第一章

电子签名与认证法律制度

知识目标

1. 熟悉电子签名的概念。
2. 了解电子签名的种类。
3. 掌握电子签名的效力。
4. 熟悉电子签名的程序。
5. 熟悉电子认证机构。

能力目标

1. 通过运用正确电子签名的过程，保护企业的正当权益。
2. 通过运用所学电子签名的知识，避免企业与企业、企业与用户之间产生纠纷。

情境导入

张莹在北京慧通网络发展有限公司工作初期，被安排做网络游戏开发工作中的联络沟通工作，以保证每个员工工作有序。每个游戏项目的开发需要一系列工序，包括游戏策划、美工、动画、音乐创作、测试支持等流程。每个流程结束均要求负责人签字。该游戏公司采用了OA办公电子签名系统，通过电子签名来确认工序的完成。在其工作过程中，张莹遇到如下问题。

1. 美工组的组长因为生病，由其组员李娜代替其进行签名。

2. 由于采用的是秘钥方式进行签名的传递，音乐创作的秘钥被其他公司盗取了，并且新创作的动画配乐被拿掉了。

3. 由于公司的会计部门处于交接中，会计部门未能按时交电费，导致供电局突然停

止供电，公司动画部正在制作的动画未能保存造成客观的经济损失。公司与供电局理论，认为不能随便断电，但是供电局答复曾经给公司的财务部门多次发过邮件催缴，但是无人理会，故此采取断电方式。

如果你是张莹，遇到上述问题应当如何解决？并说明理由。

网络是一个虚拟的世界，交易各方信息的交流是通过互联网进行的，电子商务中交易各方可能从来没有见过面，从而使得各方无法确定对方的身份，因此必然使人们对交易的安全感到担心，而且由于网络的开放性，人们还担心数据在传输过程中被篡改。所以如何鉴定各方的身份，保证数据传输的真实性，以保证交易的安全，是电子商务中一个非常重要的问题。为了解决这一问题，人们发明了电子签名技术，并建立了具有第三方地位的中立的认证机构，以确保交易各方身份的真实性和数据传输的可靠性。但是，电子签名和以网络技术为基础的认证机构，是从来没有过的新鲜事物，现行法律很难直接适用。因此如何对电子签名和认证机构进行调整，是必须明确的法律问题。

第一节 电子签名概述

电子签名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。通俗地说，电子签名就是通过密码技术对电子文档的电子形式的签名，并非是书面签名的数字图像化，它类似于手写签名或印章，也可以说它就是电子印章。

小贴士

电子签名和纸质签名有类似的效力。电子签名是电子商务安全的重要保障手段。特别是在联合国《电子商务示范法》颁布之后，国际组织及一些发达国家，都将其立法的焦点从书面问题转向了电子签名。这是一个如何使交易者的身份与其电子记录相联系的技术性问题，同时又是一个全新的法律问题[①]。

传统上的签名，是指在书面材料上写上执笔者的名字。美国《统一商法典》对“签名”的定义为：包括当事人意图认证一份书面材料所作的或所使用的任何符号。签名的决定性因素是签署者当时证明书面文件的意图。而认证可能是打印的、盖章的，或书写的，还可能仅仅是简写或指模，甚至在某些特定的案件里，可将信笺印刷的字迹作为签名。

电子签名并非是书面签名的数字图像化。它其实是一种电子代码，利用它，收件人便能在网上轻松验证发件人的身份和签名。它还能验证出文件的原文在传输过程中有无变动。如果有人想通过网络把一份重要文件发送给外地的人，收件人和发件人都需要首先向一个许可证授权机构 CA(GlobalSign)申请一份电子许可证。这份加密的证书包括了

① 张楚.《电子商务法初论》[M]. 北京：中国政法大学出版社，2000.

申请者在网上的公共钥匙即“公共电脑密码”，用于文件验证。

但是，数据电文不带有手写的签字，而且也不在纸上。电子形式的信息很容易在不被发现的情况下被截获和篡改，所以利用数据电文欺诈的潜在可能性很大。因此，数据电文要被广泛使用，必须有这样的技术手段，即在电子环境下能够借助于这些手段履行被认定为手写签字所独具的某些或全部功能。这类技术可统称为“电子签名”。电子签名与一般将手写签字扫描到计算机存为文件截然不同，后者如通过电子邮件方式传送给他人，收件人可以轻易地复制该签名而达到伪造文件或欺诈的目的；前者经过加密处理，他人无法轻易地复制该签名或更改文件内容，安全性相当高。[①]

一、电子签名的概念

对于电子签名的概念有几种不同的认识，各种认识都有其一定的合理性。

（一）广义的电子签名

广义的电子签名，是指包括各种电子手段在内的电子签名。联合国贸易法委员会《电子签字示范法》[②]第二条第一款规定：“电子签字系指在数据电文中，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，它可用于鉴别与数据电文相关的签字人和表明签字人认可数据电文所含信息。”

电子签字的概念意图指出，电子签名与手写签字具有相同用途，这些用途是为了鉴别个人以及将之与文件的内容联系起来。将电子签字界定为能够表明认可信息，这主要是为了确定一个技术先决条件，以便承认某项技术手段能够等同于手写签字。但是，对电子签名所运用的技术方式几乎没有规定，凡是具有一定鉴别作用的，满足技术先决条件的数据都可成为电子签名的方式。联合国贸易法委员会《电子签字示范法》中电子签名的概念是广义电子签名概念的典型代表。

法律要求在商务活动中符合“签名”要求，实际上是要求实现上述一种或几种功能。基于此，《电子签字示范法》的起草者沿用了《电子商务示范法》所采取的“功能等同法”这样一种新方法，这种方法立足于分析传统手写签字要求的功能和目的，以确定如何通过电子商务技术来达到这些目的或作用。所以，法律只需要根据所要求实现的一种或几种功能，制定与之相适应的要求。某种电子签名只要满足特定的技术和法律要求，就可以实现所要求的一种或几种功能，就可以被认为符合书面形式的要求。这种方法就是“功能等同法”。

（二）狭义的电子签名

狭义的电子签名，是以一定的电子签名技术为特定手段的签名，通常指数字签名，它是以非对称加密方法产生的数字签名。

---

① 曾更莹．网际网络上运用电子签名所涉法律问题研究[J]．万国法律．

② The United Nations Commission on International Trade Law Model Law on Electronic Autograph，简称《电子签字示范法》。2001 年 12 月 12 日年联合国贸易法律委员会通过的《电子签字示范法》，是国际上关于电子签字方面的最重要的立法文件。

之所以排除其他形式的电子签名，而只承认数字签名在法律上的有效性，主要是出于对各种电子签名安全性和实用性差异的考虑。

狭义电子签名支持者在对现有生成电子签名的技术方法进行考察后认为，在现行的电子认证技术中，计算机口令容易被破获，其安全系数不足；对称密钥加密不适应开放型市场的需要；而笔迹、眼虹膜网等辨别技术应用成本过高，唯有非对称密钥加密（数字签名）方法，既安全可靠，又能适应开放型市场密钥分发的需要，而且成本也不太高，是较为理想的电子签名技术方案，因而应作为法定的电子签名技术予以确认。其他的电子签名技术的安全性，尚未被验证认可，或者不具有实用性，所以不应赋予法律效力。

通过立法明确肯定数字签名这一项技术的另一个理由是：泛泛地确认电子签名技术在满足一定的技术条件后具有法律效力，会使得广大消费者在判断某项电子签名技术是否达到法定条件时面临困惑，不利于电子商务被广泛推广。而只肯定数字签名这项成熟技术，可以帮助消费者建立信心，使其可以无保留地信赖数字签名，从而推动电子商务的大众化。美国犹他州以《数字签名法》确认数字签名为有效的电子签名形式，是狭义电子签名概念的典范。

（三）强化电子签名

强化电子签名，有时又称安全电子签名。它是指经过一定的安全应用程序，能够达到传统签名的等价功能的电子签名方式。其具体形式是开放型的，任何能够达到同一效果的技术方式，都可囊括在内。与上述广义与狭义的电子签名概念相比较，该电子签名概念是一种折中式的概念。

联合国贸易法委员会《统一电子签名规则（草案）》在第一条中规定："强化电子签名，是指可以通过应用安全程序，或各种安全程序的结合对其生成之时的状况进行验证的电子签名，以保证该电子签名：①对于签署者所使用的目的是独特的；②可以客观地证明数据电讯签署者的身份；③由签署者或以签署者独占控制的方式生成并附加于数据电讯；④是与数据电讯如此紧密联系的，即一旦数据电讯有任何变化，就会被反映出来。"但是，联合国贸易法委员会正式颁布的《电子签字示范法》第三条规定："除第五条外，本法任何条款的适用概不排斥、限制或剥夺可生成满足第六条第一款凡法律规定要求有一人的签字时，如果根据各种情况，包括根据任何有关协议，使用电子签字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，则对于该数据电文而言，即满足了该项签字要求。所述要求或符合适用法律要求的电子签字的任何方法的法律效力。"其根本原则是不歧视任何电子签字方法，即所有技术在是否满足特定的技术要求方面都被给予同样的机会。因此，如果符合法定要求，电子签字的电文与手写签字的书面文件之间，或各种电子签字的电文之间将同等对待。也就是说，联合国贸易法委员会放弃了强化电子签名的立场，而完全支持广义电子签名的概念。

（四）我国法律上电子签名的含义

《中华人民共和国电子签名法》[①]（以下简称《电子签名法》）第二条第一款规定："电子

① 《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于2004年8月28日通过，自2005年4月1日起施行。

签名，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。其中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。”这表明，我国采用的是广义的电子签名概念，与联合国贸易法委员会《电子签字示范法》保持了一致。

在《电子签名法》出台前，《中华人民共和国合同法》（以下简称《合同法》）避开了电子签名问题，提出另一办法，即“签订确认书”。这实际是避开了必须有确定身份的“电子签名”的问题，这个方法属于“形式等同法”，而不是《电子商务示范法》采用的“功能等同法”。签订确认书并不能使电子合同完成签字人或依赖方认证的要求，电子合同也根本无法摆脱手书签名法律的束缚。[①] 根据“后法优于前法”的规则，《电子签名法》中的规范将取代《合同法》的相关规范。

收到附有签字的数据电文的收件人，通常也认为是电子签名依赖方。《电子签名法》第三十四条第（二）项规定：“电子签名依赖方，是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。”

二、电子签名的分类

学前思考

电子签名为什么要有这样的分类呢？这样分类的作用又是什么呢？

目前，比较通用的电子签名机制是建立在公用钥匙基础结构问题和公用钥匙基础结构术语上的，这种签名被称为数字签名。当然，其他依靠非公用钥匙加密技术的电子签名的发展也是不容忽视的。

（一）依靠非公用钥匙加密技术的电子签名

与使用公用钥匙加密的“数字签名”一起，还存在着各种其他装置，也包括在广义的“电子签名”机制概念中，这些装置可能现已投入使用，或考虑今后使用，以期履行上述手写签字的一种或数种功能。

1. 电子化签名

电子化签名技术将采用以手写签字为基础的生物统计学装置进行认证。在这种装置中，签字人将亲手签字，使用一支特殊的笔，书写在计算机屏幕上或数字输入板上，然后由计算机分析手写的签字并作为一组数值储存起来。这种签字可以附在数据电文之后，由收件人显示出来加以认证。这种认证体系将有一个先决条件，即手写签字的式样事先已由生物统计学装置做过分析并储存下来。现在已经有很多电脑公司推出电子签名使用的软硬件设施，美国也有许多百货商店开始使用这些设施来让消费者签署信用卡。

---

① 李雅芳．我国电子商务立法现状、问题及建议[J]，http://www.china.com.cn/zhuanti2005/txt/2002-03/27/content_5123901.htm，2013.7.3.

2. 生理特征签名

生理特征签名技术是基于用户的指纹、声波纹、视网膜结构等独一无二的生理特征的签名方法。这种签名方法要通过一定的设备识别上述生理特征，并运用一定的计算方法将生理特征转化为电子资料，并与预先建立的庞大数据库内的数据对照，以确认身份。但是，这种技术需要预先搜集大量生理特征数据，并且设备较为昂贵。目前仍在小范围内使用。

（二）依靠公用钥匙加密的数字签名

依靠公用钥匙加密的数字签名，即数字签名。简单地说，发文者必须先制作一组“钥匙”，钥匙实际上是一长串像密码一样的数字，可以存储在硬盘、软盘或集成电路卡等介质中。这组钥匙，一个为私人钥匙，即产生数字签名的钥匙，此为发文者专有，另一个为公用钥匙，应由所有的收文者知悉，收文者凭此检测收文是否被篡改。做法是随着原始信息发送以私人钥匙加密的签名，以此向接收方保证，接收方收到的每一个字都与发送方所发的相同。数字签名与数据加密完全独立发送方计算出的签名和数据一起传送给接收方，签名值是关于发送方的私人钥匙和要发送的信息的一个数学函数的值。算法的构造保证如果不知道私人钥匙的话就不可能计算出这个签名值。接收方可以通过依赖发送方的公用钥匙、签名值和接收到的数据的另一个数学算法来验证接收到的信息就是发送方签名的信息。

三、数字签名

学前思考

张某是一名学习电子商务的大学新生，对于很多既陌生又新鲜的新词汇，他都不太理解。什么是数字签名？数字签名就是把自己的签名写在纸上然后上传到计算机里吗？数字签名要加密吗？签名能伪造吗？客户端不是有密码就行吗？怎么还有公钥和私钥？请你学习下面的知识帮助张某解决上面的这些问题。

（一）相关概念和术语

1. 加密

数字签名采用加密方法创建和核查。加密是应用数学的一个分支。加密技术的应用比较广泛，比如 IE 浏览器就使用了 128 位的密钥。

在数字签名过程中，运用某种加密方法将电文转换为表面上不可懂的形态，收件人收到后再次利用加密方法将之还原为原有形态，这将保证传送中的信息即使被第三者拦截，第三者也是无法解读的。数字签名使用所谓的“公用钥匙加密法”，常常依靠算法函数产生两套不同但数学上相关的“钥匙”（即利用一系列数学公式产生的大数乘以素数）。其中一套钥匙（私人钥匙）用于产生数字签名或将数据转变为表面上不可懂的形态；另一套钥匙（公用钥匙）用来核查数字签名或将电文还原为原有形态。利用这两套钥匙的计算机设备和软件常常合起来称为“密码系统”。

2. 公用钥匙和私人钥匙

用于数字签名的互补钥匙称作“私人钥匙”和“公用钥匙”，前者仅由签字人用以创建数字签名，后者一般更广为人知，而且由依靠方用于核查数字签名。

私人钥匙的用户，将会保守私人钥匙的秘密。用户个人并不需要了解私人钥匙。这种私人钥匙可能保留在智能卡上，或可以通过个人识别号码检索，或者是通过生物统计识别装置，例如通过拇指指纹识别装置进行检索。电脑公司往往会提供相应的软硬件设施，用户只需要进行简单的操作就可以了。

3. 散列函数

在生成数字签名的时候，如果运用私人钥匙对整篇数据电文进行计算，将会花费较长时间，所生成的签名也会比较冗长。所以，除了生成配对钥匙之外，在创建和核实数字签名时还利用另一个基本程序，一般称为“散列函数”。散列函数是一种数学的计算过程，它以建立电文的数字表示或压缩形式的算法为基础，常被称为“电文摘要”。电文摘要通常比电文短得多，但仍有其明显的独特性。在使用同一散列函数时，电文的任何变动必然产生不同的电文摘要。

4. 数字签名

为了签署一份文件或任何其他的信息项目，签字人首先精确划定拟签字的内容范围。然后，签字人软件中的散列函数为拟签字的信息计算其独有的（就所有实用技术而言）的散列结果。签字人的软件接着使用签字人的私人钥匙，将散列结果转变为数字签名。所产生的数字签名，因此为所签字的信息和用以创建数字签名的私人钥匙所独有。

典型的情况是，数字签名（电文经数字签名后的散列结果）附在电文之后并随电文一起存储或发送。不过，只要保持与电文的可靠联系，也可作为单独的数据单元发送或存储。由于数字签名为电文所独有，如果与原电文永久脱离联系，就无法操作了。

5. 数字签名的核查

数字签名的核查，是由电子签名依赖方进行或由其委托第三方进行的。数字签名的核查是通过参照原有电文和某一给定公用钥匙对数字签名进行检查的过程，从而判定是否利用了与被参照的公用钥匙相对应的私人钥匙为该原有电文创建了数字签名。在核查数字签名时，还须通过用于创建数字签名的同一散列函数计算原有电文新的散列结果。然后，核查人利用公用钥匙和新的散列结果，核对数字签名是不是利用相应的私人钥匙创建的，并核查新计算出来的散列结果是否与在签字过程中转变为数字签名的原散列结果相配对。

在下列两种情况下，核查软件将确认数字签名得到了“核查”。

（1）签字人的私人钥匙被用于对电文进行数字签名，当签字人的公用钥匙被用于核查签字时，即认为属于此种情况，因为签字人的公用钥匙将只核查采用签字人的私人钥匙创建的数字签名。

（2）电文未经改动，当核查人计算的散列结果与在核查过程中从数字签名析取的散列结果相一致时，即认为属于此种情况。

下面举例说明电子签名使用的流程。甲采用电子邮件电文的方式起草了一份要约，

利用某种散列算法算出电文摘要，依靠私人钥匙给电文摘要加密以制成数字签名，将该数字签名附在电文之后，用电子邮件将数字签名和电文发给乙；乙利用某电子认证服务提供者提供的与甲的私人钥匙对应的公用钥匙核查甲的数字签名，获得电文摘要，并利用同样的散列算法创建电文的电文摘要，对比两种电文摘要，二者一样，则乙方知道电文由甲方签署且经签字后未作改动。乙以同样方式向甲发出承诺，双方订立了合同。

（二）数字签名的过程

数字签名的使用通常涉及下列过程，由签字人执行或由数字签名电文的收件人执行。

（1）用户生成或被给予独有的配对密码钥匙。

（2）签字人在计算机上起草电文（例如，采用电子邮件电文的形式）。

（3）签字人利用一种保密散列算法起草“电文摘要”。数字签名创建时利用从签字电文中求出的并为其所独有的散列结果。

（4）签字人依靠私人钥匙给电文摘要加密。利用一种数学算法，将私人钥匙应用于电文摘要文本。数字签名由加密的电文摘要组成。

（5）签字人一般将其数字签名附在电文之后。

（6）签字人利用电子手段将数字签名和（未加密或已加密的）电文发给依赖方。

（7）依赖方利用签字人的公用钥匙核查签字人的数字签名。利用签字人公用钥匙所作的核查可提供某种程度的技术保证，确保电文完全来自签字人。

（8）依赖方也创建电文的“电文摘要”，利用同样的保密散列算法进行。

（9）依赖方对比两种电文摘要。如果二者一样，则依赖方可确定电文经签字后未作改动。电文经数字签名后，即使有一点点改动，依赖方产生的电文摘要也会与签字人产生的电文摘要不同。

（10）依赖方从电子认证服务提供者（包括通过签字人或以其他方式）取得证书，证书确认签字人电文上的数字签名。证书载有签字人的公用钥匙和姓名（可能还有其他信息），并经由电子认证服务提供者数字签名。

（三）公用钥匙基础结构和电子认证服务提供者

1. 电子认证服务的必要性

电子商务活动并不只是存在于虚拟空间，而是实实在在地存在于现实社会中。因此，商务活动的另一方当事人，也就是此时的核查人必须通过核查数字签名而追寻到现实社会中特定的个人或实体。那么，核查人必须可以取得签字人的公用钥匙，而且相信它与特定签字人的私人钥匙相对应。不过，配对的公用和私人钥匙与任何人都没有内在的联系；它们只是一对数目而已。需要有一种外加的机制才能将特定的个人或实体与配对的钥匙可靠地联系起来。如果公用钥匙的加密要达到预定的目的，就必须提供某种办法使形形色色的个人可以使用，其中许多人并不为签字人所认识，双方没有发展成相互信任的关系。为此，有关各方必须对发给的公用钥匙和私人钥匙有某种程度的信任。

下述各方之间可能存在着所需的信任程度：它们彼此信任，已打过一段时间的交道，在封闭式系统上互相联系，在非对外的集团内部经营业务，或者它们能够采取合同的方

式，例如贸易合伙人协议，用以管理它们的交易。在只涉及两方的交易中，每方只需（采用较为可靠的渠道，如信使或本身具有声音识别功能的电话系统）将各自要使用的配对钥匙中的公用钥匙通知对方即可。然而，在下述这样的各方之间就可能不存在同样的信任程度：它们彼此难得打交道，在开放的系统上联系（例如互联网上的万维网），不属于一个非对外的集团，或者未订有贸易合伙人协议或没有管理它们之间关系的其他法律。此外，由于公用钥匙密码是一种数学程度很高的技术，因此，所有用户必须信任公用钥匙和私人钥匙发布方的技能、知识和保密措施。

未来的签字人可以发表一则公开声明，说明对于可用某个给定的公用钥匙加以核查的签字，应作为出自该签字人之手的签字对待。此类声明的形式和法律效力由颁布国的法律管辖。例如，可通过在官方公报或公共当局承认的“正宗”文件上发表声明来确立将电子签字归属于某一特定签字人的推定。然而，其他各方可能不愿意接受这种声明，在事先没有合同能够有把握地证明这种公开声明的法律效力时尤其如此。如果交易最终证明对署名的签字人不利，那么当事人若信赖此种在开放系统上所作的未经证明的公开声明，便将冒巨大的风险，疏忽大意地信任骗子，或对被抵赖的数字签名不得不加以反驳。

解决这个问题的方法，是利用一个或多个受到信任的第三方将认定的签字人或签字人的名字与某个具体的公用钥匙联系起来。在大多数技术标准和指导原则中，该受信任的第三方一般称作“电子认证服务提供者”。

2. 公用钥匙基础结构

在若干国家中，这类电子认证服务提供者现在正按等级编组，组成平常所称的“公用钥匙基础结构”。建立公用钥匙基础结构是一种方法，用以使人们信任下列两点：用户的公用钥匙未被篡改，而且事实上与该用户的私人钥匙相对应；使用的密码技术是可靠的。为让人产生上述信任，公用钥匙基础结构可以提供多种服务，其中包括：①管理用于数字签名的密码钥匙；②验证一套公用钥匙对应于一套私人钥匙；③为最终用户提供钥匙；④公布公用钥匙或证书的保密目录；⑤管理个人令牌（例如智能卡），它们能够以独特的个人识别信息识别用户或者能够创建和存储个人的私人钥匙；⑥核实最终用户的标识并向它们提供服务；⑦提供时间标记服务；⑧在获准使用密码钥匙时，管理用于保密性加密的密码钥匙。

公用钥匙基础结构常以多层次的职权结构为基础。例如，某些国家为建立可能的公用钥匙基础结构而考虑的模式涉及下列层次：①一个独一无二的“总根服务提供者”，它将验证凡获准发布配对加密钥匙或签发与使用这些配对钥匙有关的证明的所有各方采用的技术和做法，并对下属的服务提供者进行登记；②多个服务提供者，置于“总根服务提供者”机构之下，负责验证用户的公用钥匙实际上与该用户的私人钥匙相对应（即未经篡改）；③多个地方登记机构，置于验证服务提供者之下，接受用户对配对加密钥匙或与使用这些配对钥匙有关的证明而提出的申请，要求提出鉴定的证据并检查潜在用户的身份。在某些国家，设想可由公证人充当或支持地方登记机构。不过，从相互验证的角度看，全球通用的必要性要求各国建立的公用钥匙基础结构应能互相沟通。

3. 电子认证服务提供者

为使配对钥匙与未来的签字人联系起来，电子认证服务提供者签发一份证书，这是一

份电子记录，将公用钥匙和证书用户的名字合列在一起，作为证书的“内容”，而且可能确认证书中所标明的未来签字人持有对应的私人钥匙。证书的主要作用是将公用钥匙与特定的持有人联系在一起。证书的“接收人”如果希望依赖证书中所标明的持有人而创建的数字签名，可利用证书中列出的公用钥匙查验数字签名是否是采用对应的私人钥匙创建的。如果这种查验获得成功，则在技术上提供了某种程度的保证，即数字签名是由签字人所创建的，而且散列函数中使用的电文部分（以及因而对应的电文）经数字签名后未被改动过。

小贴士

为了保证证书的内容和来源的真实性，电子认证服务提供者对证书加上数字签名。签发证书的服务提供者在证书上的数字签名，可以采用由另一个验证服务商签发的另一份证书中列出的该电子认证服务提供者的公用钥匙来核查，而且该另一证书可以依次再由另一份证书中列出的公用钥匙验证，如此不断进行下去，直至依赖于数字签名的个人对其真实性确信无疑为止。除了用以核查电子认证服务提供者数字签名的各种其他可能的方法之外，该数字签名还可记录在该电子认证服务提供者自己签发的证书上，这种证书有时可称为“根证书”。

在每种情况下，签发证书的电子认证服务提供者在用以核查电子认证服务提供者数字签名的另一证书的操作期间，必须对自己的证书加上数字签名。根据有些国家的法律，对电子认证服务提供者的数字签名建立起信心的一种方式可以是，在官方公告中公布电子认证服务提供者的公用钥匙或与根证书有关的某些数据。

第二节 电子签名的适用范围和法律效力

一、电子签名的适用范围

学前思考

张某和赵某是大学同学，两个人准备办理结婚登记手续，8月8日是个好日子，但是赵某被临时派到外埠，赶不回来了。张某想和民政局的工作人员商量能否以视频的方式到场，并且发邮件确认。

（1）你觉得这属于电子签名吗？

（2）如果这么做，该婚姻登记是否有效呢？

《电子签名法》第三条规定：“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。