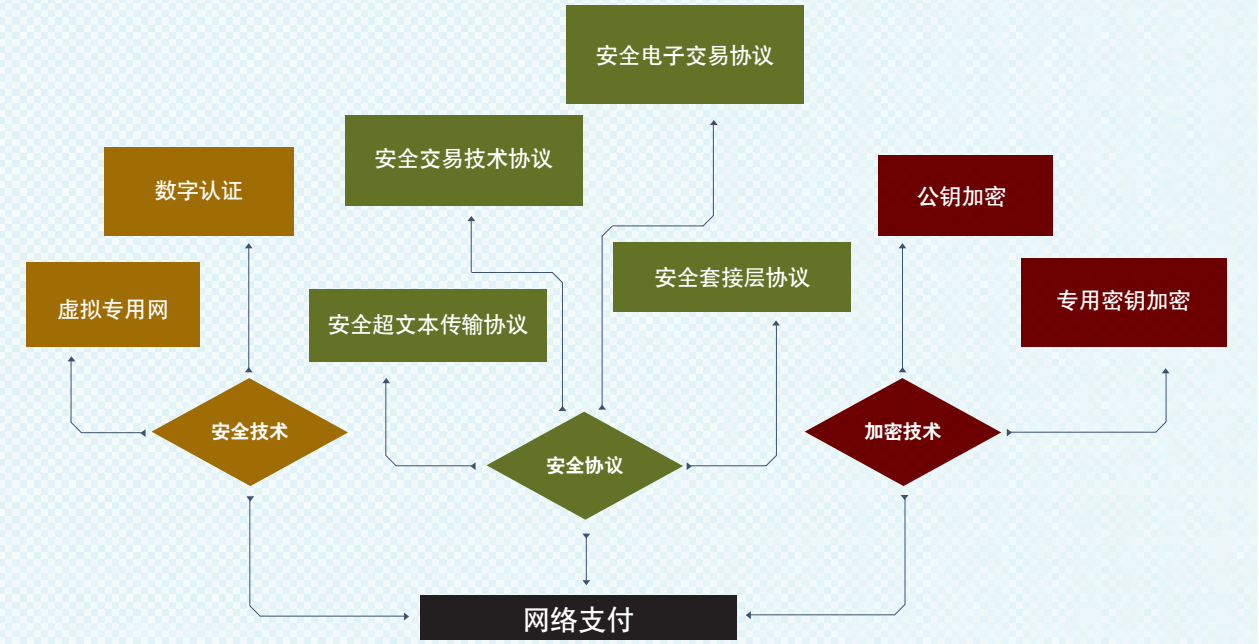
互联网支付技术架构图



安全协议

在电子商务大行其道的今天，支付手段日趋丰富，资金的安全成了无论商家还是消费者关心的第一要务，适应这种需要，网络支付中主要研发了种种协议进行数字签名的方式对资金的网络安全进行保障，保密技术乃是其中重中之重，在当前的环境中，主要应用到的是SSL，SET等形式的协议下的一些保密技术。

安全超文本传输协议（S－HTTP）

依靠密钥对的加密，保障Web站点间的交易信息传输的安全性。

安全套接层协议（SSL）

由Netscape公司提出的安全交易协议，提供加密、认证服务和报文的完整性。

安全交易技术协议（STT，Secure　Transaction　Technology）

将认证和解密在浏览器中分离开，用以提高安全控制能力。

安全电子交易协议（SET，Secure　Electronic　Transaction）

1997年5月底发布的SET　1.0涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数据认证、数据签名等，在目前中国网上银行业务中得到大量应用。

主要的安全技术

虚拟专用网（VPN）

这是可以在两个系统之间建立安全的信道（或隧道）的专用网络，用于电子数据交换（EDI）。通信的双方彼此熟悉。没有必要为所有的VPN进行统一的加密和认证。现有的或正在开发的数据隧道系统可以进一步增加VPN的安全性，因而能够保证数据的保密性和可用性。

数字认证

数字认证以电子方式甚至数据媒体的有效性（如录音、照片等）证明信息发送者和接收者的身份、文件的完整性。目前，数字认证一般都通过单向Hash函数来实现，它可以验证交易双方数据的完整性。另外，S/MIME协议也可以被集成到产品中，以便用户能够对通过E-mail发送的信息进行签名和认证。同时，商家也可以使用PGP（Pretty Good Privacy）技术，它允许利用可信的第三方对密钥进行控制。可见，数字认证技术将具有广阔的应用前景，它将直接影响电子商务的发展。

加密技术

加密技术可分为专用密钥加密和公钥加密，用来保证电子商务的保密性、完整性、真实性和非否认服务。

专用密钥加密：

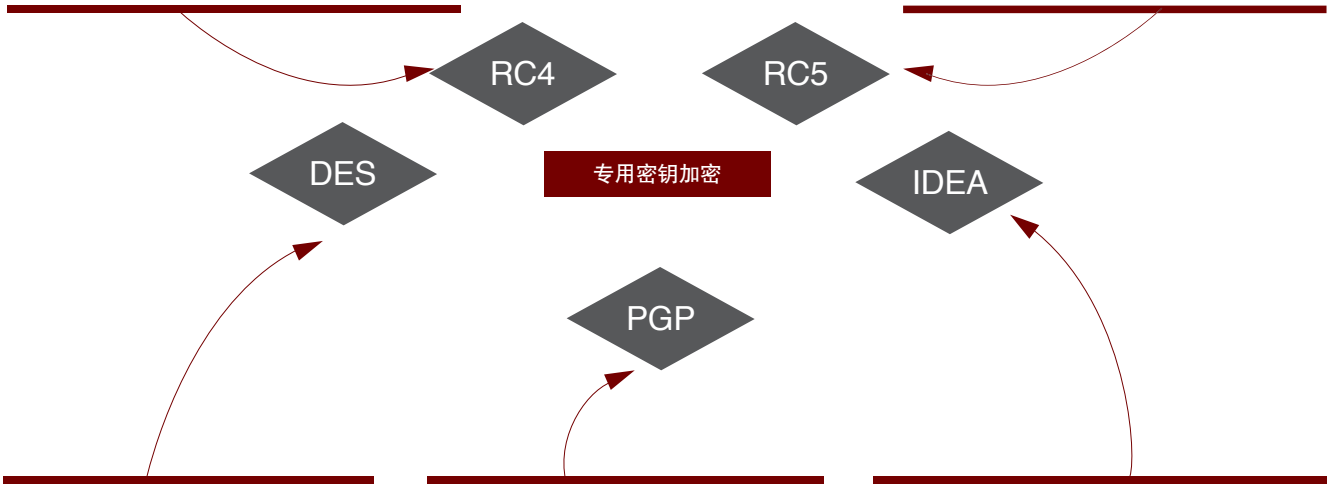
专用密钥加密（如3DES、IDEA、RC4和RC5）和公钥加密（如RSA、SEEK、PGP和EU）可用来电子商务的保密性、完整性、真实性和非否认服务。

RC4：

RC4加密算法是Ron RivestRon 设计的密钥长度可变的流加密算法簇。之所以称其为簇，是由于其核心部分的S-box长度可为任意，但一般为256字节。该算法的速度可以达到DES加密的10倍左右。

RC5：

RC5分组密码算法是1994由麻萨诸塞技术研究所的Ronald L. Rivest教授发明的，并由RSA实验室分析。它是参数可变的分组密码算法，三个可变的参数是：分组大小、密钥大小和加密轮数。在此算法中使用了三种运算：异或、加和循环。



DES：

DES使用一个56位的密钥以及附加的奇偶校验位，产生最大64位的分组大小。DES 的常见变体是三重 DES，使用 168 位的密钥对资料进行三次加密的一种机制；它通常（但非始终）提供极其强大的安全性。如果三个 56 位的子元素都相同，则三重 DES 向后兼容 DES。

IDEA(International Data Encryption Algorithm)：

IDEA是瑞士的James Massey，Xuejia Lai等人提出的加密算法，在密码学中属于数据块加密算法(Block Cipher)类。IDEA使用长度为128bit的密钥，数据块大小为64bit。从理论上讲，IDEA属于“强”加密算法，至今还没有出现对该算法的有效攻击算法。

PGP(pretty good privacy)：

PGP是一个基于RSA公匙加密体系的邮件加密软件。可用它对邮件加密以防止非授权人阅读，也可对邮件加上数字签名使邮件发送者得到确认。而且它的源代码是免费的。实际上PGP的功能还包括： PGP可以用来加密文件，还可以用PGP代替UUencode 生成RADIX 64 格式（就是MIME 的 BASE 64格式）的编码文件。 因此PGP几乎是最流行的公匙加密软件包。