第 1 章　引　　言

1.1　电子认证技术的历史演进

1.1.1　电子认证技术的出现

随着 3G 技术的出现，移动电子商务快速发展，人们通过互联网工作、娱乐和生活，互联网给人们带来便利的同时，也给个人隐私保护和信息安全带来了全新的挑战。

“十一五”时期，电子认证软、硬件和服务市场规模增长明显。数字证书认证系统建设、硬件介质数字证书发放、电子认证相关应用系统集成及服务等领域得到快速发展。截至 2010 年底，电子认证服务业市场总规模超过 20 亿元，“十一五”期间年平均增长速度约为 38%，2010 年的增长率接近 100%。工业和信息化部（工信部）公布的《电子认证服务业“十二五”发展规划》指出，到“十二五”末期，我国将形成覆盖全国的网络身份认证服务体系，基本形成可靠电子签名认证体系，并在数据电文可靠性认证服务模式探索方面取得积极进展，电子认证服务市场规模突破 80 亿元。

电子签名作为电子认证技术的核心，仅通过技术手段辨认签名人身份，并确认签署文件的发件人与发出电子文件的所属关系。然而，电子签名技术本身无法解决一些关键问题，如公共密钥的确定性和私人密钥持有者否认签发文件的可能性。这些问题涉及私人密钥持有人信用度的问题，包括密钥持有人主观恶意否认自己的行为，或因客观原因如密钥丢失、被窃或被解密，导致归责问题难以解决。

类似问题在传统商业交易活动中也存在，但传统活动有一套相对完整的解决方案。例如，在我国台湾，重要法律文件的印章真实性认证采取提前备案并提供验证证明的方式，防止抵赖或伪造。电子交易过程中，同样需要一个具有公信力的第三方安全认证机关（Certificate Authority，CA）对公钥进行辨别和认证，以防止发件人抵赖或减少密钥丢失、被盗或被解密等问题。

因此，电子签名的安全使用必须配合安全认证机关体系的建立。西方许多国

家（如美国、加拿大、德国）以及日本都已经或正在建立相应的公共密钥基础设施（Public Key Infrastructure，PKI）。网络电子签名与 CA 认证的结合解决了电子签名技术方面无法解决的信用度问题。

总体来看，电子认证技术的发展是一个逐步深化、不断完善的过程。随着网络技术的发展和网络安全威胁的增加，电子认证技术变得日益重要。从最初的电子签名到完善的电子认证体系，这一技术的发展反映了社会对安全、可靠的数字交易的迫切需求。未来，随着技术的进一步发展和应用的不断扩展，电子认证技术将继续在保护网络活动安全、促进电子商务发展等方面发挥重要的作用。

1.1.2 技术演进和关键节点

在电子认证技术初现雏形之时，主要依赖基于密码学算法的方法来确保信息的机密性。密码学是古老的学科，但它并不完全过时，在电子认证中仍扮演着重要角色。在这一阶段，认证是通过提供正确的密码来实现的。这种方法虽然简单，但存在密码被猜到或被盗用的风险。因此，需要更安全的认证方式来满足日益复杂的信息安全需求。

后来 PKI 的出现引入了公钥密钥学算法。在 PKI 中，用户拥有自己的数字证书，其中包含公钥和身份信息。这些数字证书由可信的第三方机构颁发，用于证明用户的身份和提供数字签名。这一发展提高了电子认证的公信力，为安全通信提供了更可靠的手段。数字签名允许用户对电子文档进行数字签名，以验证文档的完整性和真实性。数字签名使用非对称密钥算法，确保只有文档的所有者才能生成有效的数字签名。这一技术的兴起为电子文档的认证和身份验证提供了更高级别的安全性，从而为电子交易、合同和文件共享等应用提供了不可抵赖性和更高级别的安全性。

随着技术的进步，生物识别技术利用个体的生理或行为特征，如指纹、虹膜、面部等，来验证用户的身份。这种方法比传统的密码更安全，因为生物特征是唯一的，并且难以伪造。生物识别技术的应用为电子认证提供了更高级别的安全性，使其更难以被冒用或攻破。

再后来，多因素认证被认为是提高认证安全性的关键方式。多因素认证结合了多种认证方法，如密码、数字证书、生物识别等，以提高认证的安全性。用户需要提供多个因素才能获得访问权限，这种方法提高了系统的安全性。多因素认证逐渐成为电子认证的标准做法，特别是在敏感信息处理和金融交易等领域。

整体来看，电子认证技术的技术演进经历了多个关键节点，从密码学时代

到公钥基础设施的崛起，再到数字签名和生物识别技术的整合，以及多因素认证的崭露头角。这些发展使电子认证技术在保护信息安全和实现身份验证方面取得了巨大的进步，为安全通信和电子交易提供了坚实的基础。在信息社会中，电子认证技术的不断创新将继续发挥关键作用，以确保数字世界的安全性和可信度。

1.1.3 未来趋势的预测

信息化的发展不断加速，以及人们对网络信任的需求日益增加，将推动电子认证技术成为支撑业务创新的重要保障。

1. 医疗信息化的崛起

在医疗卫生领域，电子认证技术将发挥越来越重要的作用。随着我国新医改方案的实施，医疗信息化成为了一个重要的战略方向。基于电子病历的医院信息系统和基于电子健康档案的区域医疗卫生平台的建设正在逐步展开。这些系统将存储和处理大量敏感的患者医疗信息，为确保这些信息的安全性和真实性，电子认证技术将得到广泛应用。国家卫生健康委已发布了一系列关于推动电子认证服务和电子病历应用的政策文件，这将继续推动医疗卫生领域的电子认证市场进入快速增长阶段。电子认证将用于验证医疗专业人员的身份，确保只有授权的医生和护士才能访问患者的病历和健康档案。此外，电子认证还将用于加强医疗数据的机密性，防止患者隐私泄露和医疗数据被篡改。

2. 互联网彩票和电子发票

在彩票行业，互联网彩票和手机彩票的兴起将推动电子认证技术的广泛应用。传统的彩票销售通常依赖于实体店面，但随着互联网的普及，人们可以随时随地购买彩票。电子认证服务和产品将确保彩票销售的真实性和可信度，这对于广大的网络市场和用户群体来说至关重要，电子认证技术将用于验证购彩者的身份，防止未成年人购买彩票以及防止多次购买，有助于保护彩票行业的公平性和诚信度。还有电子发票领域，电子发票作为一种数字化的票据，需要具备高度的安全性和可信度，以确保税收征管的准确性和高效性。

3. 金融领域的数字化

金融领域一直是电子认证技术的主要应用领域。在网上证券、网上保险和网上支付等领域，电子认证已经被广泛应用。未来，随着金融业务网络化和移动化的深入，电子认证将继续发挥关键作用。例如在证券领域，非现场开户和网上交易已经成为常见的交易方式。投资者需要通过电子认证来验证其身份，以确保只有合法的用户才可以进行交易。保险领域也在不断创新，电子保单和移动展业等

新业务模式的兴起需要强大的电子认证支持，以确保保险交易的安全性和可信度。未来，电子认证在金融领域的普及率将进一步提高，在金融业务网络化、移动化进一步深入的情况下开辟新的市场空间。金融机构将积极采用电子认证技术以满足日益复杂的安全需求，保护客户的资金和信息安全。

4. 电子认证技术的拓展

除了以上提到的行业，电子认证技术还将在其他领域得到广泛应用。在电子政务中，电子认证可用于确保政府文件和数据的安全性和真实性，为公民提供更可信的政府服务。在电子商务中，电子认证能够为在线购物提供更安全的支付和身份验证方式，加强用户对电商平台的信任。电子认证技术的拓展还包括了移动化和智能化的趋势。随着移动设备的普及和智能化技术的发展，电子认证技术将适应这一趋势。移动认证、生物识别认证和多因素认证等新型认证方式将得到更广泛的应用，为用户提供便捷而安全的身份验证体验。电子认证技术将与物联网、人工智能和大数据等新兴技术相结合，为未来的数字生活提供更高级别的安全性和便利性。

1.2 电子认证技术的基本术语和概念

1.2.1 数字签名

在数字化时代，数据的安全性和可信度变得至关重要。随着互联网的快速发展和信息传输的广泛应用，确保数字信息的完整性、真实性和不可抵赖性成为一项紧迫的任务。数字签名作为一项重要的安全技术，源于对传统签名方式的数字化需求。在过去，人们在纸质文档上签字和盖章以确认文档的真实性和完整性。然而，在数字化的信息传输中，这种方式不再适用。电子文档、电子邮件和在线交易等数字信息的传输需要一种更高效、更安全的方式来验证，因此数字签名应运而生，用于验证数字信息来源的真实性和完整性，从而建立信任和保障信息交流的安全性，为数字时代的信息交流提供了解决方案。

1. 数字签名的重要性体现

（1）信息安全与完整性保护。数字签名可以确保传输的数据在传输过程中没有被伪造或修改。如果数据被篡改，数字签名验证将失败，从而提供了数据完整性的保护。这对于保护敏感信息，如金融交易或医疗记录，至关重要。

（2）身份验证。数字签名可以用于验证信息的发送者是合法和授权的。只有拥有私钥的人才能生成有效的数字签名，这确保了身份的真实性。

（3）不可抵赖性。数字签名使发送者无法否认其行为。一旦数字签名生成，发送者不能否认他们的签名，这在法律领域和商业交易中具有重要意义。

（4）防重放攻击。数字签名可以用于防止重放攻击（攻击者重复发送已经传输过的消息，以欺骗接收方），数字签名可以包括时间戳或唯一标识符，以防止此类攻击。

（5）机密性保护。虽然数字签名本身不提供数据的保密性，但可以与加密技术结合使用来确保数据在传输过程中的保密性。

2. 非对称密钥加密与数字签名的关系

非对称密钥加密系统使用一对密钥：公钥和私钥。公钥可以自由分发给任何人，而私钥必须严格保密。这两个密钥是数学上相关的，但无法从一个密钥推导出另一个密钥。信息的发送者使用接收者的公钥来加密信息，只有接收者拥有私钥才能解密并读取信息。这种机制保证了信息的机密性，如图 1-1 所示。

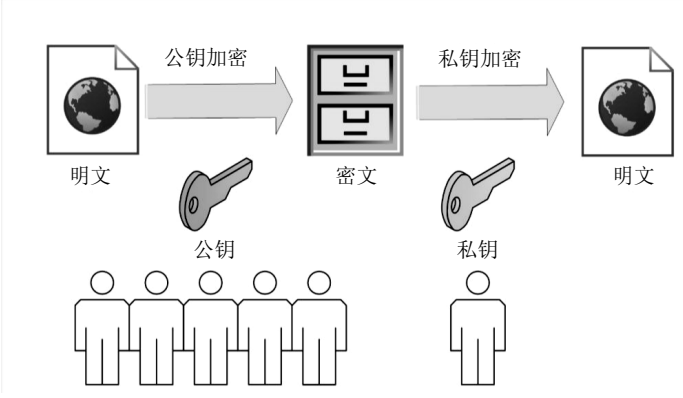

图 1-1　非对称密钥

3. 非对称算法

与非对称密钥加密相比，数字签名是用于验证信息来源和完整性的过程。发送者使用自己的私钥对信息生成数字签名，然后将数字签名附加到信息上。接收者使用发送者的公钥来验证数字签名，以确认信息的来源和完整性。数字签名的目的是提供对信息的验证，而不是保护信息的机密性。这两种技术都依赖于密钥对的使用，但用途不同：非对称密钥加密用于加密和解密信息，数字签名用于验证信息。

4. 数字摘要技术与数字签名的结合

数字签名的核心原理之一是数字摘要技术。数字摘要是一个由原始数据生

成的固定长度的字符串，通常是一种哈希值。哈希函数将输入数据转换为一串字符，这串字符的长度是固定的，而无论输入数据的大小如何。数字摘要的目的是验证原始数据在传输过程中是否被篡改。数字签名使用数字摘要来确保信息的完整性。签名过程中，发送者首先对原始数据应用哈希函数，生成数字摘要。接着发送者使用自己的私钥对数字摘要进行加密，生成数字签名。数字签名将与原始数据一起发送给接收者。在验证过程中，接收者使用发送者的公钥来解密数字签名，获得数字摘要。然后接收者对接收到的原始数据应用相同的哈希函数，生成另一个数字摘要。如果这两个数字摘要相匹配，则说明原始数据未被篡改。

数字摘要与数字签名结合使用，让数字签名不仅能验证信息的来源，还能验证信息的完整性。这就使得数字签名成为一种非常强大的工具，用于确保信息在传输和存储过程中的安全性，其优势如图 1-2 所示。

图 1-2　数字签名

5. 数字签名的工作过程

发送者。首先，发送者（签名者）需要生成一对密钥：公钥和私钥。这对密钥是基于非对称密钥加密算法生成的。公钥是可公开的，用于验证数字签名，而私钥必须保密，用于生成数字签名。发送者选择要发送的消息或文档，我们将其称为原始数据。发送者使用哈希函数对原始数据进行处理，生成消息摘要（也称为哈希值或摘要）。消息摘要的长度是固定的，不受原始数据大小的影响。然后，发送者使用自己的私钥对消息摘要进行加密，生成数字签名。最后，发送者将数字签名与原始数据一起发送给接收者，如图 1-3 所示。

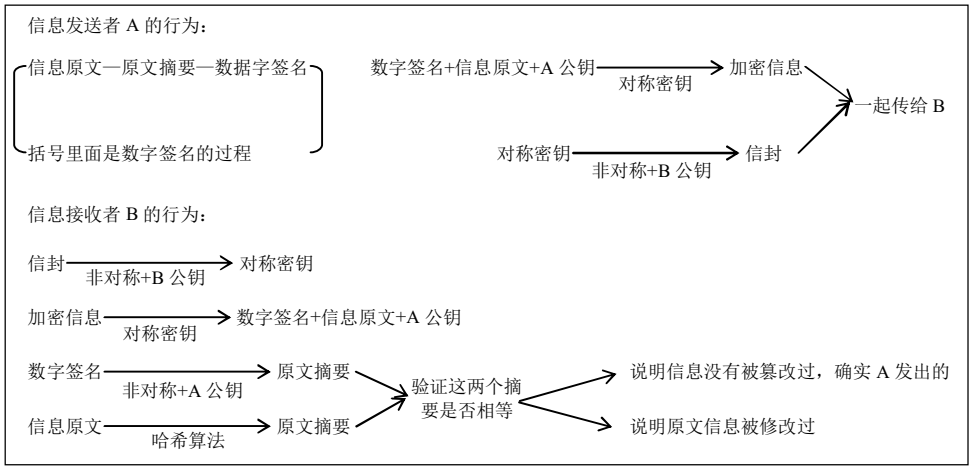

图 1-3　数字签名的工作过程

接收者。首先，接收者收到原始数据和数字签名后需要获取发送者的公钥。公钥可以通过数字证书颁发机构（CA）获得，确保公钥的可信性。然后，使用发送者的公钥来解密数字签名，得到消息摘要，再使用相同的哈希函数对接收到的原始数据生成另一个消息摘要。最后，接收者将两个消息摘要进行比较，如果两者匹配则数字签名有效，接收者可以确定消息的来源是发送者，并且消息的完整性未受到破坏；如果两个消息摘要不匹配，数字签名无效，原始数据可能已被篡改，接收者不应信任该消息。

6. 数字签名的特点和功能

特点方面，数字签名确保消息或文档的发送者是合法的，因为只有发送者拥有私钥才能生成有效的数字签名。这使得数字签名成为一种有效的身份认证机制，并且可以保护消息或文档的完整性，任何对原始数据的修改都会导致数字签名验证的失败。接收者可以确保接收到的数据没有被篡改，并且发送者无法否认自己的数字签名，因为数字签名是使用其私钥生成的。这意味着发送者不能在后期否认发送特定消息或文档的事实。

功能方面，数字签名确保数据在传输过程中未被篡改。接收者可以验证数据的完整性，确保接收到的数据与发送者的原始数据相同。数字签名用于验证消息或文档的发送者身份。接收者可以确信消息来自合法的发送者，并且发送者不能否认其签名。在电子商务和法律领域，数字签名用于签署电子合同，确保合同的完整性和不可抵赖性。这使得电子合同具有法律效力，并且数字签名也可用于在线选举和电子投票系统中，确保选票的安全性和可信度。

1.2.2 数字证书

数字证书是当今互联网通信中至关重要的一环，它扮演着标志通信各方身份信息的数字认证角色。在数字时代，我们的日常生活和商业活动越来越依赖网络，这使得信息传输和存储的安全成为至关重要的问题，数字证书的出现为我们提供了一种有效的方式来保障在线交流的安全性。

在过去的几十年里，互联网已经成为了信息共享、商业交流、社交互动和娱乐活动的核心平台。然而，随着互联网的快速发展，伴随而来的是安全隐患和威胁。网络犯罪、数据泄露、欺诈行为和恶意攻击已经成为了网络社会的一部分，给用户的个人信息和财产安全带来了巨大风险。

正是在这个背景下，数字证书作为一种数字安全技术应运而生。它不仅允许我们在网络上识别和验证通信各方的身份，还确保了在数据传输和存储过程中信息的完整性和安全性。数字证书就像是一张网络世界的身份证，能够确保通信双方是合法且可信的。这种安全性对于在线银行交易、电子邮件通信、电子商务、远程办公以及其他各种在线活动至关重要。

1. 数字证书的基本原理

数字证书的基础是非对称密钥加密，也被称为公钥加密，非对称密钥加密在上文的数字签名一节中已经提及，这里不再赘述，其工作原理是发送方使用接收方的公钥来加密要发送的消息，接收方使用自己的私钥来解密收到的消息。因为只有接收方拥有私钥，所以只有接收方才能解密消息，这种方式确保了消息在传输过程中证书持有者的身份的真实性。

2. 数字证书的颁发过程

首先，用户需要向 CA 提交数字证书的请求。这个请求通常包括用户的公钥和一些身份信息，用以证明用户的身份。然后，CA 开始验证用户的身份。这个过程可能需要用户提供身份证明文件、企业注册信息或其他相关信息，以确保用户是合法的，并且拥有请求中所述的公钥。一旦用户的身份得到验证，CA 使用自己的私钥对用户的公钥和身份信息进行签名，生成数字证书。数字证书中包含了用户的公钥、身份信息和 CA 的数字签名。最后，CA 将生成的数字证书发送给用户。这个数字证书可以通过网络传输或其他适当的方式发送给用户，如图 1-4 所示。

3. 数字证书验证过程

当用户与其他实体（如网站或服务器）进行通信时，这个实体会向用户提供数字证书。用户会收到数字证书，其中包含了公钥和 CA 的数字签名。用户需要获取 CA 的公钥，以便在验证数字证书时使用。这通常通过提前获取 CA 的公钥

并存储在用户设备中来完成，用户使用 CA 的公钥来验证数字证书的数字签名。如果数字签名有效，证明数字证书没有被篡改，且确实由 CA 签发。一旦数字证书的真实性得到验证，用户即从数字证书中提取目标实体的公钥和身份信息，并且用户可以使用目标实体的公钥来加密通信来确保通信数据的完整性。同时，用户也可以使用数字证书中的身份信息来验证目标实体的身份，如图 1-5 所示。

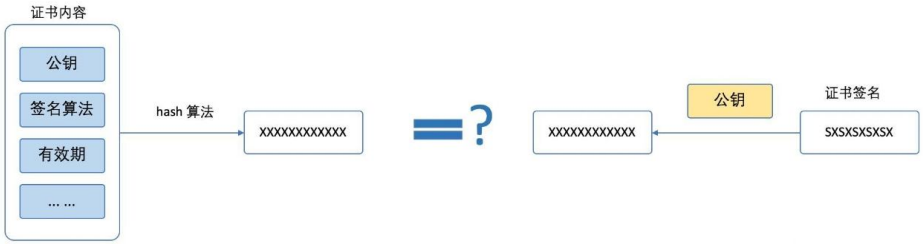

图 1-4　数字证书的合法性验证

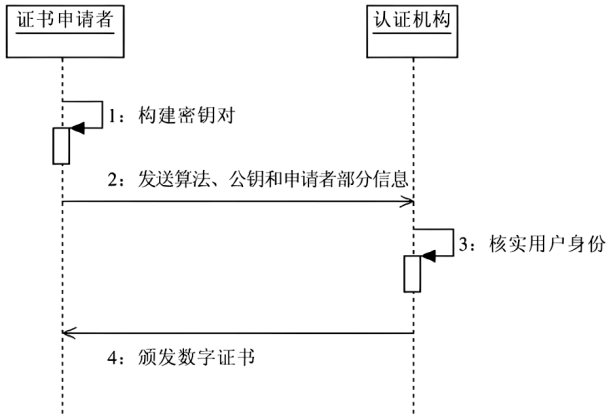

图 1-5　数字证书的验证过程

4. CA 的角色

CA 负责验证用户（实体）的身份，以确保它们合法并有资格获取数字证书，这是确保数字证书可信度的关键步骤。CA 使用自己的私钥对生成的数字证书进行签名，这个数字签名是验证数字证书真实性的依据。CA 的数字签名是公认为可信的，因此可以用于验证数字证书的来源。CA 颁发数字证书，将数字证书分发给合法的用户（实体），确保数字证书的正确性和有效性。

CA 也负责分发自己的公钥，以便其他用户（实体）可以使用它来验证数字证书的真实性。CA 的公钥需要以安全的方式分发，以防止中间人攻击。

数字证书的颁发和验证过程是建立在对 CA 的信任基础上的，这确保了网络

通信的安全性和可信度。CA 在这个过程中扮演着关键的角色，负责验证用户身份、生成数字证书、签名和分发数字证书，以及提供自己的公钥供其他实体验证。这一体系为安全通信和身份验证提供了坚实的基础。

5. 数字证书的特性

（1）安全性。数字证书使用非对称密钥加密技术，其中包括一个私钥和一个公钥。私钥只有证书持有者知道，而公钥是公开的。这种加密方式确保了证书的私密性，只有证书持有者才能使用私钥来解密数据。这种加密保障是数字证书的核心特点之一，数字证书包含了 CA 的数字签名，用于验证证书的真实性。CA 的数字签名是可信的，因为 CA 是一个受信任的第三方机构。这意味着证书持有者无法伪造数字证书，因为任何对证书的篡改都会破坏数字签名，从而被检测到。

（2）唯一性。数字证书具有一定程度的唯一性，一把钥匙开一把锁，用户的身份和公钥是绑定在一起的，一个数字证书只能用于一个特定的身份验证或通信目的，确保了唯一性。数字证书不仅仅是一个公钥的容器，它还包含了用户的身份信息，这使得数字证书可以用于身份验证，确保通信双方的真实身份。只有持有正确数字证书的用户才能建立受信任的通信。

（3）便利性。用户可以相对容易地申请、获取和应用数字证书。这一过程通常不需要用户深入了解加密技术或密钥管理，因为数字证书由 CA 负责生成和分发，用户只需按照指示操作即可迅速应用数字证书，十分便利，并且数字证书的应用通常无须用户掌握深入的加密技术或密钥管理知识。用户只需简单地选择使用数字证书，不必担心加密过程的复杂性。

1.2.3 公钥基础建设（PKI）

1. PKI 的定义

公钥基础建设（PKI），也被称为公钥基础架构，作为一种全球性的安全基础设施，已经成为保障数字世界安全的核心组成部分。PKI 是一套原理和技术，通过使用公钥密码学为数字世界提供了安全的通信和数据传输方式。在 PKI 中，公钥和私钥成对存在，公钥用于加密和验证，私钥用于解密和签名。然而，PKI 的核心不仅仅是密码学算法，它还包括了数字证书、CA、证书库、密钥备份和恢复系统、证书作废处理系统等多个组成部分，以确保整个系统的可信度和安全性。

2. PKI 的基本原理

PKI 是一种复杂而关键的安全体系，旨在确保数字通信的机密性、完整性和身份验证能力。PKI 的核心概念涉及公钥密码学、数字证书、CA、证书库和密钥

管理等多个组成部分。

（1）公钥密码学。又称非对称密码学，PKI 的基础是公钥密码学，它与传统的对称密钥密码学不同。在对称密钥加密中，发送方和接收方使用相同的密钥进行加密和解密。而在公钥密码学中，有两个密钥：公钥和私钥，公钥用于加密数据，私钥用于解密数据。由于这种不对称性，用户可以安全地共享公钥，而无须泄露私钥。

（2）数字证书。数字证书是 PKI 中的关键元素。它是一种电子文档，包含了用户的公钥、身份信息和数字签名。数字签名是由 CA 创建的，用于验证证书的真实性。数字证书充当了用户和公钥之间的桥梁，使得其他用户可以验证证书的有效性，并使用公钥安全地通信。

（3）CA。CA 是 PKI 的关键组件，是一个受信任的第三方实体。它的主要责任是验证用户的身份，签发数字证书，并对其进行数字签名以确保证书的真实性。CA 通常受到监管机构的监督，以确保其合法性和可信度。用户必须信任 CA，才能信任由其签发的证书。

（4）证书库。证书库是用于存储数字证书的集中化数据库或目录。它允许用户和应用程序检索其他用户的证书，以便进行身份验证和密钥交换。证书库必须受到严格的安全控制，以防止未经授权的访问或篡改。

（5）密钥管理。PKI 还涉及密钥的生成、备份、恢复和更新。用户的私钥必须在安全环境中生成，并且需要进行定期备份，以防止数据丢失。如果用户丢失了私钥，密钥备份和恢复机制可以帮助其重新获取访问权限。此外，为了保持安全性，私钥可能需要定期更换。

3. PKI 的工作流程

（1）用户向 CA 提交密钥对中的公钥，用来请求身份验证。

（2）CA 验证用户的身份，然后签发数字证书，将用户的公钥与身份信息绑定。

（3）CA 将私钥封装在数字证书载体中并颁发给用户。

（4）当用户需要与其他用户安全通信时，可以使用对方的公钥来进行数据加密。

（5）接收方使用对方的证书验证发送方的身份，并使用自己的私钥解密数据。

4. PKI 的构建和组成

（1）CA。CA 是 PKI 的核心组成部分，通常由政府机构、大型企业或专业的安全服务提供商运营。CA 的服务包括：

1）身份验证。CA 验证证书请求者的身份，确保他们有权且合法地获得数

字证书。

2）证书签发。一旦身份验证通过，CA 会创建包含用户公钥和身份信息的数字证书，并用 CA 的私钥对其进行数字签名，以确保证书的真实性。

3）证书更新。数字证书过期后如需继续使用，数字证书持有者可向 CA 申请更新。CA 机构完成数字证书更新请求的鉴别后批准签发证书。

4）证书撤销。如果用户的私钥泄露或证书信息发生变化，CA 需要撤销相关证书，并将其列入证书撤销列表（CRL）。

（2）数字证书。数字证书是 PKI 中的关键元素，用于验证用户身份和支持安全通信。数字证书包括以下信息：

1）用户公钥：证书中包含用户的公钥，用于加密和验证数字签名。

2）身份信息：证书包含用户的身份信息，如姓名、电子邮件地址等。

3）证书序列号：唯一标识每个数字证书的序列号。

4）数字签名：CA 使用自己的私钥对证书进行数字签名，以证明证书的真实性。

（3）证书库。证书库是用于存储和分发数字证书的集中化存储系统或目录。用户和应用程序可以从证书库中获取其他用户的证书，以进行身份验证和密钥交换。证书库必须具备以下功能：

1）安全访问控制：只有授权的用户才能访问证书库中的证书。

2）完整性保护：证书库必须防止未经授权的证书信息更改。

3）可用性：证书库必须在需要时提供快速、可靠的访问。

（4）密钥管理。PKI 涉及密钥的生成、备份、恢复和更新。用户的私钥必须在安全环境中生成并进行定期备份，以防止数据丢失。如果用户丢失了私钥，密钥备份和恢复机制可以帮助其重新获取访问权限。此外，为了保持安全性，私钥可能需要定期更换。

（5）CRL。CRL 是由 CA 定期发布的包含已被撤销证书信息的列表。用户和应用程序可以查询 CRL 以验证数字证书的状态。CRL 包括已被撤销的证书序列号和撤销原因。

（6）证书策略。证书策略规定了 CA 签发证书的条件和规则。它包括身份验证方法、证书有效期、密钥长度等方面的规定。

（7）证书撤销策略。证书撤销策略规定了何时和如何撤销数字证书。它确定了哪些情况下证书应该被撤销，以及如何通知相关各方。

（8）安全通信协议。PKI 通常涉及使用安全通信协议，如 SSL/TLS，来保护数据在传输过程中的机密性和完整性。

5. PKI 的安全性特点

PKI 是一种复杂而强大的安全架构，其核心原理和组成元素共同构成了一个安全的生态系统，以确保数据的保密性、完整性和可信性。

PKI 的核心原理是基于公钥密码学，采用非对称加密算法，即使用一对密钥，包括公钥和私钥，公钥用于加密数据，私钥用于解密数据。这种机制允许用户安全地交换数据，因为只有私钥的持有者才能解密数据，确保了数据的保密性。

PKI 使用数字签名来验证数字证书的真实性。数字证书是包含用户身份信息和公钥的文件，由可信的 CA 签名。这个签名保证了证书的完整性和可信性，因为只有 CA 才能生成有效的数字签名。PKI 的关键组成部分包括 CA、注册管理中心（RA）、证书库、密钥备份和恢复系统、证书作废处理系统和客户端证书处理系统。CA 是 PKI 的中心组织，负责颁发和管理数字证书，确保证书的真实性。RA 协助 CA 验证用户身份，并确保公钥与用户身份正确关联。证书库是存储数字证书的集中地点，供用户和应用程序访问。密钥备份和恢复系统允许用户在密钥丢失时访问其加密数据，而证书作废处理系统允许废除已失效的证书。客户端证书处理系统用于处理和存储用户的数字证书。

PKI 的安全性特点包括公钥加密、数字签名、身份验证、防抵赖性、证书撤销、密钥管理、完整性保护、可信的第三方、安全通信协议、网络安全增强、追溯性、审计、隐私保护。这些特点共同确保了数字通信的高度安全性和可信度。

1.3 国内外现状与趋势分析

1.3.1 国内现状与趋势分析

目前我国电子认证服务机构规模普遍较小，一般集中在单一地域或单一领域开展业务，但是行业内具备较强技术实力及领先服务理念的 CA 机构已经开始跨区域、跨行业开展业务。中金金融认证中心有限公司、北京天威诚信电子商务服务有限公司、北京国富安电子商务安全认证有限公司等实力较强的 CA 已在全国范围内展开竞争。随着电子认证服务全国市场的逐步形成，实力较强的 CA 在市场竞争中将具备更大的优势。

随着信息化进程的加快，电子认证在解决网络信任需求方面的优势被越来越多的行业认可，并更多地纳入到行业总体信息安全规划中，成为支撑业务创新的重要保障。这一趋势带动了电子认证业务在医疗信息化、互联网彩票、电子发票、网上证券、网上保险等领域中的应用。

在医疗卫生领域，随着我国新医改方案的实施，基于电子病历的医院信息系统和基于电子健康档案的区域医疗卫生平台的建设纷纷启动。国家卫生健康委已发布了关于推动电子认证服务、电子病历应用的系列规划和政策文件，将推动医疗卫生领域的电子认证市场进入快速增长阶段。

在彩票行业，互联网彩票、手机彩票等销售模式的使用将推动电子认证业务在彩票行业的普及和发展。电子认证服务和产品能够为互联网彩票的真实、可信提供保障，彩票行业广大的市场网络和用户群体将为电子认证业务带来较大的市场空间。

在电子发票方面，电子认证作为实现电子发票安全性、可信性的核心技术之一，在加强税收征管、优化征纳服务等方面具有较大优势。随着电子发票逐渐进入推广阶段，电子认证将在税务领域形成新的应用市场。

在金融领域，电子认证在网上证券、网上保险、网上支付等领域已开始应用，证券领域非现场开户和网上交易、保险领域电子保单和移动展业等新业务模式正在兴起，将带动电子认证服务和产品的应用。未来电子认证在金融领域普及率的进一步提高以及金融业务网络化、移动化的进一步深入，将为电子认证业务开辟出新的市场空间。

1.3.2 国外现状与趋势分析

美国大力发展基于 PKI 框架的 FICAM 数字身份证方案，在政务领域应用卓有成效。FICAM 的前身是美国网络安全委员会 CNSS 在 2008 年前后提出的 ICAM（Identity Credential and Access Management），目的是在美国涉密信息系统中建立统一的身份、证书和访问管理系统，解决联邦涉密网络间的协同工作和身份认证问题。ICAM 发布之初并未得到重视，但在 2009 年前后，美国政府接连发生严重泄密事件，特别是“维基解密事件”的发生使得联邦政府高度重视涉密系统身份验证及文档访问控制。2009 年 5 月奥巴马政府发布《网络空间政策评估——保障可信和强健的信息和通信基础设施》，将建立身份管理系统作为一项重大任务提出，ICAM 系统因而得到联邦政府资助正式演变成 FICAM。而在之后的 2011 年 4 月，随着奥巴马政府签署《网络空间可信身份国家战略》将建设网络空间可信身份体系提高到国家战略层面，FICAM 技术研究也因得到政府的大力支持而在电子政务领域全面铺开。

FICAM 通过 PKI 技术集中、统一地给美国政府机关涉密人员发放数字身份证，并以此为基础加强访问控制管理。FICAM 包含五个主要模块，分别是身份管理模块、证书管理模块、访问管理模块、身份联合模块和审计与报告模块。其工

作原理是首先由身份管理模块为访问者生成可信数字身份，然后由证书管理模块将数字身份绑定到数字证书上，最后通过访问管理模块和身份联合模块进行证书鉴权实现资源的访问控制，与此同时，审计与报告模块负责记录和分析系统活动，以确保符合安全政策和法规要求。整个 FICAM 基于 PKI 架构，其核心是证书管理模块中的军方 CA 机构，如国家安全局、国防部中间认证中心、国防部分配认证中心、联邦调查局认证中心等。截至 2016 年年底，美国联邦政府和军方基本完成了基于 PKI 框架的 FICAM 体系建设，虽然该框架仍存在访问认证效率低下、涉密安全要求不统一、跨安全域传输能力匮乏等诸多问题，但也基本解决了涉密网络人员身份验证、安全域互操作和外部网络对内部网络的安全访问等问题，应用卓有成效，主要应用于电子政务和军事领域。

欧盟积极推广 eID 电子身份证方案，在民用领域应用成绩斐然。欧盟网络发展战略的重点任务之一是要建立网络可信身份体系，并在欧盟范围内形成一个统一的身份服务市场。根据战略要求，欧盟成员国采用 eID 作为可信身份解决方案，用以识别身份、保护数据，降低网络欺诈的风险。

eID 采用高强度安全机制，可以确保密码信息无法被读取、复制、篡改或非法使用，从而确保 eID 和持有人一一对应。eID 的签发机构类似于 PKI 框架下的 CA 机构。当用户需要在网上自证身份的时候，只凭姓名和 eID，不需要其他个人隐私信息，就可以在实名的网站完成注册，而真实的个人信息保存在联邦公民基本信息库中，网站无法看到。网站将 eID 提交给联网数据库进行查询，返回结果仅是状态信息，即此人是否真实存在以及 eID 是否有效，结果中并不带有任何姓名、身份证号等个人隐私信息。这样既达到了实名的真实性要求，又达到了保护个人隐私的目的。据最新统计，欧盟 27 个成员国中已有 18 个发行了 eID，其中比利时使用人数已超过 900 万，覆盖了全国 80%以上的人口。除了在 eID 身份验证理论上进行研究，欧盟还在 eID 配套产品和公共平台研发上持续加码，如 2009 年启动最大的芯片卡研究项目 BioPass，研制符合国际标准的 eID 卡，开发具有高安全性与互操作性的 eID 卡平台；2010—2015 年开展的 ISA 项目，通过研发搭建公共平台，包括敏感数据信息交换和共享平台、多语言服务平台、数据共享安全网络平台等，促进成员国公共行政部门的合作；2012—2015 年由德国弗劳恩霍夫工业工程研究所牵头的 FutureID 项目，开发了用于移动设备的 eID 客户端，为在线服务提供商开发功能多、易用性强的应用程序，并探索研究保障用户隐私不受侵犯的新技术和新应用。