石家莊鐵道大學
SHIJIAZHUANG TIEDAO UNIVERSITY

在线开放课程

电子商务技术基础

电子商务安全技术---2

主讲 ： 赵宁

目录

认证技术---数字摘要

- 信息认证的目的
- （1）确认信息的发送者的身份；
- （2）验证信息的完整性，即确认信息在传送或存储过程中未被篡改过。
- **数字摘要：**是采用单向Hash函数对文件中重要元素进行变换运算得到固定长度的摘要码，并在传输信息时将之加入文件一同送给接收方.
- 接收方收到文件后，用相同的方法进行变换运算，若得到的结果与发送来的摘要码相同，则可断定文件未被篡改，反之亦然。

认证技术---数字签名

数字签名是指发送者根据消息产生摘要，并对摘要用自身的签名私钥加密，消息和用自身签名私钥加密的数字摘要组合成数字签名。

把HASH函数和公钥算法结合起来产生的数字签名，可以保障数据完整性、真实性和不可否认性。

数字签名的原理

①被发送文件用安全Hash编码法SHA编码加密产生128bit的数字摘要；

② 发送方用自己的私钥对摘要再加密，形成数字签名；

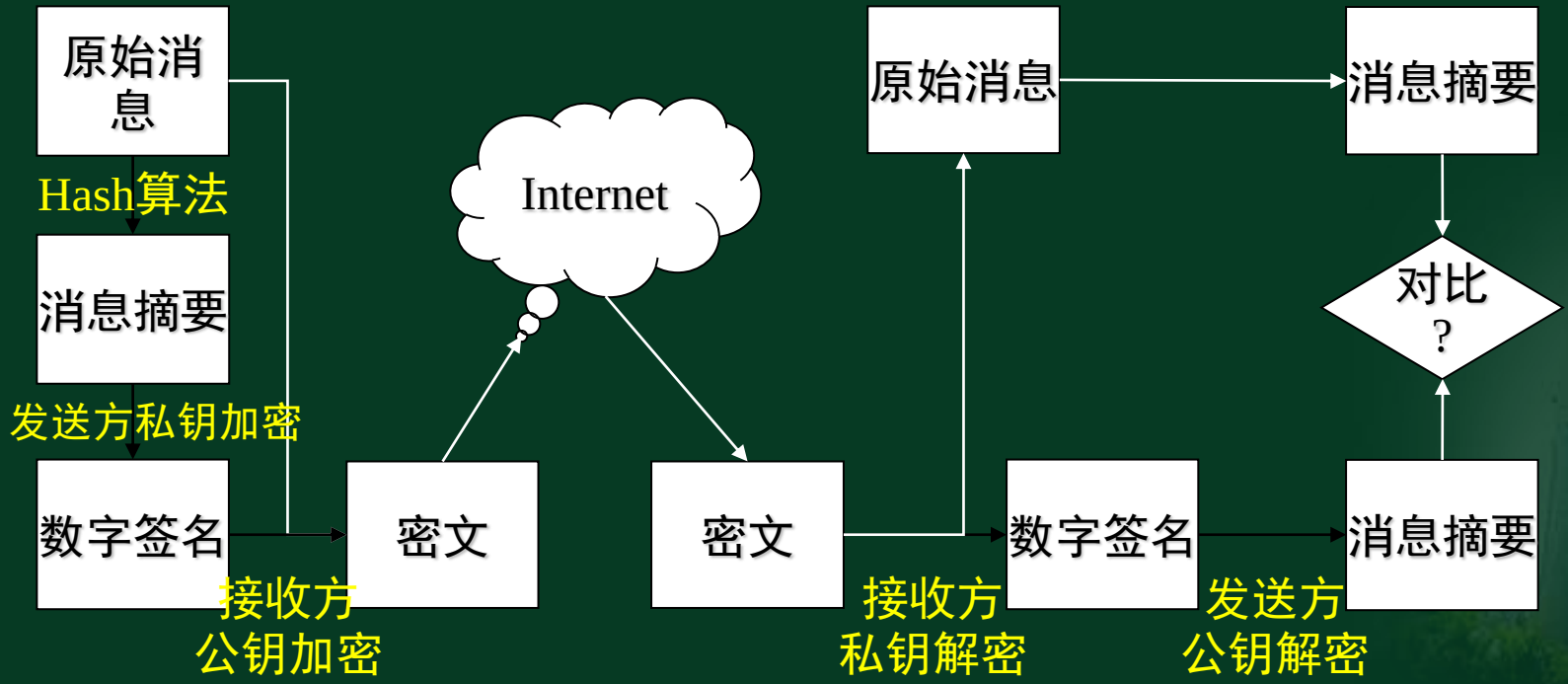
③ 将原文和加密的摘要同时传给对方；

④ 对方用发送方的公共密钥对摘要解密，同时对收到的文件用SHA编码解密产生又一摘要；

⑤ 将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。

数字签名的原理

如两者一致，则说明传送过程中信息没有被破坏或篡改过。否则不然。



例题

- 商户甲使用数字签名技术向商户乙传输合同，甲的私钥是AKD，公钥是AKE，乙的私钥是BKD，公钥是BKE，合同原文是M，摘要是H，数字签名加密算法为D。则商户甲向商户乙传输的数字签名文件是（1）。商户乙应使用（2）验证数字签名的正确性。
- 1. A、 D（M，AKD）　　B、 D（M，AKE）
- 　　C、 D（H，AKD）　　D、 D（H，AKE）
- 2. A、AKD　　B、AKE　　C、BKD　　D、BKE

CA认证系统

- 电子交易过程中必须确认用户、商家及所进行的交易本身是否合法可靠。
- 专门的电子认证中心CA(Certificates Authorities)来核实用户和商家的真实身份以及交易请求的合法性。认证中心将给用户、商家、银行等进行网络商务活动的个人或集团发电子证书。
- SET的认证（CA）
- 在用户身份认证方面，SET引入了证书（Certificates）和证书管理机构机制。

CA认证系统--证书

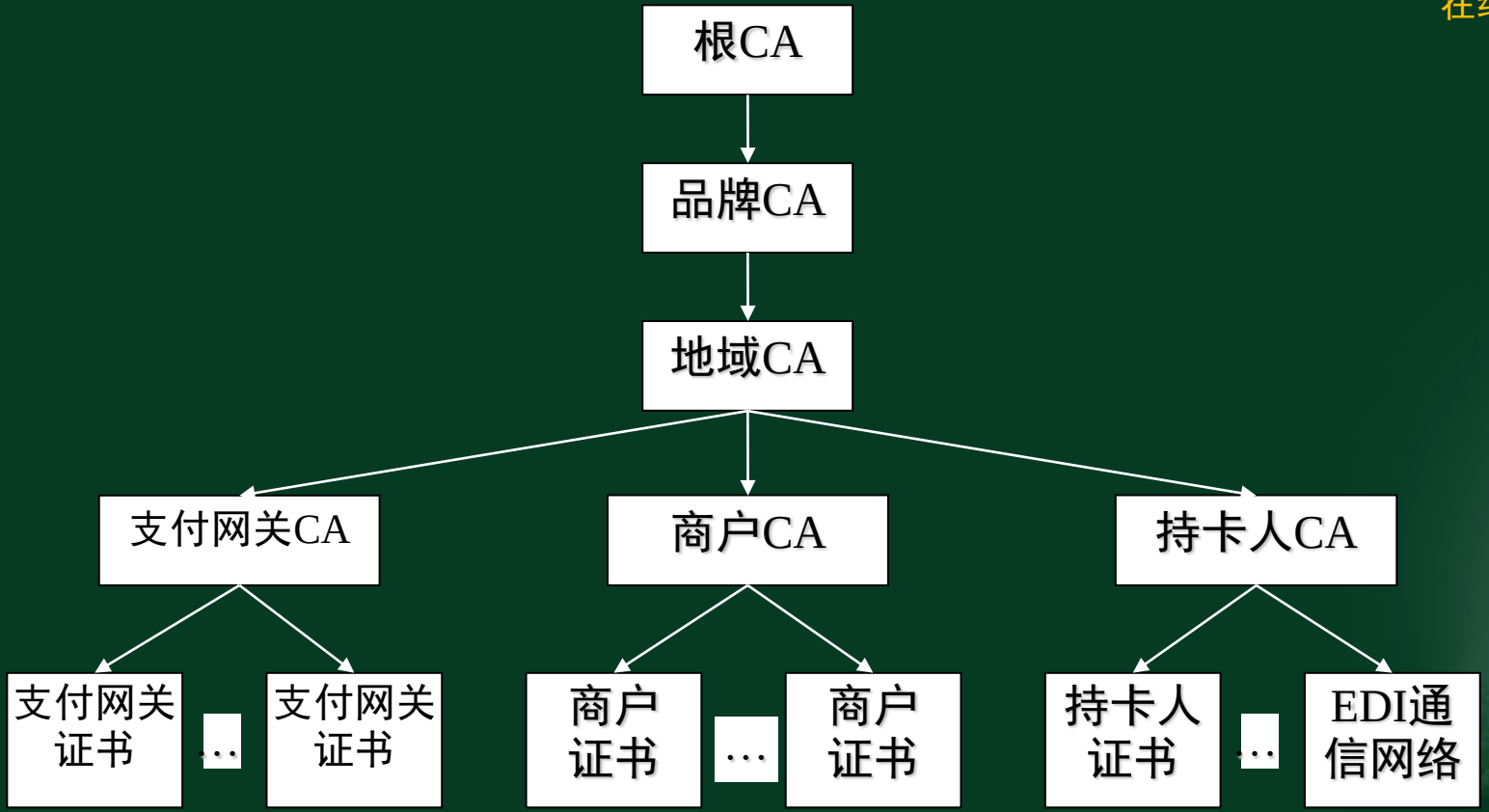
证书就是一份文档，它记录了用户的公共密钥和其他身份信息。在SET中，最主要的证书是持卡人证书和商家证书。

- 持卡人证书：它实际上是支付卡的一种电子化表示。
- 商家证书：表示可接受何种卡来进行商业结算。它是由金融机构签发的，不能被第三方改变
- 除了持卡人证书和商家证书以外，还有支付网关证书、银行证书、发卡机构证书。

CA认证系统--证书

- 2)证书管理机构
- CA是受多个用户信任，提供用户身份验证的第三方机构。证书一般包含拥有者的标识名称和公钥，并且由CA进行过数字签名。
- 3)证书的树形验证结构
- 在两方通信时，通过出示由某个CA签发的证书来证明自己的身份，如果对签发证书的CA本身不信任，则可验证CA的身份，依次类推，一直到公认的权威CA处。

CA认证系统

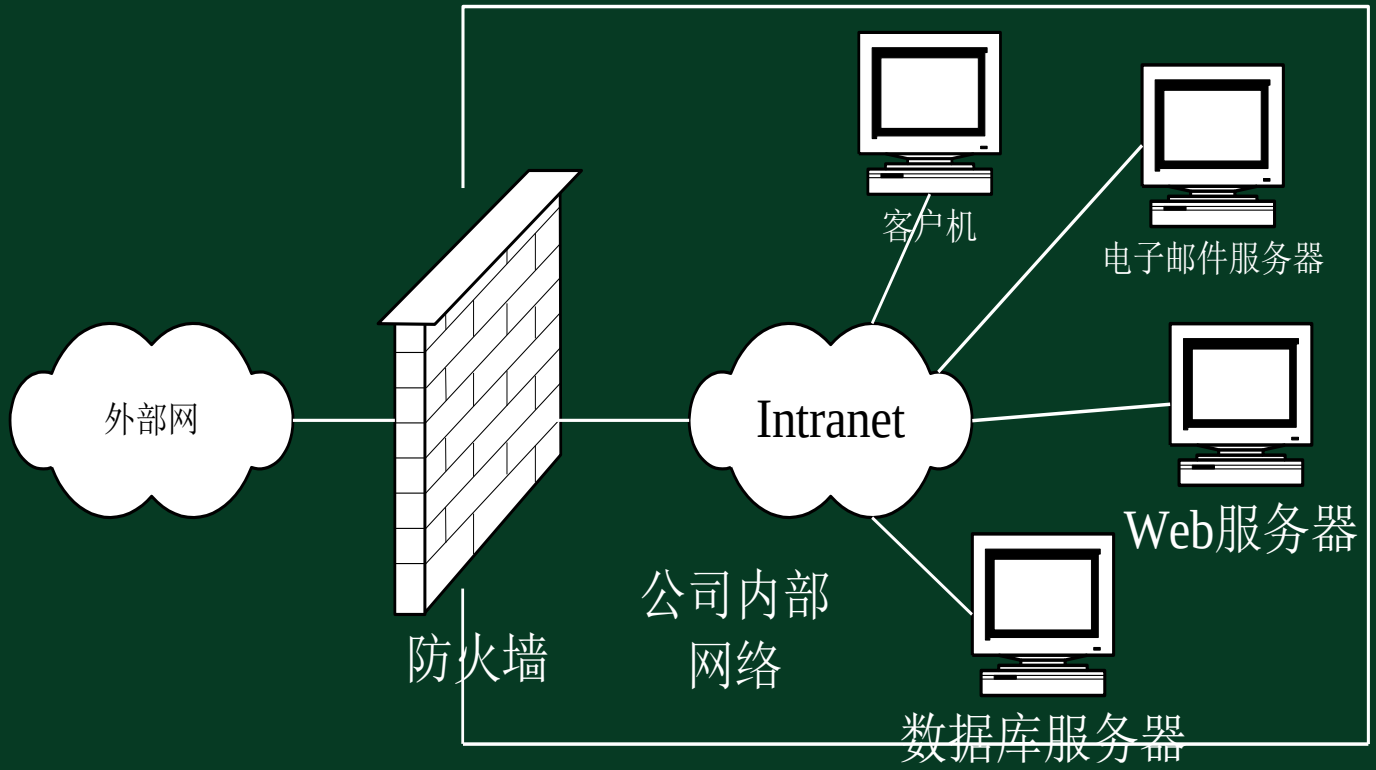

根CA
品牌CA
地域CA
支付网关CA
商户CA
持卡人CA
支付网关证书
…
支付网关证书
商户证书
…
商户证书
持卡人证书
…
EDI通信网络

防火墙技术

防火墙（Firewall）是指一个由软件和硬件设备组合而成，是在内部网和互联网之间构筑的一道屏障，是在内外有别及在需要区分处设置有条件的隔离设备，用以保护内部网中的信息、资源等不受来自互联网中非法用户的侵犯。

要使一个防火墙有效，防火墙必须只允许授权的数据通过，并且防火墙本身也必须能够免于渗透。防火墙系统一旦被攻击者突破或迂回，就不能提供任何的保护了。

防火墙技术



防火墙技术

防火墙系统的构成

防火墙主要包括安全操作系统、过滤器、网关、域名服务和电子邮件处理5部分。

防火墙的安全策略

- 一切未被允许的都是禁止的
- 一切未被禁止的都是允许的

小结

- 本部分在介绍数字摘要的基础上，重点介绍了数字签名及其工作流程，并介绍了CA认证和防火墙技术。