第3章

电子签名法律制度

学习目标

通过对本章的学习与技能训练，要求学生：

1．掌握电子签名的概念和特征，电子认证的含义，关于电子认证机构的义务与责任的法律规定。

2．理解电子签名的归属与完整性推定原则，电子签名的法律效力。

3．了解电子签名与传统签名的异同，电子认证的分类和作用。

4．熟悉电子证书的法律意义，认证机构的设立和运行。

案例导读

因电子签名被冒用，提起诉讼案增多

近年来，广东省深圳市盐田区人民法院受理的因身份信息被冒用而起诉撤销工商登记案件，呈逐年上升趋势，2016 年 27 宗，2017 年 52 宗，截至 2018 年 6 月 30 日已受理 48 宗。上述案件中，因电子签名被冒用而起诉的案件占比较大。

盐田法院有关负责人认为，导致身份信息被冒用频发的主要原因在于:

一是个人忽视电子签名的法律效力。根据相关规定，可靠的电子签名与手写签名，或者盖章具有同等的法律效力。一些不法分子通过发布招聘兼职信息的形式，以几十元到数百元不等的报酬，吸引涉世未深的大学生或文化程度不高的社会人士办理数字证书，部分风险意识薄弱的人盲目听从其指引及不实言论，任由个人名下的数字证书脱离控制，从而被不法分子获取并使用。

二是电子认证服务提供者未能严格遵守电子认证业务规则而签发电子签名认证证书。根据相关规定，电子认证服务机构在受理电子签名认证证书申请前有告知义务，某些电子认证服务机构的数字证书电子认证业务规则也载明收到申请后，应对申请者身份进行识别与鉴别，通过有效手段确保证书信息与申请信息相符，并将证书签发给正确的申请者。但在现实操作中，数字证书大多数是在电子认证服务机构授权的印章店办理的，业务人员及印章店管理者未履行清

晰、全面的告知义务，未当场交付给电子签名申请人。

（资料来源：http://legal.people.com.cn/n1/2018/0816/c42510-30232669.html）

辩证与思考：什么是电子认证？电子认证的法律意义是什么？

3.1 电子签名与电子签名法

交易安全是电子商务中所要解决的核心问题之一。如何消除电子交易带来的信任危机是电子签名产生的原因。计算机网络、电子支付系统和自动化交易系统的广泛应用，使电子签名问题显得越来越突出。因为在许多应用系统中，电子签名问题不解决，交易安全就无法保障，这些系统实际上也就不具有应用价值。这也是电子签名问题成为电子商务中的重要的技术与法律问题的原因所在。

▸▸ 3.1.1 电子签名的基本含义

签名（Signature）一般是指一个人亲笔在一份文件上写下名字或留下印记、印章或其他特殊符号，以确定签名人的身份，并确定签名人对文件内容予以认可。传统的签名必须依附于某种有形介质，而在电子商务交易中，文件是通过数据电文的发送、交换、传输、储存来形成的，不依赖于有形介质，这就需要通过一种技术手段来识别交易当事人、保证交易安全，以达到与传统的手写签名相同的功能。这种能够达到与手写签名相同功能的技术手段，一般称为电子签名（Electronic Signature）。

1. 电子签名的定义

电子签名，是电子商务的基础性技术，是使用最为广泛的现代认证技术方法，主要是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

国际社会普遍认为，凡是能在电子通信中，起到证明当事人的身份、证明当事人对文件内容的认可的电子技术手段，都可称为电子签名，电子签名即现代认证技术的一般性概念，它是电子商务安全的重要保障手段。

《中华人民共和国电子签名法》（以下简称《电子签名法》），借鉴了国际组织与发达国家对电子签名立法的研究成果，并结合我国电子商务的实际情况，给出了电子签名的定义。电子签名，指数据电文中以电子形式所含、所附，用于识别签名人身份并表明签名人认可其中内容的数据。这里的数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

通俗地说，电子签名包括用于识别签名人身份并表明签名人认可其中内容的程序、符号、声音等数据，签名人加密后把签名文件发送给交易对方，交易对方收到的签名文件是一堆“乱码”，需解密后验证。

由概念可以看出，电子签名应具备如下特征：

（1）电子签名是以电子形式出现的数据。

（2）电子签名是附着于数据电文的。电子签名可以是数据电文的一个组成部分，也可以是数据电文的附属，与数据电文具有某种逻辑关系、能够使数据电文与电子签名相联系。

（3）电子签名必须能够识别签名人身份并表明签名人认可与电子签名相联系的数据电文的内容。

2. 电子签名的形式

电子签名具有多种形式，如附着于电子文件的手写签名的数字化图像，包括采用生物笔迹辨别法所形成的图像，向收件人发出证实发送人身份的密码、计算机口令，采用特定生物技术识别工具，如指纹或是眼虹膜透视辨别法等。无论采用什么样的技术手段，只要符合电子签名的概念，均可视为电子签名。

3. 电子签名的功能

在电子商务活动中，电子签名主要有三个作用：

（1）证明文件的来源，即识别签名人。

（2）表明签名人对文件内容的确认。

（3）构成签名人对文件内容正确性和完整性负责的根据。电子签名与传统商务活动中的签名、盖章作用相同，具有同样的法律效力。

学而思：列举我国比较权威的电子签名网站。

▶▶ 3.1.2　电子签名的相关概念

由于电子签名的技术性和法律性较强，所以我国《电子签名法》中对相关的专门概念加以了界定，如电子签名人、电子签名依赖方、电子签名认证证书、电子签名制作数据、电子签名验证数据等。

1. 电子签名人（E-Signaturer）

电子签名人指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。电子签名人可以通过两种方式签名。第一，用自己的电子签名制作数据实施电子签名。第二，委托他人，使用委托人的电子签名制作数据实施电子签名。毫无疑问，通过第一种方式进行电子签名时，签名人就是制作电子签名的人。通过第二种方式进行电子签名时，签名人是指签名制作数据指代的人，并不是指实施电子签名的人。

2. 电子签名依赖方（E-Signature Dependence）

电子签名依赖方指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

当人们阅读数据电文时，要确认数据电文的制作人，人们首先会查验含在数据电文之中或附在数据电文之后的电子签名。根据电子签名技术的不同，这样的查验既可以直接进行，也可

能需要通过查验与签名对应的证书进行。查验通过后，确认数据电文内容可信，并根据数据电文的内容进行决策或行动的人，就是电子签名依赖方。

3. 电子签名认证证书（E-Signature Certificate）

电子签名认证证书指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。有些电子签名是可以直观验证的，有些电子签名则不能直观验证。不能直观验证电子签名时，技术上必须提供一种方法，能把电子签名与电子签名人联系起来。数字签名便是这样的一种技术。数字签名技术通过一种数学运算，建立起唯一匹配的一对密钥，即公钥和私钥。把公钥与签名人的信息作为验证签名人身份的中介，私钥则是签名制作数据，通过公钥与私钥的特性，建立起电子签名人与电子签名制作数据之间的联系。记载了公钥和签名人（公钥持有人）信息的数据电文，就是电子签名认证证书。

4. 电子签名制作数据（Data）

电子签名制作数据指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。进行电子签名时，往往是通过一种程序和算法对数据原文进行运算，变换成与原文唯一对应并且方便查验的数据电文。这种对原文进行变换的程序和算法就是电子签名制作数据。

5. 电子签名验证数据

电子签名验证数据指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。可以直观获得并能将签名人鉴别出来的数据，就是电子签名验证数据。比如数字签名技术中的公钥，通过公钥就可以找出电子签名人是谁。

▶▶ 3.1.3 电子签名、传统签名与数字签名

1. 签名的法律意义

在传统商务活动中，为了保证交易的安全与真实，书面文件要由当事人或其负责人签字、盖章，以便让交易双方识别，法律上才能承认该书面文件的合法的有效性。在电子商务活动中，合同或文件是以无形的电子文件形式表现和传递的。在电子文件上，传统的手写签名和盖章是无法进行的，这就必须依靠技术手段来替代。能够在电子文件中识别双方交易人的真实身份，保证交易的安全性、真实性及不可抵赖性，电子签名是起到与手写签名或者盖章同等作用的电子技术手段。所以，不论是传统商务还是电子商务，法律对签名都要求必须是一个记号，它要有某些预期的后果，它必须是由当事人来完成的。因此，签名一般是具有法律意义的行为。

2. 电子签名与传统签名的关系

（1）主要功能相同。

无论是传统签名还是电子签名，其主要功能都是一样的：一是表明文件的来源，即识别签名人。二是表明签名人对文件内容的确认。三是能够构成签名人对文件内容正确性和完整性负

责的根据。

（2）电子签名并不是传统签名的电子化。

从手段上来看，电子签名与传统签名之间并无实质联系。之所以称之为“电子签名”，只是由于电子签名使用目的和履行的功能与传统签名相同而已。

3. 电子签名与数字签名（Digital Signature）

数字签名指通过某种密码运算（Password Computing）生成一系列符号（Symbol）及代码（Code），组成电子密码（Electronic Password）进行签名，来代替书写签名或印章的技术方法。对于这种电子式的签名还可进行技术验证，其验证的准确度是一般手工签名和图章的验证无法比拟的。

数字签名具有如下特征：首先，在数字签名过程中，私钥（Private Key）只能为发件方独家拥有，正常情况下，其他人不可能拥有和使用。其次，由于原文资料经过多次加密及解密，以及公钥（Public Key）和私钥的完全对应性特征，经数字签名后的文件资料内容不能被轻易篡改。最后，验证方（Verification Party）在验证文件时是使用发件方提供的公钥进行的，任何人都可以验证。

因此，安全性是数字签名方法的基本特点，从保证交易信息的安全性、完整性以及认证的便捷和可靠性等签名的基本功能来看，数字签名是目前使用最多、技术最为成熟的电子签名技术方式。实际上，不少国家都在法律上承认数字签名，甚至有些国家的电子签名立法指定数字签名为唯一合法的电子签名形式。

“电子签名”并不是完全等同于“数字签名”。实现电子签名的技术手段有很多种，但数字签名是目前电子商务、电子政务中应用最普遍的、技术最成熟的、可操作性最强的一种电子签名方法。数字签名采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可，并且数字签名还能验证出文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。所以，当前电子签名法中提到的签名，一般指的就是“数字签名”。

▸▸ 3.1.4　我国《电子签名法》的基本框架

我国《电子签名法》制定于 2004 年，并经过了 2015 年和 2019 年的两次修正。该法的出台，是为了规范电子签名行为，确立电子签名的法律效力，维护各方合法权益，进一步促进电子商务和电子政务的发展，增强交易的安全性。该法是针对我国电子商务发展中最为重要的一些法律问题，借鉴联合国及有关国家和地区有关电子签名立法的成功经验制定的。

我国《电子签名法》共分五章、三十六条，立法的直接目的是规范电子签名行为，确立电子签名的法律效力，维护各方合法权益；立法的最终目的是促进电子商务和电子政务的发展，增强交易的安全性。《电子签名法》重点解决了五个方面的问题：一是确立了电子签名的法律效力。二是规范了电子签名的行为。三是明确了认证机构的法律地位及认证程序，并给认证机构设置了市场准入条件和行政许可的程序。四是规定了电子签名的安全保障措施。五是明确了认证机构行政许可的实施主体是国务院信息产业主管部门。其总体思路是通过确立电子签名的法律效力，明确电子签名规则，消除电子商务发展的法律障碍，维护电子交易各方的合法权益，

保障电子交易安全，为电子商务和电子政务发展创造有利的法律环境。

3.2 电子签名的法律效力

随着电子商务和电子政务的迅猛发展，电子签名的应用范围愈加广泛，但是它毕竟是新兴事物，在传统的法律环境下遇到了一些法律上的问题，特别是其法律效力的问题。

▶▶ 3.2.1 电子签名的法律效力概述

在使用电子签名时，主要遵从当事人意思自治原则，由当事人自主约定是否使用电子签名。只要符合法律规定的条件，电子签名与手写签名、书面文件具有同等的法律效力。

1. 使用电子签名应当遵从意思自治原则

意思自治，是民事法律中的一项基本原则，《中华人民共和国民法典》（以下简称《民法典》）规定“民事主体从事民事活动，应当遵循自愿原则，按照自己的意思设立、变更、终止民事法律关系”。当事人意思自治的核心是尊重当事人自主的意思选择，从法律上承认当事人可以自由决定相互之间的法律关系。即便民事活动通过计算机和互联网等方式进行，也应当遵循意思自治原则，由当事人自主约定是否使用数据电文、电子签名。有关国家的电子签名法一般都承认当事人意思自治。

借鉴国际立法经验与我国电子商务发展的实际情况，我国《电子签名法》第三条第一款明确规定：“民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。”

应该注意的是，电子签名的使用并不仅限于民事活动，还会用于电子政务活动和其他社会活动。《电子签名法》已授权国务院或者国务院规定的部门可以依据其制定政务活动和社会活动中使用电子签名的具体办法。因此，在这些活动中使用电子签名，还应遵循国务院或者国务院有关部门的具体规定。

2. 电子签名的法律适用范围

根据我国《电子签名法》第三条第二款的规定“当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力”，即在当事人约定使用电子签名、数据电文的情况下，不能以该文书中某项信息或签名采用了电子形式，作为否定其法律效力的唯一理由。电子签名虽然以电子形式出现，与手写签名、书面文件不同，但是只要符合法律规定的条件，电子签名与手写签名、书面文件具有同等的法律效力。因此，有关国际组织、国家和地区的电子商务法或电子签名法一般都对电子签名的法律效力问题做出规定，要求不得以其采用电子形式而加以歧视。

电子交易是一种新兴的交易方式，电子签名并未在社会活动中获得广泛应用，广大民众的认知度不高。同时，电子签名的应用需要借助于一定的技术手段，物质条件也会限制一部分民众使用这种方式。由于上述原因，并基于交易安全因素的考虑，我国《电子签名法》第三条第三款规定了适用例外，包括：

（1）涉及婚姻、收养、继承等人身关系的；

（2）涉及停止供水、供热、供气等公用事业服务的；

（3）法律、行政法规规定的不适用电子文书的其他情形。

▶▶ 3.2.2　电子签名的法律效力

根据《电子签名法》的规定，只要电子签名符合相应的认定标准，就可以认定为可靠的电子签名，承认其法律效力。

1. 可靠的电子签名

（1）可靠的电子签名应当具备的法定条件。

第一，电子签名制作数据用于电子签名时属于电子签名人专有。电子签名制作数据是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。它是电子签名人在签名过程中掌握的核心数据。唯有通过电子签名制作数据的归属判断，才能确定电子签名与电子签名人之间的同一性和准确性。因此，一旦电子签名制作数据被他人占有，则依赖于该电子签名制作数据而生成的电子签名有可能与电子签名人的意愿不符，显然不能被视为可靠的电子签名。

第二，签署时，电子签名制作数据仅由电子签名人控制。这一项规定是对电子签名过程中电子签名制作数据归谁控制的要求。这里所规定的控制是指一种实质上的控制，即基于电子签名人的自由意志而对电子签名制作数据的控制。在电子签名人实施电子签名行为的过程中，无论是电子签名人自己实施签名行为，还是委托他人代为实施签名行为，只要电子签名人拥有实质上的控制权，则其所实施的签名行为，满足本法此项规定的要求。

第三，签署后对电子签名的任何改动能够被发现。采用数字签名技术的签名人签署后，对方当事人可以通过一定的技术手段来验证其所收到的数据电文是否是发件人所发出的，发件人的数字签名有没有被改动过。倘若能够发现发件人的数字签名签署后曾经被他人更改过，则该项签名不能满足本法此项规定的要求，不能成为一项可靠的电子签名。

第四，签署后对数据电文内容和形式的任何改动能够被发现。电子签名的一项重要功能在于表明签名人认可数据电文的内容，而要实现这一功能，必须要求电子签名在技术手段上能够保证经签名人签署后的数据电文不能被他人篡改。否则，电子签名人依据一定的技术手段实施电子签名，签署后的数据电文被他人篡改，却不能够被发现，此时出现的法律纠纷将无法依据《电子签名法》予以解决，电子签名人的合法权益难以得到有效的保护。因此，要符合《电子签名法》规定的可靠的电子签名的要求，必须保证电子签名签署后，对数据电文内容和形式的任何改动都能够被发现。

一项电子签名如果同时符合上述四项条件，可以被视为可靠的电子签名。

（2）可靠的电子签名与手写签名、盖章具有同等的法律效力。

当事人可以约定选择可靠的电子签名应当具备的条件和采用的技术方案。由于电子签名技

术手段的多样性，当事人在从事电子商务或者其他活动中所约定采用的电子签名技术如能够满足当事人对于保障交易安全性的需求，同样可以承认其法律效力并予以保护。如计算机口令、虹膜识别技术及数字签名技术等。

案例链接

上上签电子签约添互联网法院成功判例

某信托公司与个人用户A在2019年间通过上上签电子签约平台签署了一份金融贷款合同，明文规定了贷款金额、期限、利率等事项。双方发生还款纠纷后，该信托公司及时向法院提交了双方签署的贷款合同、平台服务协议以及基于电子存证技术保留的全周期电子数据证据。北京互联网法院对上上签平台出具的电子证据予以采信，充分认可信托公司电子合同的合法性，并以此为依据对此案做出了裁决。在上上签的帮助下，该信托公司的合法权益不仅得到了法律的保护，也大大节省了维权成本。目前，上上签平台提供的在线签约、线上留痕、线上存证的模式已成为电子签约行业标配，上上签也成为司法判例成功率非常高的电子签约服务商。

（资料来源：https://www.sohu.com/a/386524323_100275129）

2. 电子签名人的法律义务

（1）电子签名人应当妥善保管电子签名制作数据。

电子签名制作数据是将电子签名与电子签名人可靠联系起来的重要手段。电子签名人应当妥善保管电子签名制作数据，一旦电子签名制作数据失密，他人有可能利用电子签名人的电子签名制作数据从事违法行为或者牟取非法利益，给电子签名人和电子签名依赖方造成损失。在实践中，电子签名制作数据的载体包括磁盘、光盘等，尽管这些载体在使用过程中需要加入电子签名人的安全指令才能启动，但是这些载体一旦丢失或者被他人窃取，则他人通过破解这些相对简单的安全指令就可以在互联网上以电子签名人的名义从事交易活动。与传统交易不同，网上交易过程中当事人之间往往并不见面，当事人之间主要凭借的是对方当事人的电子签名来验证和核实相互间的身份，电子签名制作数据的丢失会给不法分子提供可乘之机。因此，电子签名人应当妥善保管电子签名制作数据，防止丢失或者为他人所窃取，以免给自己和对方当事人造成不必要的损失。

（2）电子签名制作数据已经失密或者可能已经失密。

电子签名人知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名制作数据。即便电子签名人尽到妥善保管的义务，电子签名制作数据仍然存在泄密的可能。所谓的“知悉电子签名制作数据已经失密或者可能已经失密”包含两层意思：一是电子签名人已经明确知道电子签名制作数据已失密，例如，电子签名人发现未经自己允许，有人在互联网上以电子签名人的名义从事商业活动。二是电子签名人知悉电子签名制作数据有可能已经失密，例如，电子签名人发现自己存放电子签名制作数据的磁盘丢失，在这种情况下，丢失的磁盘中的安全指令有可能被破译，电子签名制作数据有可能被他人用于非法活动。

在这两种情况下，依据《电子签名法》的规定，电子签名人应当做到：

一是立即停止使用电子签名制作数据。因为在电子签名制作数据已经失密或者可能已经失

密的情况下，电子签名人继续使用其电子签名制作数据有可能使电子签名依赖方更加难以确认电子签名的真伪，给交易安全带来更多的不确定性。

二是及时告知有关各方当事人，避免有关各方当事人因继续信赖电子签名人的签名而造成损失或者损失的进一步扩大。

3. 伪造、冒用、盗用他人的电子签名的法律责任

由于电子商务活动中，交易各方彼此不见面，这为形形色色的违法犯罪行为提供了有利条件。伪造、冒用、盗用他人的电子签名，就是一种扰乱市场秩序，侵犯他人权益的行为。同时，这种行为也严重影响了电子交易的安全，法律对这些行为应当严厉制裁。

伪造他人的电子签名，是指未经电子签名合法持有人的授权而创制电子签名，或者创制一个认证证书，列明实际并不存在的用户签名等。

冒用他人的电子签名，是指非电子签名持有人未经电子签名人的授权以电子签名人的名义实施电子签名的行为。

盗用他人的电子签名，是指秘密窃取并使用他人电子签名的行为。

（1）伪造、冒用、盗用他人电子签名的刑事责任。

伪造、冒用、盗用他人电子签名的犯罪，主要是指构成《刑法》第二百八十条关于妨害国家机关公文、证件、印章的犯罪，伪造公司、企业、事业单位、人民团体印章的犯罪。构成该条的犯罪，必须具备以下条件：一是主观上是故意。二是客观上实施了伪造他人的电子签名的行为。对于构成犯罪的，依照《刑法》第二百八十条的规定，伪造、变造国家机关的公文、证件、印章的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上十年以下有期徒刑。伪造公司、企业、事业单位、人民团体的印章的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

（2）伪造、冒用、盗用他人电子签名的民事责任。

民事责任，是指进行了民事违法行为的人在民法上承担的对其不利的法律后果。合法的民事权益受法律保护，如果受到他人的非法侵害，则需要给权利人以充分的法律救济，这就是民事责任制度。伪造、冒用、盗用他人电子签名属于侵权的民事责任，承担方式主要包括：停止侵害、排除妨碍、消除危险、返还财产、恢复原状、赔偿损失、赔礼道歉等。对于承担民事责任的几种方式，可以单独适用，也可以合并适用。

3.3　电子认证及其法律效力

电子认证与电子签名一样都是电子商务中的安全保障机制。为了完成网络交易，交易双方的身份必须通过权威的第三方加以确认，该权威第三方就是电子商务认证机构。电子商务中的身份认证并不是政府部门行使行政管理的手段，而应由企业遵循政府的指导意见或政策性指南，按照市场需求和规范来运作。

3.3.1 电子认证的概念

认证，是指权威的、中立的、没有直接利害关系的第三人或机构，对当事人提出的包括文件、身份、物品及其产地、品质等具有法律意义的事实与资格，经审查属实后，做出的证明。电子认证是认证的现代方式。

1. 电子认证的定义

电子认证（Electronic Authentication）是以电子认证证书（又称数字证书）为核心的加密技术，它以 PKI（Public Key Infrastructure，公钥基础设施，即利用公钥理论和技术建立的提供网络信息安全服务的基础设施）技术为基础，对网络上传输的信息进行加密和解密、数字签名和签名验证。电子认证是电子政务和电子商务中的核心环节，可以确保网上传递信息的保密性、完整性和不可否认性，保证网络应用的安全性。

2. 电子认证的特性

电子认证以其所具有的四大特性显示其在信息化应用中基础性、关键性的作用。

第一，电子认证具有真实性。要确保交流双方、交易双方身份的真实，信息内容的真实，以及交流信息、交易时间发生的真实。

第二，电子认证具有完整性。要确保交流双方、交易双方的信息是完整的，没有被篡改和伪造过。

第三，电子认证具有机密性。确保交换数据、电文、信息的隐蔽性。

第四，电子认证具有不可否认性。一旦需要从第三方的角度，按照法律的要求取证，在整个交流交易的过程中，需要不可否认性。

这四大特性构成的电子认证是支撑信息化应用的坚实基础。在信息网络化应用的过程中，我们也确实能感受到，进行网上聊天时可以不关心对方的身份及是否值得信赖，但如果是在网上开展商业活动的时候，就要求对对方的身份以及对方发出的信息的真实性加以确认，在这种情况下，电子认证就变得非常重要了。

3.3.2 电子签名和电子认证的关系

电子签名确保了合同的有效成立，确定了合同的内容，以及当事人的身份和愿意接受合同约束的意思表示，保证了合同因签名而具有的证明当事人交易关系的能力。然而，电子签名只是从内部为当事人提供了数据信息安全性的保障。如果有人盗用电子签名进行交易以达到其诈骗的目的，如果交易一方否认合同义务而不予履行，那么合同另一方当事人仍是处于危险之中的，交易信用安全仍然岌岌可危。因而，从外部对当事人合同关系进行切实有效的保护，以及对电子签名、当事人身份、合同内容等信息的真实性进行证明显得尤为重要。此种外部保护就是由不涉及合同利益的第三方公平地对交易信息的真实性，主要是当事人电子签名的真实性进行证明，它依赖于电子认证以及认证机构。

电子签名和电子认证都着力解决电子商务的安全问题，但二者却存在着明显的区别。电子签名解决的是文件归属与身份辨别的问题，即交易者是谁的问题；电子认证解决的是签名者的可信度问题，即交易对方是否确实就是签署名字所代表的人，而且是由公正的第三方来保证签名者的身份。电子签名属于网络安全的技术保证，即从技术角度进行的身份认证；电子认证则属于网络安全的制度保证，即从制度角度进行的身份认证。因此，电子签名是电子认证产生的前提条件，电子认证则是电子签名的有效保障，两者是既相互一致，又相互区别的关系。

▶▶ 3.3.3　我国电子认证立法

《电子签名法》是我国对电子认证服务业实施管理的基本法律依据，在设立电子认证服务市场准入制度的同时，考虑到我国电子认证业务还处于发展起步阶段的情况，规定了政府部门有必要对电子认证机构实施有效的、适度的监管，并明确授权国务院信息产业主管部门制定电子认证服务业的具体管理办法，对电子认证服务提供者实施监督管理。《电子签名法》颁布后，信息产业部、国家密码管理局根据该法授权，分别制定了《电子认证服务管理办法》和《电子认证服务密码管理办法》，对电子认证服务机构的设立、运营等做出了具体规定。

▶▶ 3.3.4　电子签名认证证书制度

为了保证电子商务交易安全，加强身份认证，由电子认证机构颁发电子签名认证证书无疑是最为有效的办法。电子签名认证证书与电子认证机构是电子认证的两大核心要素。电子签名认证证书是身份（或站点）的数字证明，内含公钥，可以广为散发。该证书是由一个权威的机构发放，并由该机构担保其有效性，该机构就是身份认证机构（Certificate Authority，CA），我国称为电子认证服务机构。

1. 电子签名认证证书的概念

电子签名认证证书就是数字证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录，是电子认证的核心。通俗地讲，电子签名认证证书用来表明网络通信各方真实身份，由权威的、中立的第三方电子认证服务机构发行和管理的个人或单位在网络上的身份证。电子签名认证证书必须具有唯一性和可靠性。

根据证书的持有者不同，电子签名认证证书可分为个人身份证书、个人安全电子邮件证书、企业身份证书、企业安全电子邮件证书、信用卡电子签名认证证书和电子合同认证证书等。

根据我国《电子签名法》第二十一条规定“电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：电子认证服务提供者名称、证书持有人名称、证书序列号、证书有效期、证书持有人的电子签名验证数据、电子认证服务提供者的电子签名、国务院信息产业主管部门规定的其他内容”。

2. 电子签名认证证书的作用

依赖于互联网的电子商务系统必须保证具有十分可靠的安全保密技术，也就是说，必须保证网络安全的四大要素，即信息传输的保密性、数据交换的完整性、发送信息的不可否认性、

交易者身份的确定性。

（1）信息的保密性。

交易中的商务信息均有保密的要求，如信用卡的账号和用户名被人知悉，就可能被盗用，订货和付款的信息被竞争对手获悉，就可能丧失商机。因此在电子商务的信息传播中一般均有加密的要求。

（2）交易者身份的确定性。

网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先必须能够确认对方的身份，对商家来说要考虑客户端是不是骗子，而客户也会担心网上的商店是不是一个从事欺诈的“黑店”。因此能方便而可靠地确认对方的身份是交易的前提。对于为顾客或用户开展服务的银行、信用卡公司和销售商店，为了做到安全、保密、可靠地开展服务活动，都要进行身份认证的工作。对有关的销售商店来说，他们对顾客所用的信用卡的号码是不知道的，商店只能把信用卡的确认工作完全交给银行来完成。银行和信用卡公司可以采用各种保密与识别方法，确认顾客的身份是否合法，同时还要防止发生拒付款问题及确认订货和订货收据信息等。

（3）不可否认性。

由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。例如，订购黄金，订货时金价较低，但收到订单后，金价上涨了，如收单方否认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。因此电子交易通信过程的各个环节都必须是不可否认的。

（4）不可修改性。

交易的文件是不可被修改的，如上例所举的订购黄金。供货单位在收到订单后，发现金价大幅上涨了，如其能改动文件内容，将订购数 1 吨改为 1 克，则可大幅受益，那么订货单位可能就会因此而蒙受损失。因此电子交易文件也必须做到不可修改，以保障交易的严肃性和公正性。

3. 电子签名认证证书的使用流程

以电子商务活动为例，来说明电子签名认证证书的使用流程。

（1）电子商务的参与各方。

电子商务应用中主要有以下五个交易参与方：买家、服务商、供货商、银行和电子认证中心（CA）。

（2）交易流程的主要阶段。

交易流程主要有以下三个阶段：

第一阶段，电子签名认证证书的注册申请。交易各方通过认证中心（CA）获取各自的数字。

第二阶段，银行的支付中心对买家的电子签名认证证书进行验证，通过验证后，将买家的所付款冻结在银行中。此时服务商和供应商也相互进行电子签名认证证书的验证，通过验证后，可以履行交易内容进行发货。

第三阶段，银行验证服务商和供货商的电子签名认证证书后，将买家冻结在银行中的货款转到服务商和供货商的户头上，完成了此项电子交易。由于参与交易的各方都持有认证中心（CA）所颁发的电子签名认证证书，所以，能够保证在交易的过程中参与各方的真实身份，防止他人假冒。

4. 电子签名认证证书的应用领域

电子认证服务机构所发放的电子签名认证证书可以应用于公众网络上的行政作业活动和商务活动，包括支付型和非支付型电子商务活动，其应用范围涉及需要身份认证及数据安全的各个行业，包括传统的商业、制造业、流通业的网上交易，以及公共事业、金融服务业、工商税务海关、政府行政办公、教育科研单位、保险、医疗等网上作业系统。它主要应用于电子政务、网上购物、企业与企业的电子贸易、安全电子邮件、网上证券交易、网上银行等方面。

（1）网上报税。

利用基于电子签名认证证书的用户身份认证技术对网上报税系统中的申报数据进行数字签名，确保申报数据的完整性，确认系统用户的真实身份和申报数据的真实来源，防止出现抵赖行为和他人伪造、篡改数据；利用基于电子签名认证证书的安全通信协议技术，对网络上传输的机密信息进行加密，可以防止商业机密或其他敏感信息泄露。

（2）网上办公。

网上办公系统综合国内政府、企事业单位的办公特点，提供了一个虚拟的办公环境，并在该系统中嵌入数字认证技术，展开网上政文的上传下达，通过网络联结各个岗位的工作人员，通过电子签名认证证书进行数字加密和数字签名，实行跨部门运作，实现安全便捷的网上办公。

（3）网上招标。

以往的招投标受时间、地域、人文的影响，存在着许多的弊病，如外地投标者的不便、招投标各方的资质，以及招标单位和投标单位之间存在的猫儿腻。而实行网上的公开招投标，经贸委利用数字身份证书对企业进行身份确认，招投标企业只有在通过经贸委的身份和资质审核后，才可在网上展开招投标活动，从而确保了招投标企业的安全性和合法性，企业双方通过安全网络通道了解和确认对方的信息，选择符合自己条件的合作伙伴，确保网上的招投标在一种安全、透明、信任、合法、高效的环境下进行。通过该网上招投标系统，企业能够制定正确的投资取向，根据自身的实际情况，选择合适的合作者。

（4）网上交易。

利用电子签名认证证书的认证技术，对交易双方进行身份确认以及资质的审核，确保交易者信息的唯一性和不可抵赖性，保护了交易各方的利益，实现安全交易。

（5）安全电子邮件。

邮件的发送方利用接收方的公开密钥对邮件进行加密，邮件接收方用自己的私有密钥解密，确保了邮件在传输过程中信息的安全性、完整性和唯一性。

另外，不同的电子认证机构所发放的电子签名认证证书有其特定的使用范围。如上海市电子商务安全证书管理中心有限公司（SHECA）现已完成证书系统的建设，面向用户发放电子签名认证证书。其中 SET 证书已应用在东方航空公司网上售票系统，整个交易流程符合 SET 协议，与国际接轨。通用证书（Universal Certificate）已在网上购物、企业与企业的电子贸易、安全电子邮件、网上证券交易、网上银行等领域得到了广泛的应用。为了配合社会保障工作，方便百姓，SHECA 将根据用户的需要，把个人电子签名认证证书存放在社会保障卡内，为个人网上安全作业提供便利。SHECA 还与上海市企业代码证中心合作，将企业代码证和企业电子签名认证证书一体化，为企业网上交易、网上报税、网上报关、网上作业奠定基础，免去企业面对众多的服务窗口之苦。

3.3.5 电子认证机构

电子认证服务机构主要是为了保证用户之间在网上传递信息的安全性、真实性、可靠性、完整性和不可抵赖性，而对用户的身份真实性进行验证，负责向电子商务的各个主体颁发并管理符合国内、国际安全电子交易协议标准的电子商务安全证书的权威第三方。

1. 电子认证服务机构的定义

我国《电子签名法》第十六条则规定：电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。这里的电子认证服务提供者，即电子认证服务机构，指为电子签名人和电子签名依赖方提供电子认证服务的第三方机构。

从定义中可以看出，电子认证服务机构具有以下特性：

（1）权威性。

一个认证机构必须具有权威性，否则其验证的电子签名或载有电子签名的文件将毫无公信力可言。为此，该机构必须具有法律授权，被依法批准设立，并且在实际工作中依赖于认证机构本身的服务水平，成为值得客户信赖的认证机构。

（2）可信性。

由于使用了专业的技术，有专业的人员，专门的设备、设施、场所资金的要求、密码技术方面的规范，以及法律和法规要求的其他条件，保证了认证机构的安全性和可信度。

认证机构掌握了众多授权的个人或实体的隐私或机密资料，从职业守则而言，负有保密的职责，因此认证机构的工作人员应当具有良好的职业道德，忠于职守，保证信息不被泄露给任何非授权的个人或实体。同时，认证机构应当配备完善的安全设备，有效地防范黑客的非法入侵等。

（3）公正性。

认证机构的职责在于为客户提供值得信赖的真实信息，故其所提供的各类信息必须真实、准确、完整、可靠，且应遵守法律及行业规则，严禁为客户提供虚假信息。为此，其必须独立于交流双方、交易双方，绝不介入双方的利益，从而确保其认证的公正性。

学而思：列举我国较为权威的电子认证机构。

2. 电子认证服务机构的职能

电子认证服务机构的职能包括以下内容：

（1）颁发证书。

电子认证服务机构接收、验证用户（包括下级认证中心和最终用户）的电子认证证书的申请，将申请的内容进行备案，并根据申请的内容确定是否受理该证书的申请。如果接受该证书的申请，则进一步确定给用户颁发何种类型的证书。新证书用电子认证服务机构的私钥签名以后，发送到目录服务器供用户下载和查询。为了保证消息的完整性，返回给用户的所有应答信息都要使用认证中心的签名。

（2）更新证书。

电子认证服务机构可以定期更新所有用户的证书，或者根据用户的请求来更新用户的证书。

（3）查询证书。

证书的查询可以分为两类，其一是证书申请的查询，电子认证服务机构根据用户的查询请求返回当前用户证书申请的处理过程；其二是用户证书的查询，这类查询由目录服务器来完成，目录服务器根据用户的请求返回适当的证书。

（4）证书的作废。

当用户的私钥由于泄密等原因造成用户证书需要申请作废时，用户需要向电子认证服务机构提出证书作废的请求，电子认证服务机构根据用户的请求确定是否将该证书作废。另外一种证书作废的情况是证书已经过了有效期，电子认证服务机构自动将该证书作废。电子认证服务机构通过维护证书作废列表（Certificate Revocation List，CRL）来完成上述功能。

（5）证书的归档。

证书具有一定的有效期，证书过了有效期之后就将作废，但是不能将作废的证书简单地丢弃，因为有时可能需要验证以前的某个交易过程中产生的数字签名，这时我们就需要查询作废的证书。基于此类考虑，电子认证服务机构还应当具备管理作废证书和作废私钥的功能。

3. 电子认证机构的设立

为了保证电子认证的严肃性和公正性，我国《电子签名法》第十六条规定：“电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。”

（1）电子认证服务机构申请设立的条件。

根据《电子签名法》和《电子认证服务管理办法》的相关要求，设立电子认证服务机构，提供电子认证服务，应当具备下列条件：

具有独立的企业法人资格；具有与提供电子认证服务相适应的人员；从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和客户服务人员不少于三十名，并且应当符合相应岗位技能要求；注册资本不低于人民币三千万元；具有固定的经营场所和满足电子认证服务要求的物理环境；具有符合国家有关安全标准的技术和设备；具有国家密码管理机构同意使用密码的证明文件；法律、行政法规规定的其他条件。

（2）电子认证服务许可的申请与颁发。

取得电子认证服务许可证书即取得电子认证服务机构资格。根据《电子签名法》第十八条规定：“从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起四十五日内做出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上公布其名称、许可证号等信息。”

《电子认证服务许可证》的有效期为五年。

取得电子认证服务许可的电子认证服务机构，应当持《电子认证服务许可证》到工商行政管理机关办理相关手续，进行企业登记，依法办理确定主体资格的事项，才可能开始电子认证服务活动。

取得认证资格的电子认证服务机构，在提供电子认证服务之前，应当通过互联网公布下列信息：机构名称和法定代表人；机构住所和联系办法；《电子认证服务许可证》编号；发证机关和发证日期；《电子认证服务许可证》有效期的起止时间。

4. 电子认证服务的内容

（1）电子认证服务机构的业务范围。

根据我国《电子认证服务管理办法》规定，电子认证服务机构的业务范围包括：制作、签发、管理电子签名认证证书；确认签发的电子签名认证证书的真实性；提供电子签名认证证书目录信息查询服务；提供电子签名认证证书状态信息查询服务。

（2）电子认证业务规则的制定及备案制度。

电子认证服务是专业性很强的活动，由电子认证服务提供者制定有关业务规则是合理的，也是符合实际的。当然，电子认证服务者不得制定损害电子签名人和电子签名依赖方利益的、不公平的“霸王条款”。为了防止这种情况的出现，《电子认证服务管理办法》规定了两项要求：一是电子认证服务者制定的电子认证业务规则要符合国家有关规定，并在提供电子认证服务前予以公布；二是电子认证业务规则要向国务院信息产业主管部门备案，以接受监督。

第一，电子认证业务规则的主要内容。

责任范围。电子认证服务提供者在提供认证服务过程中，由于未履行其应尽义务，尤其是保证其签发证书的真实、可靠性的义务，既可能产生对电子签名人的责任，也可能产生对电子签名依赖方的责任。电子认证服务提供者与电子签名人，即电子签名认证证书持有者，是民事合同的关系，电子认证服务提供者依照合同约定承担责任。电子认证服务提供者对电子签名依赖方的责任是基于法律规定而产生的，即两者是法律上的信赖关系，电子认证服务提供者对电子签名依赖方的法定义务是其承担责任的基础。同时也应当看到，电子认证服务是一个高风险的行业，既有内部风险又有外部风险，并且一旦发生风险往往会造成非常严重的后果。电子认证服务提供者在从事电子认证服务活动时，当然应尽合理的注意义务，但在无过错的情况下，不应承担责任，而无过错的举证责任要由认证机构承担。这是因为电子认证服务提供者处于中立的第三方，其行为和信誉直接关系到电子签名人与电子签名依赖方的利益，且相对于电子签名人及电子签名依赖方又处于强势地位，一些国家均规定了较为严格的责任制度，并且设立了举证责任倒置的制度，即电子认证服务提供者如能证明其对于责任事项无任何过错方可免责。

作业操作规范。电子认证作业操作规范包括的内容非常广泛。如电子签名认证证书申请过程中，对申请实体的身份进行审查的作业操作规范包括要求申请实体提供相应的有效身份证件，并明示审查流程等内容。在电子签名认证证书更新的操作规范中，则包括了证书更新的情形、请求证书更新的实体、更新请求的处理、颁发新证书时对订户的通告、构成接受更新证书的行为、电子认证服务机构对更新证书的发布和对其他实体的通告等内容。

信息安全保障措施。电子认证服务提供者是为互联网用户提供身份认证服务的。由于其负责接受证书申请、审核申请人身份、签发证书及管理证书等服务，与其他互联网服务提供商一样，电子认证服务提供者所提供的服务也面临着安全威胁，存在被攻击的可能，如非法入侵、植入病毒、窃取密钥等外部攻击。另外，认证系统内部也存在威胁，如内部工作人员的管理、机房的安全管理、软件的管理等。这些都需要制定具体的信息安全保障措施，防范风险。

第二，备案制度。

根据我国《电子签名法》第十九条规定，电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。同时，我国《电子认证服务管理办法》也规定：“电子认证服务机构应当按照工业和信息化部公布的《电子认证业务规则规范》等要求，制定本机构的电子认证业务规则和相应的证书策略，在提供电子认证服务前予以公布，并向工业和信息化部备案。电子认证业务规则和证书策略发生变更的，电子认证服务机构应当予以公布，并自公布之日起三十日内向工业和信息化部备案。”

（3）电子认证过程中有关各方的义务性规定。

① 电子认证服务机构在受理电子签名认证证书申请前的告知义务。

根据我国《电子认证服务管理办法》规定，电子认证服务机构在受理电子签名认证证书申请前，应当向申请人告知下列事项：电子签名认证证书和电子签名的使用条件；服务收费的项目和标准；保存和使用证书持有人信息的权限和责任；电子认证服务机构的责任范围；证书持有人的责任范围；其他需要事先告知的事项。

② 电子签名认证证书申请过程中申请人的法定义务。

根据我国《电子签名法》第二十条第一款规定，电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。

在电子认证关系中，电子签名人是电子认证服务提供者的客户，是接受电子认证服务的一方。电子签名人除了应履行一般的支付费用义务，还应当履行一些与电子认证服务关系的特性相应的义务。电子签名人申请电子签名认证证书时，要负担起保证所提供的信息的真实性、准确性和完整性的义务。诚实信用义务最直接的表现是真实陈述的义务，即真实陈述电子认证服务提供者颁发证书时要求其提供的事项。这是电子签名人在申请证书时所应当履行的基本义务，因为其身份、地址、营业范围、证书信赖等级的真实陈述，是证书可信赖性产生的前提，否则将构成对证书体系信赖性的损害，应承担相应的法律责任。

③ 电子签名认证证书申请过程中电子认证服务提供者的有关义务。

根据我国《电子签名法》第二十条第二款规定，电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查。

该条款主要规定了电子认证服务提供者的谨慎审核义务，要求电子认证服务提供者在收到电子签名认证证书申请后，对申请者所提交的有关材料的真实性，应当谨慎地加以审核，因为证书的发布、信赖方的信赖都依赖于对这些材料真实性的审查。另外，还要严格查验申请人的身份。这些都是为了保证其所发放的证书具有可靠的权威性和可信性。对个人电子签名认证证书申请者，电子认证服务提供者一般要求其提供个人的姓名、个人身份证的原件及复印件、身份证号、联系电话、住址、通信地址、邮政编码、电子邮箱等个人资料；对单位电子签名认证证书申请者，除对具体的经办人要求提供上述个人资料外，还要求提供申请单位的资料，如单位名称、单位所属行业类别、单位地址、单位注册号码、单位组织机构代码、单位电子邮箱、电话、传真、单位有效证件的原件与复印件等资料。

④ 电子认证服务提供者有关保证义务的规定。

电子认证服务提供者最重要的任务就是制作、发放和管理电子签名认证证书，所以其首要义务就是保证认证证书的真实性、完整性和准确性，即所发放认证证书的公共密钥同某个确定身份的人是一一对应的，以保证发放的证书具有可靠的权威性和可信性。电子认证服务提供者要保证发布的认证信息及时可靠，这其中还包括要让有关当事人能够随时证实证书申请人所拥

有的身份证、许可证或者营业执照等关系该人行为能力的文书或者证件的效力。为此，我国《电子签名法》第二十二条规定："电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。"

⑤ 电子认证服务提供者妥善保存与认证相关的信息及保存期限的要求。

电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。这些信息涉及的面比较广，既可能包含申请人的个人隐私，也可能涉及申请人的商业秘密，如果这些信息被泄露，可能会损害电子签名人的利益，因此，我国《电子签名法》要求电子认证服务提供者妥善保存与认证相关的信息的义务，并规定信息保存期限至少为电子签名认证证书失效后五年。

如果电子认证服务提供者违反上述规定，由国务院信息产业主管部门责令限期改正；逾期未改正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。

（4）对电子认证服务提供者签发的电子签名认证证书的质量要求。

电子签名认证证书是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件，它是电子交易当事人在互联网上从事电子商务活动的身份证和通行证。在电子商务交易中互不认识的双方当事人用其证书证明各自签名的真实性，可以在双方之间建立相互信任的基础。因此，电子签名认证证书不仅具有证明电子签名的真实性与完整性的作用，还可以为交易当事人提供身份及从事交易的资格、权限等方面的证明。基于电子签名认证证书的重要作用，电子认证服务提供者签发的电子签名认证证书应当准确无误，否则就可能产生损害电子认证、电子交易的后果，影响电子签名认证证书的权威性和可信性。

（5）电子签名认证证书的内容。

根据我国《电子认证服务管理办法》的相关要求，电子认证服务机构所提供的电子签名认证证书的内容应包括：签发电子签名认证证书的电子认证服务机构名称；证书持有人名称；证书序列号；证书有效期；证书持有人的电子签名验证数据；电子认证服务机构的电子签名；工业和信息化部规定的其他内容。

此外，电子认证服务提供者还可以根据实际需要载明其他内容，如载明证书的种类与等级等信息。

5. 电子认证服务提供者的业务承接

电子认证服务提供者拟暂停或者终止电子认证服务的，将会影响到相关方的利益，因此我国《电子签名法》第二十三条要求应当在暂停或者终止服务九十日前，就业务承接及其他有关事项通知有关各方。此外，电子认证服务提供者拟暂停或者终止电子认证服务的，还应当履行以下义务：

（1）报告。

电子认证服务提供者应当在暂停或者终止服务六十日前向国务院信息产业主管部门报告，使其了解情况。

（2）协商承接。

电子认证服务提供者除在法定期限内向国务院信息产业主管部门报告外，还要与其他电子

认证服务提供者就业务承接进行协商，协商达成一致意见的，对业务承接事项做出妥善安排。

（3）指定承接。

电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。

对于电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行。

▶▶ 3.3.6　电子认证服务过程中的法律责任

在电子认证过程中，不同的法律关系主体在享有权利的同时，也将对自己的行为承担相应的法律责任。这里的电子认证法律关系主体指电子认证法律关系的参加者，包括代表国家行使监管权力的行政主管部门、电子认证证书持有人、电子签名依赖方和电子认证服务机构。

1. 电子认证机构的法律责任

（1）过错赔偿责任。

电子签名人知悉电子签名制作数据已经失密或者可能已经失密未及时告知有关各方，并终止使用电子签名制作数据，未向电子认证服务提供者提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。也就是说，如果电子认证服务提供者能够证明自己没有过错，则不承担赔偿责任。电子认证服务提供者承担举证责任。

（2）违法提供电子认证业务的法律责任。

未经许可提供电子认证服务应承担的法律责任：未经许可提供电子认证服务的，由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得；违法所得三十万元以上的，处违法所得一倍以上三倍以下的罚款；没有违法所得或者违法所得不足三十万元的，处十万元以上三十万元以下的罚款。

暂停或者终止电子认证服务未按规定报告的法律责任：电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务六十日前向国务院信息产业主管部门报告的，由国务院信息产业主管部门对其直接负责的主管人员处一万元以上五万元以下的罚款。

（3）对电子认证服务提供者违法行为的处罚。

电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的，由国务院信息产业主管部门责令限期改正；逾期未改正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。吊销电子认证许可证书的，应当予以公告并通知工商行政管理部门。

2. 电子认证服务提供者在境外签发的电子签名认证证书的法律效力

我国《电子签名法》第二十六条明确规定：“经国务院信息产业主管部门根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务提供者在境外签发的电子签名认证证书与依照本法设立的电子认证服务提供者签发的电子签名认证证书具有同等的法律效力。”

3. 伪造、冒用、盗用他人的电子签名的法律责任

伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

4. 监督管理部门工作人员的法律责任

依照《电子签名法》负责电子认证服务业监督管理工作的部门的工作人员，不依法履行行政许可、监督管理职责的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

案例与思考

电子签名第一案

2004 年 1 月杨先生结识了韩小姐。2004 年 8 月 27 日，韩小姐给杨先生发短信，借钱应急，短信内容为："我需要 5 000 元，刚回北京做了眼睛手术，不能出门，你汇到我卡里。"杨先生随后将钱汇给了韩小姐。一周后，韩小姐再次以短信方式向杨先生借款 6 000 元。由于均是短信来往，两次汇款杨先生都没有索要借据，只保留该短信内容及汇款单据。此后，因韩小姐一直没提过还款的事，并又多次向杨先生借款。为此，杨先生产生了警惕，多次向其催要未果。于是，杨先生向北京市海淀区人民法院提起诉讼，要求韩小姐归还自己 11 000 元钱，并提交了银行汇款单及存单两张。但韩小姐却称这是杨先生归还的以前欠她的欠款。在庭审中，杨先生还提交了自己使用的号码为"1391166××××"的飞利浦移动电话一部，其中记载了部分短信息内容。如：2004 年 8 月 27 日 15 时 5 分，"那就借点资金援助吧"，2004 年 8 月 27 日 15 时 13 分，"我需要五千，这个数不大也不小，另外我昨天刚回北京做了个眼睛手术，现在根本出不了门口，见人都没法见，你要是资助，就得汇到我卡里"等韩小姐发来的 18 条短信内容。后经法官核实，杨先生提供的发送短信的手机号码，拨打后接听者是韩小姐本人，其本人也承认，自己从去年七八月份开始使用这个手机号码。

法院审理认为，依据 2005 年 4 月 1 日起施行的《中华人民共和国电子签名法》的规定，经法院对杨先生提供的移动电话短信息生成、储存、传递数据电文方法的可靠性、保持内容完整性方法的可靠性、用以鉴别发件人方法的可靠性进行审查，确认了该移动电话短信息内容的真实性。根据证据规则的相关规定，录音录像及数据电文可以作为证据使用，杨先生提供的通过韩小姐使用的号码发送移动电话短信息内容中载明的款项往来金额、时间与中国工商银行个人业务凭证中体现的杨先生给韩小姐汇款的金额、时间相符，且移动电话短信息内容中亦载明了韩小姐偿还借款的意思表示，两份证据之间相互印证，可以认定韩小姐向杨先生借款的事实。据此对杨先生要求韩小姐偿还借款的诉讼请求予以支持。

本案是我国《电子签名法》实施后，法院依据《电子签名法》判决的第一案，意味着我国的电子签名法真正开始走入司法程序，通过《电子签名法》的实施，基本上所有与信息化有关的活动在法律的层面都有了自己相应的判断标准。

（资料来源：http://china.findlaw.cn/jingjifa/dianzishangwufa/dzqm/qmxl/498.html）

思考：

1. 在本案中，短信是否可以作为证据使用？
2. 在未来，微信等新型社交软件内容是否可以作为证据使用？

本章实践技能操作

1．通过互联网注册网易电子邮箱，并发送一篇 Word 文档，查看收到的 Word 文档是否有变化，以了解数据电文在传输过程中的完整性与保密性。

操作步骤：

（1）打开 IE 浏览器，输入网址：http://www.126.com；

（2）点击左侧“注册”；

（3）创建一个新的 126 邮箱地址，输入要注册的电子地址，点击“下一步”；

（4）设置密码，并填写相关的信息，点击“我接受下面的条款，并创建账号”；

（5）点击进入邮箱，输入收件人地址和主题、内容，点击“添加附件”，找到所要发送的 Word 文档，点击“打开”，点击“发送”。

2．通过修改电子文件的生成时间（以 Word 文档为例），以了解数据电文的易篡改性和易破坏性。

操作步骤：

（1）找到一篇以前生成的 Word 文档，选中后点击鼠标右键/属性，查看该文档生成的时间；

（2）打开该文档，将所有内容复制；

（3）打开文件菜单，点击“新建”，将复制的内容粘贴到新建文档中；

（4）点击“保存”，选择文件存放地点，填入文件名，点击“保存”；

（5）选中新生成文档，选中后点击鼠标右键/属性，查看该文档生成的时间。

3．浏览上海市数字证书认证中心网站，了解认证中心的工作内容。

操作步骤：

（1）打开浏览器，输入网址：http://www.sheca.com/default.aspx；

（2）分别点击“证书申请”“证书更新”“证书查询及下载”“下载中心”“大客户服务直通车”“在线支付”等栏目，了解相关的服务内容；

（3）点击导航栏“产品”“方案”，了解上海市数字证书认证中心的精品产品与精选方案；

（4）点击导航栏“支持”，了解上海市数字证书认证中心的大客户服务。

本章知识自测

名词解释

1．电子签名　　2．数字签名　　3．电子签名认证证书　　4.《电子签名法》

5．电子认证　　6．电子认证机构

单选题

1．电子签名，指（　　）中以电子形式所含、所附，用于识别签名人身份并表明签名人认可其中内容的数据。

A．书面文件　　B．数据电文　　C．比特　　D．以上都不对

2．（　　）指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

A．电子签名人　　B．电子签名依赖方

C．电子签名认证证书人　　D．电子签名制作数据人

3．电子认证的核心是（　　）。

A．公钥　　B．电子认证证书　　C．私钥　　D．个人身份证书

4．身份认证机构，我国称为电子认证服务机构，其简称为（　　）。

A．CIA　　B．CA　　C．CBA　　D．FIA

5．电子签名认证证书必须具有（　　）。

A．安全性　　B．临时性　　C．唯一性和可靠性　　D．多重性

多选题

1．电子签名应具备如下特征（　　）。

A．电子签名是以电子形式出现的数据

B．电子签名附着于数据电文

C．电子签名必须能够识别签名人身份并表明签名人认可与电子签名相联系的数据电文的内容

D．以上都不对

2．在电子商务活动中，电子签名主要有以下作用（　　）。

A．证明文件的来源，即识别签名人

B．表明签名人对文件内容的确认

C．是构成签名人对文件内容正确性和完整性负责的根据

D．电子签名是以电子形式出现的数据

3．现行《电子签名法》的电子签名的法律效力范围包括（　　）。

A．涉及婚姻、收养、继承等人身关系的文书

B．涉及土地、房屋等不动产权益转让的文书

C．涉及停止供水、供热、供气、供电等公用事业服务的文书

D．法律、行政法规规定的不适用电子文书的其他情形

4．可靠的电子签名应当具备的法定条件包括（　　）。

A．电子签名制作数据用于电子签名时，属于电子签名人专有

B．签署时，电子签名制作数据仅由电子签名人控制

C．签署后，对电子签名的任何改动能够被发现

D．签署后，对数据电文内容和形式的任何改动能够被发现

5．电子认证的特性包括（　　）。

A．真实性　　B．完整性　　C．机密性　　D．不可否认性

简答题

1. 简述电子签名的法律效力范围。
2. 简述电子签名人的法律义务。
3. 简述电子签名和电子认证之间的区别。
4. 简述电子签名认证证书的作用。
5. 简述电子认证服务机构的职能。