第8章 网络安全协议

罗文坚

主要内容

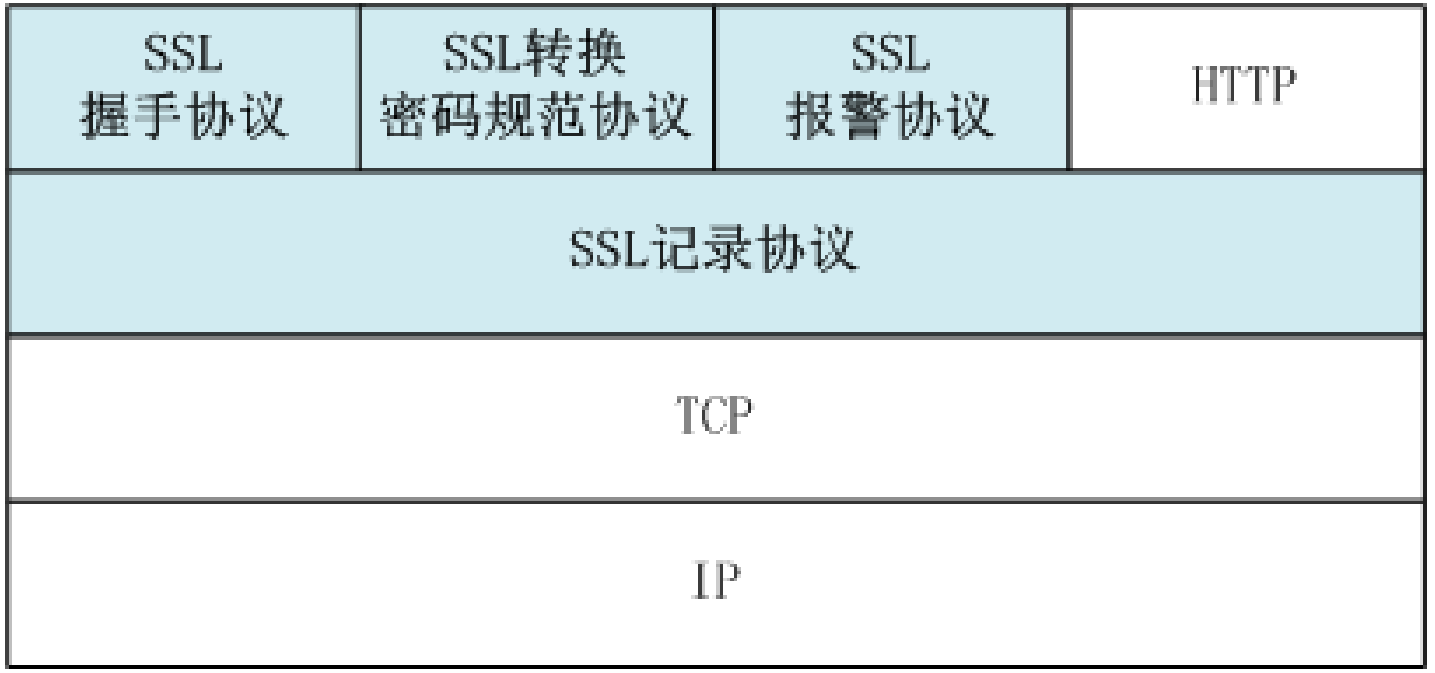
- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
  - 8.3.1 SSL协议的体系结构
  - 8.3.2 SSL协议规范
  - 8.3.3 HTTPS
- 8.4 安全电子交易协议

SSL (Secure Sockets Layer)

- SSL协议是NetScape公司于1994年提出的。
  - 一种保护客户端与服务器之间数据传输安全的加密协议，其目的是确保数据在网络传输过程中不被窃听及泄密。
  - 1996年发布了SSL v3.0，技术上更加成熟和稳定，成为事实上的工业标准，得到了多数浏览器和WEB服务器的支持。
  - 1997年，IETF发布了传输层安全协议TLS v1.0（Transaction Layer Security），可以看成是SSL v3.1。

- SSL协议提供的服务主要有：
  - 认证用户和服务器，确保数据发送到正确的客户机和服务器；
  - 加密数据以防止数据中途被窃取；
  - 维护数据的完整性，确保数据在传输过程中不被改变。

SSL协议的体系结构

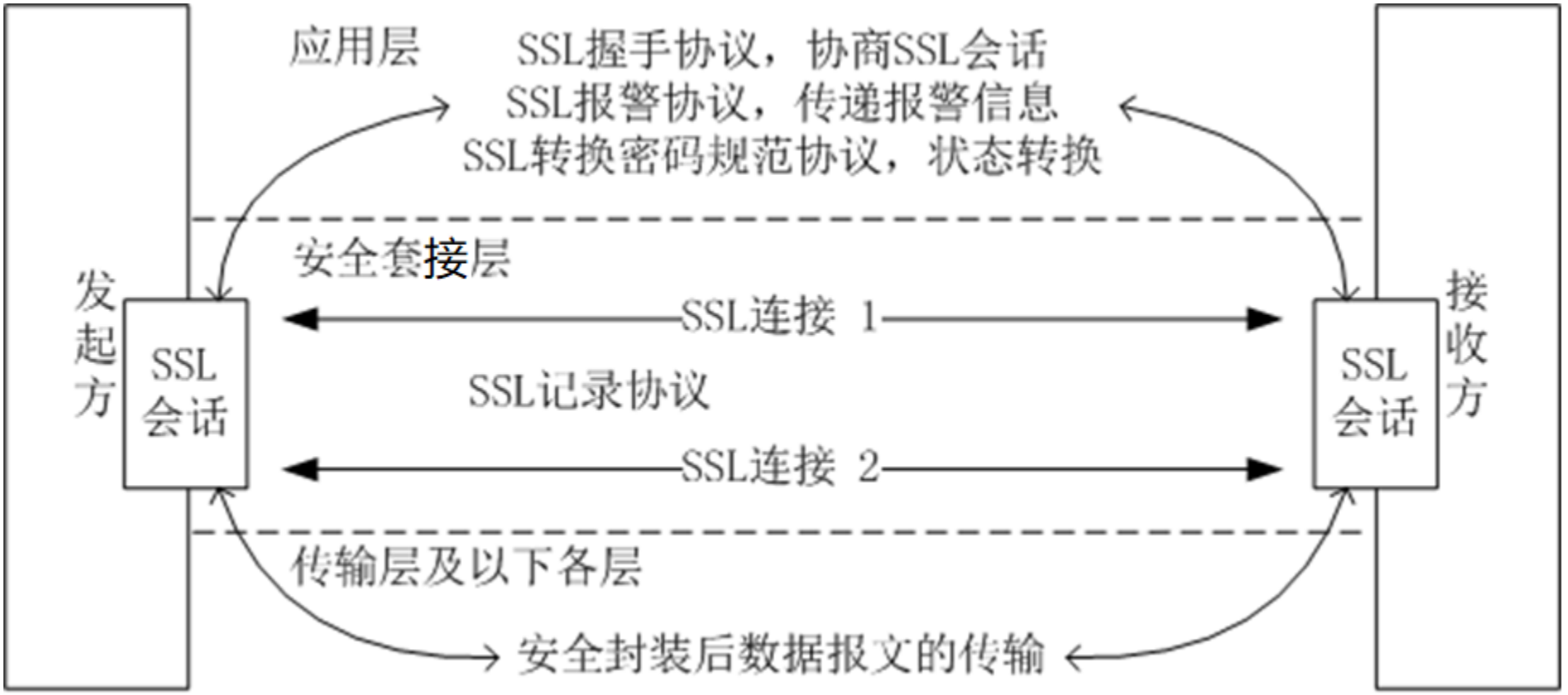


- **SSL协议族由4个协议组成：**
  - 记录协议 **Record Protocol**、握手协议 **Handshake Protocol**、转换密码规范协议 **Change Cipher Spec Protocol**和报警协议**Alert Protocol**。
  - 双层协议：**SSL**记录协议被定义为在传输层与应用层之间，其它三个协议则为应用层协议。

SSL连接和SSL会话

- SSL协议的双层协议构建了一个完整的通讯结构：
  - 应用层的三个协议用于构建安全环境；
  - 下层的SSL记录协议则完成数据的安全封装。
- 构建安全环境涉及两个重要的概念，即SSL连接和SSL会话。
  - SSL连接表示的是对等网络关系，即发起方（客户端）与接收方（服务器）之间的一条位于传输层之上的逻辑链路关系，具体的传输依靠其下层协议实现。
    - 连接是暂时的，使用结束之后即刻释放。
    - 连接依赖于一定的规范，而这些规范会在一个会话中被描述，即每个连接与一个会话有关。
  - SSL会话是发起方和接收方之间的安全关联，它描述了一个（或多个）连接共享的安全参数集合。
    - 会话是SSL握手协议创建的，一个会话可以为多个连接共享。

SSL连接和SSL会话



SSL连接和SSL会话

- SSL会话与多种状态相关，状态可以理解为描述特定过程的特征信息集合。
- SSL协议中，最主要的两个状态就是会话状态和连接状态。
- 会话状态包含标识会话特征的信息和握手协议的协商结果，用来描述一个SSL会话的特征参数。
- 连接状态包含客户端和服务器在传输过程中使用的加密密钥、MAC密钥、初始化位移量、一些客户端和服务器选择的随机数，主要用来描述与一个SSL连接相关联的特征参数。
  - 客户端和服务器只需在一个连接存在时记录该连接的状态，连接状态提供的参数为SSL记录协议层使用。

SSL会话状态参数定义

字段名	定义
会话标识（Session Identifier）	服务器选择的一个任意字节序列，用以标识一个活动的或可激活的会话。
对等证书（Peer Certificate）	用于鉴别实体身份的一个X.509.v3的证书，可为空。
压缩算法（Compression Method）	加密前进行数据压缩的算法。
密码规范（Cipher Spec）	指明数据加密的算法（无，或DES等）以及计算MAC的散列算法（如MD5或SHA-1），还包括其它参数，如散列长度。
主密钥（Master Secret）	48位密钥，在client与server之间共享。
可恢复性（Is Resumable）	指明该会话是否可被用于初始化一个新连接。

SSL连接状态参数定义

字段名	定义
服务器和客户端随机数	server 和 client 为每一个连接所选择的字节序列。
服务器写MAC密码	一个密钥，用于对server 送出的数据进行MAC操作。
客户端写MAC密码	一个密钥，用于对client送出的数据进行MAC操作。
服务器写密钥	用于server 进行数据加密，client进行数据解密的对称密钥。
客户端写密钥	用于client 进行数据加密，server进行数据解密的对称密钥。
初始化位移量IV	当数据加密采用CBC方式时，每一个密钥保持一个IV。该字段首先由SSL Handshake Protocol初始化，以后保留每次最后的密文数据块作为IV。
序列号	每一方为每一个连接的数据发送与接收维护单独的顺序号。当一方发送或接收一个改变的cipher spec message时，序号置为0，然后递增，最大$2^{64}-1$。

待用状态和当前操作状态

- SSL会话还定义了当前操作状态和待用状态。

- 当SSL握手协议建立起SSL会话后，会话进入了当前操作状态。
  - 当前操作状态包含了当前SSL记录协议正在使用的压缩算法、加密算法和MAC算法以及加、解密的秘钥等参数。

- 当一个连接结束时，SSL会话又从当前操作状态进入待用状态。
  - 待用状态包含了之前握手协议协商好的压缩算法、加密算法和MAC算法，以及用于加、解密的秘钥等参数。

- 因此，SSL会话从建立开始不断地在当前操作状态和待用状态之间切换，直到该会话结束。

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
  - 8.3.1 SSL协议的体系结构
  - 8.3.2 SSL协议规范
  - 8.3.3 HTTPS
- 8.4 安全电子交易协议

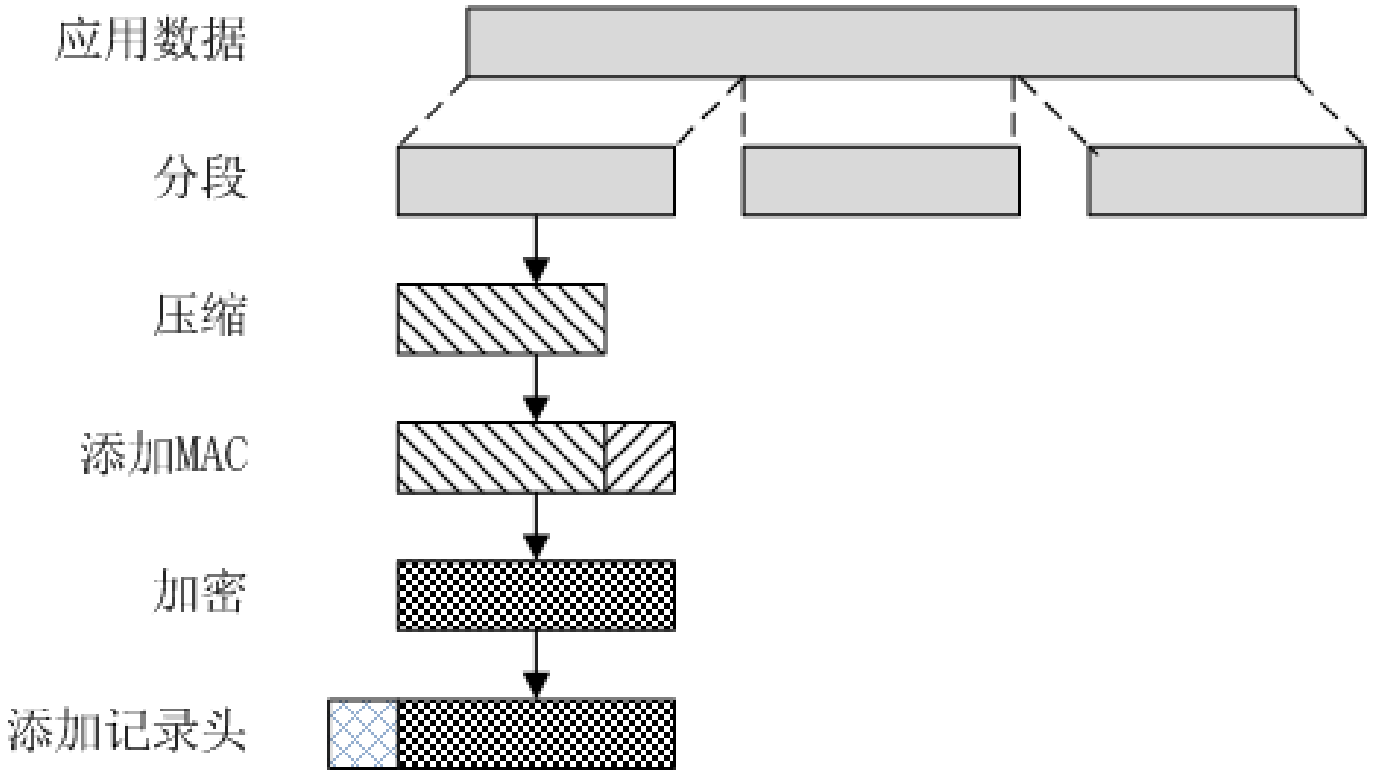
SSL记录协议

- SSL记录协议为SSL连接提供了两种服务。
  - 保密性：握手协议定义了共享的、可用于对SSL有效载荷进行常规加密的秘钥。
  - 消息完整性：握手协议定义了共享的、可用来形成报文的鉴别码（MAC）的秘钥。

- SSL记录协议的功能是根据当前会话状态指定的参数以及连接状态中指定的参数等内容，对当前的连接中要传送的高层数据实施压缩与解压缩、加密与解密、计算与校验MAC等操作。

SSL记录协议

- SSL记录协议对应用层数据文件的处理过程分为5个步骤。



SSL记录协议的操作

SSL记录格式

- 完整的SSL记录格式包括六个部分。

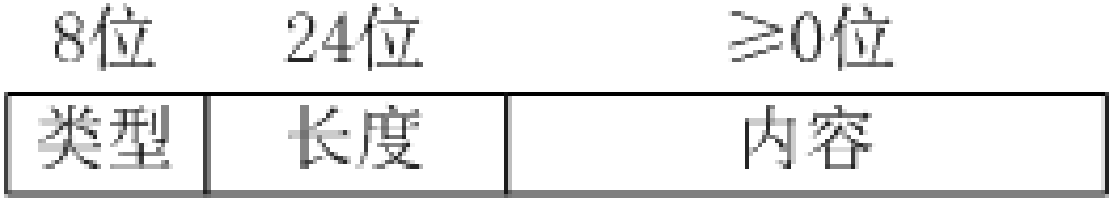
a. SSL记录协议

SSL记录格式

- 内容类型（8位）：用来指明封装数据的类型， 已定义的类型包括转换密码规范协议、报警协议、握手协议和应用数据四类。
- 主版本（8位）：指明SSL使用的主版本。
- 从版本（8位）：指明SSL使用的从版本。
- 压缩长度（16位）：明文负载（如压缩，则为压缩后负载）的字节长度。
- 负载（可变）：指待处理的明文数据经过压缩（可选）、加密后形成的密文数据。
- MAC（16或20字节）：针对压缩后的明文数据进行计算得到的消息认证码。
  - 如基于SHA-1进行计算时，MAC的长度为20个字节；基于MD5进行计算时，MAC的长度为16个字节。

SSL握手协议

- **SSL握手协议的作用：**
  - 用于建立会话、协商加密方法、鉴别方法、压缩方法和初始化操作；使服务器和客户能够相互鉴别对方的身份、协商加密和MAC算法；用来保护在SSL记录中发送数据的加密密钥。
- SSL握手协议的内容作为SSL记录协议的负载，包含在SSL记录中，其报文格式主要包括以下三个字段：
  - 类型（1字节）：为10种报文类型中的一种。
  - 长度（3字节）：以字节为单位的报文长度。
  - 内容（大于等于1字节）：与报文类型相关的参数。



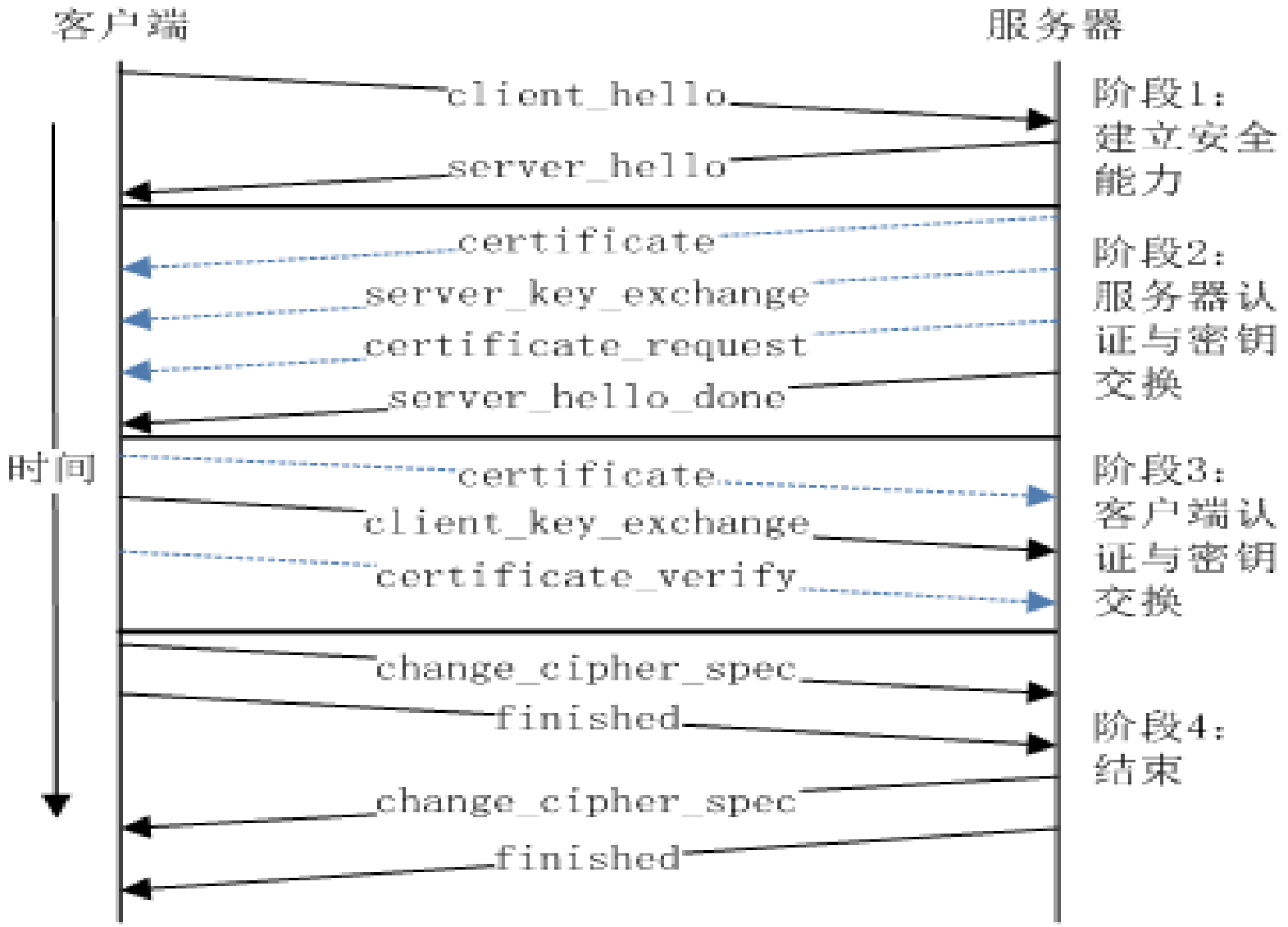
b. 握手协议

SSL握手协议的报文类型

报文类型	报文内容
hello_ request	空
client_hello	版本、随机数、会话 ID、密码规范、压缩方法
server_hello	版本、随机数、会话 ID、密码规范、压缩方法
certificate	X. 509v3 证书链
server_key_exchange	参数、签名
certificate_request	类型、授权
server_done	空
certificate_verify	签名
client_key_exchange	参数、签名
finished	散列值

SSL握手协议操作的整个过程

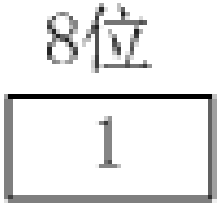
- SSL握手协议通过在客户端和服务器之间传递消息报文，完成会话协商谈判。



SSL转换密码规范协议

- 目的是通知对方将已挂起（或新协商）的状态复制到当前状态中，用于更新当前连接使用的密码规范。

- 协议报文包含1个字节的信息，值为1表示更新使用新的密码规范。

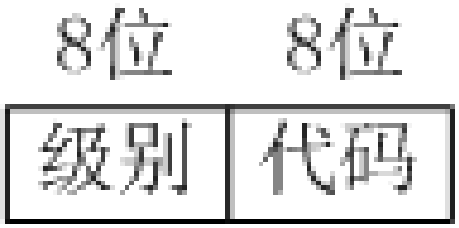


c. 转换密码规范协议

SSL报警协议

- 报警协议是用来将SSL传输过程中的警报信息传送给对方。
  - 报警协议内容作为SSL记录协议的负载被包含在SSL记录中，并按照会话的当前操作状态指定的方式进行压缩和加密。

- 该协议的每个报文由两个字节组成。
  - 第一个字节的值是警报级别，分为致命错误和警告两级。
    - 如果级别是致命错误，SSL将立刻中止该连接。
  - 第二个字节给出特定警报的代码信息。



d. 报警协议

SSL报警协议

- 致命错误：
  - 意外消息：接收到不正确的信息；
  - MAC记录出错：接收到不正确的MAC；
  - 解压失败：解压函数接收到不正确的输入；
  - 握手失败：双方无法在给定的选项中协商出可以接受的安全参数集；
  - 非法参数：握手消息中的某个域超出范围或与其他域出现不一致性。

SSL报警协议

- 警告类型
  - 结束通知：通知对方将不再使用此连接发送任何信息；
  - 无证书：如果无适当证书可用，此消息可作为对方证书请求的响应发送；
  - 证书出错：证书被破坏，签名无法通过验证；
  - 不支持的证书：不支持接收到的证书类型；
  - 证书撤销：该证书被其签名者撤销；
  - 证书过期：证书超过使用期限；
  - 未知证书：处理证书时，出现其他错误，证书无法被接受。

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
  - 8.3.1 SSL协议的体系结构
  - 8.3.2 SSL协议规范
  - 8.3.3 HTTPS
- 8.4 安全电子交易协议

HTTPS

- Netscape提出了HTTPS协议，用于解决HTTP协议的安全性问题。
  - 简单讲是HTTP的安全版，在HTTP下加入SSL协议。

- SSL一般以两种形式出现：
  - 一是将SSL嵌入到操作系统内核，其安全机制对所有上层应用软件透明；
  - 二是在应用层以函数库形式出现，应用程序的通信部分源码需要按照SSL通信协议格式规范来编写，并连接SSL函数库，编译生成可执行代码。
  - 第一种形式实现SSL具有层无关特性，较为实用，HTTPS也是基于此方式实现的。

HTTPS

- HTTPS的思想：
  - 客户端向服务器发送一个连接请求，然后双方协商一个SSL会话，并启动SSL连接，接着就可以在SSL的应用通道上传送HTTPS数据。
  - 注意：HTTPS使用与传统HTTP不同的端口，IANA（Internet Assigned Numbers Authority）将HTTPS端口定为443，以此来区分非安全HTTP的80端口，同时采用“https”来标识协议类型。
- HTTPS的主要作用：
  1. 建立一个信息安全通道，用来保证数据传输的安全；
  2. 确认网站服务器和客户端的真实性，这就需要CA证书及认证服务。
     - HTTPS的身份认证可分为单向身份认证和双向身份认证。

HTTPS

- 单向身份认证：通过验证服务器的CA证书来核实其身份，为多数非电子商务交易服务所采纳。
- 双向身份认证：多应用于电子商务交易中。

- 在HTTPS服务中，CA证书的认证非常重要，主要体现在两方面：
  - 服务器的信任问题；
  - 客户端的信任问题。

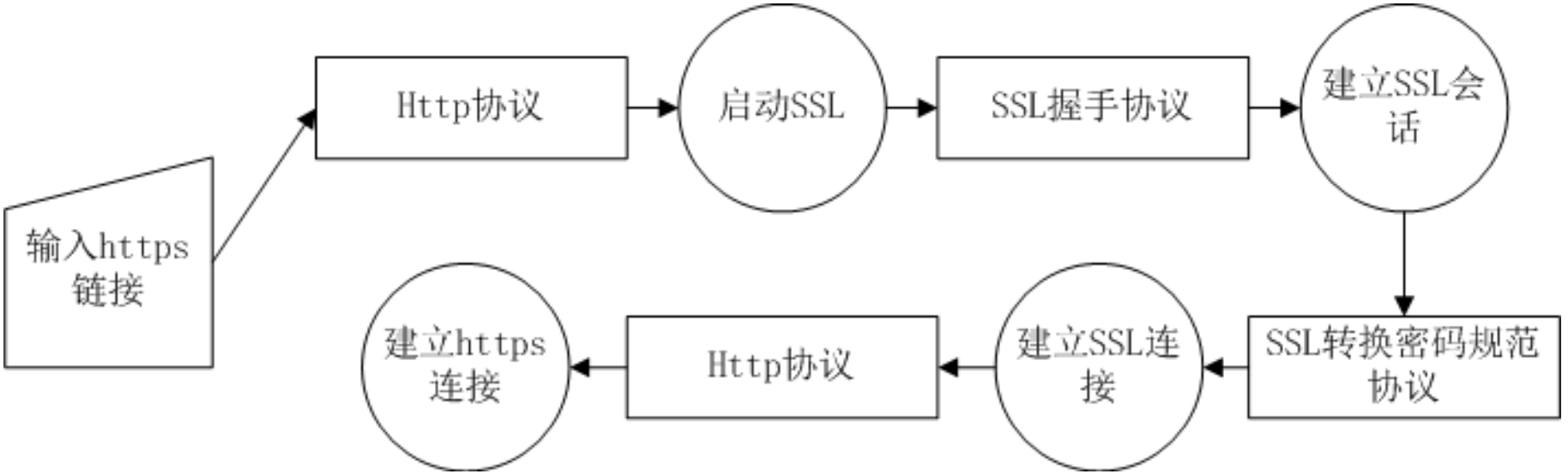
- 服务器的信任必须依靠CA证书解决：
  - HTTPS 的服务器必须从CA认证服务中心申请得到一个用于证明服务器身份的证书；
  - 只有服务器能够提供该证书时候，客户端完成对CA证书的验证，才能信任此服务器。

HTTPS

- 在一些电子商务交易过程中，有时也会要求客户端提供有效的CA证书，以保证电子交易的有效性。

- 目前，多数用户的CA证书都是备份在U盘（即U盾中），并经过特殊的强加密处理及相应的密码身份验证来确保其安全性。

- HTTPS协议处理过程：



主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议
  - 8.4.1 电子商务安全
  - 8.4.2 SET协议概述
  - 8.4.3 SET的安全机制
  - 8.4.4 交易处理
  - 8.4.5 SET与SSL的比较

安全电子交易协议

- SET（Secure Electronic Transaction），Visa和MasterCard发起，联合IBM、Microsoft、Netscape、GTE等公司，于1997年6月1日推出的用于电子商务的行业规范。

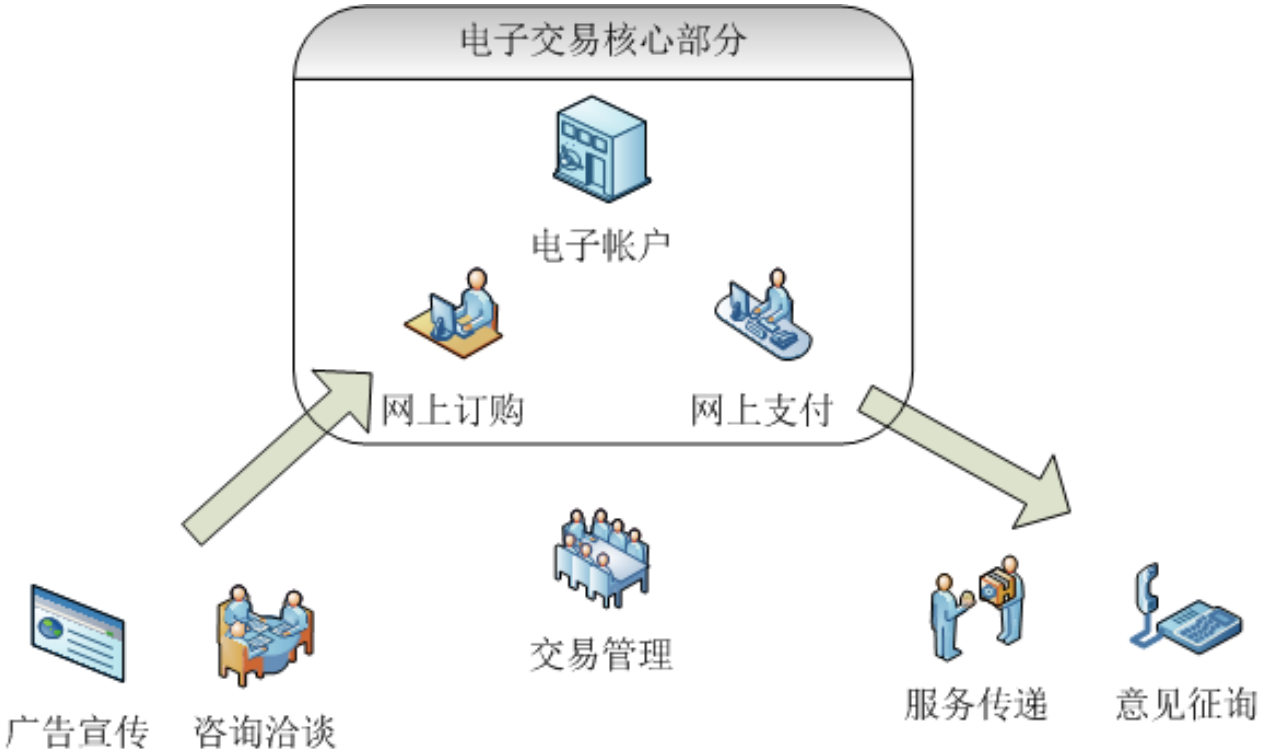
- SET是一种应用在Internet上、以信用卡为基础的电子付款系统规范，目的是为了保证网络交易的安全。

- SET妥善地解决了信用卡电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。

- SET已获得IETF标准的认可，是电子商务的发展方向。

电子商务安全

- 电子商务（Electronic Commerce），以网络技术为手段、以商务为核心，把销售、购物渠道移到互联网上来，打破国家与地区的壁垒，使销售达到全球化、网络化、无形化。
- 电子商务提供网上交易和管理等全过程的服务，包括广告洽谈、网上交易和服务传递三部分，其中网上交易是其核心。



安全问题及安全技术

- 面临的安全问题
  - 有效性
  - 真实性
  - 机密性
  - 不可否认性

- 安全技术
  - 网络安全技术
  - 加密技术
  - 认证技术
  - 安全协议

主要内容

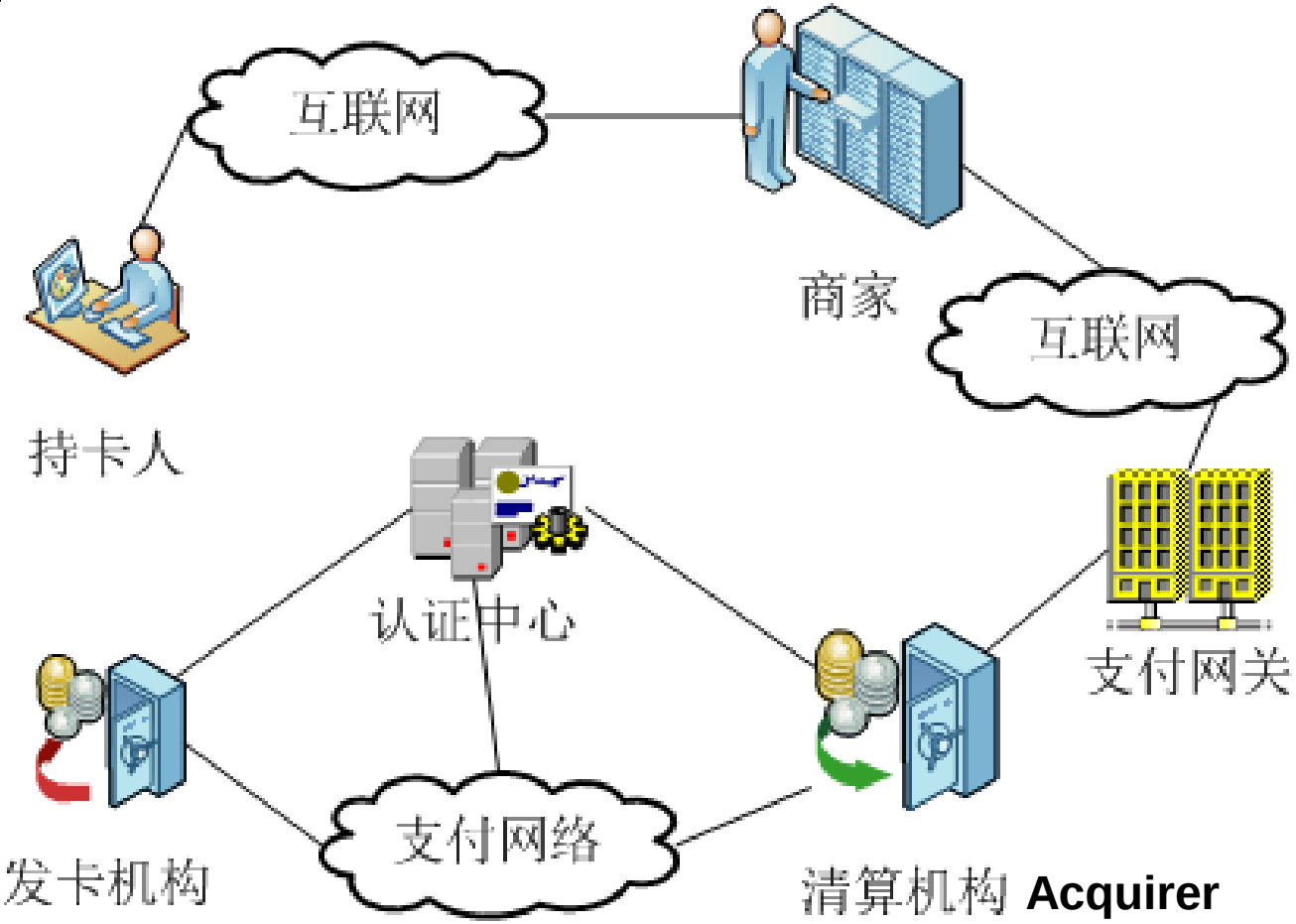
- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议
  - 8.4.1 电子商务安全
  - 8.4.2 SET协议概述
  - 8.4.3 SET的安全机制
  - 8.4.4 交易处理
  - 8.4.5 SET与SSL的比较

SET协议概述

- SET协议是依据网络电子交易的特点，专门用于解决交易的安全问题的协议。
- SET安全协议的目标：
  1. 保证交易信息在互联网上安全传输，防止数据被黑客或被内部人员窃取。
  2. 保证电子商务参与者信息的相互隔离。客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。
  3. 持卡人和商家相互认证，以确定通信双方的身份，由第三方机构负责为在线通信双方提供信用担保。
  4. 保证网上交易的实时性，使支付过程都是在线的。
  5. 要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容性和互操作功能。

SET的组件结构

- SET的六组件
  - Cardholder、Merchant、Issuer、Acquirer、Payment Gatewav、Certificate Authoritv



基于SET的网络交易流程

① 顾客（持卡人）通过Internet选定物品，填写并提交订货单。

② 商家作出应答，告诉消费者所填订货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

③ 消费者选择付款方式，核定订单。此时SET开始介入。

④ 顾客在验证商家的CA证书后，发送给商家一个包含完整订购信息和支付信息的订单。

⑤ 商家接受订单后，验证顾客的身份，并向其支付卡所在金融机构（一般为银行）请求支付授权。

- 有关信息通过支付网关到清算机构，再到发卡机构确认。批准交易后，返回确认信息给商家。

⑥ 商家发送订单确认信息给顾客。

⑦ 商家发送货物或提供服务，到此一个网上交易结束。

⑧ 商家通知清算机构请求支付货款。

- 清算银行经过一定时间间隔将钱从顾客帐号转移到商家帐号。

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议
  - 8.4.1 电子商务安全
  - 8.4.2 SET协议概述
  - 8.4.3 SET的安全机制
  - 8.4.4 交易处理
  - 8.4.5 SET与SSL的比较

SET的安全机制

- SET协议安全性主要依靠其采用的多种安全机制：
  - 对称密钥密码
  - 公开密钥密码
  - 数字签名
  - 消息摘要
  - 电子信封
  - 数字证书
  - 双重签名
- 安全机制解决了包括机密性、完整性、身份认证和不可否认性等问题，提供了更高的信任度和可靠性。

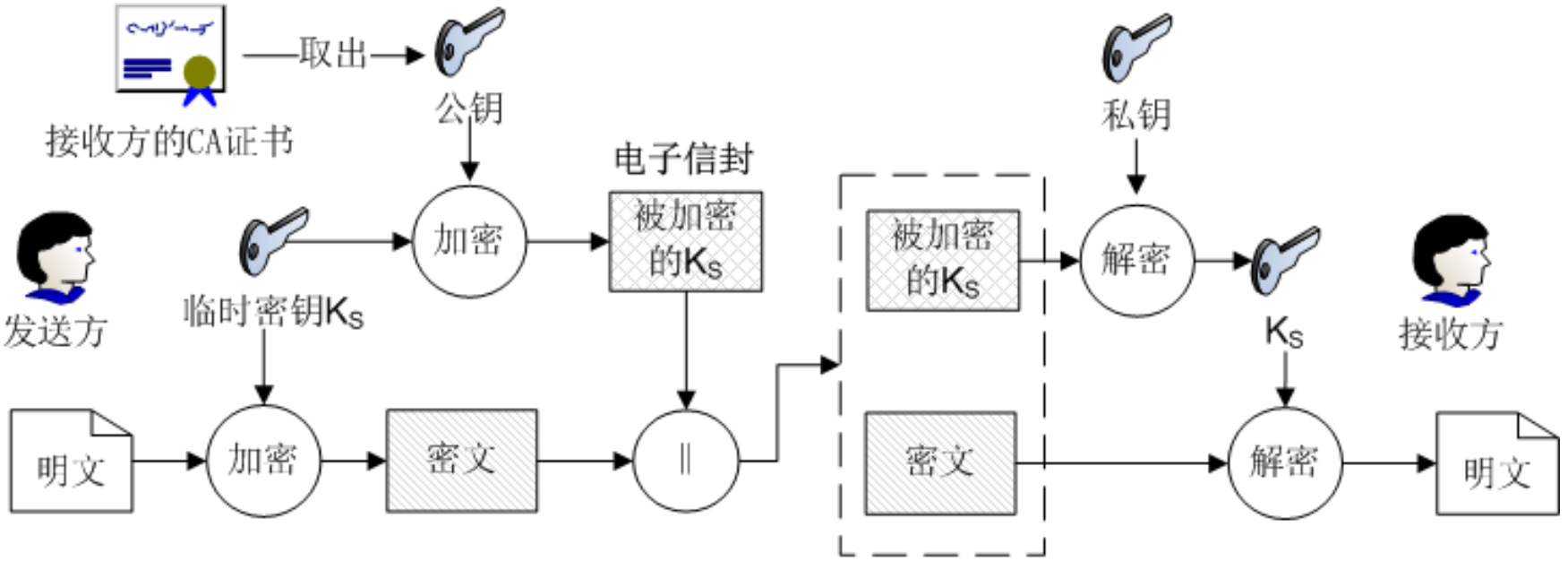
- SET协议使如何保证商家、顾客和银行之间数据隐私的安全性？

CA证书

- CA证书就是一份文档，它记录了用户的公开密钥和其他身份信息。
- 最重要的证书是持卡人证书和商家证书。
- 除此以外，还包括支付网关证书、清算机构（银行）证书、发卡机构（银行）证书。
- 这些证书均由一个权威的CA签发，如某金融机构的认证中心。
- 整个交易过程中，SET各实体可以通过数字证书证实自己的真实身份，同时可以提供自己的公钥给对方，以便交换重要的保密信息，如电子信封应用。

电子信封

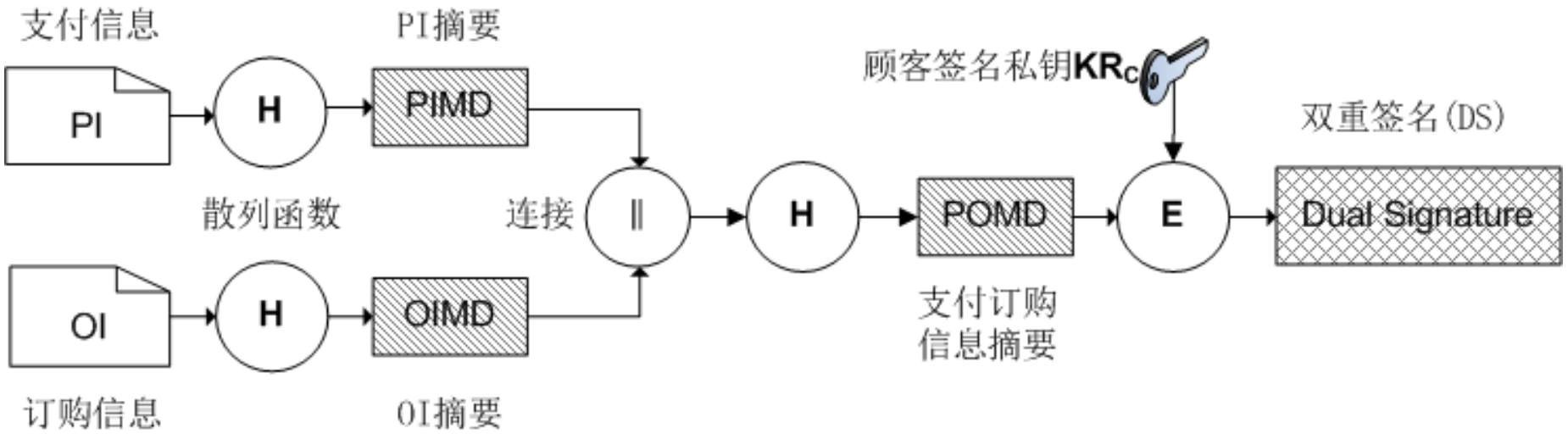
- SET协议使用电子信封来传递更新的密钥。
- 电子信封涉及到两个密钥：一个是接收方的公开密钥；另一个是发送方生成的临时密钥（对称密钥）。
  - 发送方使用接收方的公钥加密临时密钥，一般将这个被加密的秘钥称为电子信封，接收方用其私钥解密出临时秘钥。



电子信封的使用过程

双重签名

- SET协议核心内容是订购信息OI和支付信息PI。
- DS（Dual Signature）技术将OI和PI这两部分的摘要信息绑定，确保电子交易的有效性和公正性。
- 分离PI与OI，确保商家不知道顾客的支付卡信息，银行不知道顾客的订购细节。
- $DS = E_{KRc}[H(H(PI) \| H(OI))]$



双重签名的使用过程

- 顾客针对PI和OI生成DS，将DS、OI和PIMD发送给商家。
- 商家计算得到POMD=H（PIMD ll H（OI））， 然后计算POMD’=D_{KUc} [DS]，其中KUc为顾客的公开密钥。如果POMD= POMD’，则商家可以认为该DS正确，批准实施进一步交易。
- 顾客需要生成一个对称密钥K_S，使用银行的公钥加密K_S，并使用K_S加密DS、PI和OIMD，通过商家将E_{KUb} [K_S]IIE$_{Ks}$[DS ‖ PI IIOIMD]转发给银行。
  - 其中KUb为银行的公开密钥。
- 银行计算POMD=H（H（PI）ll OIMD）和POMD’=D_{KUc} [DS]，如果POMD= POMD’，则银行可以认为该DS正确，批准实施交易。

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议
  - 8.4.1 电子商务安全
  - 8.4.2 SET协议概述
  - 8.4.3 SET的安全机制
  - 8.4.4 交易处理
  - 8.4.5 SET与SSL的比较

交易处理

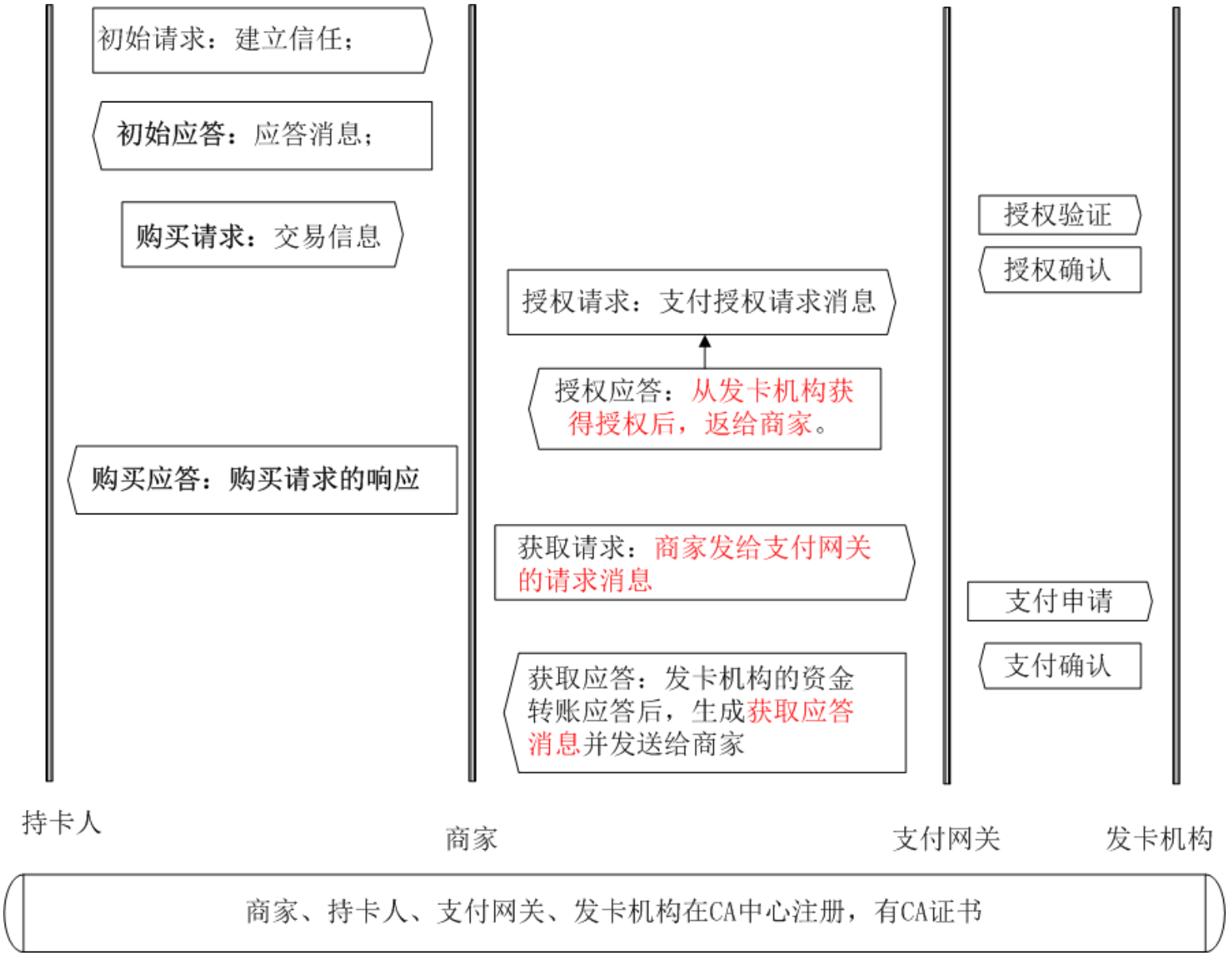
- SET协议为电子商务交易设计了多种类型的交易处理。

- 这些交易处理可以各自完成相应的功能，相互衔接配合，共同构建了一个完整的电子商务交易业务平台。

- 在处理中，持卡人注册和商家注册是进行安全交易的前提，购买请求、支付授权和支付获取是进行交易的核心。

类型
持卡人注册
商家注册
购买请求
支付授权
支付获取
证书询问和状态
交易状态询问
撤销认可
撤销获取
信用
撤销信用
支付网关证书请求
批管理
出错信息

交易处理


初始请求：建立信任；
初始应答：应答消息；
购买请求：交易信息
授权请求：支付授权请求消息
授权应答：从发卡机构获得授权后，返给商家。
购买应答：购买请求的响应
获取请求：商家发给支付网关的请求消息
获取应答：发卡机构的资金转账应答后，生成获取应答消息并发送给商家
授权验证
授权确认
支付申请
支付确认
持卡人
商家
支付网关
发卡机构
商家、持卡人、支付网关、发卡机构在CA中心注册，有CA证书

购买请求

- 初始请求是顾客为了建立与商家之间的基本信任关系而发出的第一个消息。
  - 包括顾客的支付卡品牌、对应此次请求/应答的标识ID和用于保证时限的临时值nonce。

- 初始应答是商家回应顾客初始请求的应答消息。
  - 包括从顾客的初始请求中得到的nonce、要求在下一条消息中包含的新nonce和交易标识ID，这部分消息将被商家使用其私钥签名。

购买请求

- 购买请求是顾客发送给商家具体的交易信息，主要内容包括OI和PI。首先顾客通过CA验证商家和支付网关的证书，然后生成购买请求消息发送给商家。
  - 具体的购买请求消息如下：
    - $E_{Ks}[PI \| DS \| OIMD] \| E_{KUb}[Ks] \| PIMD \| OI \| DS \| CA证书_{顾客}$
- 购买应答是商家针对顾客的购买请求消息进行的相关响应处理。
  - 当商家收到购买消息后，首先验证顾客的CA证书，用顾客的公钥验证双重签名；
  - 将$E_{Ks}[PI \| DS \| OIMD] \| E_{KUb}[Ks]$ 转发给支付网关请求验证及支付授权，构造购买应答消息回应顾客。
    - 购买应答消息主要包括：购买确认的应答分组、相对应的交易号索引以及商家的CA证书，前两部分将使用商家的私钥签名。

支付授权

- 商家需要向支付网关申请支付授权，支付网关与发卡机构进行支付信息的确认，确保商家在完成交易后，可以收到有关支付款。
- 支付授权包括两个消息：授权请求和授权应答。
- 授权请求是商家发送给支付网关的支付授权请求消息，包括以下三部分：
  - 顾客生成的购买信息：包括PI、DS、OIMD和顾客与支付网关之间的电子信封；
  - 商家生成的授权信息：使用商家私钥签名并用商家生成的临时密钥Ks加密的交易标识ID（称为认证分组）和商家生成的电子信封（使用支付网关公钥加密的临时密钥Ks）；
  - 证书：顾客的CA证书、商家的CA证书。

支付授权

- 收到商家发送的授权请求后，支付网关需要验证所有CA证书；
  - 解密商家的电子信封，解密认证分组并验证商家签名；
  - 解密顾客的电子信封，验证顾客生成的DS；
  - 比较从商家得到的交易标识ID和从顾客得到PI的交易标识ID，最后请求并接收发卡机构的认证。
- 授权应答是支付网关从发卡机构获得授权后，返给商家的支付授权应答消息。包括：
  - 支付网关生成的授权相关信息：包括使用支付网关私钥签名，并用支付网关生成的临时密钥Ks加密的授权标识和支付网关生成的电子信封；
  - 授权获取标记信息：该信息用来保证以后的支付有效。
  - 证书：支付网关的CA证书。

支付获取

- 商家为了获得货款，与支付网关之间进行支付获取消息交换，包括获取请求和获取应答两部分。

- 获取请求是商家发给支付网关的请求消息，告知支付网关已向顾客提供了商品或服务，并向支付网关申请索取支付款。
  - 获取请求消息包括被签名加密的付款金额、交易标识部分以及在之前支付授权的消息中包含的授权获取标记信息和商家的证书。

支付获取

- 当支付网关接收到获取请求消息后，验证相关信息，通过支付网络将结算信息发送给发卡机构，请求将顾客消费的资金款项转到商家在清算机构（银行）中的账户上。
- 在得到发卡机构的资金转账应答后，支付网关生成获取应答消息并发送给商家，以便核对其在清算机构账户中的收款情况。
- 支付获取应答消息包括被签名加密的获取应答报文以及支付网关的证书。
- 商家将此获取应答保存下来，用于匹配商家在清算机构上的账户的支付账款信息。

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议
  - 8.4.1 电子商务安全
  - 8.4.2 SET协议概述
  - 8.4.3 SET的安全机制
  - 8.4.4 交易处理
  - 8.4.5 SET与SSL的比较

SET与SSL的比较

- SSL与SET都可以提供电子商务交易的安全机制，但是运作方式存在着明显的区别。

- 不同点主要表现在以下几个方面。
  - 认证机制
  - 安全性
  - 网络协议体系
  - 应用领域
  - 应用代价

SET与SSL的比较

- 认证机制：
  - 早期SSL没有商家身份认证机制；
  - SSL 3.0可以实现浏览器和Web服务器双方的身份验证，但不能实现多方认证；
  - SET要求参与交易的成员（持卡人、商家、发卡机构、清算机构和支付网关）都必须提供数字证书进行身份识别。
- 安全性：
  - SET协议规范了整个商务活动的流程，在持卡人、商家、支付网关、认证中心和支付卡结算中心支局的信息流方向以及必须采用的加密方法和认证方法都收到严密的SET标准规范，最大限度地保证了商务性、服务性、协调性和集成性。
  - SSL只对持卡人和网络商家的信息交换进行加密保护，可以看做是用于传输的那部分的技术规范。

SET与SSL的比较

- 网络协议体系：
  - SSL是基于传输层的通用安全协议；
  - SET位于应用层，对网络上其他各层协议都有涉及。

- 应用领域：
  - 如果电子商务应用只是通过Web或电子邮件，可以不要SET。
  - 如果电子商务应用是一个涉及多方交易的平台，则使用SET更安全、更通用些。

- 应用代价：
  - SET协议提供了B2C平台上信用卡在线支付的方式，但实现非常复杂。

作业

1. 习题2（5）：HTTPS是如何实现数据的安全性的？
2. 习题2（6）：SET协议要解决的主要问题有哪些？
3. 习题2（7）：SET协议是如何保证商家、顾客和银行之间数据隐私的安全性的。