商用密码服务——CA与数字证书

主讲人：薛宏开

天津市商用密码行业协会

目录

CONTENTS

01 PKI体系之数字证书

02 PKI体系之CA

03 数字证书基本应用

PKI体系之数字证书

PART. 01

数字证书的定义

数字证书：**通俗的说就是个人或单位甚至是实体在Internet上的身份证**；比较专业的数字证书定义是，数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。

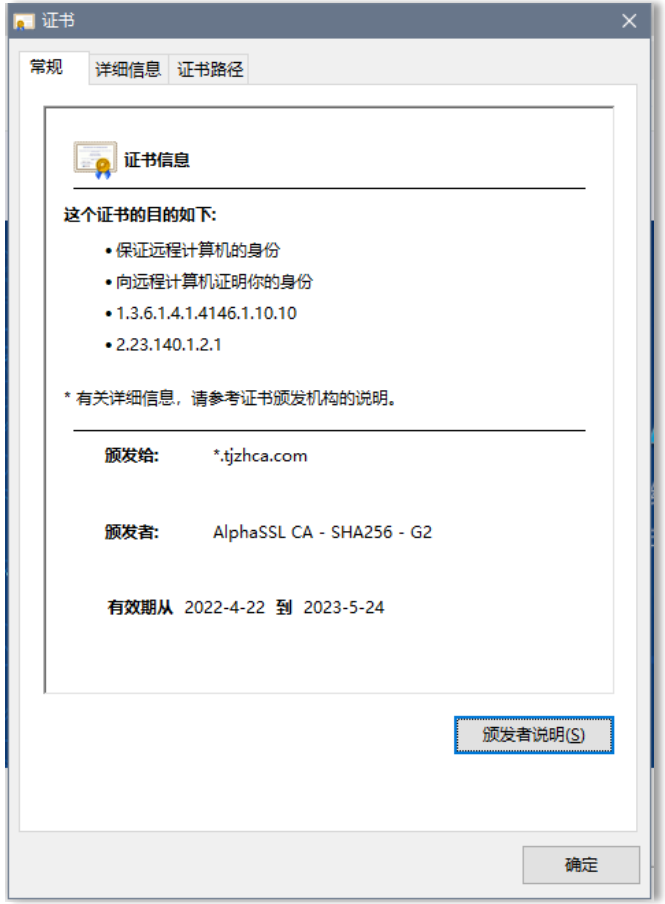
- 电子身份证
- 能够鉴定个人和团体
- 包含相关信息：
  - 姓名、地址、公司、名称、电话号码、 …
- 包含所有者的公钥
- 被可信的第三方验证或者证明有效
  - 由可信的证书颁发机构颁发
- 证书颁发机构的签名可防止擅改证书上的任何资料

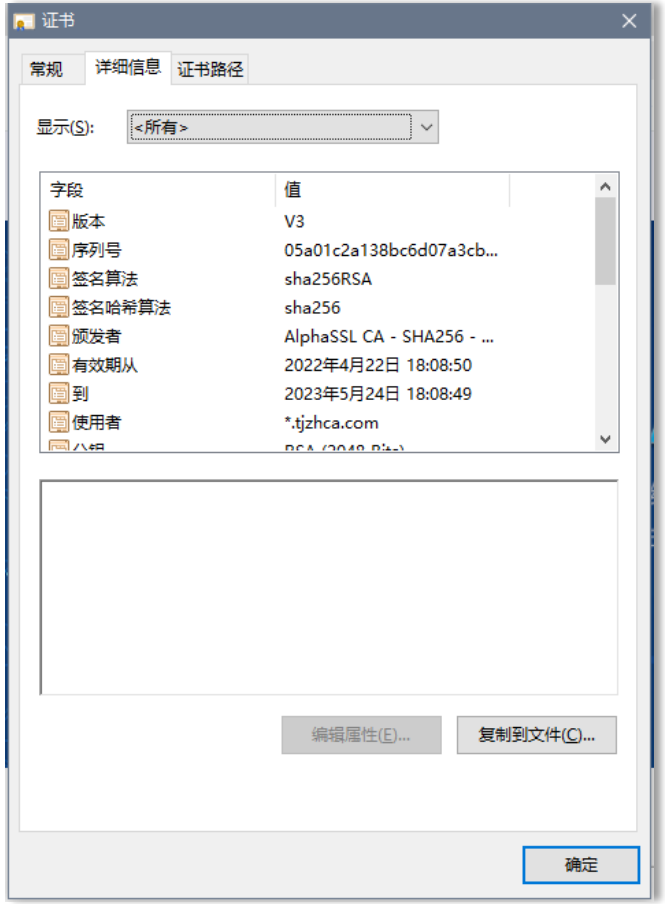
证书类型

- **自签名证书：**又称根证书，是自己颁发给自己的证书，即证书中的颁发者和主体名相同。
- **CA证书：**CA自身的证书。
- **本地证书：**CA颁发给申请者的证书。
- **设备本地证书：**设备根据CA证书给自己颁发的证书，证书中的颁发者名称是CA服务器的名称。

数字证书的基本内容

最简单的证书包含一个公钥、名称以及证书授权中心的数字签名。





数字证书的颁发机构

一个PKI体系由终端实体、证书认证机构、证书注册机构和证书/CRL存储库四部分共同组成。

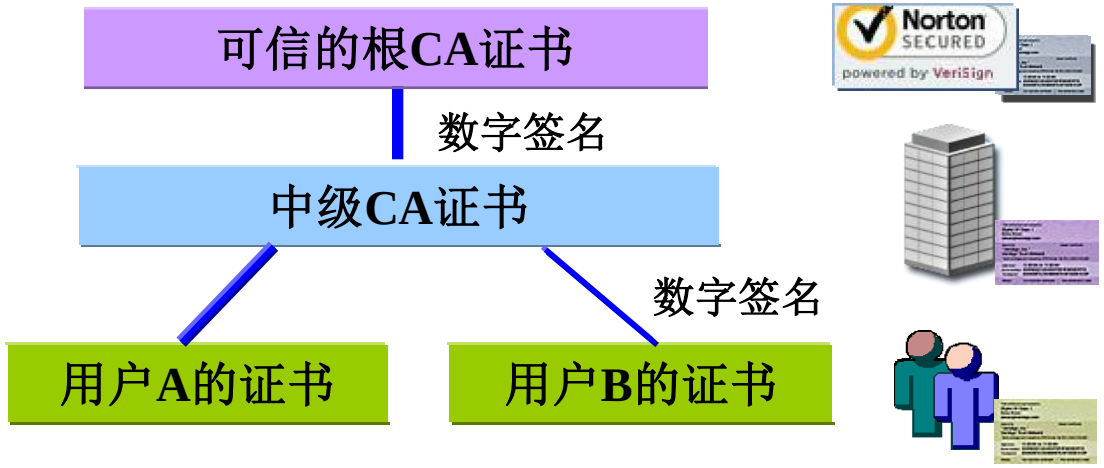
- 证书认证机构CA（ Certificate Authority）

  -CA是PKI的信任基础，是一个用于颁发并管理数字证书的可信实体。它是一种**权威性、可信任性和公正性的第三方机构**。

  - 提供网络身份认证服务
  - 负责签发和管理数字证书
  - 具有权威性和公正性的第三方信任机构
  - 作用类似于颁发证件的公司— 如身份证办理机构
  - 在公开体系下，人人都有CA的公钥（人人信任CA）

数字证书的信任原理--证书链

当某个PKI实体信任一个CA，则可以通过证书链来传递信任，证书链就是从用户的证书到根证书所经历过的一系列证书的合集。当通信的PKI实体收到待验证的证书时，会沿着证书链依次验证其颁发者的合法性。



- **CA建立**证书认证体系
  - 由公正第三方产生可信的根CA证书，用户都相信根CA 证书
  - 由根CA为企业签发中级CA证书
  - 中级CA为下面的用户AB签发用户证书
  - 验证证书有效性时，需要验证其上级CA证书 可验证到最终可信的根CA证书

PKI体系之CA

PART. 02

CA的法律要求

《电子签名法》

第十四条：**可靠的电子签名与手写签名或盖章具有同等的法律效力。**

第十六条：电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

《电子认证服务管理办法》

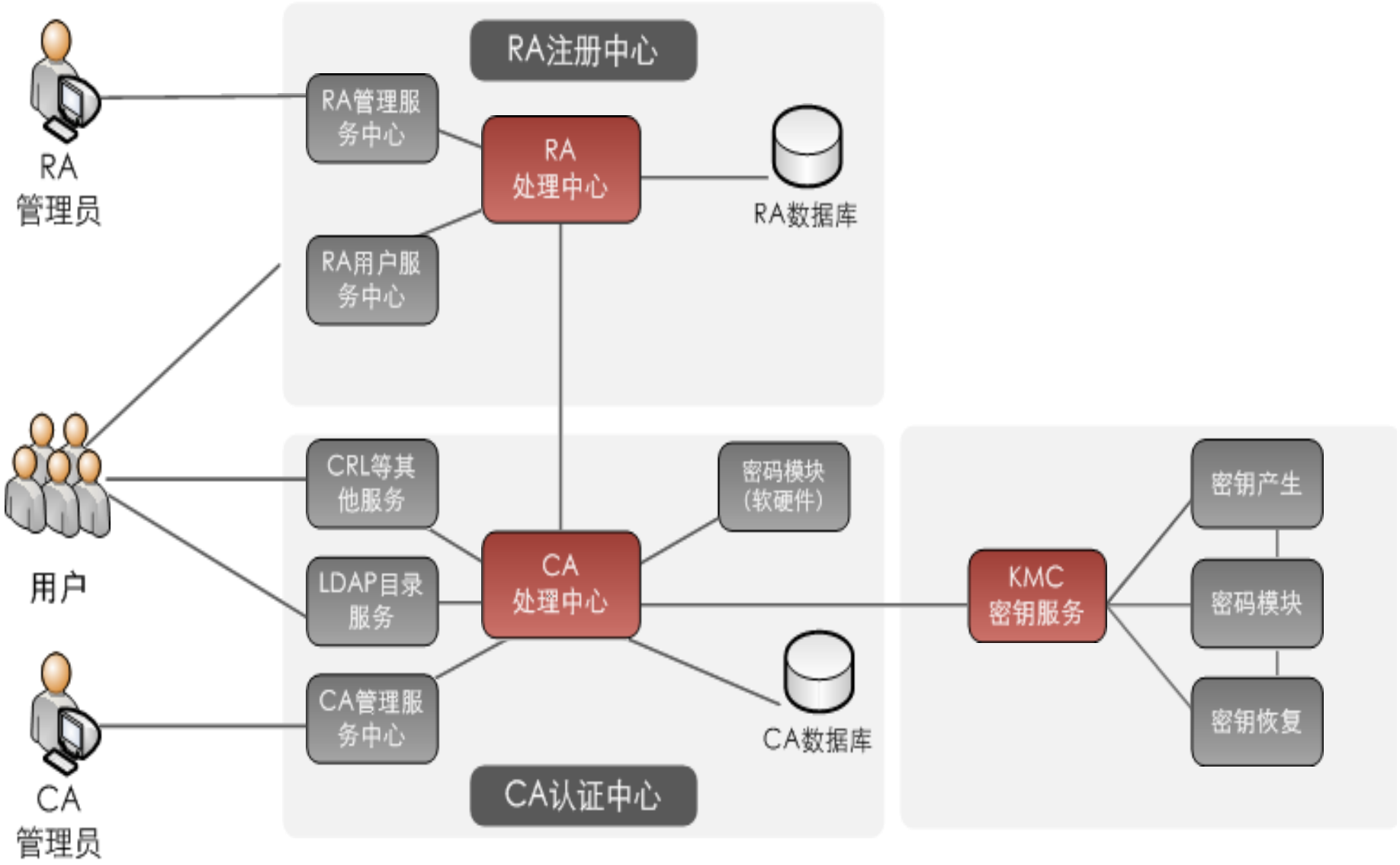
第十六条：电子认证服务机构应当按照公布的电子认证业务规则提供电子认证服务。

第十九条：电子认证服务机构应当建立完善的安全管理和内部审计制度。

第二十条：电子认证服务机构应当遵守国家的保密规定，建立完善的保密制度。

第二十二条：电子认证服务机构受理电子签名认证申请后，应当与证书申请人签订合同，明确双方的权利义务。

CA的典型结构


RA注册中心
RA管理服务中心
RA处理中心
RA数据库
RA用户服务中心
RA管理员
用户
CRL等其他服务
LDAP目录服务
CA处理中心
密码模块(软硬件)
CA管理服务中心
CA数据库
CA认证中心
CA管理员
KMC密钥服务
密钥产生
密码模块
密钥恢复

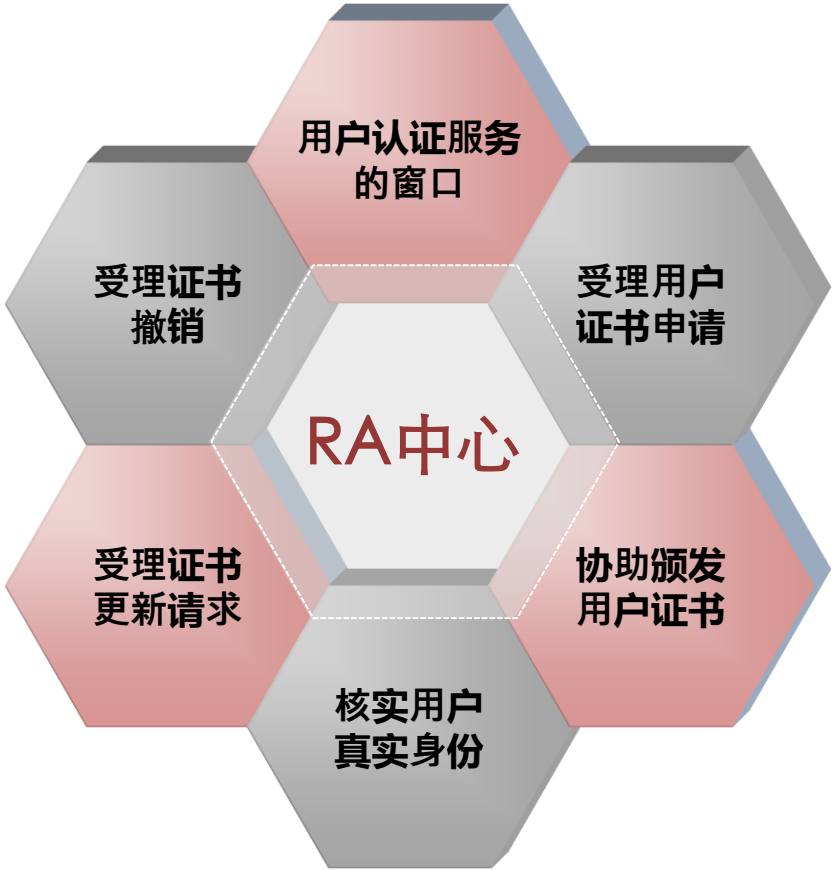
CA中心功能

公安局

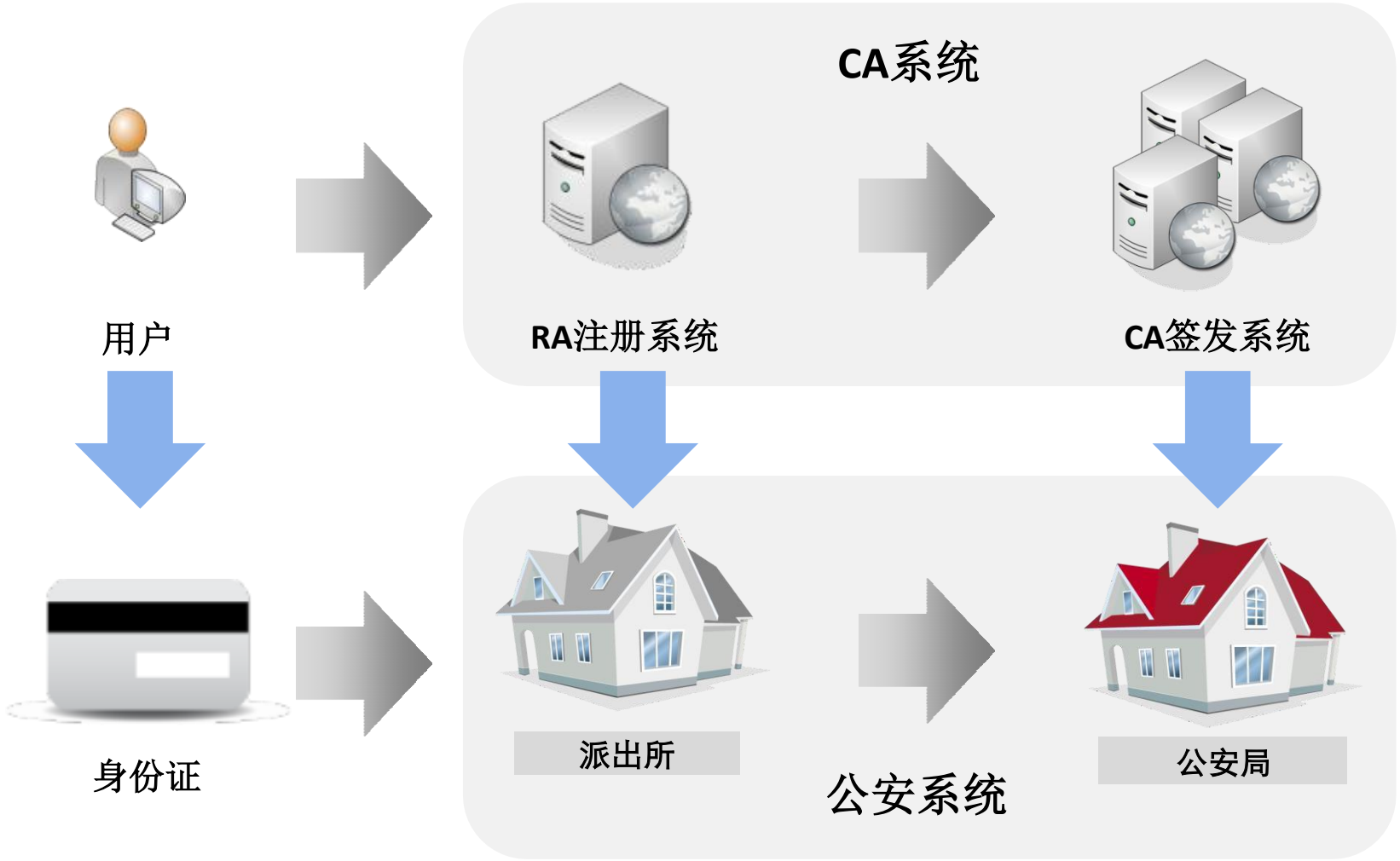
权威性和公正性

RA中心功能

派出所


用户认证服务
的窗口
受理证书
撤销
受理用户
证书申请
RA中心
受理证书
更新请求
协助颁发
用户证书
核实用户
真实身份

CA/RA在CA系统中的作用



数字证书基本应用

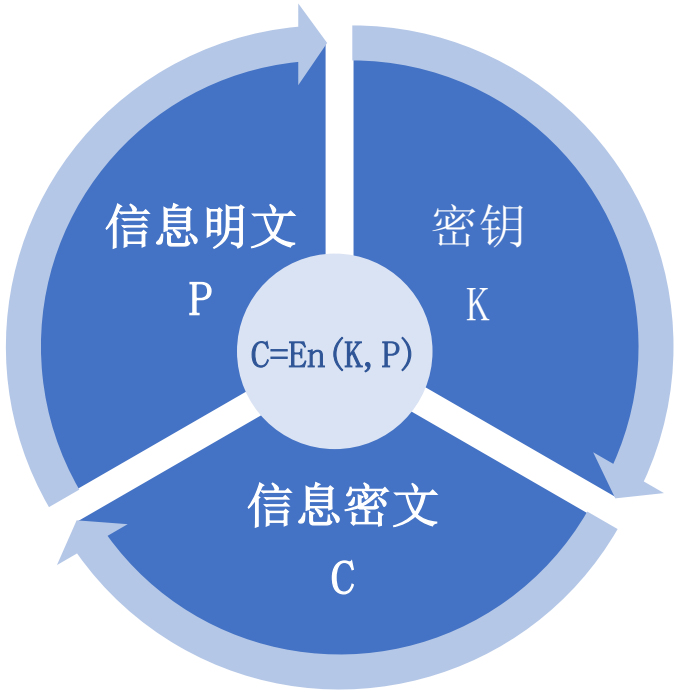
PART. 03

身份认证

身份认证服务提供一种**鉴别实体真伪**的方法。由于数字证书在申请时身份已经得到发证机构确认，所以把数字证书用于应用系统对用户的身份认证是非常合适的。在应用中集成数字证书进行身份认证时，主要是验证用户是否拥有证书对应的私钥，即**验证用户私钥对一段特定数据的签名是否正确。**

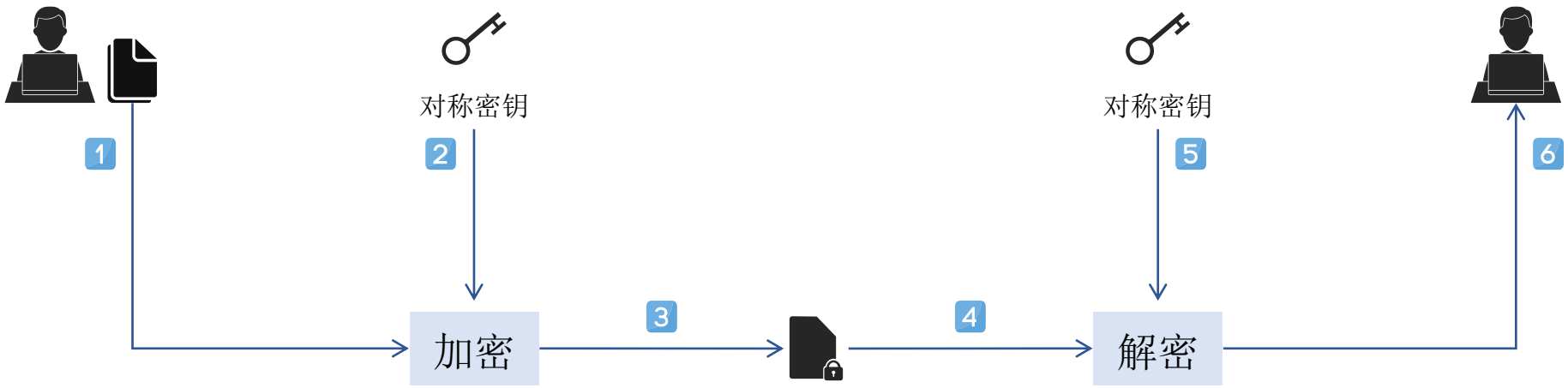
保密性（加解密）

保密性是对数据进行加密的操作，使数据只能被授权的实体看到。使用数字证书中的公钥对静态数据（如文档）或动态数据（如交易报文）进行加密，只有持证人才能使用对应的私钥进行解密，从而实现各种敏感数据的保密性。



	优点	缺点
对称加密	**加解密速度快**	密钥分发问题
非对称加密	**密钥安全性高**	加解密对速度敏感

保密性（加密算法）



对称加密算法

甲与乙事先协商好对称密钥，具体加解密过程如下：

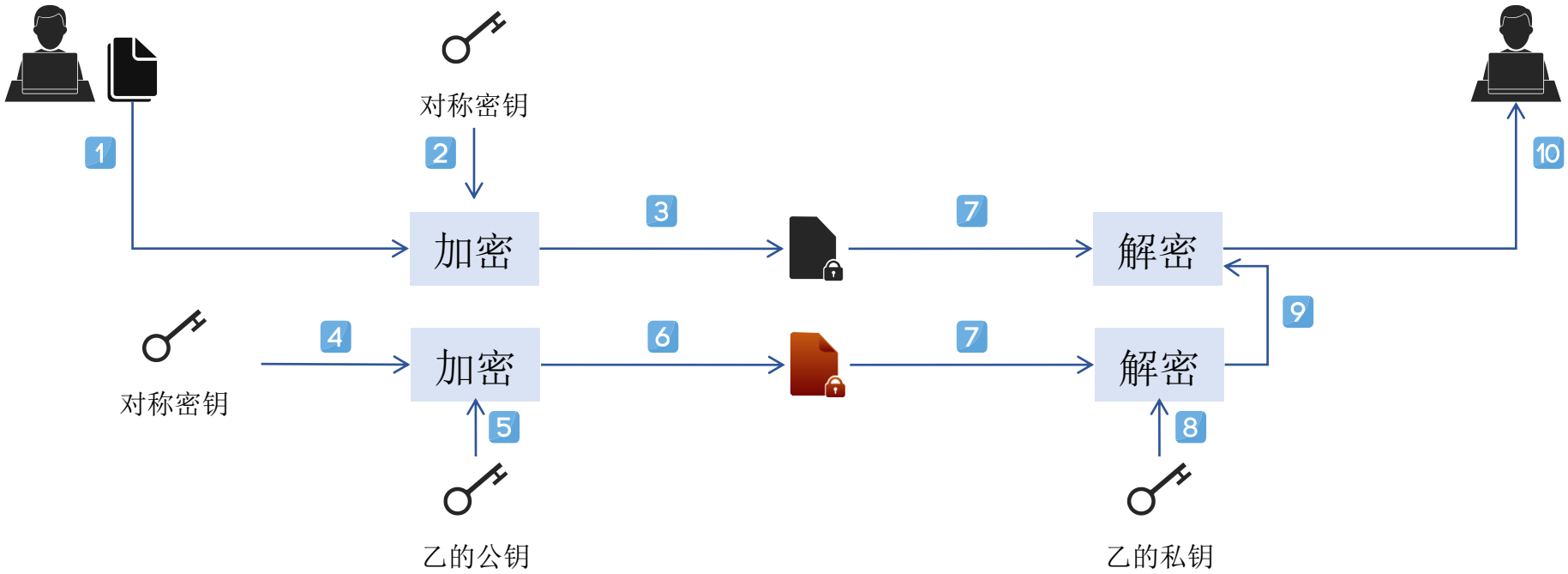
- 甲使用对称密钥对明文加密，并将密文发送给乙。
- 乙接收到密文后，使用对称密钥对密文解密，得到最初的明文。

非对称加密算法

甲事先获得乙的公钥，具体加解密过程如下：

- 甲使用乙的公钥对明文加密，并将密文发送给乙。
- 乙收到密文后，使用自己私钥对密文解密，得到最初的明文。

保密性（数据加密）



甲事先获得乙的公钥，具体加解密过程如下：

- 甲使用对称密钥对明文加密，生成密文信息；
- 甲使用乙的公钥加密对称密钥，生成数字信封；
- 甲将数字信封和密文信息一起发送给乙；
- 乙接收到甲的加密信息后，使用自己的私钥打开数字信封，得到对称密钥；
- 乙使用对称密钥对密文信息进行解密，得到最初明文。

完整性（签名验证）

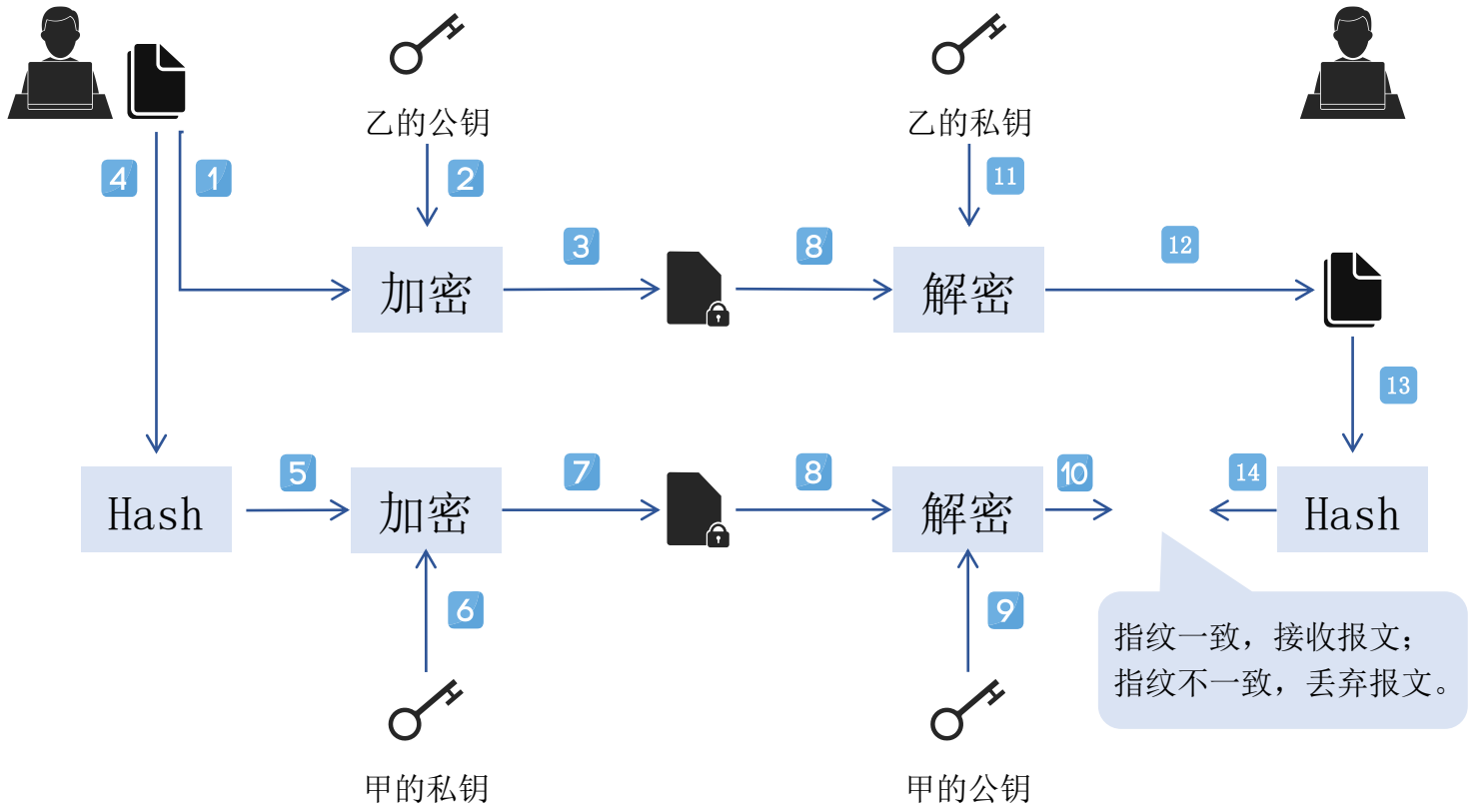
完整性是指在传输、存储信息或数据的过程中，**确保信息或数据不被未授权地篡改或在篡改后能够被迅速发现**。

- 应用场合
  - 发送签名邮件
  - 验证签名邮件

完整性（数字签名）

数字签名是指发送方用自己的私钥对数字指纹进行加密后所得的数据。

数字指纹又称为信息摘要，它是指发送方通过HASH算法对明文信息计算后得出的数据。



甲事先获得乙的公钥，具体加解密过程如下：

- 甲使用乙的公钥对明文加密，生成密文信息；
- 甲使用HASH算法对明文进行HASH运算，生成数字指纹；
- 甲使用自己的私钥对数字指纹进行加密，生成数字签名；
- 甲将密文信息和数字签名一起发送给乙；
- 乙使用甲的公钥对数字签名进行解密，得到数字指纹；
- 乙接收到甲的加密信息后，使用自己的私钥对密文信息进行解密，得到最初的明文；
- 乙使用HASH算法对明文进行HASH运算，生成数字指纹；
- 乙将生成的数字指纹与得到的数字指纹进行比较，如果一致，乙接受明文；如果不一致，乙丢弃明文。

抗抵赖性（时间戳）

抗抵赖提供一种防止实体对其行为进行抵赖的机制，它从技术上保证实体对其行为的认可。由于实体的各种行为只能发生在它被信任之后，所以可**通过时间戳标记和数字签名来审计实体的各种行为**。通过将实体的各种行为与时间和数字签名绑定在一起使实体无法抵赖其行为。

- 应用场合
  - 在实际应用中，经常使用签名和时间戳对要发布的软件进行签名，这样用户安装软件时，就可以对软件的可信性进行验证。一般使用专用签名工具完成带时间戳的签名。

证书有效性验证--验证CA签名

- 将待验证证书设置为当前证书。
- 根据当前证书中签发者信息查询签发者证书，并使用签发者证书验证当前证书中的数字签名是否正确。
- 如果不正确，则待验证证书无效。
- 如果正确且签发者证书是预先确定的可信任CA证书，则说明待验证证书的CA签名正确；否则，将签发者证书设置为当前证书，重复上述步骤

证书有效性验证--验证证书有效期

- 如果待验证证书中notBefore在当前日期之后，则该证书未生效。
- 如果待验证证书中notAfter在当前日期之前，则该证书已过期。
- 否则，该证书处于有效期内。

证书有效性验证--验证证书状态

- 基于CRL验证证书状态
  - 根据待验证证书中扩展项 CRLDistributionPoints信息获得CRL地址，并根据该地址下载CRL文件。
  - 检查CRL文件是否在有效期内，若不在则重新下载。
  - 验证CRL中数字签名是否正确，若不正确则重新下载。
  - 如果CRL中包括待验证证书的序列号，则说明该证书状态为无效；否则说明该证书状态为有效。

- 基于OCSP验证证书状态
  - 将待验证证书的序列号组织成OCSP请求包。
  - 将OCSP请求包发送给OCSP服务器。
  - 从OCSP服务器获得OCSP响应包。
  - 解析OCSP响应包获得该证书的当前状态。

证书有效性验证--验证证书其他属性

- 验证证书密钥用途：KeyUsage、ExtKeyUsage、NetscapeCertType。
- 验证证书策略：CertificatePolicies。
- 其他专用属性。

感谢聆听

天津市商用密码行业协会