电子商务综合辅导：电子签字与强化电子签字 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/264/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_264038.htm 1996年6月14日，联合国国际贸易法委员会第29届年会通过了《电子商务示范法（简称〈示范法〉》。这个《示范法》确认在纸张环境下签字所具备的功能包括：确定一个人的身份；肯定是该人自己的签字；使该人与文件内容发生关系。除此之外，视所签文件的性质而定，签字还有多种其他功能。例如，签字可以证明一个当事方愿意受所签合同的约束；证明某人认可其为某一案文的作者；证明某人同意一份经由他人写出的文件的内容；证明一个人某时身在某地的事实。 为了确保须经过核证的电文不会仅仅由于未按照纸张文件特有的方式加以核证而否认其法律价值，《示范法》确定了在何种一般情况下，数据电文即可视为经过了具有足够可信度的核证，而且可以生效执行，视之达到了签字要求。《示范法》第7条规定：（1）如法律要求要有一个人签字，对于一项数据电文而言，倘若情况如下，即满足了该项要求：(a)使用了一种方法，鉴定了该人的身份，并且表明该人认可了数据电文内含的信息；(b)从所有各种情况看来，包括根据任何相关协议，所用方法是可靠的，对生成或传递数据电文的目的来说也是适当的。
（2）无论本条第1款所述要求是否采取一项义务的形式，也无论法律是不是仅仅规定了无签字时的后果，该款均将适用。《示范法》第7条侧重于签字的两种基本功能：一是确定一份文件的作者，二是证实该作者同意了该文件的内容。第（1）（a）款确立的原则是，在电子环境中，只要使用一种

方法来鉴别数据电文的发端人，并证实该发端人认可了该数据电文的内容，即可达到签字的基本法律功能。在保证安全可靠的基础上，第（1）（b）款提出了灵活性原则，数据电文的发端人与收件人之间的任何协议只要可靠，就适宜于生成或传递该数据电文所要达到的目的。1997年和1998年，在联合国国际贸易法委员会电子商务工作组第30次、31次会议上，委员会根据《示范法》不偏重任何媒体的方针，确定在数据电文的签字中，任何一种签字方法不应妨碍其他认证技术的使用，需要就数字签字和其他电子签字日益普遍使用而引起的新的法律问题达成一致。从这一立场出发，委员会决定起草《电子签字统一规则草案》，从而提出了电子签字的基本概念。电子签字 根据联合国国际贸易法委员会电子商务工作组第35次会议印发的《电子签字统一规则草案》第2条，“ 电子签字是指在数据电文中，以电子形式所含、所附或在逻辑上与数据电文有联系的数据，和与数据电文有关系的任何方法，它可用以鉴别与数据电文有关的签字持有人和表明此人认可数据电文所含信息。 ”在上述定义中，使用了“ 以电子形式 ”、“ 有关系的任何方法 ”等词语，与《示范法》中有关提法相一致。 电子签字概念的提出，将电子商务活动中的数据签字（Digital signature）和其他电子签字统一起来，充分体现了不偏重任何媒体的方针，在促进数据签字发展的同时，也考虑到公钥加密技术的替代问题，考虑到其他电子签字方式的发展问题，例如使用生物测定法或其他一些此类技术。强化电子签字 根据联合国国际贸易法委员会电子商务工作组第35次会议印发的《电子签字统一规则草案》第2 条，“ 强化电子签字是指一种电子签字，对于这种电子签字，通

过使用一种安全程序可以表明该签字：（1） 在其使用范围内，对签字持有人而言独一无二；（2） 由签字持有人或以签字持有人单独掌握的方法所制造并附以数据电文中；（3） 其制造及与有关数据电文的连接方式对电文的完整性提供可靠的保证。《电子签字统一规则草案》第6 条进一步规定了签字的推定：（1）如对于一数据电文使用了强化电子签字，则推定该数据电文已经签字。（2）在法律规定需要某人的签字时，如果使用的电子签字根据各种情况，包括根据任何有关协议，既适合生成或传送数据电文所要达到的目的，而且也同样可靠，则对该数据电文而言，即满足了该项签字要求。（3）在法律规定需要某人签字时，如果使用了强化电子签字，则对该数据电文而言，即满足了该项签字要求。《电子签字统一规则草案》第8 条还规定，颁布国规定的主管机关或机构可确定某一电子签字是一种强化电子签字。也就是说，颁布国可指定一个机关或机构有权确定哪种具体的技术符合强化电子签字的条件。 强化电子签字通常采用公开密钥加密体制。这种加密体制是1976年美国的Diffie和Hallman提出的。它的基本思想是设计一对不同的加密算法E和解密算法D。E和D之间具有如下性质：（1） D{E（M）}= M，即对数据M用加密算法E加密后再用解密算法D解密，仍可还原为M；（2） 加密算法E和解密算法D都是易于计算的；（3） 从加密算法E难以推导出解密算法D的结构。 网络中的用户各自选定一对加密算法E和解密算法D，并将加密算法E公开，放入网络用户都可访问的公共存储区，将解密算法D严格保密。如果A用户希望向B用户发送数据（M），A首先从公共存储区中取得B的加密算法Eb，并用Eb对数据进行

加密，产生Eb（M），传输给B。B接收到密文后，用解密工具Db 进行解密，获得明文数据M。根据性质（3），B以外的所有用户都不掌握解密算法Db，并且无法从公开的Eb中推导出Db，所以即使攻击者获得了密文，也无法解出相应的明文。由于这种体制的加密密钥可以公开，因此被称为公开密钥加密体制；也是由于使用了不同的加密和解密密钥，又被称为非对称密钥密码体制。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com