几个著名的电子商务协议 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/65/2021_2022__E5_87_A0_E4_B8_AA_E8_91_97_E5_c40_65259.htm 一、Digicash Digicash是一个匿名的数字现金协议。所谓匿名是指消费者在消费中不会暴露其身份，例如现金交易虽然钞票有号码，但交易中一般不会加以记录。该协议的步骤如下：1．消费者从银行取款，他收到一个加密的数字钱币(Token)，此Token可当钱用；2．消费者对该Token作加密变换，使之仍能被商家检验其有效性，但已不能追踪消费者的身份 3．消费者在某商家消费即使用该Token以购物或购买服务，消费者进一步对该Token用密码变换以纳入商家的身份；4．商家检验该Token 以确认以前未收到过此 Token ；5．商家给消费者发货；6．商家将该电子 Token 送银行；7．银行检验该 Token 的唯一性。至此消费者的身份仍保密。除非银行查出该 Token 被消费者 重复使用，则消费者的身份将会被暴露，消费者的欺诈行为也暴露了。 在以上的第 3 步若发生了通信故障，则消费者无法判断商家究竟是否已收到该电子 Token 。 此时消费者有两种选择：*将其电子 Token 返回给银行或到另一商家处消费。如果消费者这样做了，而商家事实上在第 3步已收到了该 Token ，则当商家去银行将该 Token 兑现时会发现该 Token 的重复使用。*消费者不采取行动，既不另行消费也不退还给银行。如果消费者这样做了，而商家在第 3 步 事实上未收到该 Token ，则商家自然不会发货。这样一来，消费者既未收到所购之物，也未花 费该电子钱币，肯定受到了损失。 可见该数字现金协议是有缺陷的。 二、First Virtual First

Virtual 允许客户自由地购买商品，然后 First Virtual 使用 Email 同客户证实每一笔交易。First Virtual 对通信安全持怀疑态度并采取某种加密形式，并将每个电子商务交易转换为信用卡交易。First Virtual 比 Digicash 要好一些，但比其他电子商务系统要差。 三、SSL Netscape的安全套接层方法 (Secure Socket Layer ， SSL) 使用加密的办法建立一个安全的通信通道以便将客户的信用卡号传送给商家。它等价于使用一个安全电话连接将用户的信用卡通过电话读给商家。这一协议当然不能防止心术不正的商家的欺诈，因为该商家掌握了客户的信用卡号。商家欺诈是信用卡业所面临的最严重的问题之一。 四、SET SET(Secure Electronic Transaction)是 Visa 和 MasterCard 联合开发的一个协议，它具有很强的安全性。该协议由若干以前发表的协议形成，它们是： STT(Visa/Microsoft) 、SEPP(MasterCard) 和 iKP 协议族 (IBM) 。 SET 及其适合的诸协议是基于安全信用卡协议的一个例子。按照 SET ，客户将采购请求和价格进行数字签名，然后用银行公共密钥将付款信息 (例如信用卡号) 加密。商家认可该采购并将该请求传给银行。银行加工该请求，若价格匹配，则银行对客户的帐号扣款并指令商家完成该笔买卖。 SET的安全性超过 SSL，它可防止商家欺诈。值得指出的是，set协议不同寻常地复杂，该协议的描述有好几百页之多! SET显式地允许开一"后门"，商家可通过它获取客户的信用卡，这是否是一个安全问题？着实值得考究。 五、 Netbill 卡内基梅隆大学(现加州大学克利分校)的J.D.Tygar教授的研究组开发了Netbill协议，并正和CyberCash、Mellon Bank 和 Visa International一起在卡内基梅隆开发Netbill 的 Alpha 版。该协议已获得CyberCash 的商业

用途许可，CyberCash的CyberCoin协议也使用Netbill的方法。Netbill 协议涉及三方：客户、商家及 Netbill 服务器。客户持有的 Netbill 帐号等价于一个虚拟电子信用卡帐号。协议步骤如下：1．客户向商家查询某商品价格；2．商家向该客户报价；3．客户告知商家他接受该报价；4．商家将所请求的信息商品 (例如一个软件或一首歌曲) 用密钥 K 加密后发送给客户；5．客户准备一份电子采购订单 (Electronic Purchase Order， EPO) ，即三元式（价格、加密商品的密码单据、超时值）的数字签名值，客户将该已数字签名的 EPO 发送给商家。6．商家会签该 EPO ，商家也签上 K 的值，然后将此二者送给 Netbill 服务器；7． Netbill 服务器验证 EPO 签名和会签。然后检查客户的帐号，保证有足够的资金以便批准该交易，同时检查 EPO 上的超时值看是否过期。确认没有问题时， Netbill 服务器即从客户的帐号上将相当于商品价格的资金划往商家的帐号上，并存贮密钥 K 和加密商品的密码单据。然后准备一份包含值 K 的签好的收据，将该收据发给商家；8．商家记下该收据单传给客户，然后客户将第 4 步收到的加密信息商品解密。 Netbill协议就这样传送信息商品的加密拷贝，并在Netbill服务器的契据中记下解密密钥。