款中说明的任何违约事件发生，贷款和票据将立即到期并应支付，不需要对借款方再行宣布或通知。

第十一条：合同变更或解除：除《合同法》规定允许变更或解除合同的情况外，任何一方当事人不得擅自变更或解除合同。当事人一方依据《合同法》要求变更或解除合同时，应及时采用书面形式通知当事人，并达成书面协议，本合同变更或解除后，借款方占用的借款和应付的利息，仍应按本合同的规定偿付。

第十二条：本合同经双方签字后生效，合同一式二份，贷款方、借款方双方各持一份。双方应按合同条款履行义务，如有一方违反，对方有权向人民法院提起民事诉讼，要求赔偿贷款金额50%违约金。

第十三条：解决合同纠纷的方式，执行本合同发生争议，由当事人双方协调解决。协商不成，双方同意按（1）或（2）项处理。

（1）上海仲裁委员会仲裁。

（2）向人民法院起诉。

贷款方：上海崇明宝岛小额贷款有限公司　　借款方签字：_____

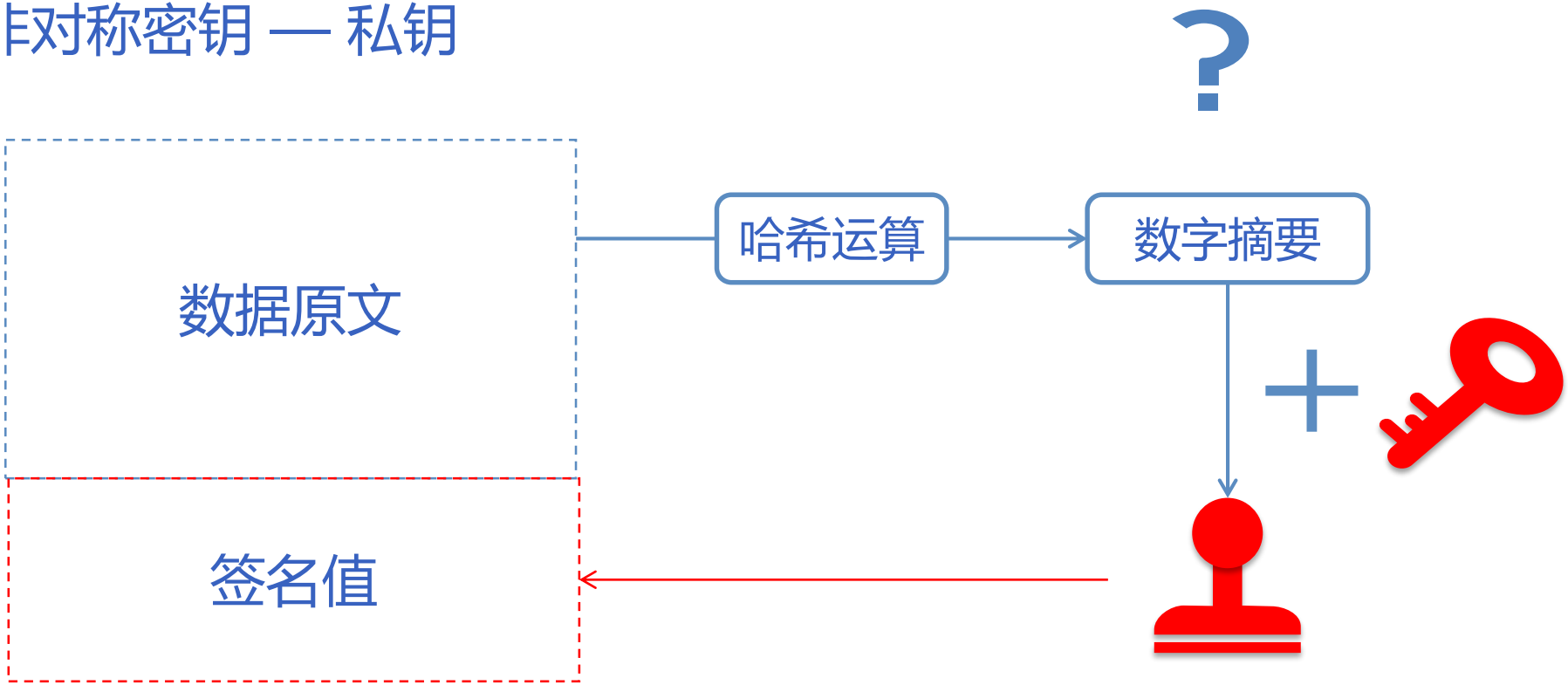
企业法人：_____　　按手印处：_____

Benjamin Franklin的签名

密码学基础-数字签名

CFCA

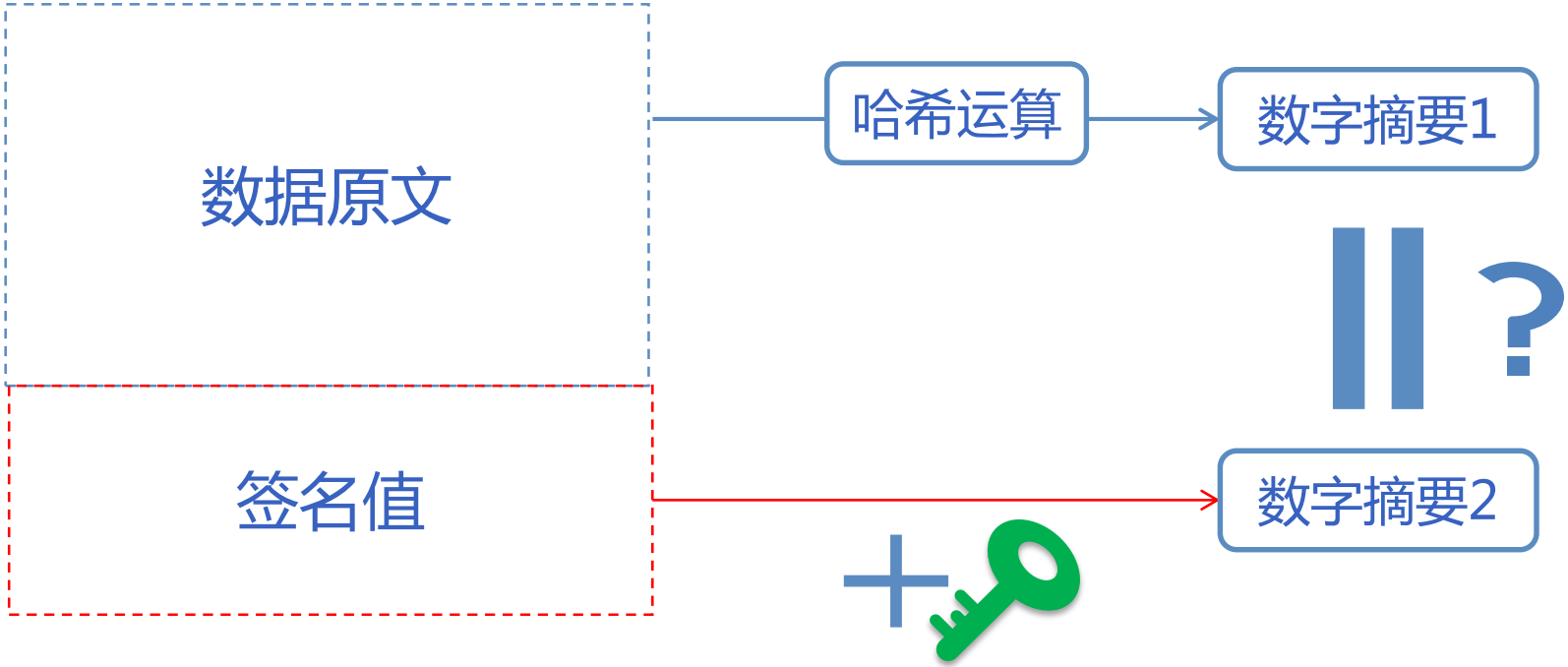
非对称密钥 — 私钥



密码学基础-签名验证

CFCA

非对称密钥 — 公钥



密码学基础-非对称密钥加解密 vs 签名验签

CFCA

数字签名 

签名验证 

非对称加密 

非对称解密 

密码学基础-小结

CFCA

保密性 ⇐ 加密 ⇐ 

完整性 ⇐ 数字摘要

不可抵赖性 ⇐ 签名 ⇐ 非对称密钥

身份确定性 ⇐ PKI & 数字证书

CFCA

PKI

Public Key Infrastructure

是基于非对称密码学，利用公钥证书机制来实施和提供信息安全服务的普适性基础设施

PKI基本概念-发展历史

CFCA

- 1976年，非对称密码被提出
- 1978年，RSA算法被提出
- 20世纪80年代，美国学者提出了PKI的概念
- 1996年，IBM、Netscape等企业及数家银行推出SET协议，推出CA和证书概念
- 1999年，PKI论坛成立
- 2001年6月13日，在亚洲和大洋洲推动PKI进程的国 际组织宣告成立，该国际组织的名称为“亚洲PKI论 坛”，其宗旨是在亚洲地区推动PKI标准化，为实现全 球范围的电子商务奠定基础……

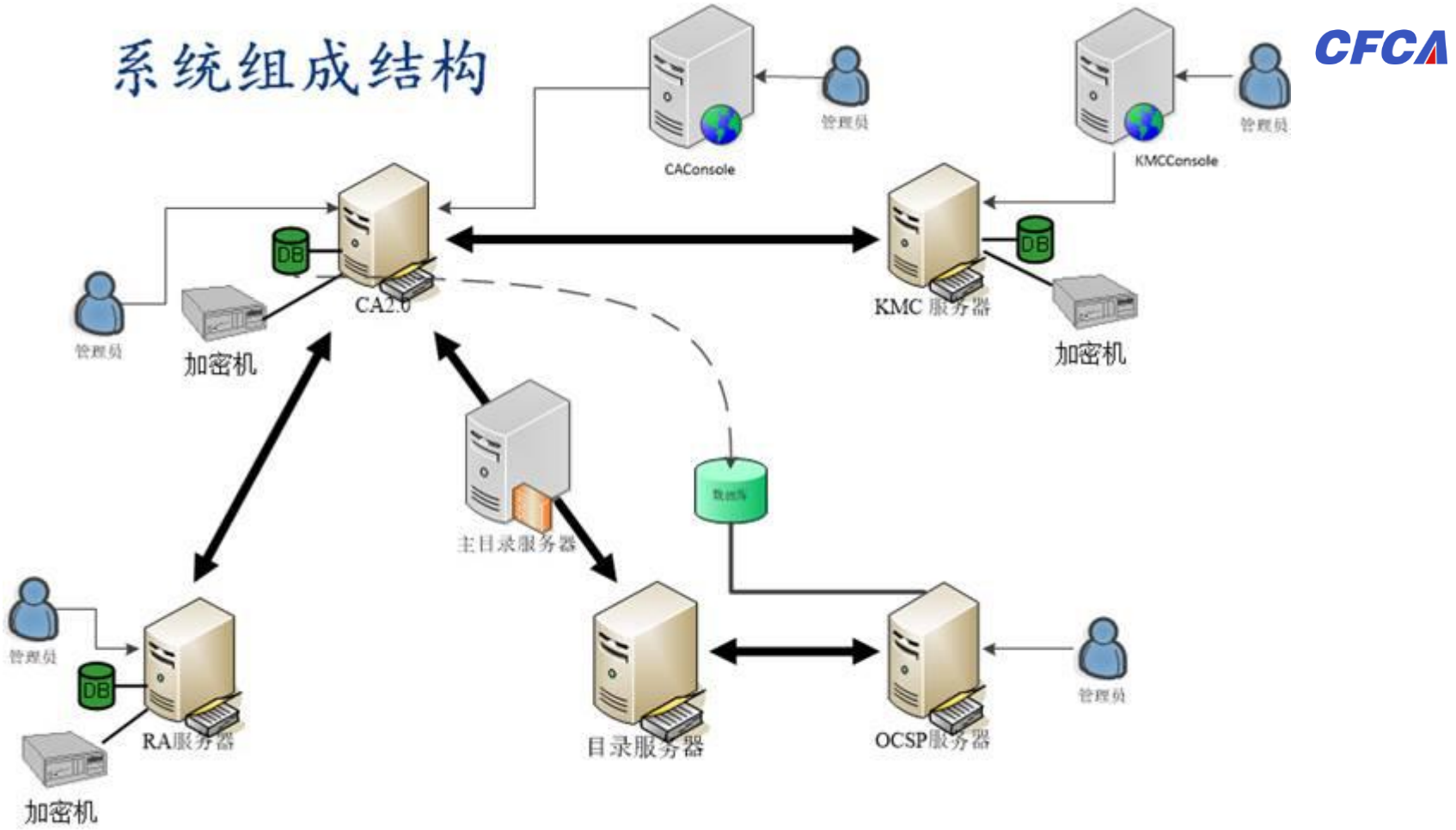
PKI基本概念 主要组成

CA	PKI的核心执行机构，被政策CA授权以后，可签发、管理权威的、证明网上身份的数字证书。CA被称作网络“公安局”
RA	证书注册申请和审核批准机构
KM	密钥管理系统,提供加密密钥的产生、存储、更新、发布、查询、撤销、归档、备份及恢复等管理服务
目录服务器	采用目录服务器(LDAP)的方式存储和发布用户的证书信息，用户可访问目录服务器，查询证书的信息
OCSP服务器	为应用程序提供在线证书状态查询服务
标准	PKCS#1,PKCS#3，… 等公钥密码标准，用于证书申请、更新、证书作废表发布等 X.509 v3标准：证书格式结构标准

CFCA

PKI基本概念

系统架构

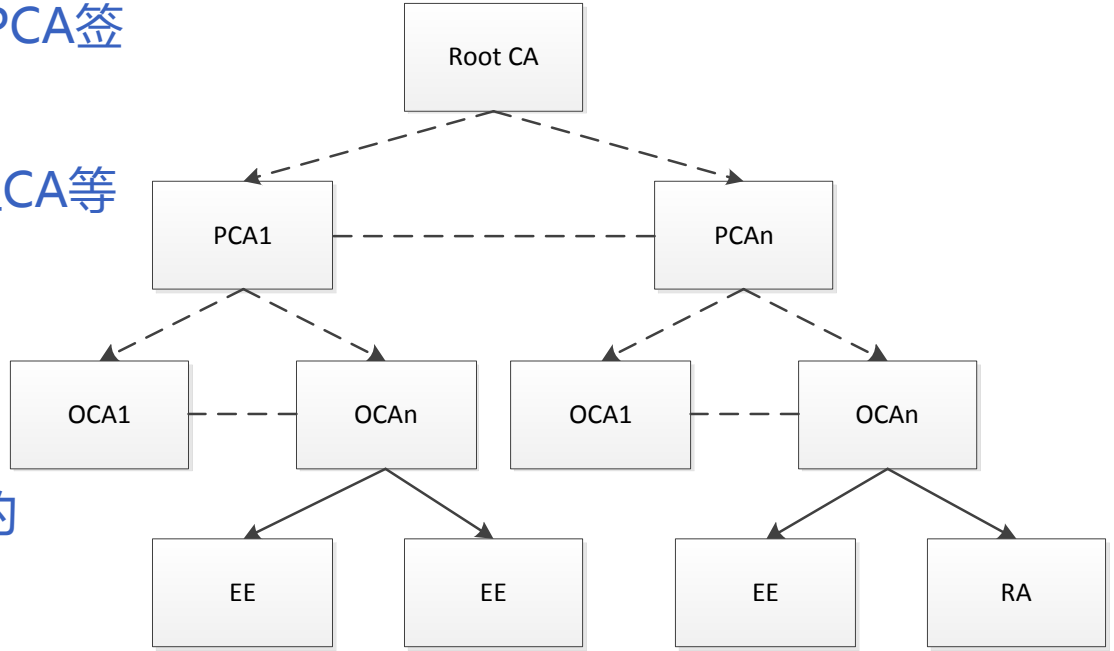


PKI基本概念-多层次CA

根CA：如一个国家或一个地域性的CA,创建整个PKI系统的方针，政策，为下属PCA签发证书

PCA：根CA下设的政策性CA,如行业CA等，为下属CA签发证书

CA：认证机构，按照上级PCA制定的政策，担任具体的用户公钥证书的签发，生成和发布CRL。

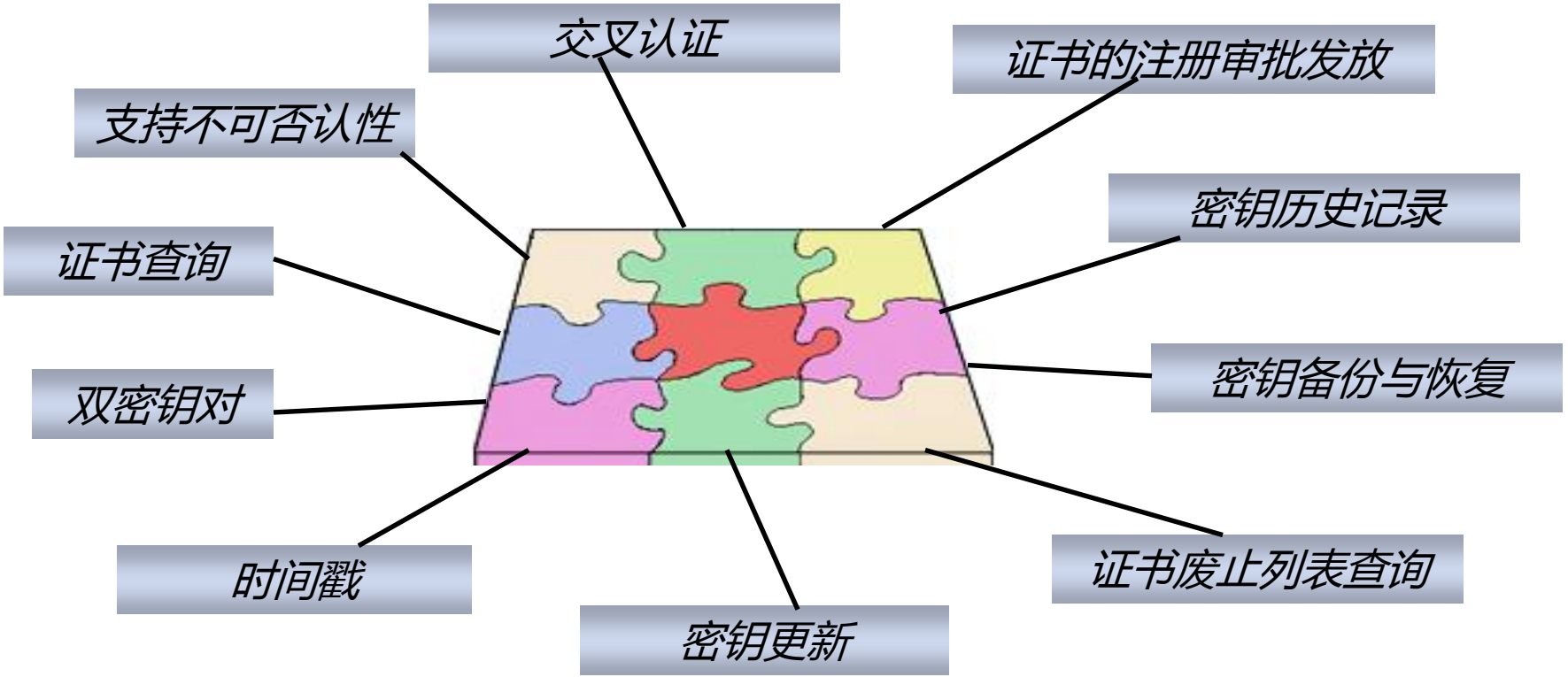


PKI基本概念-CA职责

- 证书管理
  - 签发证书
  - 撤销证书
  - 冻结、解冻
  - 更新证书（补发、换发）
- 发布证书废止列表（CRL、黑名单）
- 密钥管理
- 交叉认证

PKI基本概念-服务

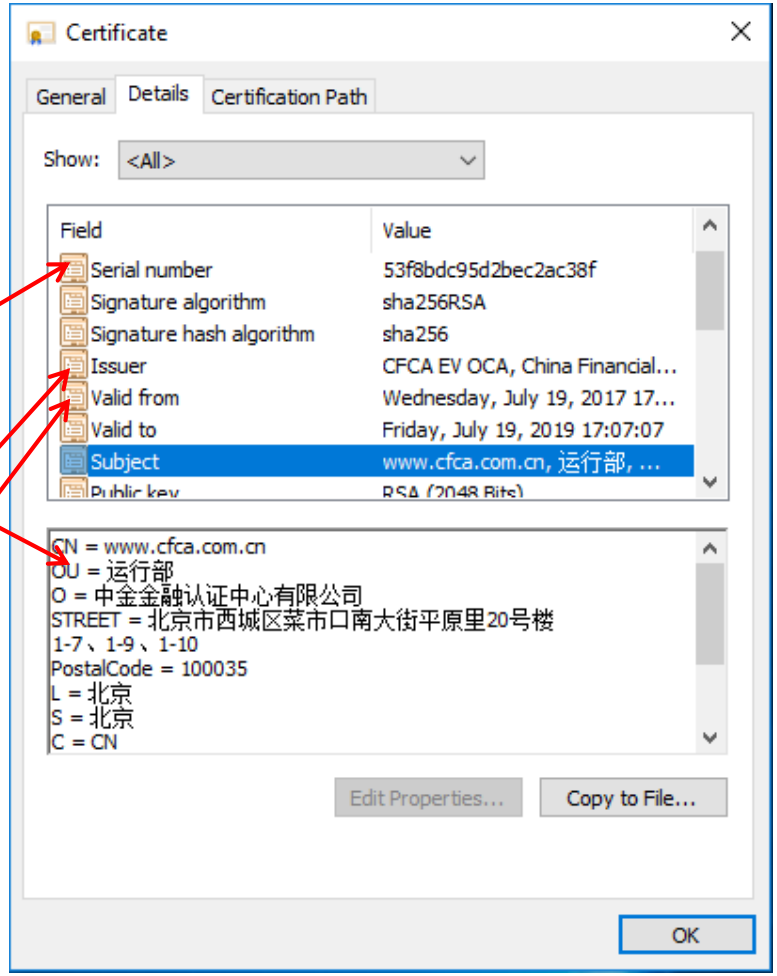
CFCA



数字证书

数字证书基本概念-定义

CFCA



数字证书基本概念-定义

CFCA

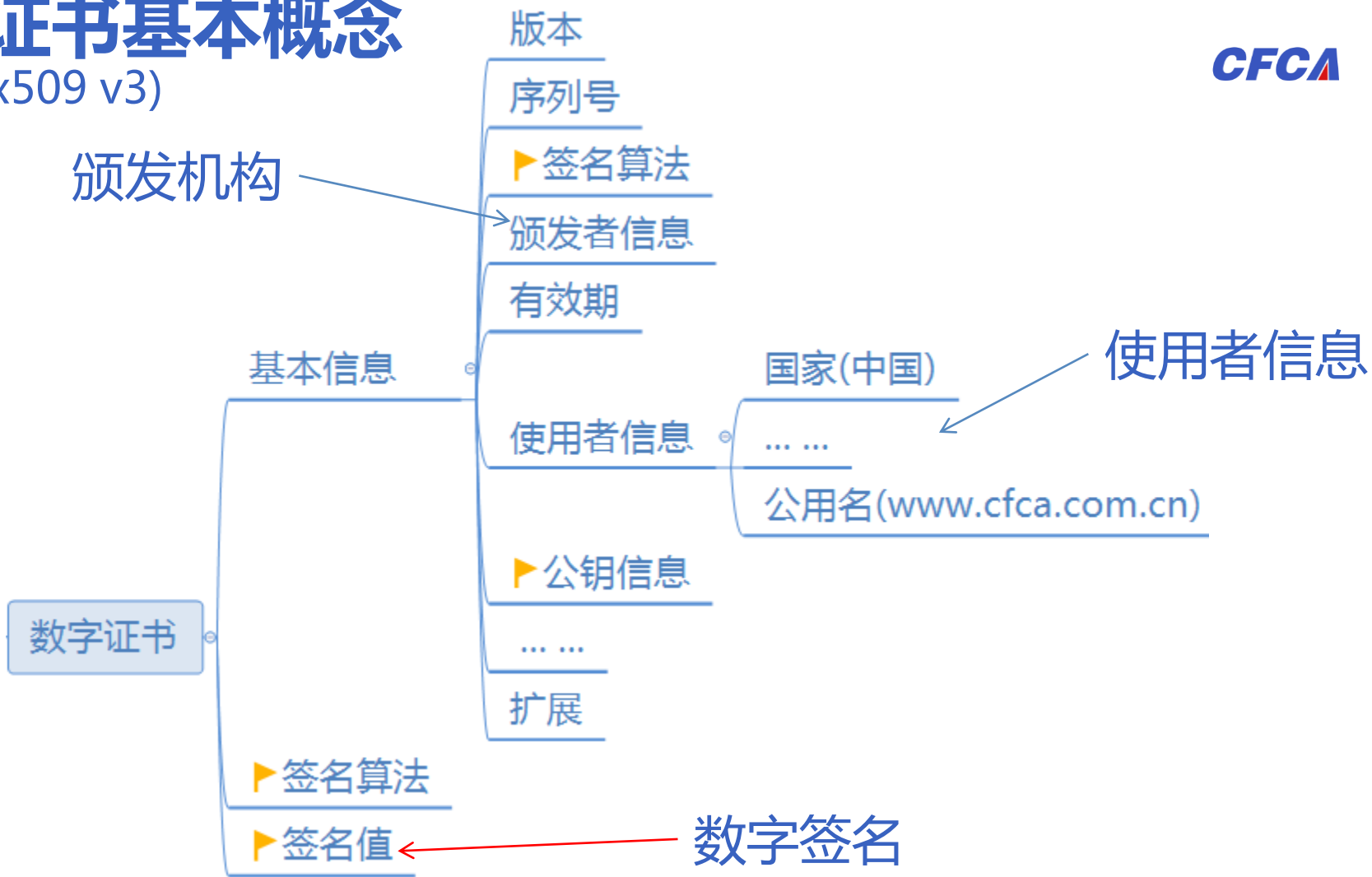
定义
- 可信权威机构签发
- 包含公钥信息
- 包含实体信息
- 标准结构数据流

作用　　证书实体与公钥的对应关系

数字证书基本概念

-结构(x509 v3)

CFCA



数字证书基本概念-证书私钥

私钥存储

- 私钥不可导出
- 防探测
- 访问授权

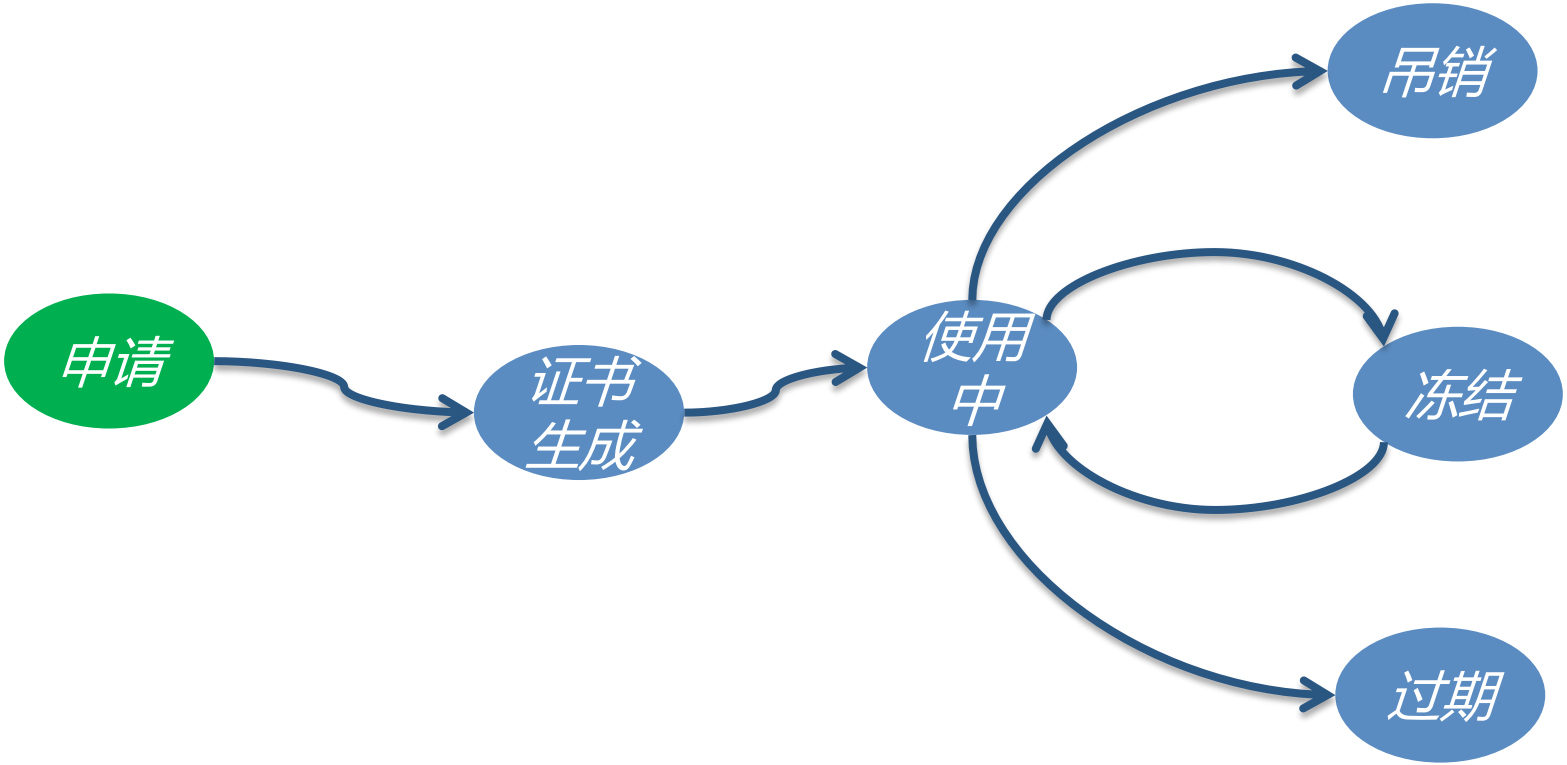
CFCA

01 数字证书基本概念

02 数字证书生命周期

03 数字证书的应用

数字证书生命周期



数字证书生命周期

证书申请

信息采集

申请人确认

CFCA

数字证书生命周期-证书申请

CFCA

CFCA SSL在线工具 v3.0.3.2　　SSL证书技术支持手册 下载

CSR生成　CSR查看　证书查看　证书公私钥匹配检查　证书格式转换　站点认证配置　SSL网站检测　SSL漏洞检测　证书链下载　CAA查询

填写信息

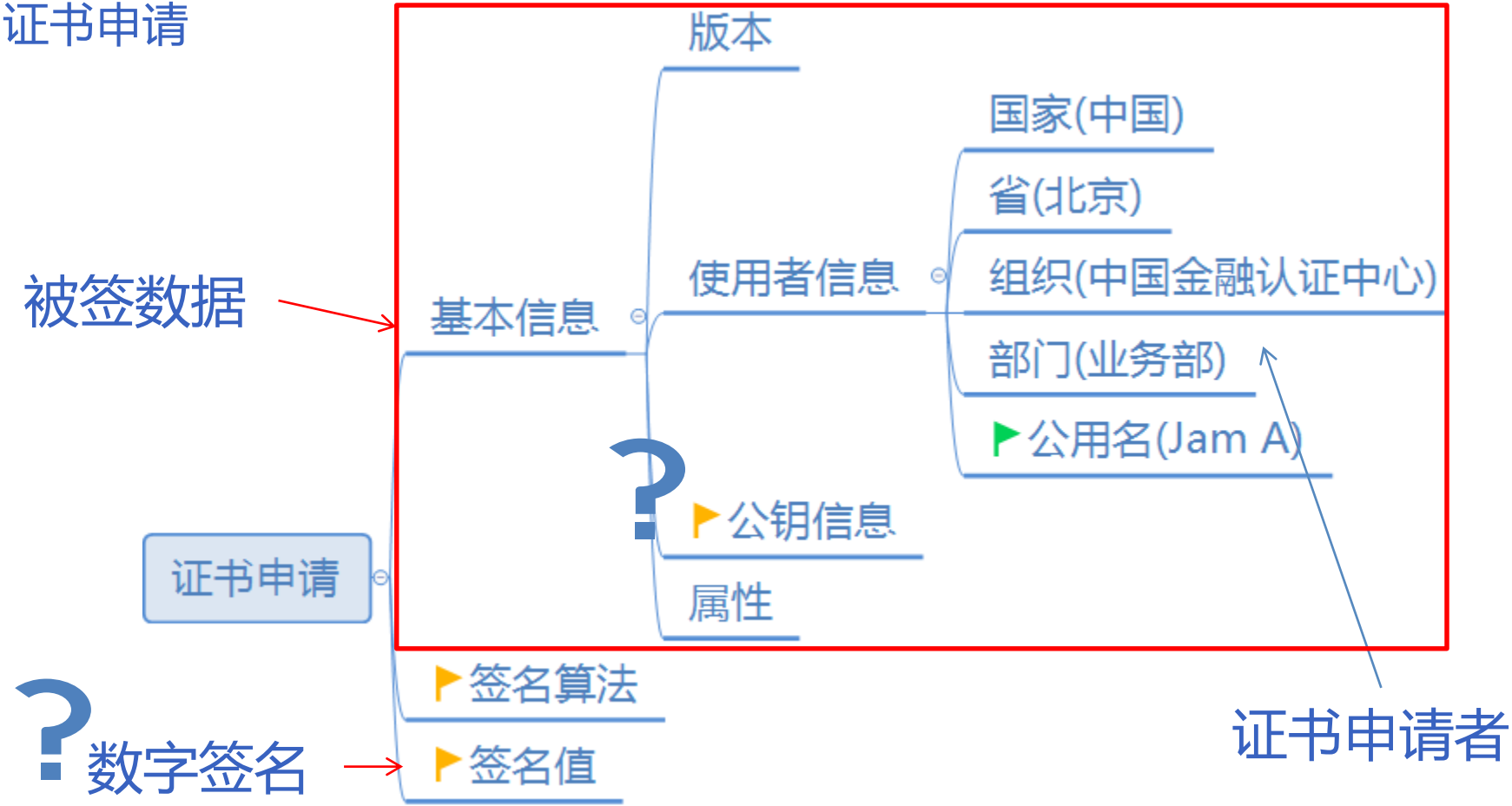
* 通用名(CN)	Zhang San
组织单元(OU)	技术部
* 组织(O)	China Financial Certification Authority
* 城市(L)	Beijing
* 省份(S)	Beijing
* 国家(C)	CN
KEY密码	11111111

生成CSR

数字证书生命周期

-证书申请

CFCA



数字证书生命周期-证书申请

CFCA

密钥对产生

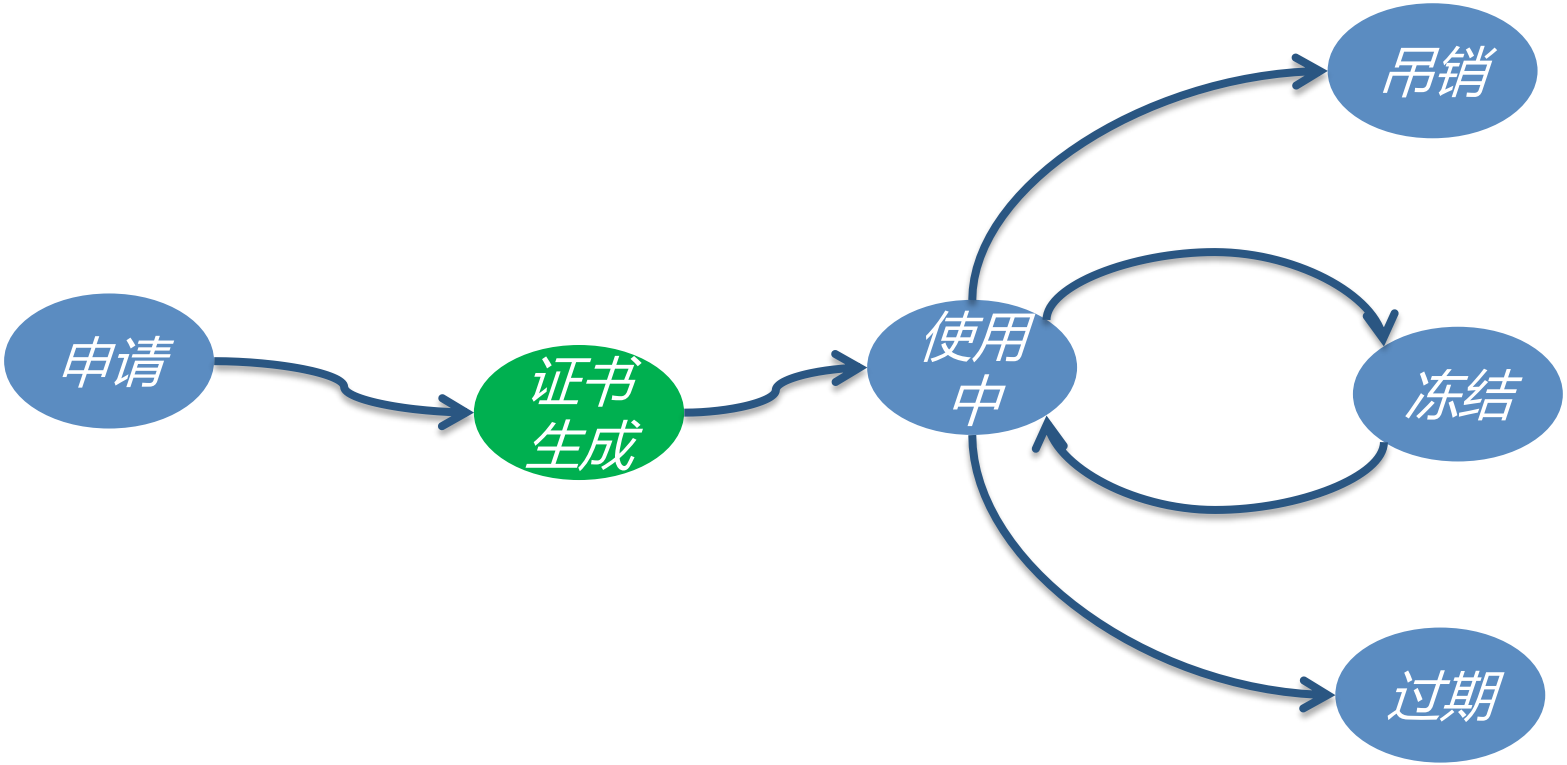
硬件

证书保险箱

软件

数字证书生命周期-证书申请

数字证书生命周期



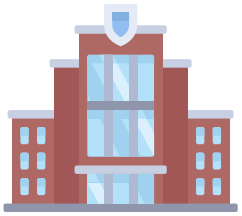
数字证书生命周期-证书生成

申请人

证书申请

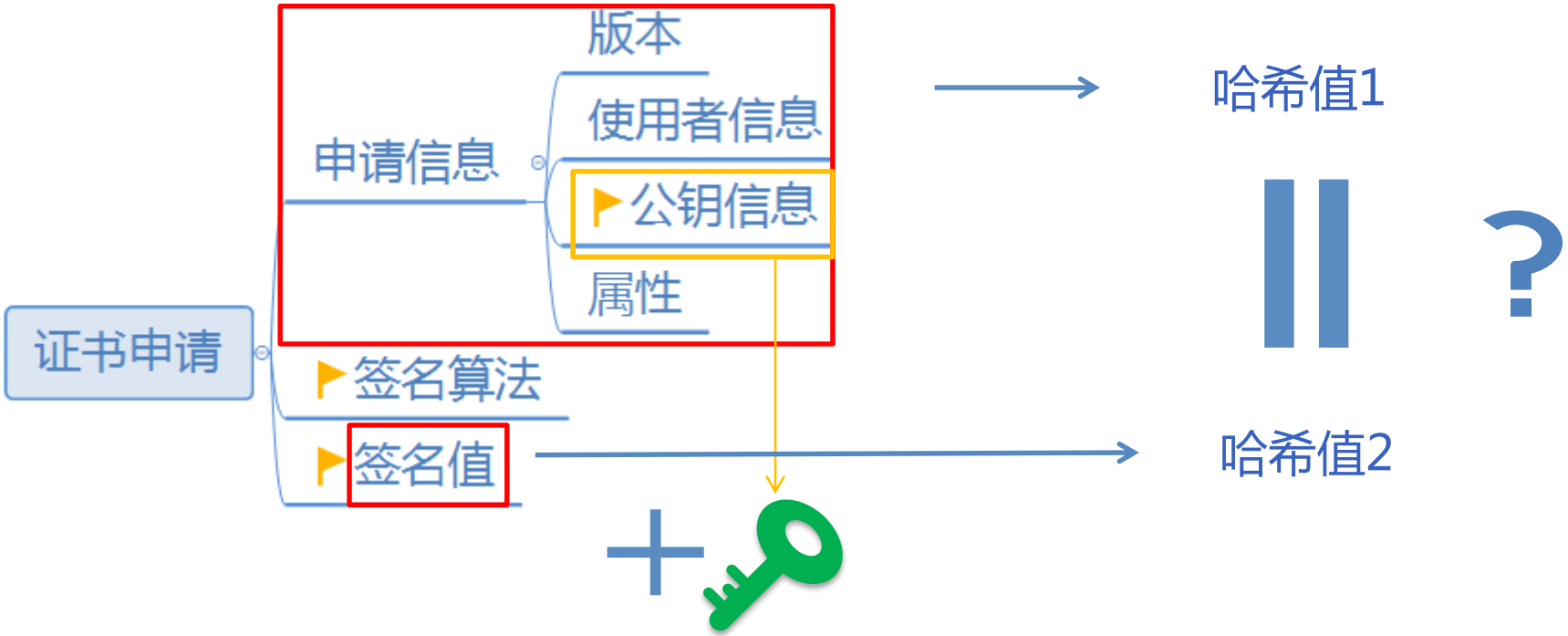
RA审核

证书申请



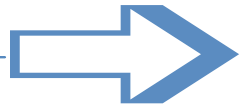
CA签发

数字证书生命周期-证书生成

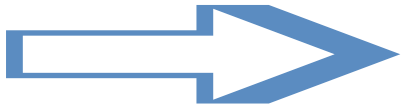


数字证书生命周期-证书生成

申请人信息
签发机构信息
其他信息

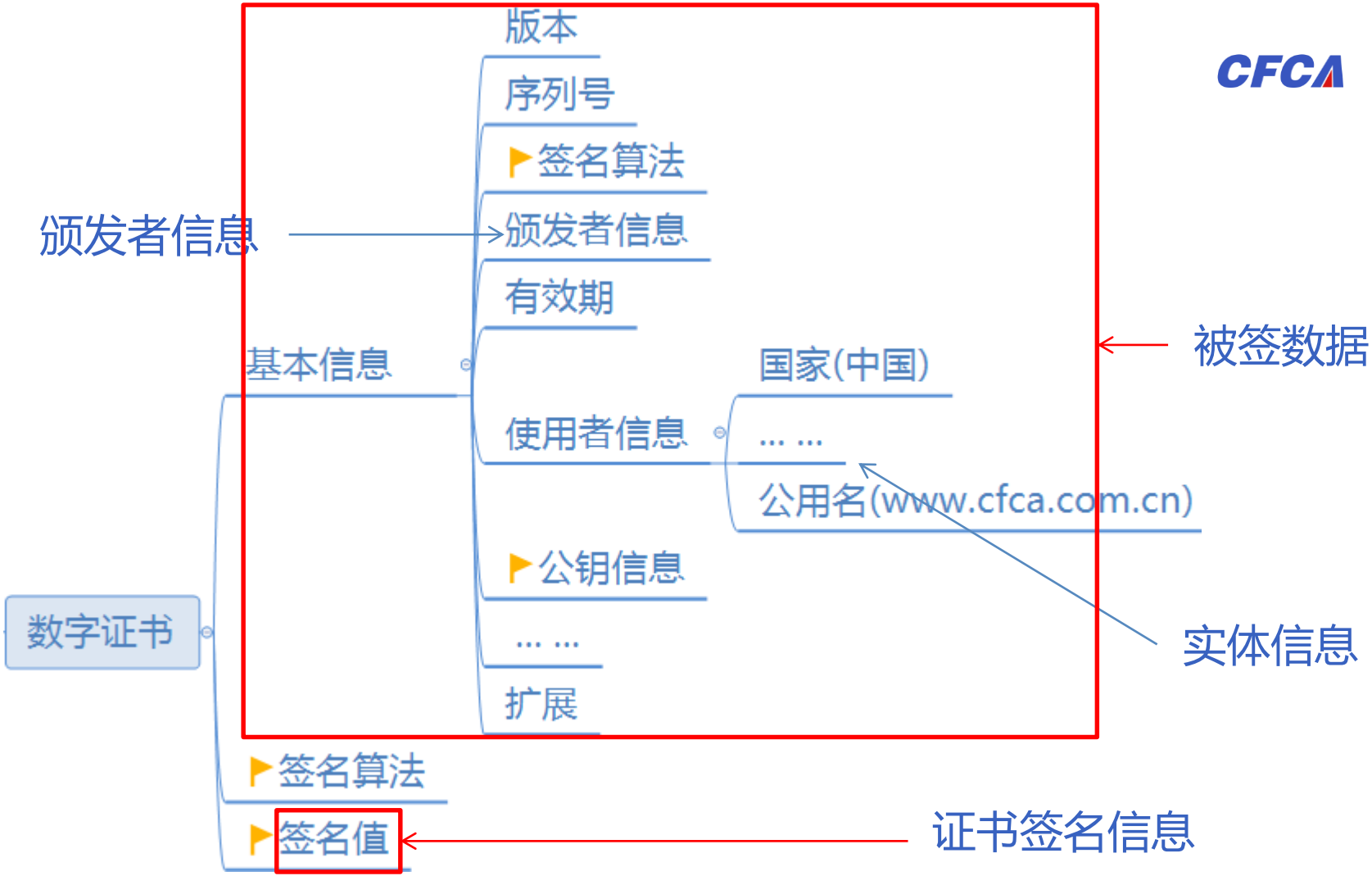


哈希值



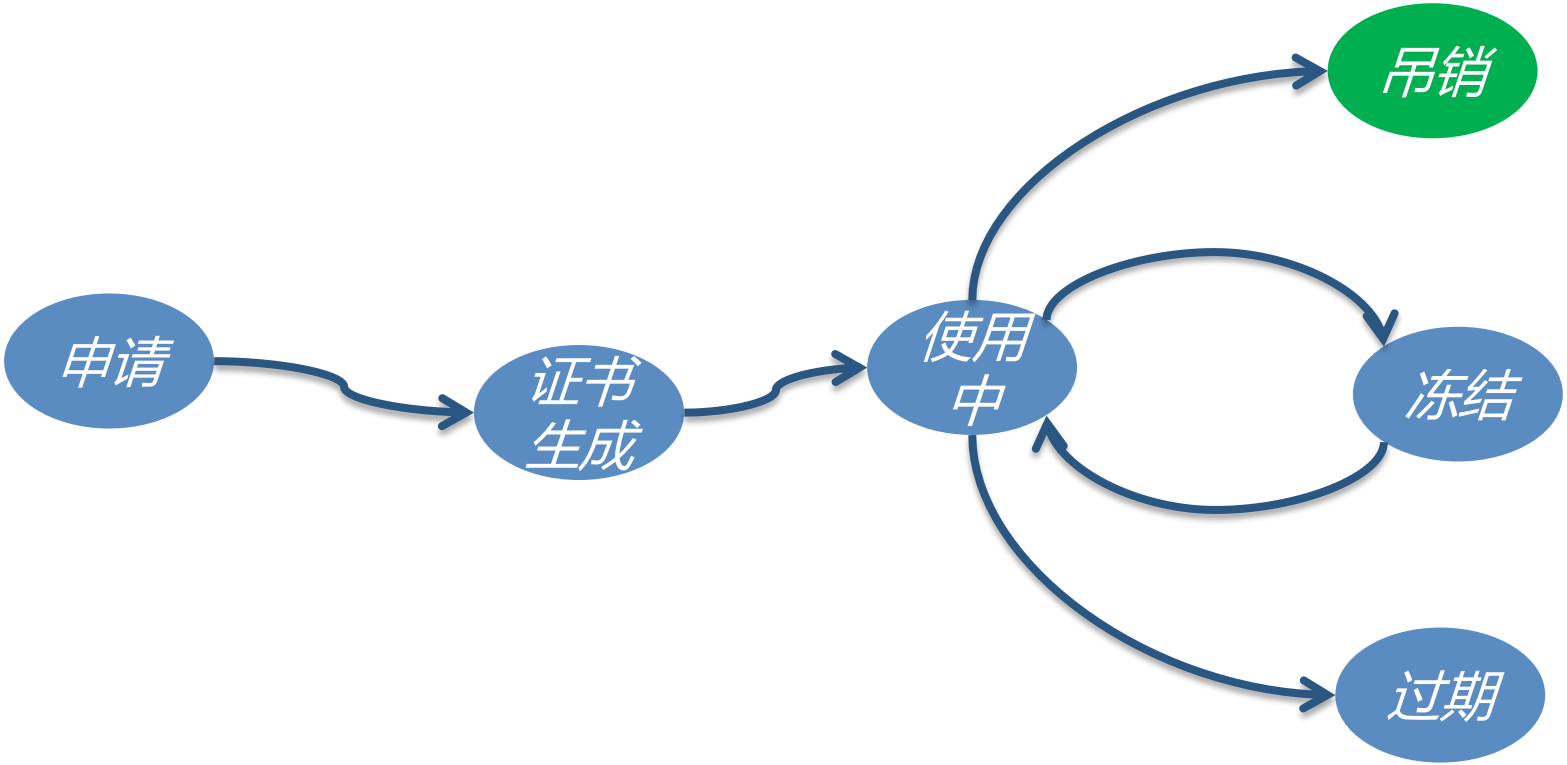
数字证书生命周期

证书生成

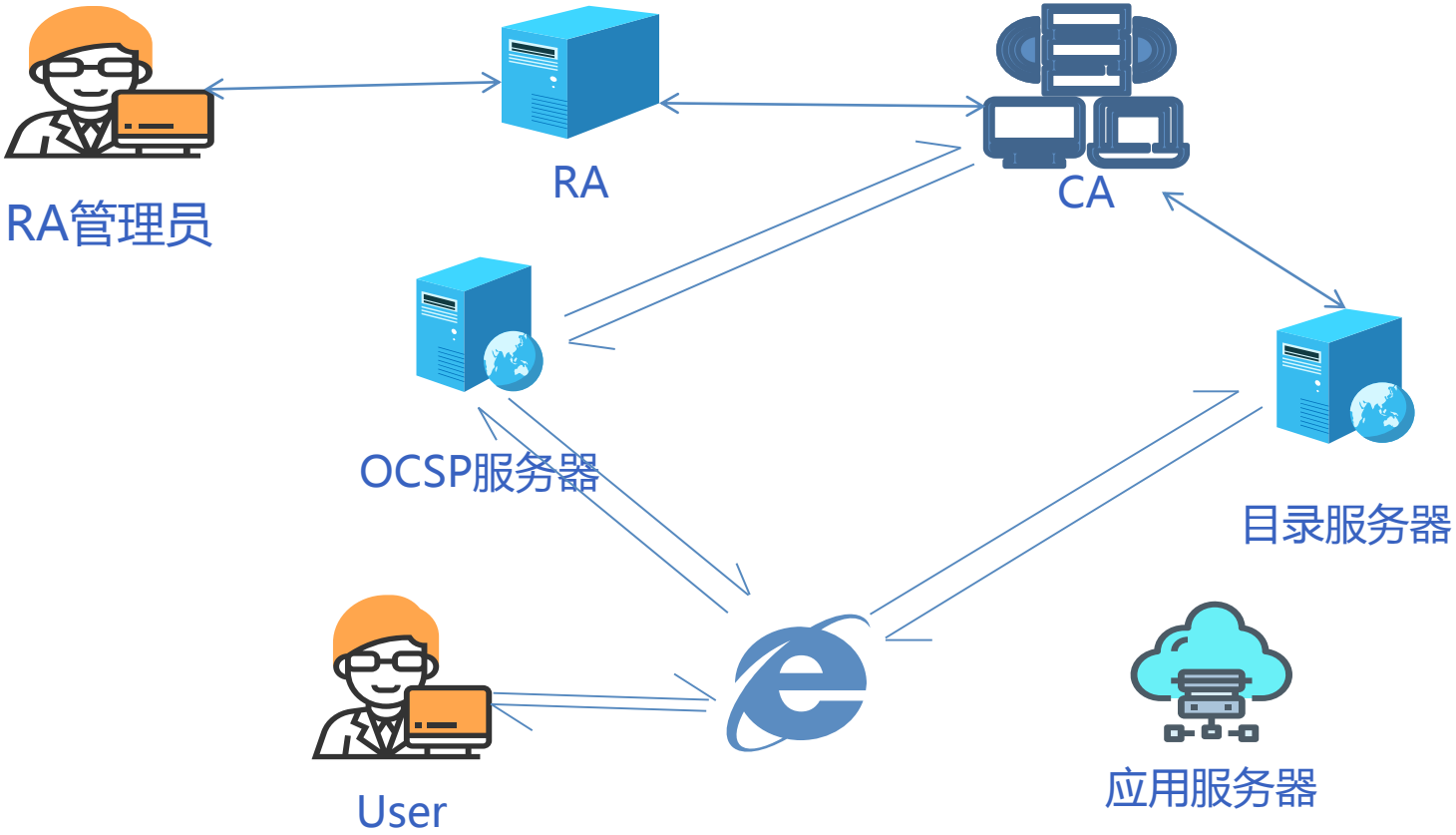


数字证书生命周期

CFCA



数字证书生命周期-吊销



CFCA

01 数字证书基本概念

02 数字证书生命周期

03 数字证书的应用

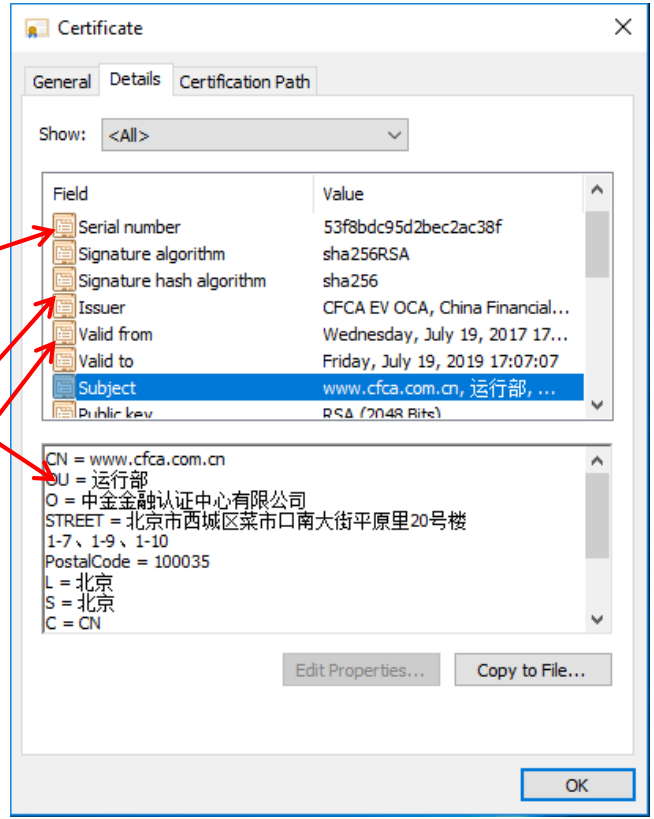
数字证书的应用

CFCA

数字证书的验证

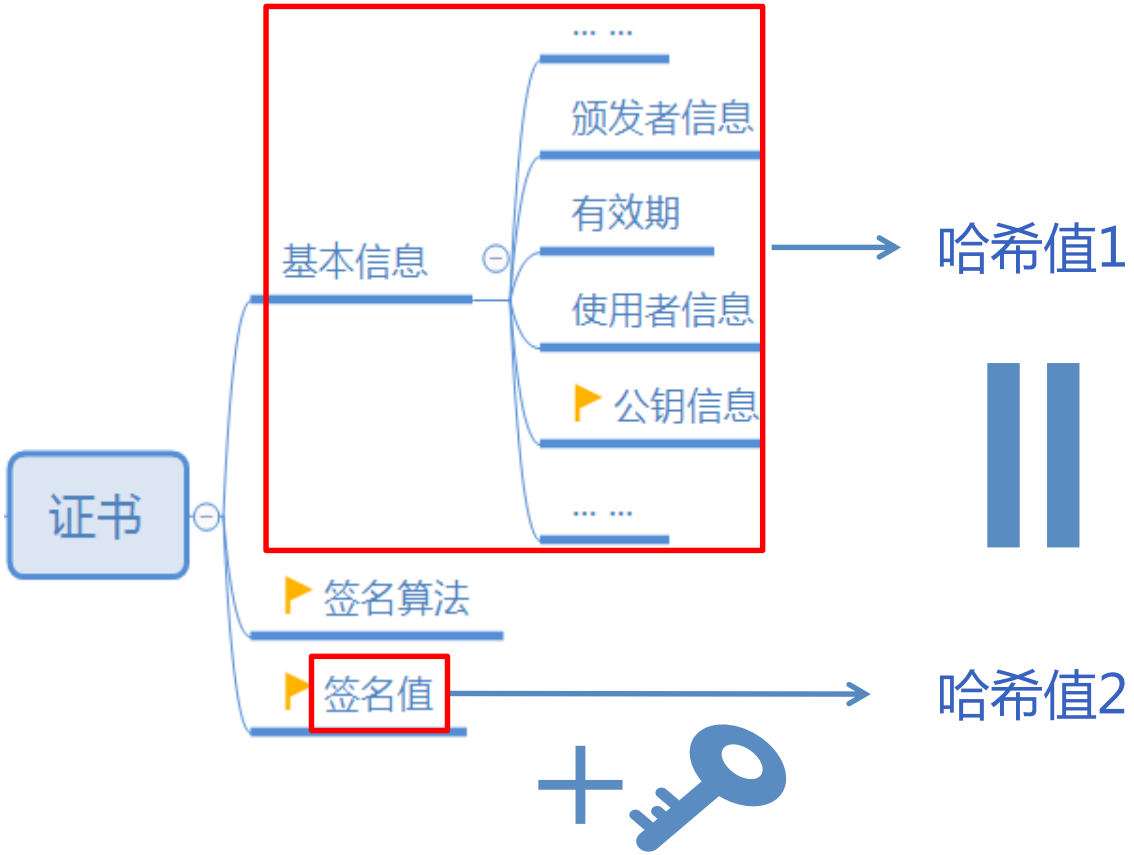
数字证书与SSL

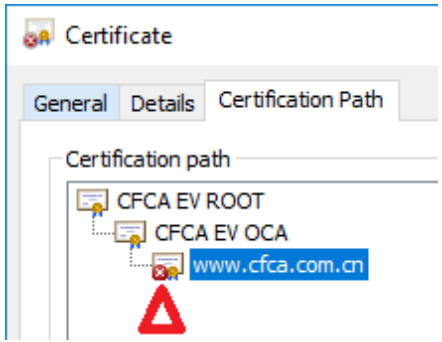
数字证书的应用-证书验证

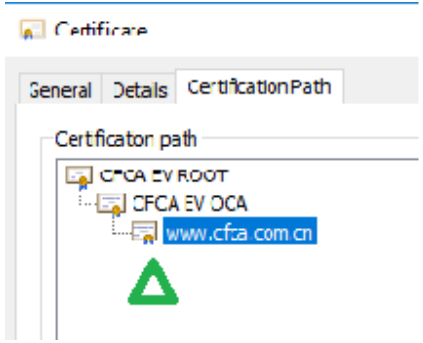


数字证书的应用-证书验证

CFCA







?

数字证书的应用-证书验证

CFCA

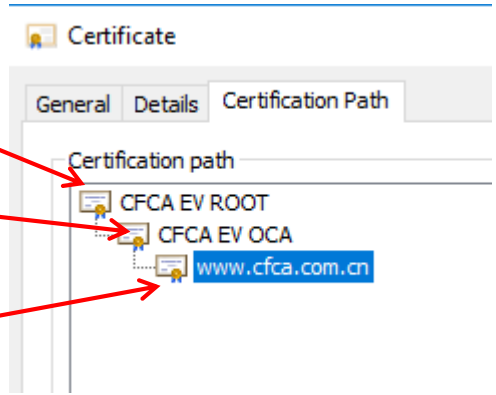
身份证机构链

公安部

派出所

身份证

数字证书链



数字证书的应用-SSL

CFCA

SSL

- Secure Sockets Layer
- 数据保密服务
- 数据完整性服务
- 安全保障的传输协议
- PKI 服务的综合应用

版本

- SSL 3.0
- TLS1.0
- TLS1.1
- TLS1.2
- GM SSL v1.1

数字证书的应用-SSL

CFCA

应用场景

- 网页浏览
- 邮件发送
- 网页助手
- 云访问
- 即时通讯

…

数字证书的应用-SSL

CFCA

某客户端A

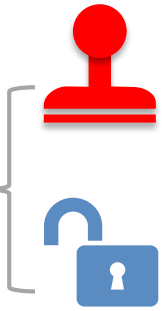
哈希计算

CFCA 服务器

签名验证

信息交互

回话密钥



应用数据

应用数据

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

你好，CFCA

部分密钥参数A

收到请回复

Client Hello →

← Server Hello

你好

部分密钥参数B

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

Server Certificate

请查收并验证

Server Key Exchange

部分密钥参数C

已签名，请查收

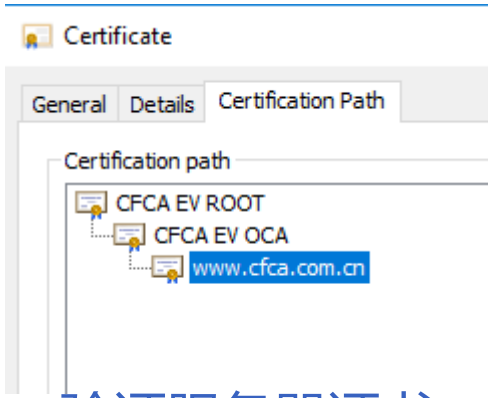
Server Hello Done

回复完毕

请确认并回复

数字证书的应用-SSL

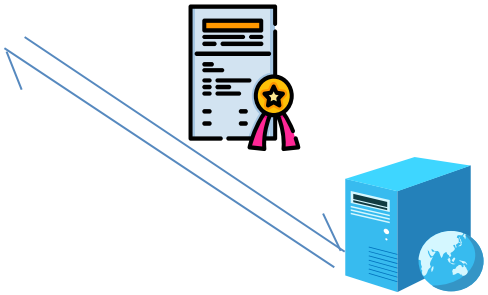
CFCA



CFCA 服务器

验证服务器证书

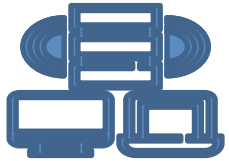
某客户端A



查询证书状态　　目录服务器

数字证书的应用-SSL

CFCA

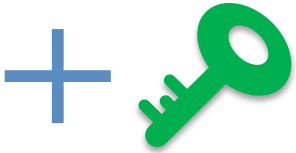


CFCA 服务器

CFCA 服务器证书

某客户端A

密钥参数D

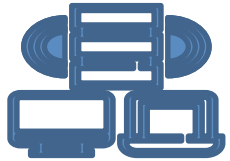


密钥参数D

数字证书的应用-SSL

CFCA

某客户端A



CFCA 服务器

密钥参数D

请查收

Client Key Exchange

将进行加密通信

Change Cipher Spec

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

密钥参数A
密钥参数B
密钥参数C
密钥参数D

消息C-0 Client Finish

Change Cipher Spec

将进行加密通信

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

密钥参数A
密钥参数B
密钥参数C
密钥参数D

密钥参数D

Server Finish

消息S-0

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

怎样算协商成功

回话密钥

应用数据 ⟷ 应用数据

数字证书的应用-SSL

CFCA

某客户端A

CFCA 服务器

数字证书在SSL过程中的
作用是什么？

服务器身份确认

密钥交换

走进神秘的PKI世界-总结

CFCA

- 密码技术
  PKI技术基础
  - 对称密码
    - 相关概念
    - 加解密过程
    - 凯撒加密
    - 密钥交换
  - 非对称密码
    - 产生及算法
    - 加解密过程
    - 强度分析
    - 密钥交换
  - 数字摘要
    - 概念
    - 应用
  - 数字签名
    - 概念
    - 签名过程
    - 验签过程
    - 签名验签 vs 加解密

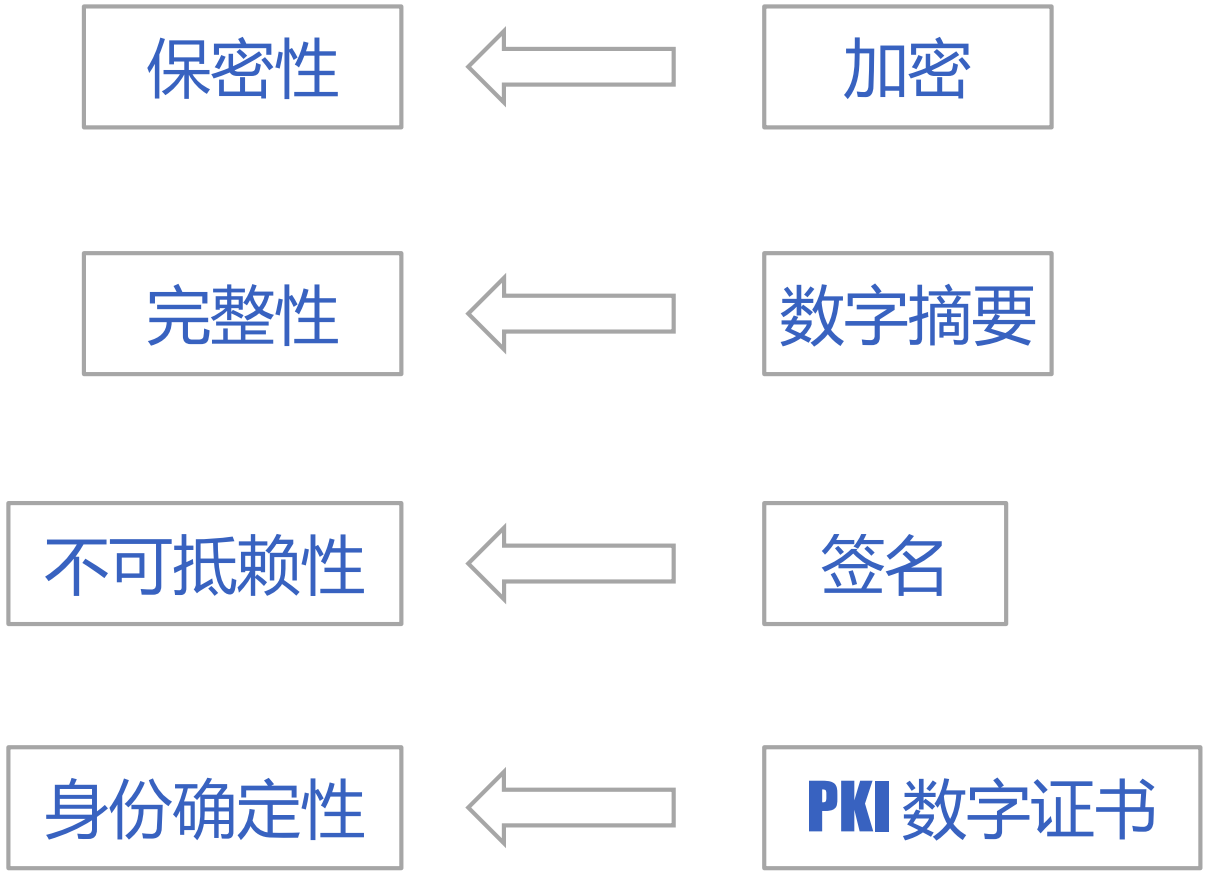
走进神秘的PKI世界-总结

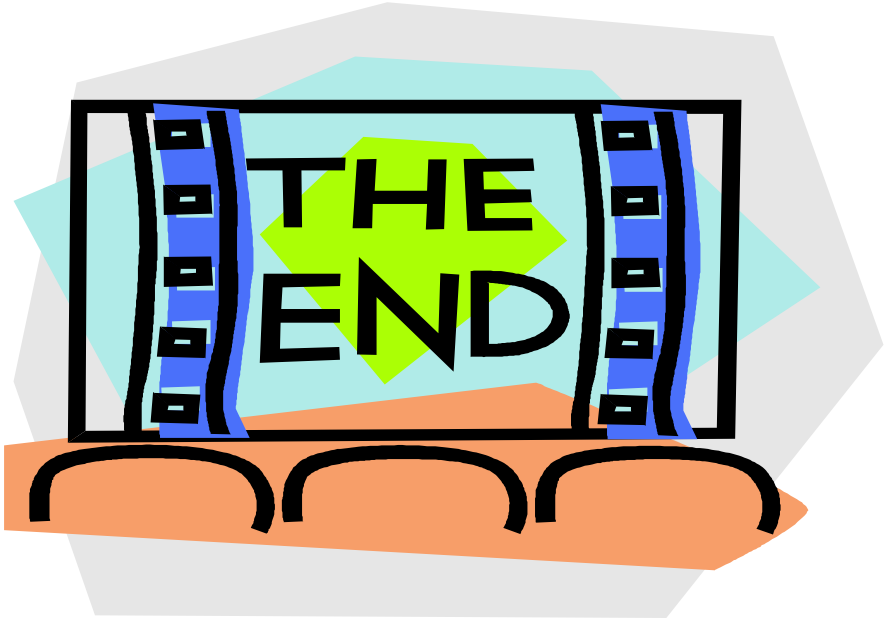
CFCA

- PKI基本概念
  - 定义
  - 组成
    - 硬件软件
    - 标准
  - 结构
    - 系统部署结构
    - 层次结构
- 数字证书
  PKI基本元素
  - 定义
  - 结构
  - 生命周期
    - 证书申请
    - 证书签发
    - 证书吊销
    - 证书冻结及过期
  - 应用举例
    - 证书链验证
    - 证书与SSL

走进神秘的PKI世界-总结

CFCA





Thank you !