第8章 网络安全协议

主要内容

8.1 概述

8.2 IPSec

8.3 SSL

8.4 安全电子交易协议

8.1 概述

- 许多网络攻击都是由网络协议（如TCP/IP）的固有漏洞引起的，因此，为了保证网络传输和应用的安全，各种类型的网络安全协议不断涌现。
- 安全协议是以密码学为基础的消息交换协议，也称作密码协议，其目的是在网络环境中提供各种安全服务。
- 安全协议是网络安全的一个重要组成部分，通过安全协议可以实现实体认证、数据完整性校验、密钥分配、收发确认以及不可否认性验证等安全功能。

网络安全协议层次

- 网络安全协议基本上与TCP/IP协议族相似
  - 分为四层，即网络接口层、网络层、传输层和应用层。
  - 网络接口层：L2TP 、L2F、PPTP；
  - 网络层：IPSec协议（IP Security）；
  - 传输层：SSL、TLS和SOCKS v5等；
  - 应用层：种类繁多（SSH、PGP和SET）。
- 网络安全协议建立在密码体制基础上，运用密码算法和协议逻辑来实现加密和认证。
  - 密钥管理主要分为人工管理和协商管理两种形式。
  - 密钥管理都需要通过应用层服务来实现。
  - 网络安全协议所处的网络层次不同，存在包含关系，但存在特殊应用的情况除外。

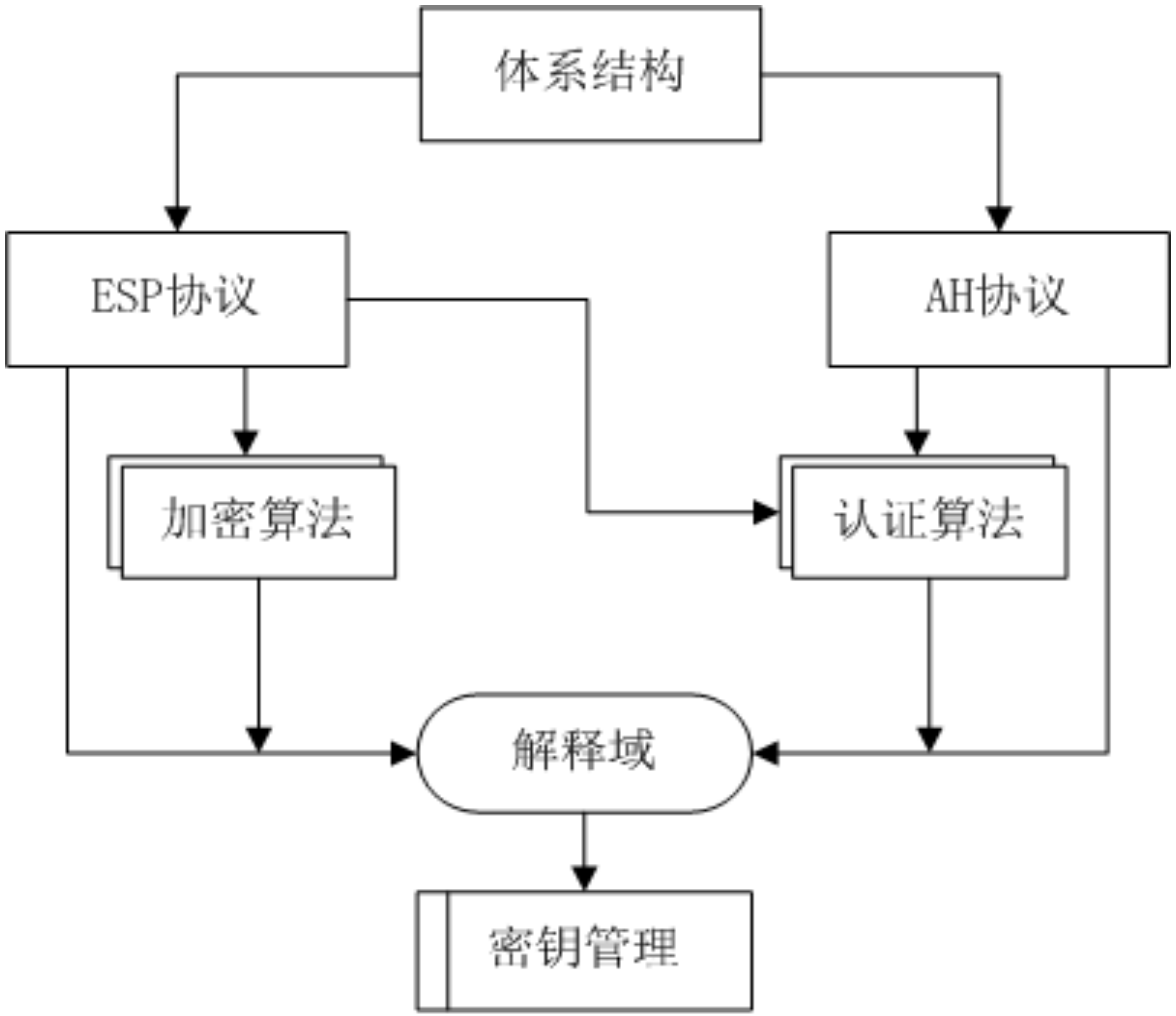
8.2 IPSec

- 1994年，IAB（Internet Architecture Board），《互联网体系结构中的安全问题》
- 1994年，IETF专门成立IP安全协议工作组。
- 1995年，IPSec细则颁布
- 1998年11月，被提议为IP安全标准
- IPSec是一个标准的第三层安全协议族。
- IETF为IPSec一共定义了12个标准文档RFC（Request For Comments）
- IPSec对于IPv4是可选的，对于IPv6是强制性的。

IPSec协议的优点

- IPSec在传输层之下，对于应用程序是透明的。
- IPSec对终端用户是透明的，因此不必对用户进行安全机制的培训。
- IPSec可以为个体用户提供安全保障，可以保护企业内部的敏感信息。

8.2.1 IPSec协议族的体系结构



IPSec的体系结构

基本协议

- ESP（Encapsulating Security Payload）协议
  - 对IP数据报文实施加密和可选认证双重服务，提供了数据保密性、有限的数据流保密性、数据源认证、无连接的完整性以及抗重放攻击等服务。
- AH（Authentication Header）协议
  - 对IP数据报文实施认证服务，提供数据源认证、无连接的完整性以及一个可选的抗重放服务。
- AH协议和ESP协议都支持认证功能，但二者的保护范围存在着一定的差异。
  - AH的作用域是整个IP数据包，包括IP头和承载数据。
  - ESP认证功能的作用域只是承载数据，不包括IP头。

IPSec基本要件

- ESP和AH的有效工作依赖于四个要件。
  - 加密算法、认证算法、解释域DOI（Domain of Interpretation）以及密钥管理。

①加密算法

- 描述各种能用于ESP的加密算法，IPSec要求任何实现都必须支持DES（数据加密标准），也可使用3DES、IDEA(国际加密算法)、AES(高级加密算法)等其他算法。

②认证算法

- 用于AH和ESP，以保证数据完整性及进行数据源身份认证。IPSec用HMAC-MD5和HMAC-SHA-1作为默认认证算法，同时也支持其他认证算法，以提高安全强度。

③ 解释域

– DOI(Domain of Interpretation)是一个描述IPSec所涉及到的各种安全参数及相关信息的集合。通过对它的访问可以得到相关协议中各字段含义的解释，可以被与IPSec服务相关的系统参考调用。

④ 密钥管理

– 密钥管理主要负责确定和分配AH和ESP中加密和认证使用的密钥，有手工和自动两种方式。IPSec默认的自动密钥管理协议是IKE(Internet Key Exchange)。

安全关联

- 安全关联SA（Security Association）是一个IPSec单项连接所涉及的安全参数和策略的集合
  - 决定了保护什么、如何保护以及谁来保护通信数据；
  - 规定了用来保护数据包安全的IPSec协议类型、协议的操作模式、加密算法、认证方式、加密和认证密钥、密钥的有效存在时间以及防重放攻击的序列号等；
  - AH和ESP均使用SA，而且IKE协议的一个主要功能就是建立和维护SA；
  - 一个SA定义了两个应用实体（主机或网关）间的一个单向连接，如果需要双向通讯，则需要建立两个SA。

- SA是通过三元组 < 安全参数索引，IP目的地址，安全协议标识 > 来标识；
  - SPI（Security Parameter Index）：是一个与SA相关联的位串。一般在IKE 确立一个SA时，产生一个伪随机导数作为该SA的SPI。SPI 也可以人为设定。
  - IP目的地址：目前IPSec仅支持使用单播地址来表示SA的目的地址。
  - 安全协议标识：标识该SA是一个AH或ESP协议的安全关联。

SPD

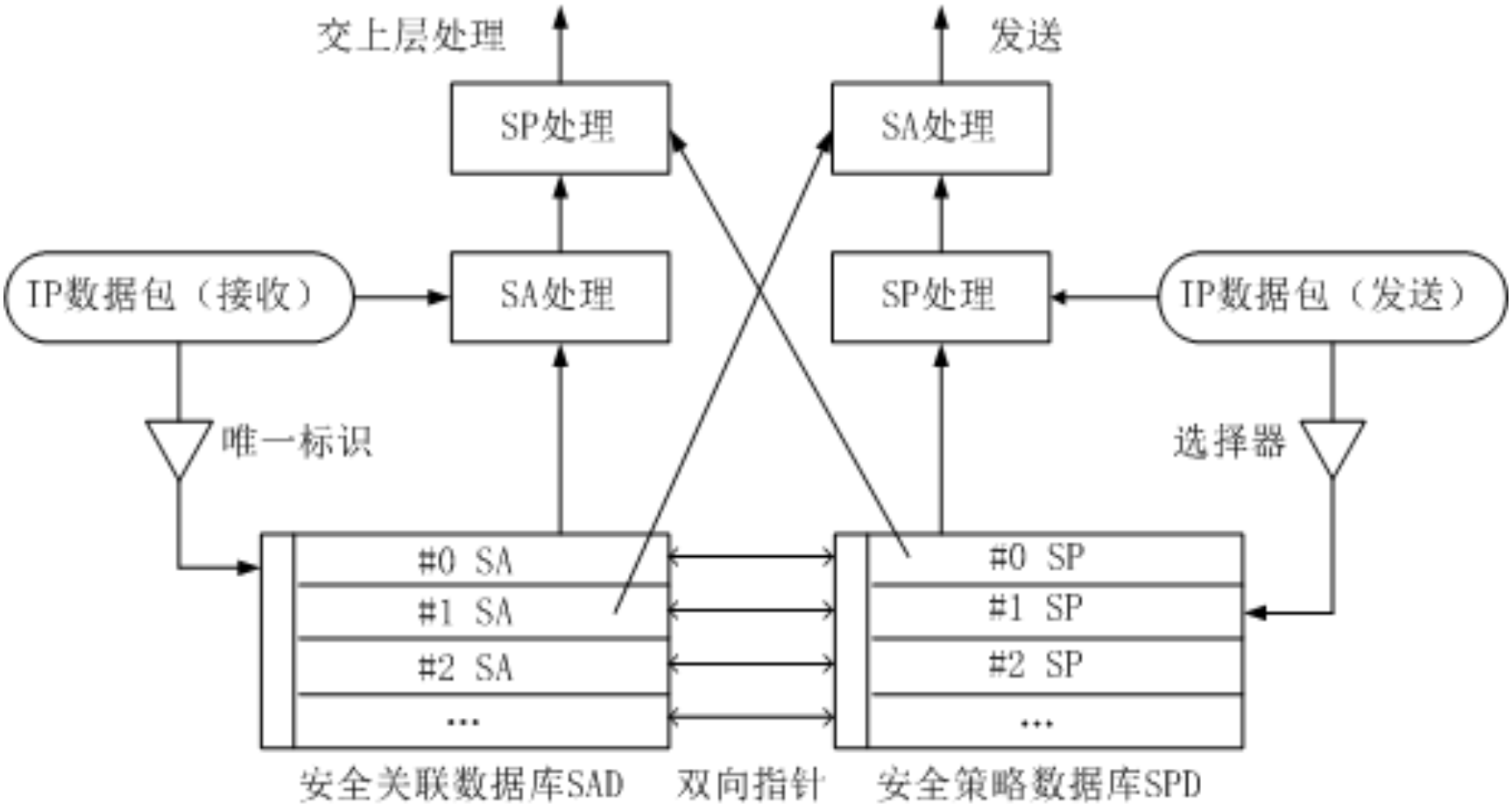
- SPD中的安全策略SP是通过选择因子来确定
  - 选择因子是从网络层和传送头内提取出来的，主要包括：目的地址、源地址、名字、协议、上层端口等。
- 安全策略数据库SPD 是SA处理的核心之一，每个IPSec实现必须具有管理接口，允许用户或系统管理员管理SPD。
- SPD有一个排序的策略列表，针对接收数据和发送数据有不同的处理策略。
  - SPD的处理方式主要有三种：Discard，Bypass IPSec，Apply IPSec。

SAD

- SAD中的任意SA都被定义了以下参数（即SAD的字段）：
  - 目的IP地址：目前的SA管理机制只支持单播地址的SA。
  - IPSec协议：标识SA用的是AH还是ESP。
  - SPI：32比特的安全参数索引，标识同一个目的地的不同的SA。
  - 序号计数器：32比特，用于产生AH或ESP头的序号，仅用于发送数据包。
  - 序号计数器溢出标志：标识序号计数器是否溢出。
    - 如溢出，产生审计事件，禁止用SA继续发送数据包。

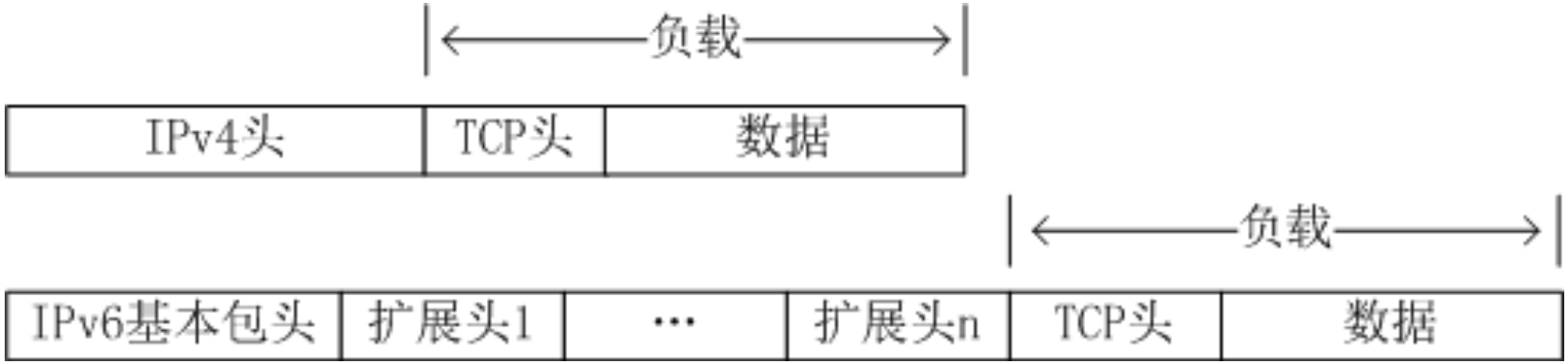
- 抗重放窗口：32比特计数器，用于决定进入的AH或ESP数据包是否为重发，仅用于接收数据包。
- AH信息：指明认证算法、密钥、密钥生存期等与AH相关的参数。
- ESP信息：指明加密和认证算法、密钥、初始值、密钥生存期等与ESP相关的参数。
- SA的生存期：一个特定的时间间隔或字节计数。
- IPSec协议模式：指明是隧道、传输或混合方式（通配符），这些内容后面讨论。
- Path MTU（路径最大传输单元）：指明预计经过路径的MTU及延迟变量。

安全关联SA的工作原理



8.2.2 IPSec协议的工作方式

- IPv4与IPv6数据包结构

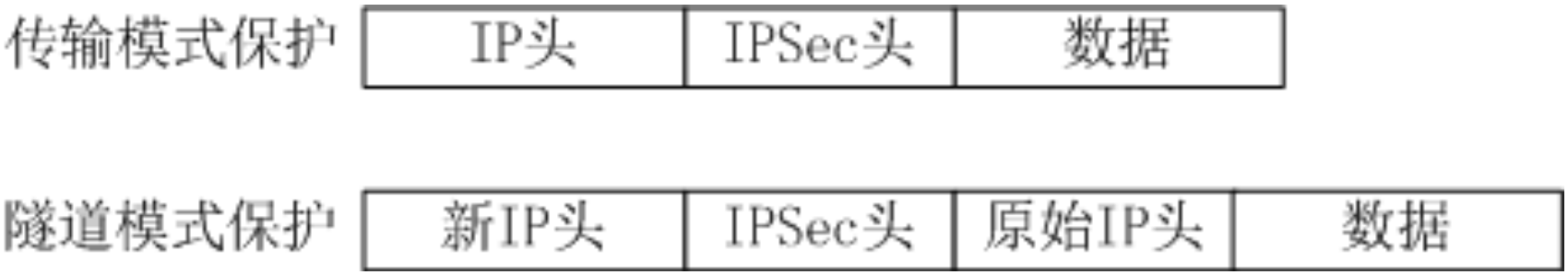


a、IPv4报头

b、IPv6报头

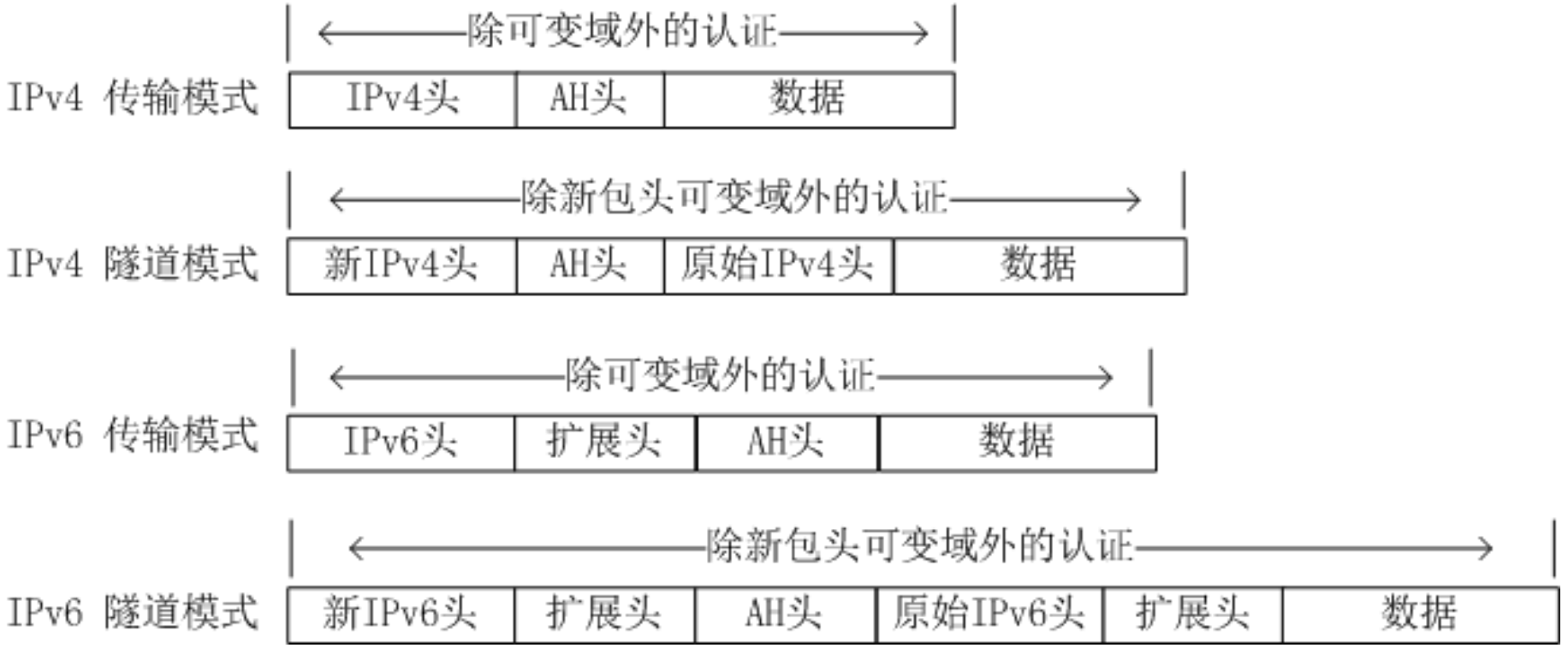
IPSec的工作模式

- IPSec 标准定义了 IPSec 操作的两种不同模式：
  - 传输模式（Transport Mode）和隧道模式（TunnelMode）
- 安全协议AH和ESP，都可以以这两种模式工作。



认证头AH

- AH的工作原理
  - 可变内容一般被填充“0”后参与计算

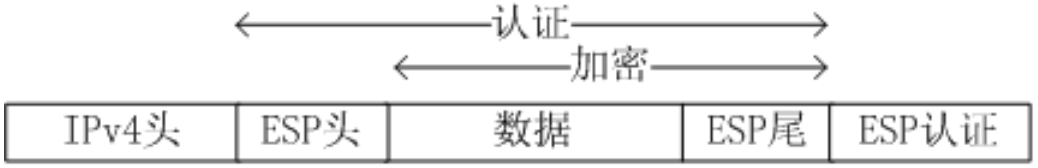


AH头格式

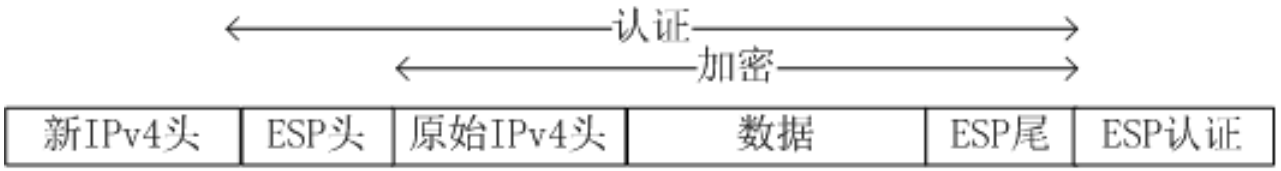
- 下一个头（8位）：用来标记下一个扩展头的类型；
- 载荷长度（8位）：表示认证头数据的长度减2，以字（字长32位）来计，
- 保留（16位）：备用；
- SPI（32位）：用来标识安全关联；
- 序列号（32位）：收发双方同时保留一个序列号计数器，每收发一个IP包，序列号将递增1，当递增到2^{32}后复位；
- 认证数据（32N位）：认证数据域的长度可变，但必须是32的整数倍，默认为3个字（96位）。

封装安全有效负荷ESP

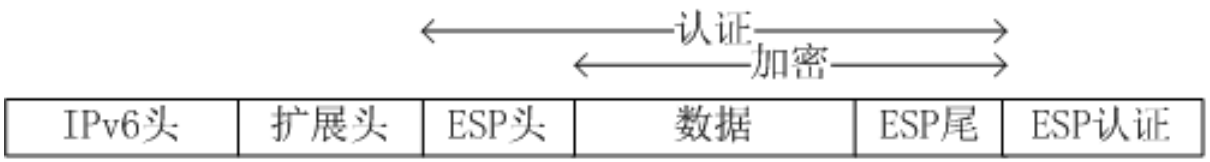
- ESP的工作原理



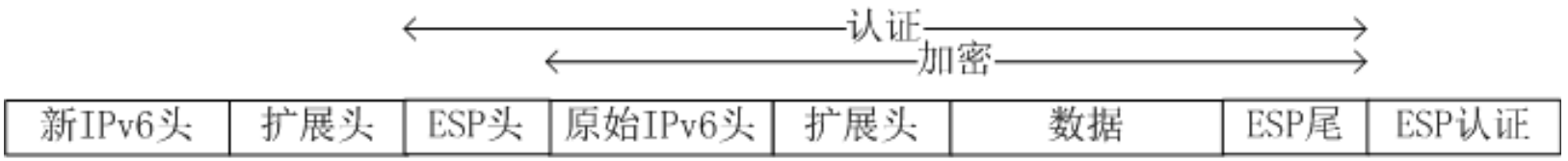
（a）IPv4 传输模式



（b）IPv4 隧道模式

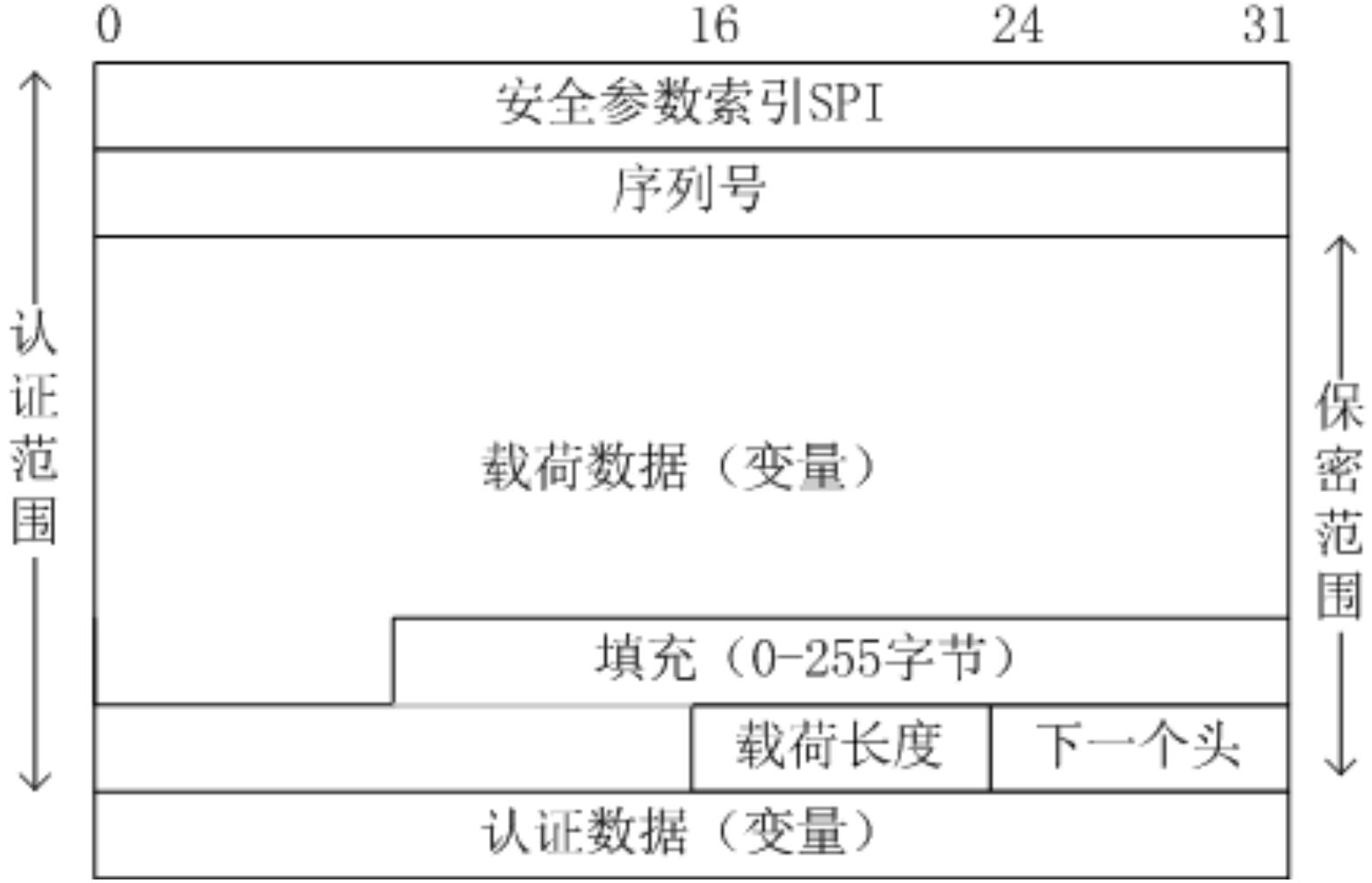


（c）IPv6 传输模式



（d）IPv6 隧道模式

ESP的封装格式


0
16
24
31
安全参数索引SPI
序列号
载荷数据（变量）
填充（0-255字节）
载荷长度
下一个头
认证数据（变量）
认证范围
保密范围

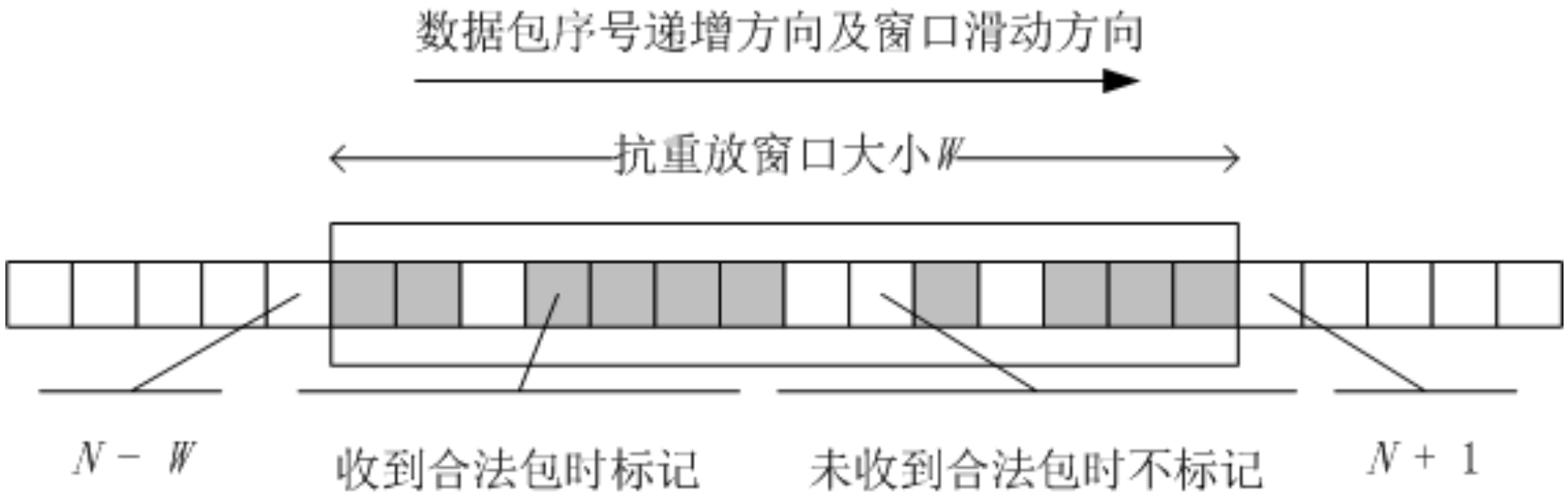
- 安全关联索引：用来标识安全关联；
- 序列号：与AH相同，用来防范IP包的重发攻击；
- 载荷数据：被加密的传输层数据（传输模式）或整个原始IP包（隧道模式）；
- 填充域：提供规整化载荷数据，并隐藏载荷数据的实际长度；
- 填充长度：填充数据的长度；
- 下一个头：用来标记载荷中第一个包头的类型，具体值与AH相同；
- 认证数据：针对ESP包中除认证数据域外的内容进行完整性计算，得到的完整性校验值，具体计算方法与AH相同。

反重放攻击服务

- 重放攻击主要分为：
  - 简单重放攻击：攻击者简单地复制一条消息，以后再重新发送它；
  - 反向重放攻击：攻击者复制一条消息，只修改源/目的地址，然后反向发送给消息源（消息发送者）。
- 抵御重放攻击主要方法包括：
  - 序列号：使用一个序列号来给每一个消息报文编号，仅当收到的消息序数顺序合法时才接受；
  - 时间戳（Timestamp）：A接受一个消息，仅当该消息包含一个时间戳，该时间戳足够接近当前时间时才接受；
  - 盘问/应答方式（Challenge/Response）： A期望从B获得一个新消息，首先发给B一个临时值（Challenge），并要求后续从B收到的消息（Response）包含正确的临时值或对其正确的变换值。

抗重放窗口

- Ipsec使如何防范重放攻击的？



8.2.3 Internet密钥交换协议

- IPsec在提供认证或加密服务之前，必须针对安全协议、加密算法和密钥等内容进行协商，并建立SA，这个过程可以手工进行和自动完成。
- IPSec默认的自动密钥管理协议是Internet密钥交换协议IKE（Internet Key Exchange）。
  - IKE是一个多用途的安全信息交换管理协议，被定义为应用层协议，主要用于安全策略协商以及加密认证基础材料的确定，
  - SNMPv3、OSPFv2及IPSec等都采用IKE进行密钥交换。
  - IKE是3个协议的混合体，这三个协议分别是ISAKMP、Oakley和SKEME。

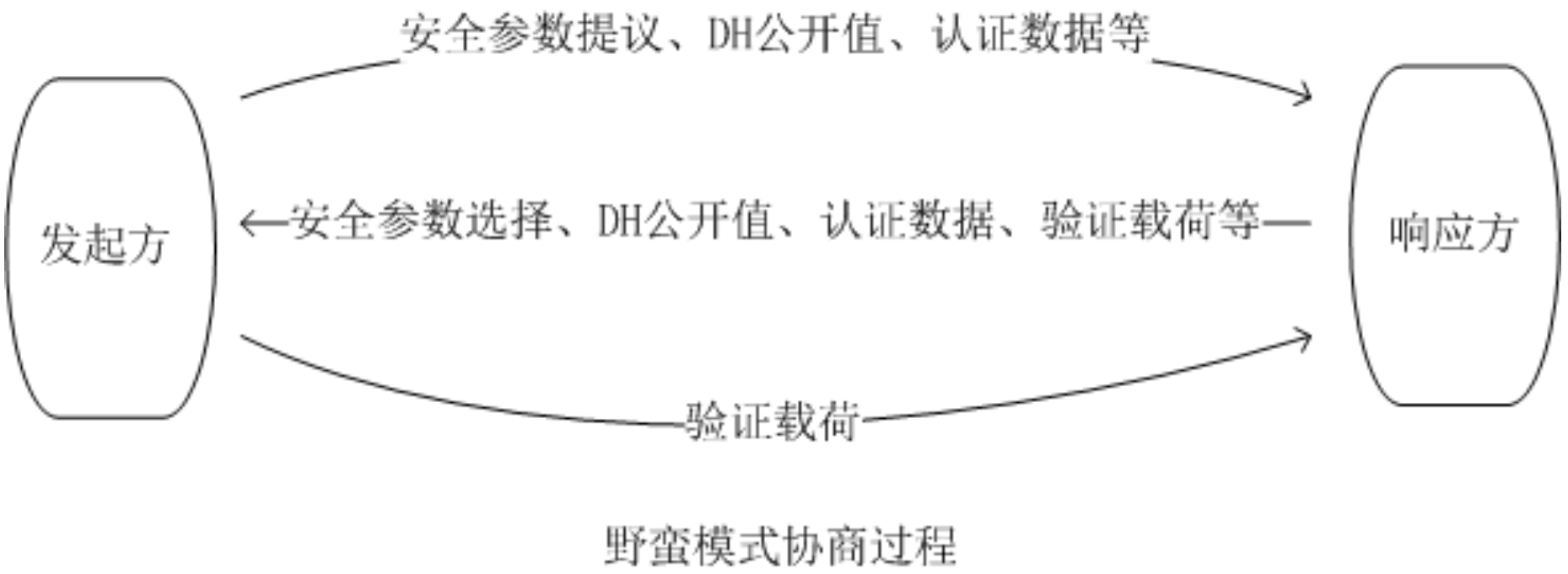
- ISAKMP（Internet Security Association and Key Management Protocol）设计了一个用于通信双方完成认证和密钥交换的通用框架，在此框架下可以协商和确定各种安全属性、密码算法、安全参数、认证机制等，这些协商的结果统称为安全关联SA。
- Oakley算法是一种以Diffie-Hellman算法为基础的自由形态的协议，允许他人依据本身的需要来改进协议状态。
  - IKE在Oakley基础上，进行有效的规范化，形成了可供用户选择的多种密钥交换模式。
- SKEME（Secure Key Exchange Mechanism）采用公开密钥加密的手段来实现匿名性、防抵赖和密钥更新等服务，可以提供密码生成材料技术和协商共享策略。

IKE

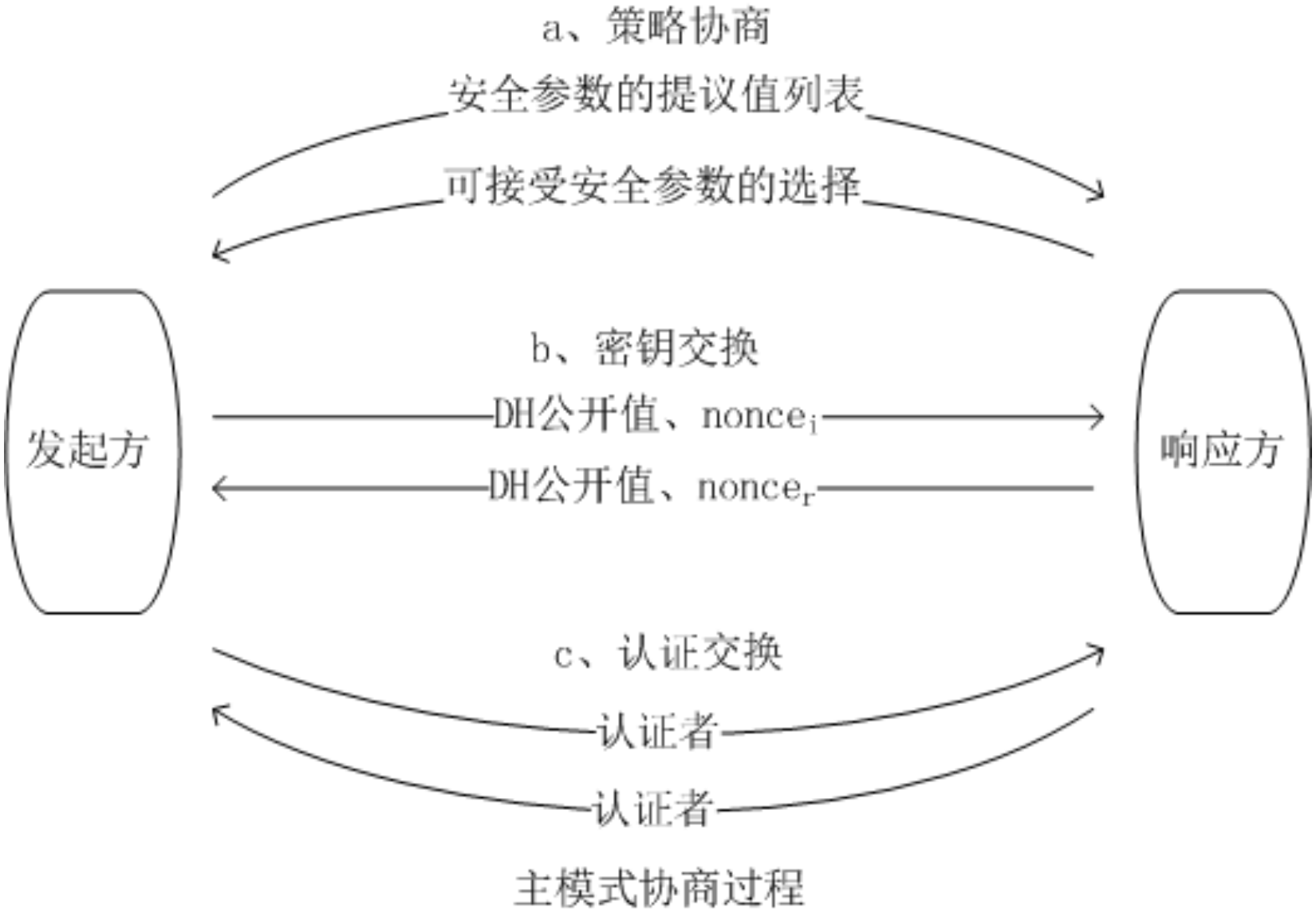
- IKE对IPSec的支持就是在通信双方之间，建立起共享安全参数及密钥（即安全关联SA）。
- IKE建立SA的过程分为两个阶段，
  - 第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步的IKE通信提供机密性、消息完整性以及消息源验证服务；
  - 第二阶段，使用已建立的IKE SA建立IPsec SA。
- 实体进行IPSec连接，
  - 如果已经创建了IKE SA，就可以直接通过第二阶段，交换创建新的IPsec SA；
  - 如果还没有创建IKE SA，就要通过两个阶段交换创建新的IKE SA及IPsec SA。

第一阶段

- IKE定义了两种信息交换模式，
  - 主模式（Main Mode）、野蛮模式（Aggressive Mode）



野蛮模式协商过程

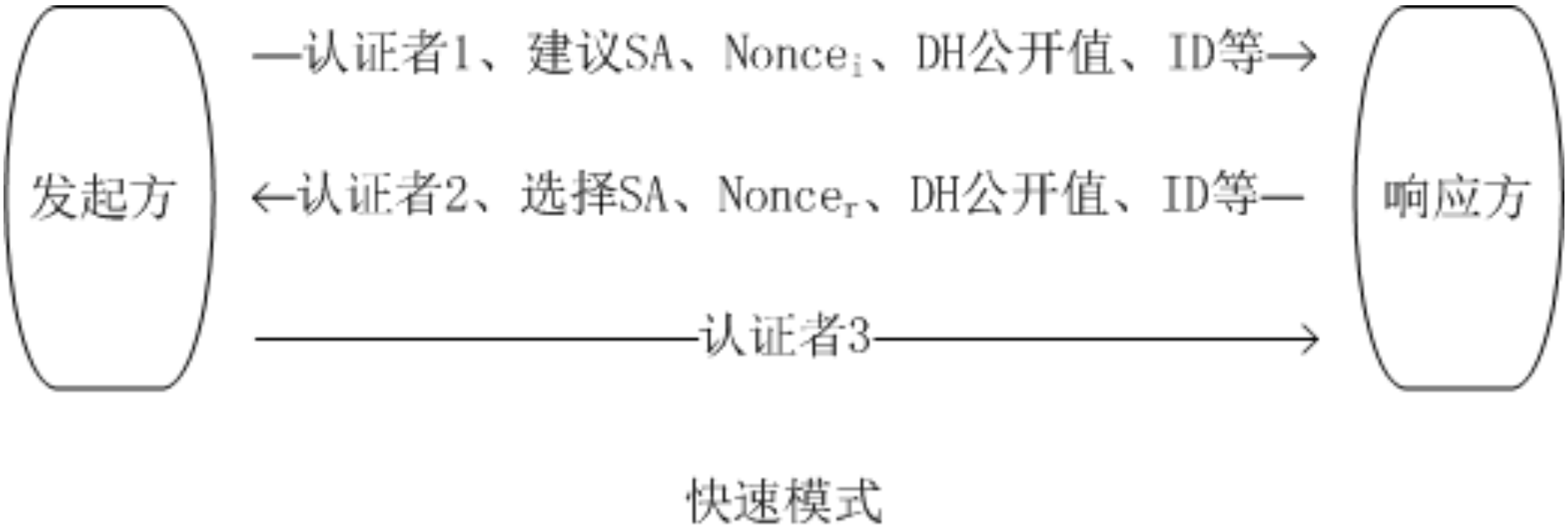

a、策略协商
安全参数的提议值列表
可接受安全参数的选择
发起方
b、密钥交换
DH公开值、$nonce_i$
DH公开值、$nonce_r$
响应方
c、认证交换
认证者
认证者

主模式协商过程

第二阶段

- IKE已经拥有了第一阶段建立起的IKE SA，通信双方的进一步协商采用SA保护，任何没有SA保护的消息将被拒收。
- 通常在第二阶段至少要建立两条SA，一条用于发送数据，一条用于接收数据。
- 此阶段IKE使用三种信息交换，
  - 快速模式（Quick Mode）、新组模式（New Group Mode）和ISAKMP信息交换（ISAKMP Info Exchange）。

快速模式（Quick Mode）



快速模式

新组模式和ISAKMP信息交换

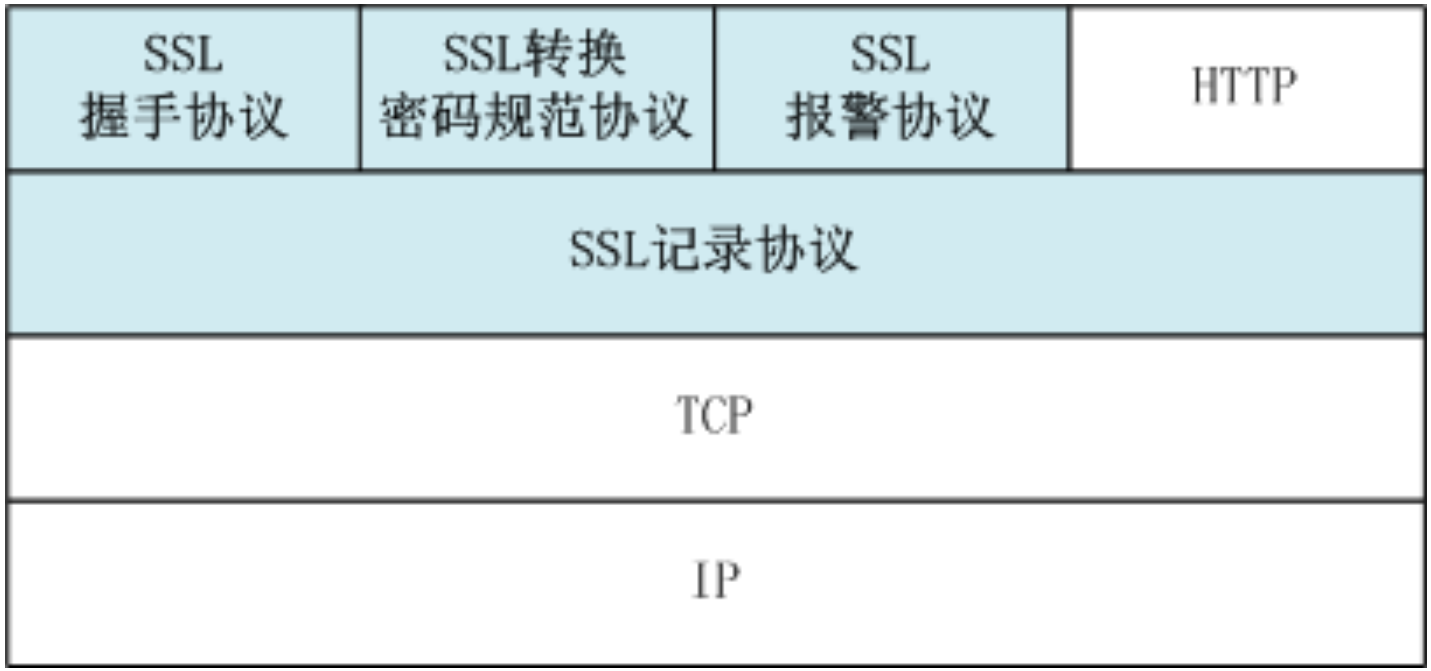
- 新组模式主要用于实现通信双方交换协商新的Diffie－Hellman组，属于一种请求/响应交换。发送方发送提议的DH组的标识符及其特征，如果响应方能够接收提议，就用完全一样的消息应答。
- ISAKMP信息交换主要功能是实现通信一方向对方发送错误及状态提示消息，这并非真正意义上的交换，而只是发送单独一条消息，不需要确认。

8.3 SSL

- SSL协议是NetScape 公司于1994年提出的
  - 保护客户端与服务器之间数据传输安全的加密协议。
  - 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）。
- 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。

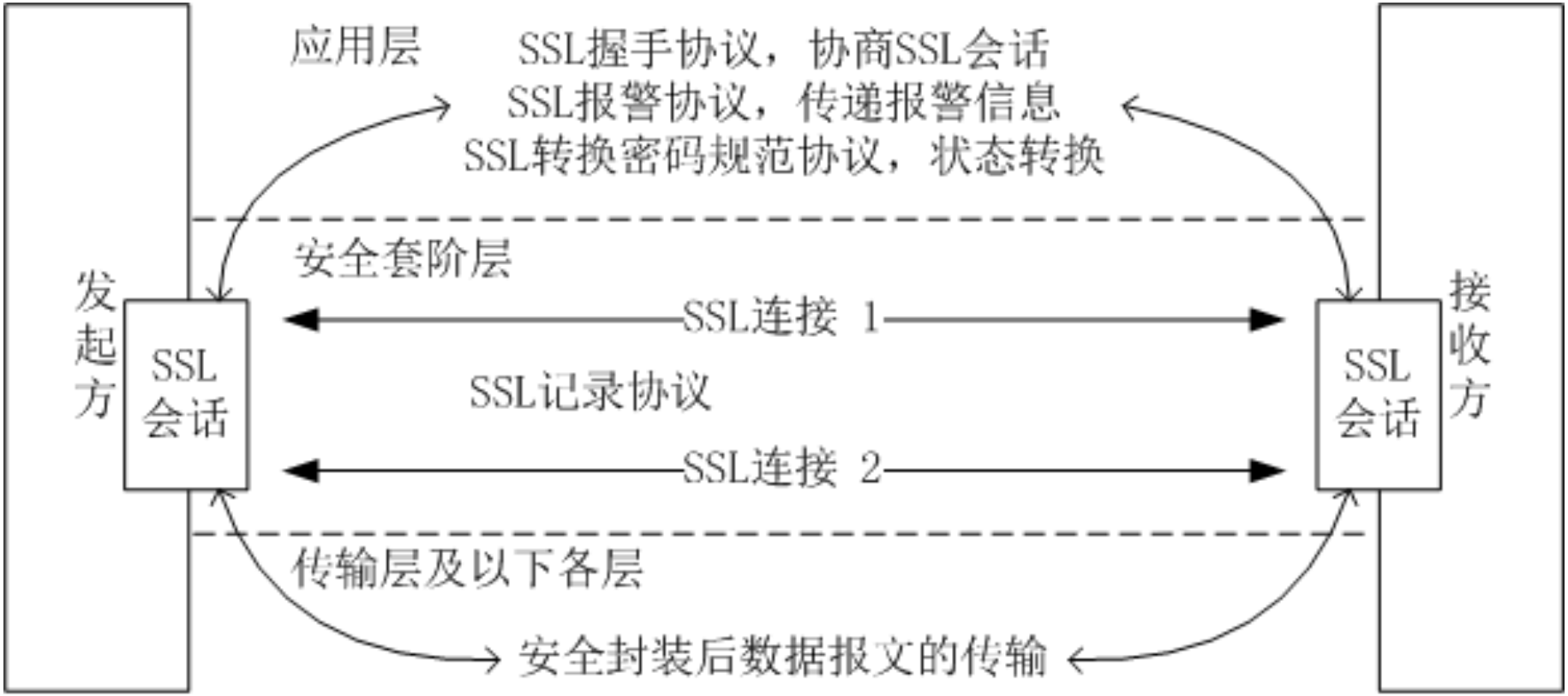
8.3.1 SSL协议的体系结构

- SSL协议族
  - 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。
  - 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。
- 两个重要的概念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连接与SSL会话

SSL会话状态参数定义

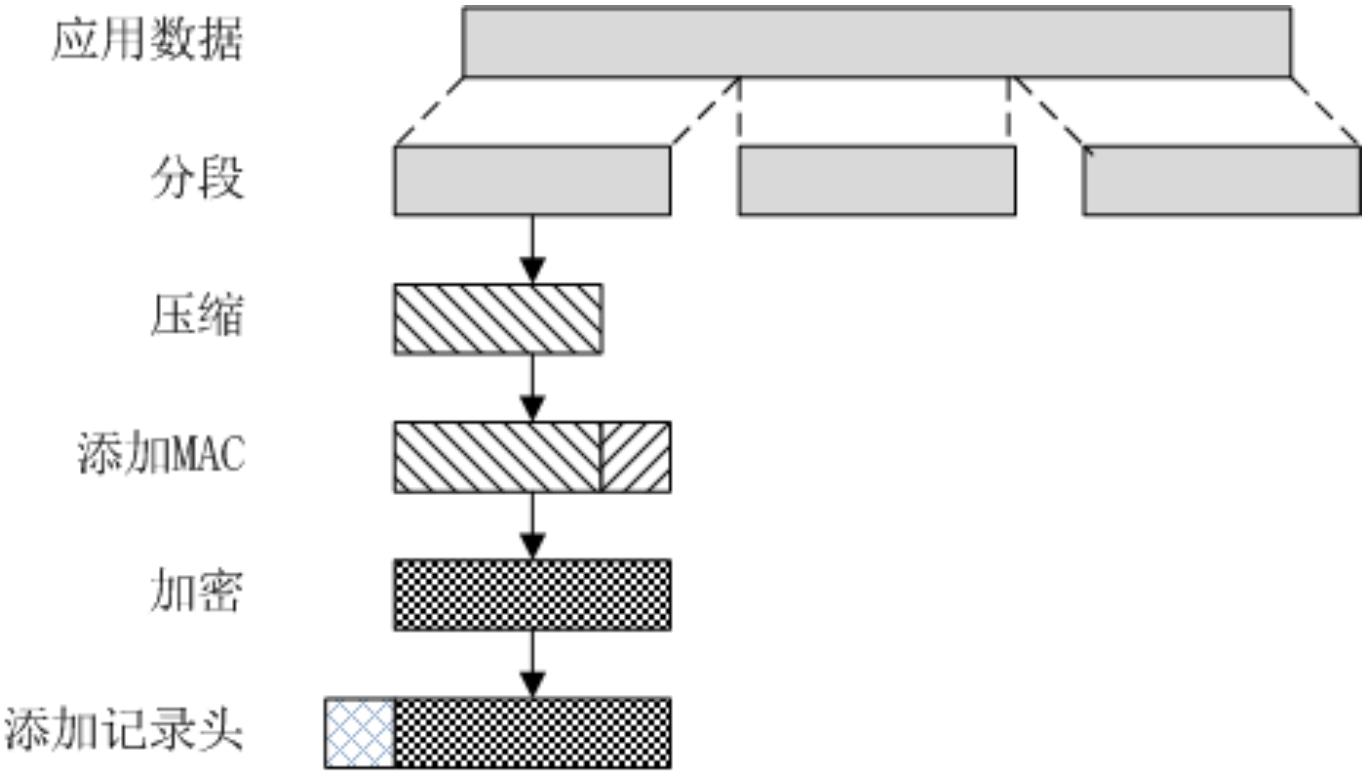
字段名	定义
会话标识（Session Identifier）	服务器选择的一个任意字节序列，用以标识一个活动的或可激活的会话。
对等证书（Peer Certificate）	用于鉴别实体身份的一个X.509.v3的证书，可为空。
压缩算法（Compression Method）	加密前进行数据压缩的算法。
密码规范（Cipher Spec）	指明数据加密的算法（无，或DES等）以及计算MAC的散列算法（如MD5或SHA-1），还包括其它参数，如散列长度。
主密钥（Master Secret）	48位密钥，在client与server之间共享。
可恢复性（Is Resumable）	指明该会话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$2^{64}-1$。

8.3.2 SSL协议规范

- SSL记录协议
  - 根据当前会话状态指定的参数以及连接状态中指定的等参数内容，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记录协议的操作

SSL记录格式

a. SSL记录协议

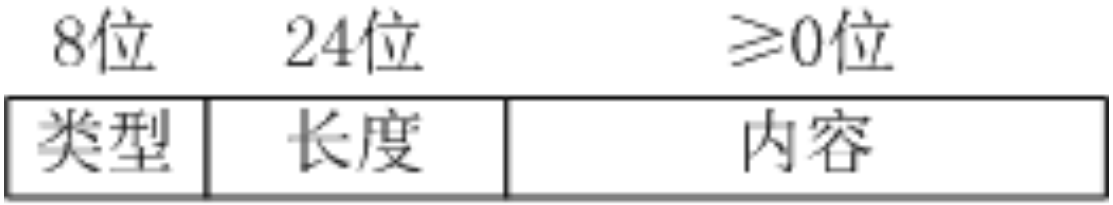
- 内容类型（8位）：用来指明封装数据的类型
- 主版本（8位）：指明SSL使用的主版本，
- 从版本（8位）：指明SSL使用的从版本
- 压缩长度（16位）：明文负载（如压缩，则为压缩后负载）的字节长度。
- 负载（可变）：指待处理的明文数据经过压缩（可选）、加密后形成的密文数据。
- MAC（16或20字节）：针对压缩后的明文数据进行计算得到的消息认证码。
  - 如基于SHA-1进行计算时，MAC的长度为20个字节，基于MD5进行计算时，MAC的长度为16个字节。

SSL握手协议

- 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。

格式

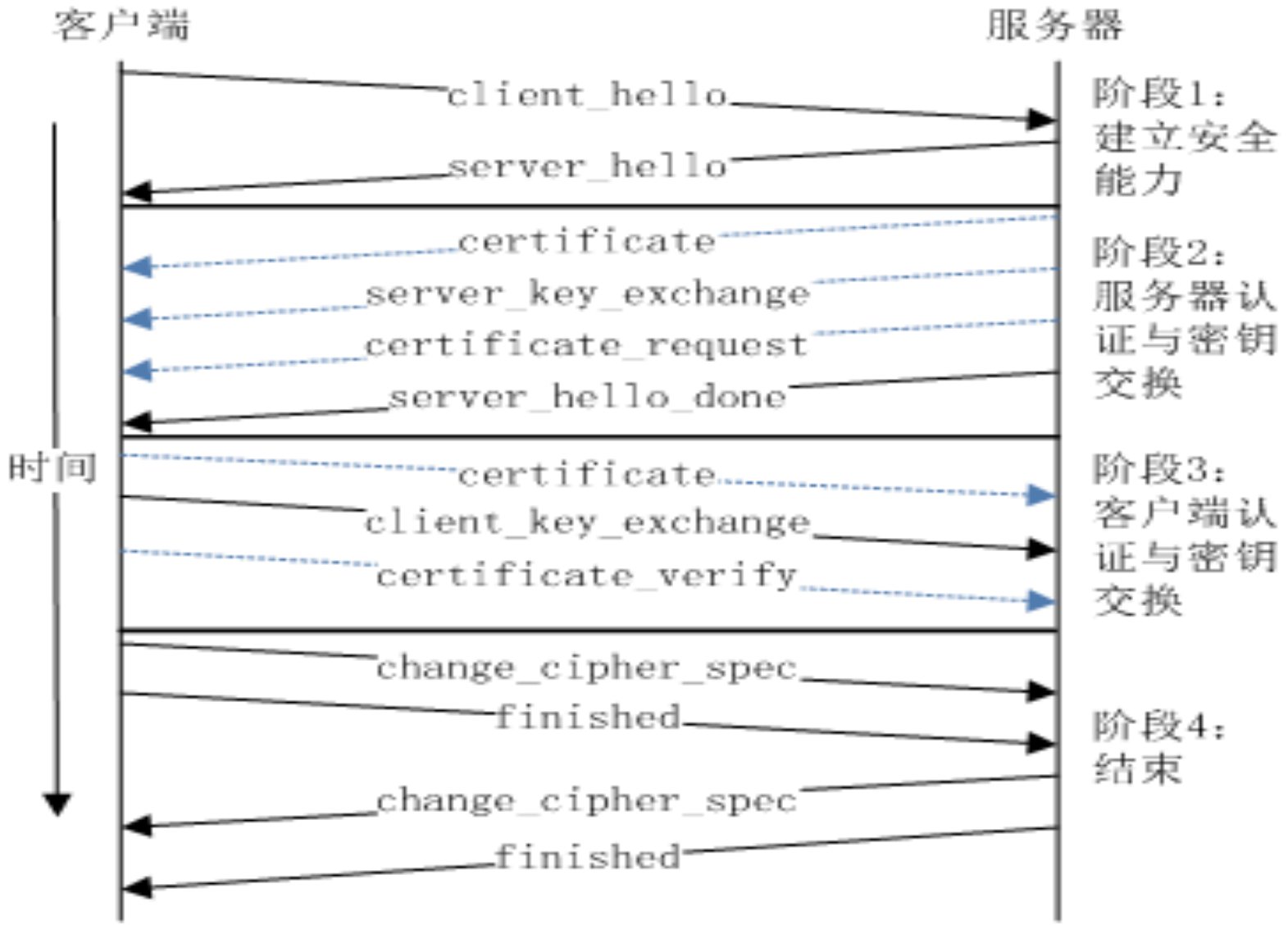
- 主要包括以下三个字段：
  - 类型（1字节）：为10种报文类型中的一种。
  - 长度（3字节）：以字节为单位的报文长度。
  - 内容（大于等于1字节）：与报文类型相关的参数。



b. 握手协议

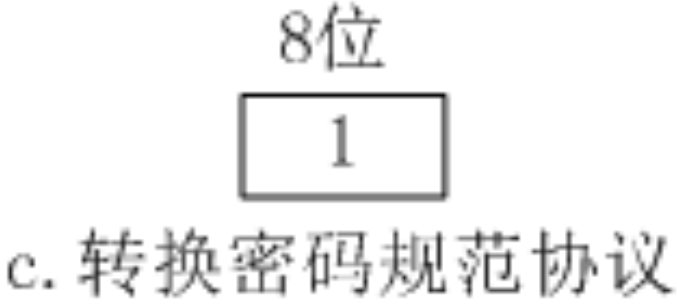
SSL握手协议操作的整个过程

- 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

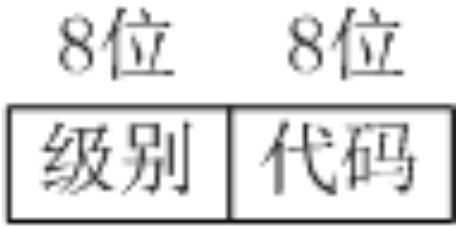
- 目的就是通知对方已将挂起（或新协商）的状态复制到当前状态中，用于更新当前连接使用的密码规范。
- 协议报文包含1个字节的信息，值为1表示更新使用新的密码规范。



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

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。

警告类型

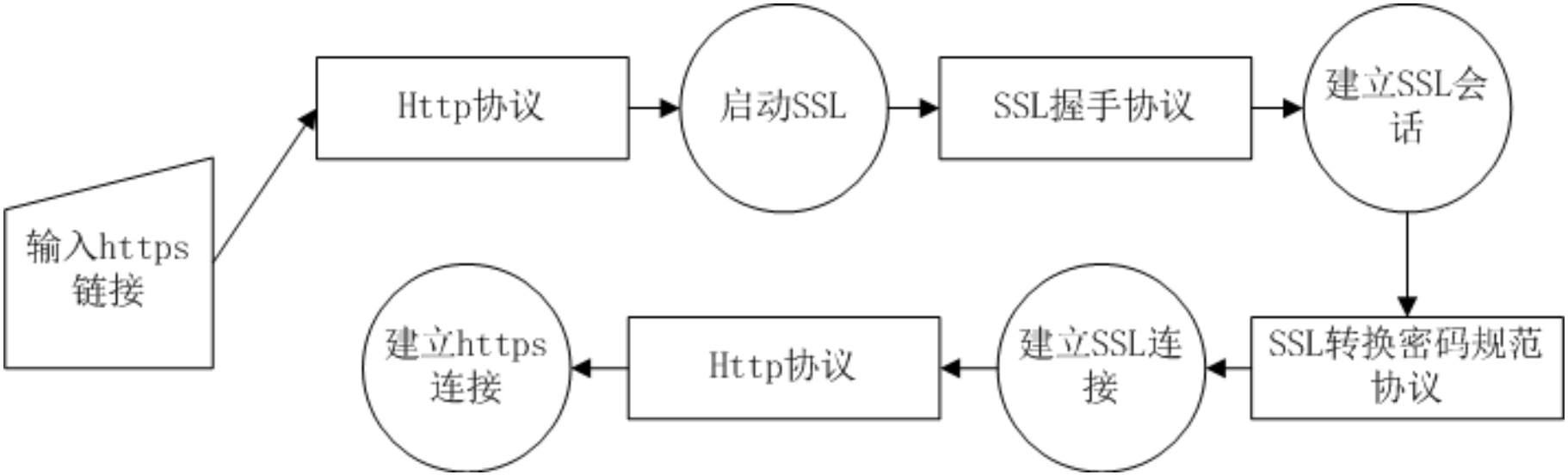
- 结束通知：通知对方将不再使用此连接发送任何信息；
- 无证书：如果无适当证书可用，此消息可作为对方证书请求的响应发送；
- 证书出错：证书被破坏，签名无法通过验证；
- 不支持的证书：不支持接收到的证书类型；
- 证书撤销：该证书被其签名者撤销；
- 证书过期：证书超过使用期限；
- 未知证书：处理证书时，出现其他错误，证书无法被接受。

8.3.3 HTTPS

- Netscape，HTTPS协议，解决HTTP协议的安全性。
- 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
  - 建立一个信息安全通道，用来保证数据传输的安全；
  - 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的身份认证可以分为单向身份认证和双向身份认证。

HTTPS协议处理过程



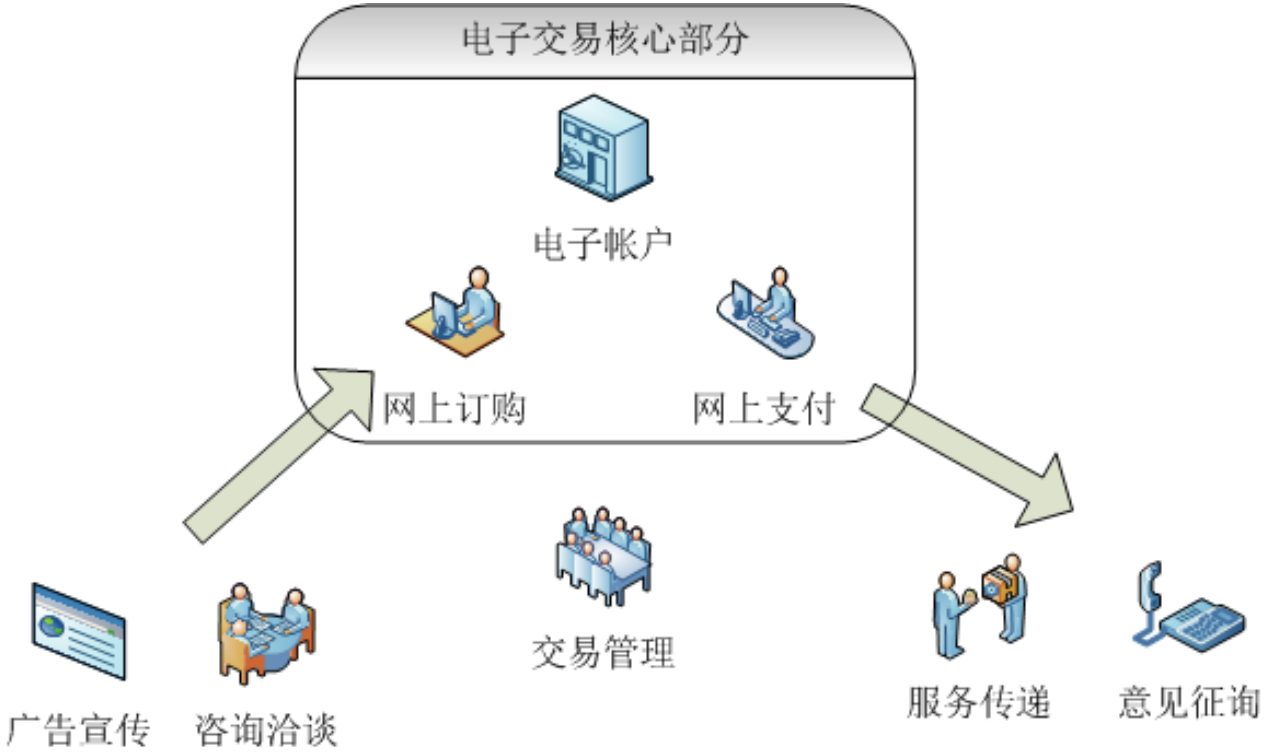
- CA证书的认证问题
  - 服务器的信任问题和客户端的信任问题。
  - 服务器的信任必须依靠CA证书解决，
    - HTTPS 的服务器必须从CA认证服务中心申请得到一个用于证明服务器身份的证书，
    - 只有服务器能够提供该证书时候，客户端完成对CA证书的验证，才能信任此服务器。

8.4 安全电子交易协议

- SET（Secure Electronic Transcation），Visa和MasterCard发起，联合IBM、Microsoft、Netscope、GTE等公司
- 1997年6月1日推出的用于电子商务的行业规范。
- 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已获得IETF标准的认可，是电子商务的发展方向。

8.4.1 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。主要部分：广告洽谈、网上交易和服务传递，网上交易是的核心。



安全问题及安全技术

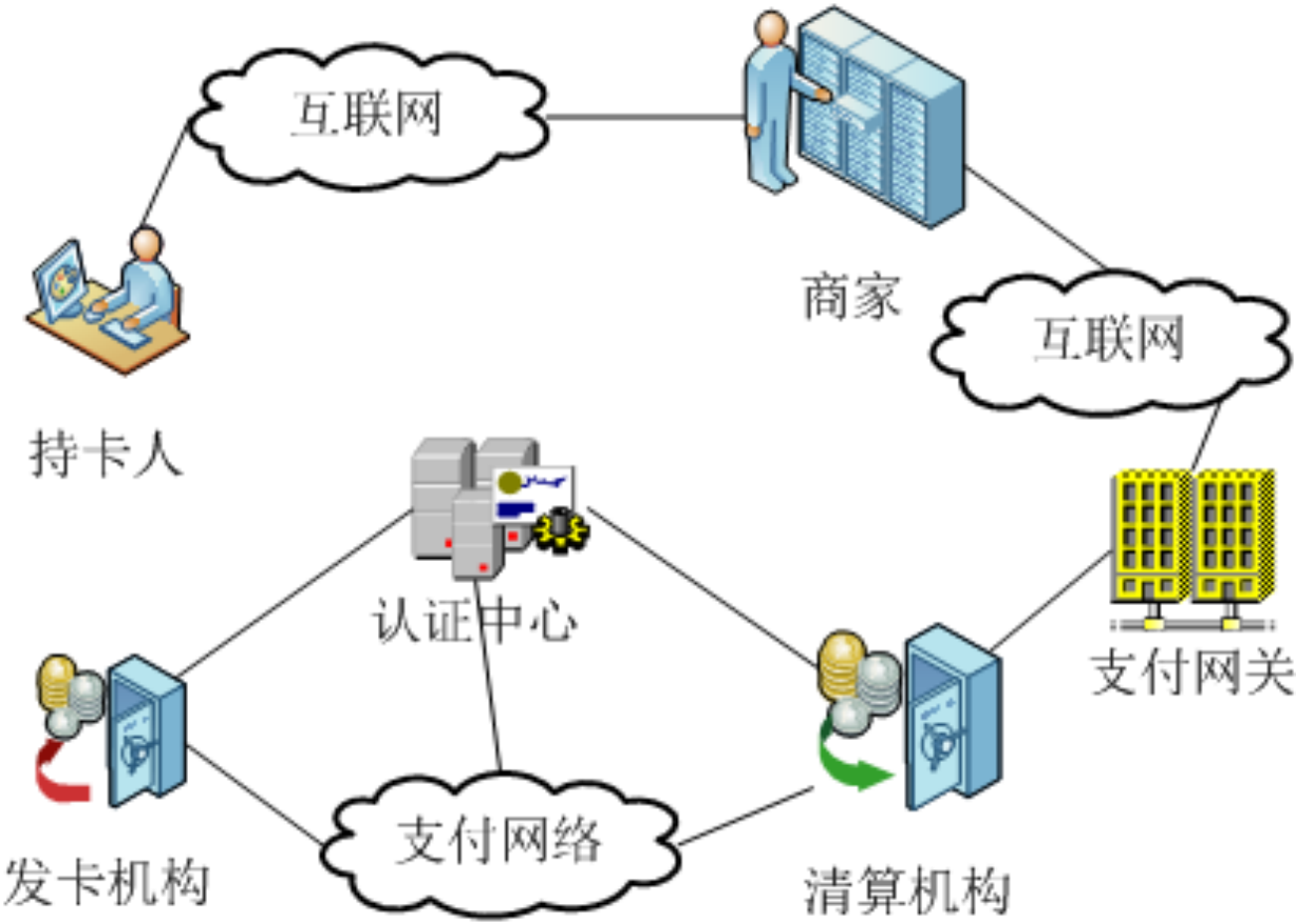
- 面临的安全问题
  - 有效性
  - 真实性
  - 机密性
  - 不可否认性
- 安全技术
  - 网络安全技术
  - 加密技术
  - 认证技术
  - 安全协议

8.4.2 SET协议概述

- SET安全协议的目标：
  - 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。
  - 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。
  - 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。
  - 保证网上交易的实时性，使支付过程都是在线的。
  - 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 Gateway、Certificate Authority



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。

8.4.3 SET的安全机制

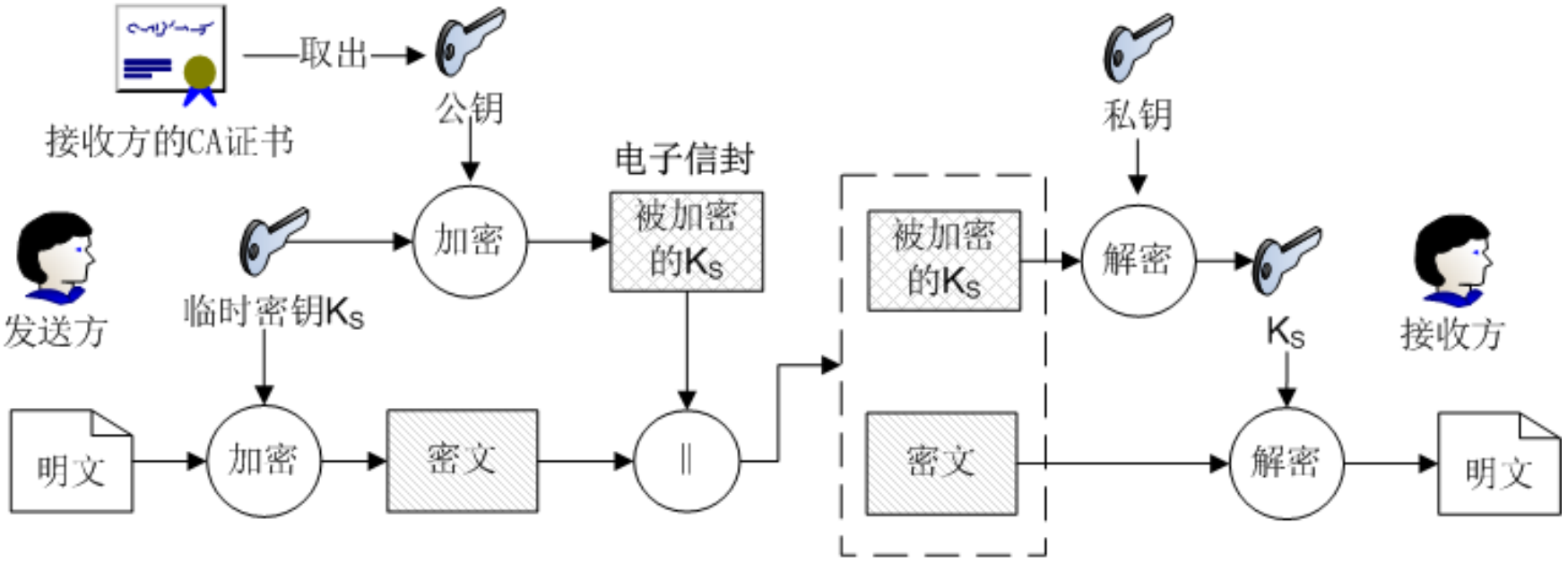
- SET协议安全性主要依靠其采用的多种安全机制，
  - 对称密钥密码
  - 公开密钥密码
  - 数字签名
  - 消息摘要
  - 电子信封
  - 数字证书
  - 双重签名
- 安全机制解决了包括机密性、完整性、身份认证和不可否认性等问题，提供了更高的信任度和可靠性。
- SET协议使如何保证商家、顾客和银行之间数据隐私的安全性？

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。
- 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。

电子信封

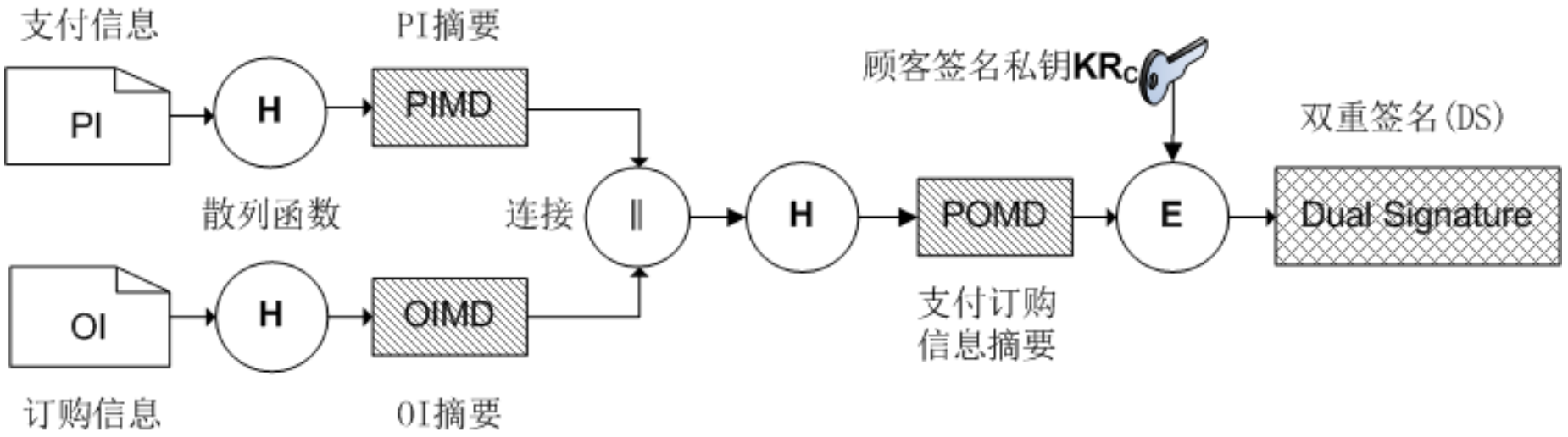
- SET协议使用电子信封来传递更新的密钥
- 电子信封涉及到两个密钥
  - 一个是接收方的公开密钥
  - 另一个是发送方生成临时密钥（对称密钥）



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。
- $DS = E_{KRc}[H(H(PI) \| H(OI))]$



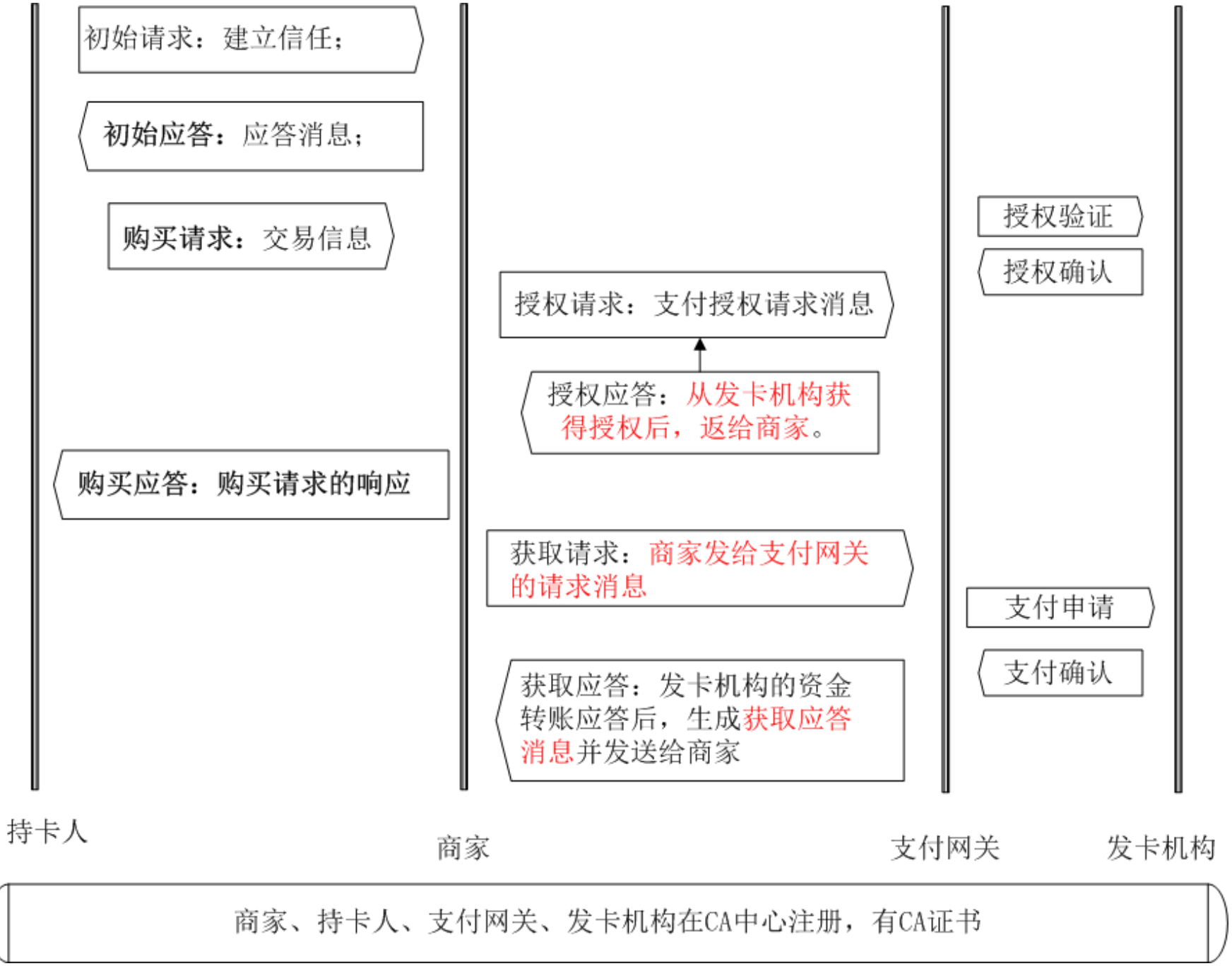
双重签名的使用过程

- 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 IIH（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）II 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。

8.4.4 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。

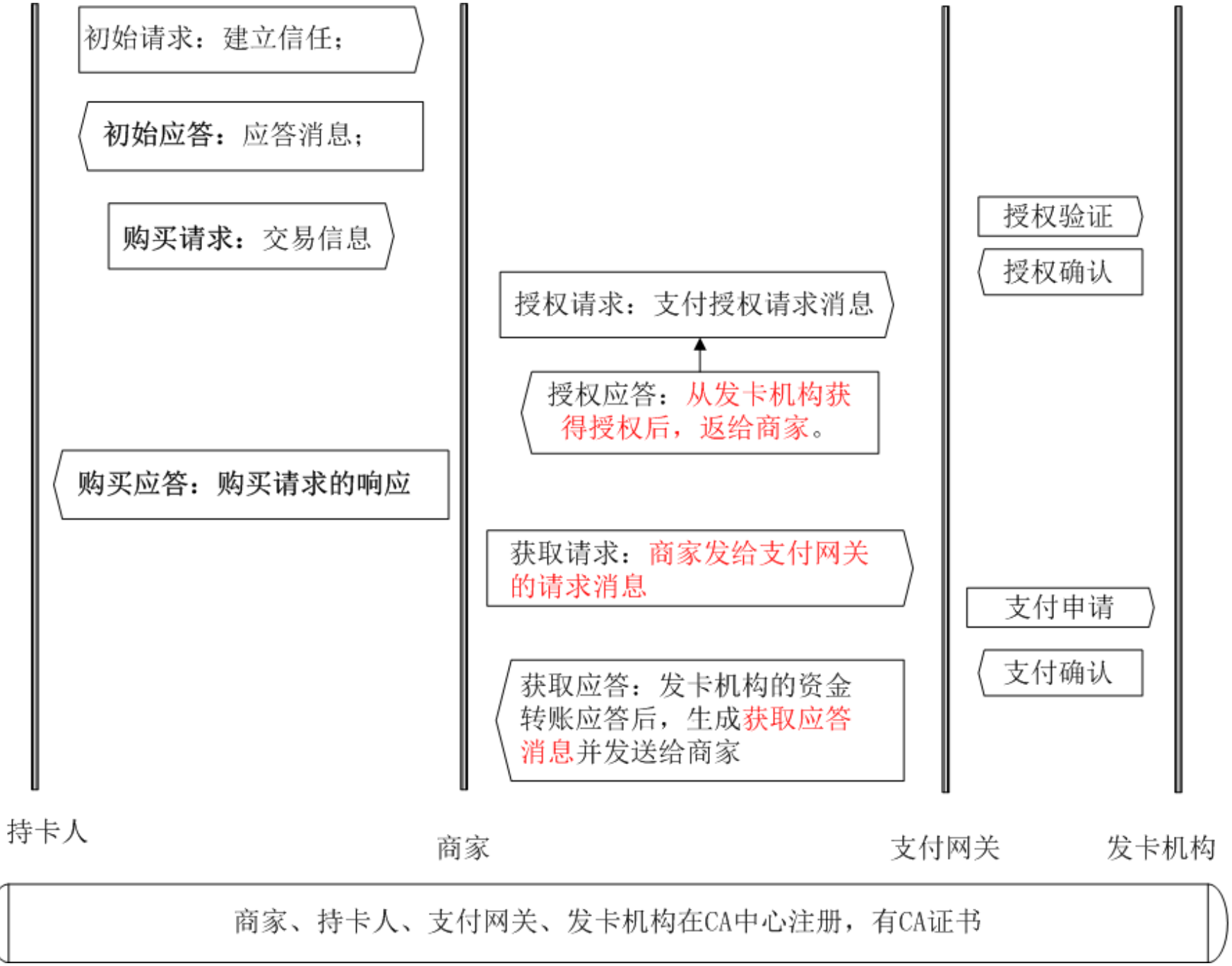
类型
持卡人注册
商家注册
购买请求
支付授权
支付获取
证书询问和状态
交易状态询问
撤销认可
撤销获取
信用
撤销信用
支付网关证书请求
批管理
出错信息


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**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。

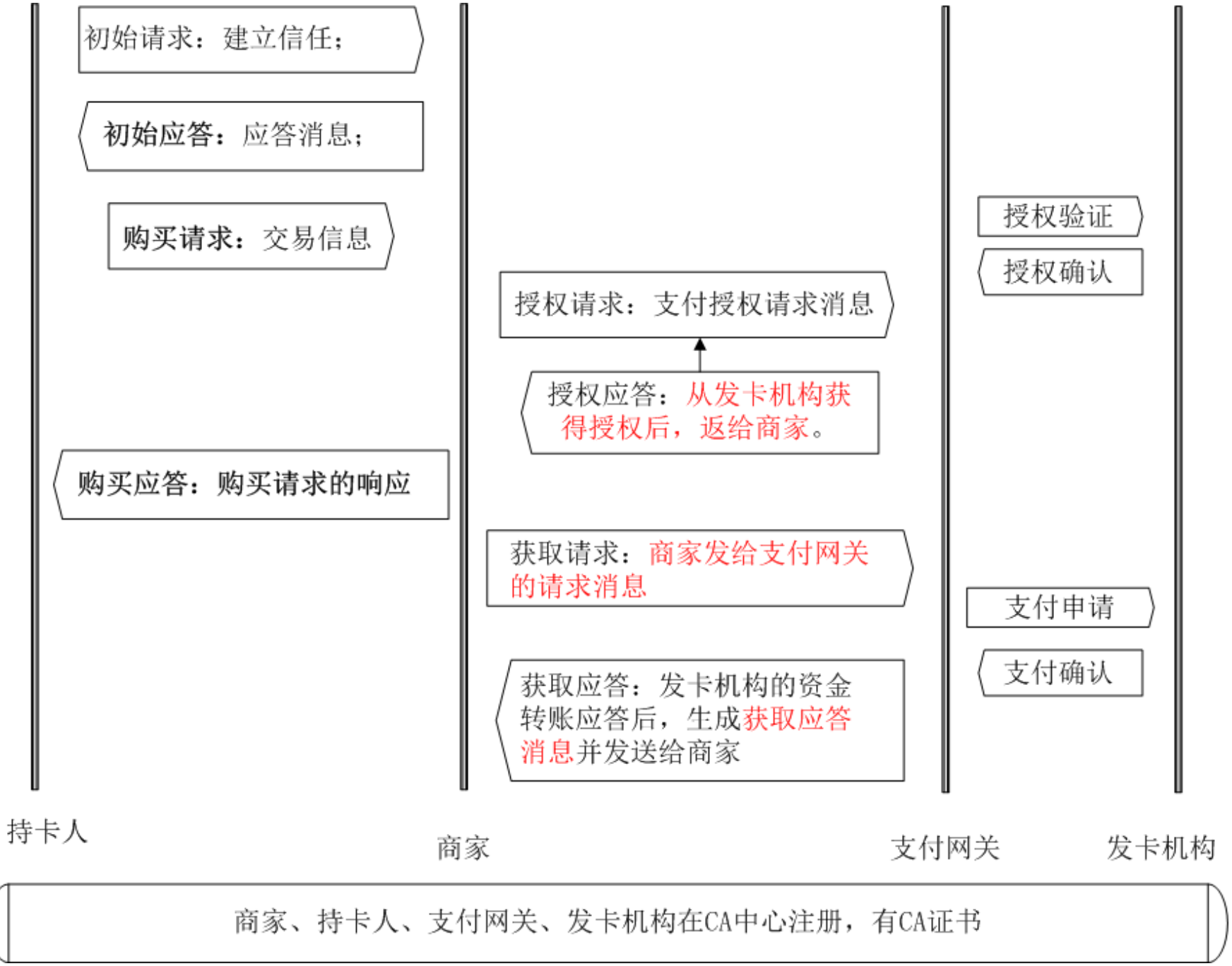

初始请求：建立信任；
初始应答：应答消息；
购买请求：交易信息
授权请求：支付授权请求消息
授权应答：从发卡机构获得授权后，返给商家。
购买应答：购买请求的响应
获取请求：商家发给支付网关的请求消息
获取应答：发卡机构的资金转账应答后，生成获取应答消息并发送给商家
授权验证
授权确认
支付申请
支付确认
持卡人
商家
支付网关
发卡机构
商家、持卡人、支付网关、发卡机构在CA中心注册，有CA证书

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。

授权应答

- 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；


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

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。

- 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。

8.4.5 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

- 你所了解的网络安全协议有哪些？分别工作在五层网络模型的哪一层？并分析一下在这一层所带来的优势和缺点？

Any question?