电子认证 2.0 白皮书

（2018 版）

全国信息安全标准化技术委员会

鉴别与授权工作组

2018 年 4 月

目录 *CONTENTS*

第一章 前言

随着互联网和物联网技术的快速发展，网络实体身份呈爆炸式增长态势，虚拟化技术的普遍应用加速了网络实体在网上的快速迁移，网络实体身份管理面临重大的挑战和变革。当前，网络实体身份资源已经成为大企业乃至国家的重要战略资源，对网络实体的可管可控已成为网络空间掌控能力的重要体现。电子认证技术[1]是实现网络实体身份可信管理的技术，是网络信任体系的基础核心技术，也是网络空间安全治理的重要技术支撑。

电子认证技术旨在解决网络实体的身份管理问题，涉及网络实体的身份标识、身份验证与证明、身份鉴别和授权管理等方面。在当前的网络环境下，面对日益猖獗的网络欺诈、个人信息买卖以及身份黑市活动，传统电子认证技术面临着重大的挑战。但在业界的共同努力下，电子认证技术已在诸多方面呈现出不同于以往的新特征，我们认为电子认证技术已从 1.0 时代迈向 2.0 时代，主要表现在：以离线数字证书为主导的身份证明演化为以在线服务为主导的身份管理；以静态的双因素身份鉴别技术发展为以风险控制为主导并融合多种技术的身份鉴别；简单的是或否单一判断模式

1 本白皮书中的“电子认证”采用了民间的电子认证的概念，指广义的电子认证技术，包含身份标识（Identification）、身份验证与证明（Certification and Proof）、身份鉴别与授权（Authentication and Authorization），该定义并未采用严格的学术定义，无对应的英文单词。严格来说，Certification 才能叫认证，Authentication 应该翻译成鉴别，而 Identification 是指身份标识。

的电子认证转变为具有多模式多安全等级的电子认证；专业化的共享共用身份管理服务逐步替代孤岛隔离的分散的身份管理；基于大数据的行为溯源和追踪技术加强网络实体的可信管理与追溯等。

《中华人民共和国网络安全法》（以下简称《网络安全法》）中规定“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认”。本白皮书以《网络安全法》为指引，面向当今网络发展的新趋势，在已有电子认证技术的基础上，提出并描绘电子认证 2.0 的技术特点和标准体系，希望与业界从业者达成共识，进而规范网络实体的身份管理和服务，降低政府及企业在防伪防欺诈等方面的成本消耗，推动国家网络可信身份生态体系的建设。

本白皮书的撰写得到了全国信息安全标准化技术委员会的指导和帮助，得到了中国密码学会的大力支持和指导，是全国信息安全标准化技术委员会鉴别与授权工作组及中国密码学会电子认证专业委员会专家集体智慧的结晶，在此向指导和参与工作的领导和同事一并表示感谢。文字工作主要由刘丽敏、荆继武、吕娜、国强等编辑完成，在此也一并表示感谢。

本白皮书以工作组内专家观点为主导，力求正确反映技术走向，错误和疏漏之处在所难免，文中观点也可能与其他专家观点有所不同，欢迎大家批评指正，共同为国家电子认证发展出力献策。任何建议与意见可联系全国信息安全标准化技术委员会鉴别与授权工作组秘书处（邮箱：tc260_wg4@is.ac.cn）。

第二章　网络发展推动新的电子认证需求

截至 2017 年 12 月，我国网民数量已经达到 7.72 亿，稳居世界第一网络大国。我国互联网的发展关乎国家经济发展、社会稳定繁荣，更是影响我国国家安全和主权安全的重要因素。移动互联网、云计算、物联网、区块链、大数据等新技术的出现为网络世界带来了广阔的发展空间和崭新的机遇，同时也带来了新的需求和挑战。

2.1　网络实体和网络应用呈爆炸式增长态势

移动互联网和物联网的发展使得网络实体的类型和数量快速增长，类型多样化和数量大幅增长的身份管理需求对认证技术提出了新的要求。每位用户、每台设备（如手机、笔记本电脑、平板电脑、台式计算机等）、每个传感器节点（如摄像头、指纹传感器、红外线传感器、RFID 等）在多种场景中的不同应用里都可能拥有不同的身份和不同的管理者。用户、设备、传感器节点等网络实体接入网络直接导致了网络身份的爆炸式增长。

与此同时，网络应用数量也呈现爆炸式增长。根据应用市场分析显示，苹果 APP Store 中的应用数在 2016 年已超过 200 万。每个应用都有对应的开发者，不仅开发者拥有自己的身份，每个具体的应用、用户通常也会有一个相关的身份，如：由邮件地址与口令构成的电子邮件身份、由 QQ 号和口令构成的 QQ 身份、由淘宝账号与口令构成的淘宝身份等。网络用户数量

的增加，伴随着大量设备的接入，使得网络用户的身份不断复杂化并呈现出大规模、爆炸式增长态势（见图 2-1）。

如何唯一标识数量巨大且不断变化的网络实体，如何通过身份标识唯一体现和反映复杂的实体间控制或从属关系以便强化追踪与管理，如何支持同一实体在不同应用中的实名或匿名等不同的安全需求确保不同应用和用户实体安全，都是新形势下电子认证技术和标准的重要问题。

图 2-1 网络主体和网络应用爆炸式增长

2.2 服务和身份虚拟化技术迅速普及

移动互联网、云计算使得网络中的计算、服务、身份等资源的虚拟化发展迅速普及，身份管理技术必须适应虚拟计算环境下的身份虚拟化和不断变化的身份关联。用户使用不同的终端设备（如手机、笔记本电脑、平板电脑、台式计算机等）通过云端的应用和代理服务控制或使用远端虚拟机进行计算和服务，使得一个身份可以动态延伸到不同网络和设备中。不同的

服务也将产生诸多不同的副本身份并在网络上不断迁移。

计算机以及服务器可以通过虚拟化，使参与网络行为的各种实体能够在网络上随着计算机与服务器的迁移而高速漂移，导致网络控制关系的快速不断变化，这使采用传统方法实施网络实体的管理追溯和控制也变得更加困难。

网络虚拟化条件下的实体管理和身份鉴别对身份管理技术提出了新的需求，网络实体的快速延伸，网络实体间的控制、从属等关系都将变得更加复杂，网络实体的变化和移动也将更加快捷，实体的鉴别、追踪和审计管理将成为新形势下身份管理的重要问题。

2.3 数字化财富追赶现实世界的财富

随着互联网经济的发展，互联网技术与金融、文化、制造等产业得到了有机的结合，数字化财富正在赶超现实世界的财富。各大银行纷纷推出了互联网金融业务，支付宝、微信等第三方支付方式得到了广泛应用，各大电商企业、P2P 模式的网络借贷平台也如火如荼的发展，各种类型的手机金融理财业务也层出不穷，财富正在从现实世界向数字世界迅速转化且势不可挡。

数字世界处处存在价值，资产形式多样化，不再拘泥于现实世界的币种。如，近些年来风靡全球的比特币，在 2009 年诞生之初，1300 个比特币仅值一美元，到了 2018 年，10000 美元才可以兑换一枚比特币。又如，近两年来逐渐升值的网络身份，也包含巨大价值，2016 年的网络红人 papi 酱，成功融资 1200 万元。名人在新浪微博、腾讯 QQ 的 VIP 账号，甚至网络游

戏中的皮肤和装备，也已经成为一种新的资产形式。

数字世界已不再是虚拟时空，不仅控制着虚拟的财富，也影响着现实世界的经济发展。在信息媒体蓬勃发展的今天，数字世界已变得越来越重要，而其与现实世界的融合和接轨使其在某些方面比现实世界更为重要。与此同时，利益驱动下的犯罪和攻击将变得更加频繁。从技术和标准上维护网络实体身份可信、确保网络上数据、信息或虚拟实体的完整、真实、可鉴别，以及确保现实实体和网路实体的关系安全，包括关系的真实、完整、可控以及可证明将成为新时代下经济发展的新挑战。

2.4 网络协作成为网络发展的主流

云计算技术等的快速发展，标志着网络专业化服务的兴起，预示着网络协作将成为网络发展的主流。基于云计算的专业化服务，将逐步改变过去信息系统自给自足的服务模式。网络协作以及网络专业化服务的市场体系，将使得网络经济发展更具效率和活力。

网络协作需要多个参与方，参与方之间的互相信任是网络协作得以正常、稳定运作的重要基础。网络信任体系的建设已成为主流数字世界发展的重中之重。作为网络信任体系构建的基础技术，电子认证技术也必将成为推动我国网络经济快速发展的重要基础技术。

2.5 身份数据资源成为互联网企业竞争力和国家网络治理重要支撑

网络身份数据资源已成为互联网企业的核心竞争力，网络身份和认证信息是企业提供后续服务的前提。通过网络身份和认证信息，网络实体及

用户信息的管理者或服务者能更容易获得用户的网络行为、爱好等信息。因此，网络应用为用户提供更好服务的同时，从某些方面也为掌握网络用户的上网活动提供了条件。

拥有用户是企业拥有财富的一个重要标志。Facebook 用户数量已经达到 22 亿，其公司价值是按照用户数量来评估的；腾讯拥有超过 8 亿的用户量；360 通过杀毒软件、手机助手等软件拥有了 6.4 亿用户；支付宝拥有 4.5 亿实名用户。管理用户的数量直接反映了企业未来的价值，已经成为互联网企业的生命线。

网络实体包括现实世界的网络用户，是网络经济发展的主体，控制着网络资源。聚集的实体身份信息直接关系到国家的网络经济安全和其对网络资源的控制力。非法获取网络身份信息，是当前网络犯罪寄生的基础。非法获取和利用这些身份信息，将会威胁到网络用户的虚拟经济、现实经济甚至人身安全；合法应用这些身份信息，才能保障网络秩序和谐，促进产业快速发展。

在网络疆域和边界不断变化的情况下，网络身份管理的规模和能力已经成为国家网络治理能力的重要标志，大力发展网络身份管理与服务技术，研究适应新时代的不断增长变化的网络身份管理与服务相关标准规范和安全技术要求，推进我国自主的网络身份服务生态体系及可管可控网络秩序建设，也是我国参与世界网络治理的一个重要体现。

第三章　电子认证技术存在重重挑战

3.1　网络欺诈严重危害互联网生态环境和社会公共安全

我国稳居世界第一网络大国，但是大多数网民的网络安全知识匮乏，安全意识淡薄，安全技能有限，身份保护能力不足。如，钓鱼网站和合法网站的网址存在着细微的差异，但网民基本不会注意观察浏览器的地址栏；公众场合随处可得免费 Wi-Fi，但也成为了有些不法分子冒充合法网络引诱网民、进而欺诈网民的途径；出于简单易用的考虑，弱口令现象普遍，网民倾向于采用用户名/口令的方式来登录网络应用，并通常使用自己的生日或简单单词等作为口令，还常常使用同一个口令登录不同的网络应用或服务商，给口令被破解带来隐患。又如，大多数网民为了网络生活的便利，不经意间在网络中泄露了个人身份信息，而这些信息一旦被不法分子窃取，就会成为他们谋取利益的对象，如网民们选择在使用抢票软件抢购火车票时，就需要在这些软件上输入其在 12306 网站上的用户名和口令，增加了用户名和口令遭到泄露的风险。

互联网技术的快速发展催生出各式各样的网络欺诈手段，技术水平越来越高，广大网民难以甄别。不法分子从多个渠道收集攻击目标的家庭情况、社会关系和个人信息，利用社会工程学对攻击目标进行网络欺诈。这种精心定制的网络欺诈手段，网民通常难以辨别，信以为真，从而造成巨

额损失。如，不法分子利用钓鱼网站、手机病毒等方式盗取银行账号及密码、冒充国家机关发布虚假信息、盗取 QQ 或微信账号冒充亲友骗取钱财。欺诈手段随着技术发展而不断翻新，勒索病毒等新的犯罪模式也逐渐涌现，对个人的财产及人身安全带来巨大威胁，也加深了对社会的信任感危机。如：2016 年的“徐玉玉”事件，因电信诈骗付出了生命的惨痛代价；2016 年某高校教师因信息泄露，被犯罪分子冒充公检法骗走 1760 万元。

互联网欺诈事件频发对互联网生态环境产生了诸多不良影响，严重阻碍了我国信息产业尤其是互联网+等新业态的健康、快速发展。

3.2 企业保护个人信息技术亟待规范

我国互联网发展迅速，网络活动越来越丰富，公民个人真实信息已经大量并广泛存在于多种网络中。电子政务、社交网络、网上购物、网上理财、即时通信等，网民参与的大部分网络行动均需要进行实名登记。大量的真实身份信息，包括个人身份证/护照号、手机号、联系地址等都被收集并常常被保存在不同的网络服务器上。

我国互联网企业也通过各种服务途径，如网上购物、手机导航等掌握了大量用户的真实信息，除个人基本信息外，还包括：家庭住址、兴趣爱好、网络社交行为、购物习惯、真实行动轨迹等。互联网企业针对个体用户提供的安全保护服务，也会收集用户的个人隐私信息。

目前，多数互联网企业安全和隐私保护能力不足，导致用户个人信息泄露事件频发。许多互联网企业为降低成本，或安全意识薄弱，对用户个人信息的保护不够重视。企业关注点主要在自身提供的网络产品和服务的

发展方面，部分企业大量收集甚至超范围收集用户的个人信息，却对用户数据缺乏必要的保护，如直接明文存储用户个人信息等。据相关新闻报道，2015 年，知名连锁酒店锦江之星、速八等被爆出存在高危漏洞，黑客可轻松获取千万级顾客开房信息；2015 年，10 万高考考生信息遭到泄露；2016 年 9 月 22 日，雅虎承认其与至少 5 亿用户相关的信息遭人窃取；2017 年 10 月，雅虎再次宣布所有 30 亿用户个人信息被泄露。

大规模隐私泄露事件频发的案例，折射出令人堪忧的个人真实信息的网络安全处境。事实上，大量的个人真实信息可以轻易通过极低的代价获取。据南方都市报报道，仅需 850 元就能获取个人的开房记录、列车记录、航班记录等 11 项个人信息，其中开房时间可以精确到秒；提供身份证号还能够查询到四大银行的存款余额；查询手机定位经纬度可精确到小数点后六位。

综上所述，我国诸多网民的身份信息处于“裸奔”状态，迫切需要相关企业采取安全措施保护用户隐私，相关技术要求标准和规范亟待制定。对大多数组织来讲，正确管理身份信息对于保持组织业务过程的安全至关重要；对于个人来讲，正确的身份管理对于隐私保护十分重要。为有效管理基于身份信息做出决策的数据处理系统以及隐私保护问题，国际上近年来已开展了诸多研究并发布了相关标准，如 ISO/IEC 24760 系列标准、《信息技术 安全技术 隐私框架》（ISO/IEC 29100）、《信息技术 安全技术 隐私能力评估模型》（ISO/IEC 29190）等，为我国在身份信息管理以及隐私保护方面的研究和标准化工作提供了重要指导。

3.3 身份非法买卖严重影响网络实名制实施效果

网络身份买卖的黑色产业链源于网络身份与现实身份的绑定需求。网民在使用大部分网络产品和服务时，需要将其网络身份与现实身份进行一对一的绑定，包括：银行开户、淘宝注册、酒店入住、电信开户等。将网络身份与现实身份进行绑定，可实现对网民身份的认证，保护网民合法利益并更好实现对网络行为的监管。对于网络诈骗、洗钱等非法行为而言，使用他人的真实身份信息绑定网络身份，是一个绝佳的掩护手段。如，犯罪分子从黑市购买被盗身份证，开办银行卡洗钱；为了隐藏个人真实财产，持有多个身份证。一些个人，为隐私保护的目的，也会从黑市购买身份，进行网络登记或网上聊天等。

部分企业以实名制为名，大肆收集公民个人信息。网络身份黑色产业链不断完整，技术也不断提升。比如，地下黑色产业链可利用作弊工具产生虚假的但可验证通过的身份证号码，从而绕过简单的实名注册；针对提供身份证复印件或者手持身份证拍照等验证信息的方式，黑色产业链通过非法收集并售卖全套的淘宝验证数据，包括身份证复印件、手持身份证拍照照片等，来绕过实名注册。

目前，我国身份买卖黑市已经形成一定规模，网络身份买卖价格低廉，通过极低的代价即可将网络身份绑定到一个不属于个人的现实身份。身份买卖服务包括身份证买卖、配套资料销售（与身份证对应的 U 盾、手机卡、开户资料等）、假证办理等。据新华社报道，只需要 900 元就可购买到他人全套的银行开户资料，包括开户的银行卡、身份证原件、网银 U 盾、银行卡绑定的手机号码卡等一系列证件，单以银行卡买卖为例，就已经形成

了一条完整的非法利益链。

实名制推行的初衷，是为了便于监管和责任追查，但由于身份黑市交易可以将个人的网络身份绑定到了一个不属于本人的现实身份，同时配套的身份管理技术手段比较单一、体系不够完备，企业具体执行不到位，影响了以规范互联网环境、抑制网络犯罪为目标的实名制推进效果。

3.4 单一鉴别技术面临不断发展的安全威胁

正所谓没有绝对的安全，安全是动态发展的，静态的身份鉴别面临严峻挑战。事实上，一种鉴别技术从设计理念到具体实施，处处都可能面临着攻击技术进步的威胁和风险。无论何种单一的鉴别技术，都不能确保绝对的安全。

鉴别技术采用的密码算法，其算法原理可能存在威胁。如众所周知的 MD5 和 SHA-1 杂凑算法一直作为最为广泛应用的密码算法应用在金融、电子商务、电子政务等领域，目前这两个算法已被宣布存在安全隐患。

鉴别技术在技术实现时可能存在安全漏洞，如果技术实现不准确，就会存在中间人攻击的威胁。如广泛用于保护互联网上数据传输安全的 SSL 协议，SSL 协议安全隐患的存在可能使用户受到各种极具破坏力的网络攻击，其中中间人攻击(Man-in-the-MiddleAttack,简称 MITM 攻击)就是非常危险的一种攻击方式。事实上，任何信息技术在具体编码实现时，安全漏洞的存在是必然的，身份鉴别服务提供者在发现安全漏洞时，只能尽快做好修复和补救措施。

鉴别技术在实际应用时也可能存在安全威胁，如采用被动式的签名机

制无法应对中间病毒的攻击。

3.5 身份鉴别需适应网络应用多样化发展需求

网络应用类型及应用场景呈多样化趋势，多样化的应用和差异化的场景需要多样化的身份鉴别技术。

网络应用已逐渐深入应用到金融、政务、教育、交通、通信、社交等各个行业中，包括在线支付、社交应用、金融服务、手机导航等。不同的应用类型需要不同安全级别和不同方式的鉴别技术。

网络应用的场景也呈现出多样化的趋势，如支付宝具备普通社交、小额支付、大额支付等应用场景，微信兼具有社交、即时通讯、支付、电商等应用场景。不同的应用场景也需要不同的身份鉴别技术，以满足用户在不同应用场景下的易用性及安全性需求。如小额支付可以免密支付，大额支付需要进行更加严格的鉴别后才可进行；又如用户在常规应用上登录只需要简单身份鉴别即可，而在高安全应用上登录需要提高身份鉴别强度。

过多的需求会导致身份管理的差异化，无序的差异化发展必然带来互联互通问题。如何将过多的安全需求归纳整理，研制既满足多级别安全需求、又简单易行的安全技术标准无疑是推动我国身份管理良性发展的新挑战。

第四章　电子认证 2.0 时代已经到来

网络身份已经成为互联网的重要战略资源，电子认证服务模式和认证方式也在发生巨大变化。生物特征识别、云计算、大数据等技术的融合发展，极大地丰富了电子认证的内涵，促进了电子认证在金融、政务、医疗等各大领域的应用，推动电子认证从 1.0 时代走向电子认证 2.0 时代。

4.1　由离线数字证书为主导的证书服务演化为以在线身份服务为主导的身份管理

传统的电子认证服务通常使用离线的数字证书服务模式。数字证书认证机构给用户颁发一个包含用户个人信息和公钥的数字证书，用户通过数字证书进行网络身份鉴别，鉴别时一般不需要数字证书认证机构在线，只需要有最新的证书撤销列表。尽管多数的数字证书认证机构还提供在线的证书状态协议，实现了用户证书撤销的快速响应，但该协议对网络连接要求高，采用证书撤销列表仍是传统实现的主要方式。虽然基于数字证书的身份鉴别安全性高，但传统的以专有硬件（如 USBKey）为数字证书载体的用户身份鉴别易用性不够好。

随着 3G、4G 移动互联技术的不断发展，网络无处不在，用户可通过不同的终端接入方式，访问形式多样的网络应用和服务，这对电子认证的安全性和易用性提出了新要求。

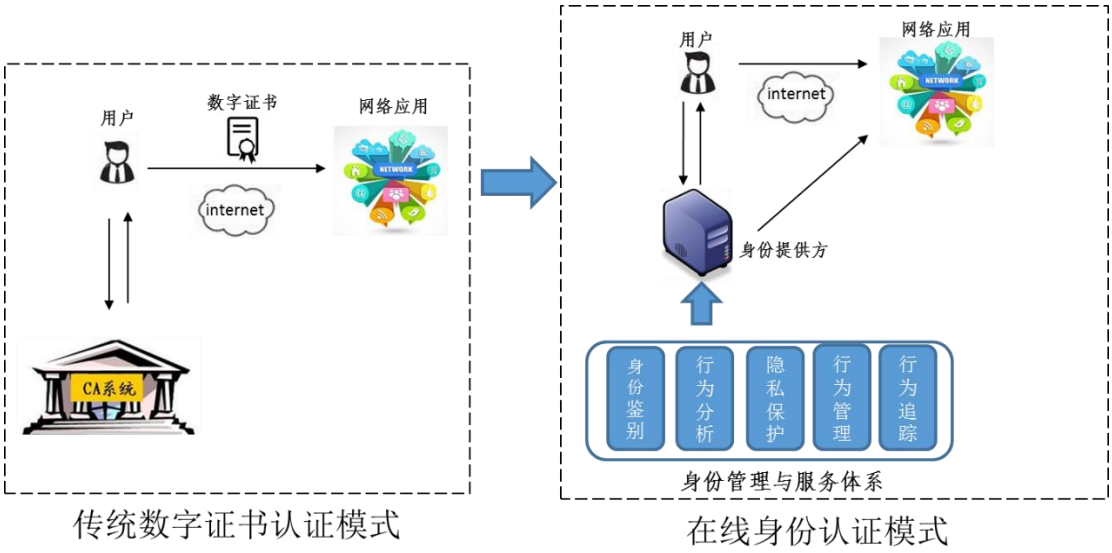

图 4-1 电子认证服务模式的转变

在线的专业化的身份管理与服务已经成为当今网络身份认证的主要方式和发展方向。在新的模式下（见图 4-1），用户在访问网络应用时，可通过在线的专业化身份服务提供方实现对用户身份的鉴别，完成身份鉴别后再将相关数字凭据在线实时返回给相关应用，具有更好的安全时效性。专业化的身份服务也向用户提供了更佳的易用性和安全性，包括单点登录，多级安全支持，不再受限于专有硬件等。同时，网络应用与服务管理者无需管理用户身份信息，可节约开发经费，降低系统复杂度，减少隐私信息泄露风险。

4.2 静态的双因素身份鉴别走向以风控为主导融合多种技术的身份鉴别

传统的双因素身份鉴别技术面临诸多安全挑战。传统的身份鉴别一般在身份注册阶段验证用户的真实身份（如通过身份证号、手机号、邮箱地址等），为用户颁发鉴别凭证，通常是口令、令牌或者数字证书，然后网络

应用可以利用凭证鉴别用户。当发放的令牌或证书是无法复制的独立介质，同时也要求提供用户记忆的口令时，这种鉴别方式也被称为双因素鉴别，即知道什么和拥有什么。在部分情况下，也会加上第三个因素来进行鉴别，如利用生物特征识别。

双因素身份鉴别技术在实际应用中遇到了越来越大的挑战。由于生成凭证的技术所限，凭证的复制和假冒时常发生。盗号木马、钓鱼网站等手段也可以获取用户的真实凭证信息，进而攻击用户的账户。简单的静态双因素或多因素身份鉴别无法确保当前网络攻击下的身份安全。同时，简单多因素身份鉴别技术给用户带来了使用上的不便，例如要求用户记住口令、拥有 IC 卡或证书硬件介质等，登录过程繁杂。

基于用户历史行为的、引入风险控制机制的身份鉴别技术（以下简称基于风控的身份鉴别），已经成为目前身份鉴别技术发展的重要方向。在基于风控的身份鉴别中，将根据用户操作所需要的授权决定用户鉴别的安全要求，用户的凭证不再成为应用鉴别用户的唯一因素，用户的网络行为和相关知识也同时作为鉴别判定的重要因素。通过对用户的基本信息（见图 4-2）提取以描摹个体，获取对用户的认知。在用户登录时，通过对环境信息进行动态监测和用户行为的动态监测以进行用户判定。目前，市场上主流的互联网企业，如腾讯、阿里巴巴等均已使用基于行为的身份鉴别技术，通过监控每个用户的登录行为，并根据行为状态来判定是否允许该用户登录或者进行某些关键操作（例如支付）。

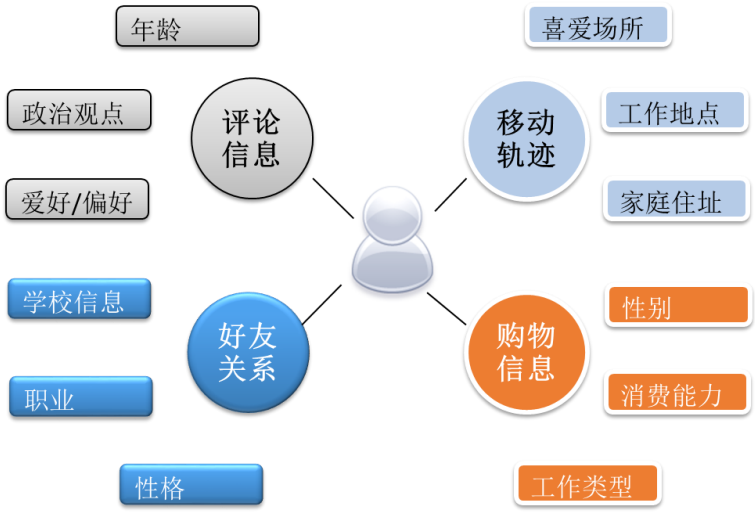

图 4-2 用户基本信息

同时，基于可信执行环境的移动终端的发展使得基于生物特征识别的身份鉴别技术应用得到迅速推广，以 FIDO、IFFA、SOTER 等为代表的基于生物特征识别的身份鉴别服务得到了较大范围的应用，如指纹识别、虹膜识别、人脸识别等，大大提升了身份鉴别服务的易用性。

4.3 多模式多安全等级电子认证成为满足应用需求又节约成本的最佳选择

互联网应用和服务层出不穷、形式多样、更新频繁，不同网络应用或服务对用户的可信安全需求也各不相同。即使相同的应用，在不同的环境和场景下对用户的鉴别也有不同的安全要求。支持多等级的安全身份鉴别，以满足不同类型、不同规模的应用在安全性、隐私保护能力、赔付能力等方面的差异化需求是现代身份鉴别的重要内容。应用或服务可能需要针对不同的用户和应用场景，配置不同的安全策略。举例来说，对于需要处理不太敏感信息的应用，仅通过一般鉴别强度的用户实体就可使用；对于安全风险较大的环境，需要使用更强鉴别功能的令牌。

针对不同的应用/机构/软件/服务，根据相应的安全需求，制定多安全等级的认证策略，采用不同安全要求的身份鉴别技术，以达到更好的安全性和易用性的平衡。

4.4 在线身份管理服务的共用共享能更好实现网络个人信息保护

身份管理边界不断演变，并逐渐被打破，从以应用为中心的身份管理到以机构为中心的身份管理，逐步向着以用户为中心的身份管理方向发展。在以应用为中心的身份管理中，每个应用或者服务负责管理自己用户的身份，而每个应用的身份与其他应用不能互通。每个用户需要记住很多应用的登录账号和口令。对当前不断发展的应用来说，无论是用户还是管理员都要做大量的身份管理操作，不仅费时，而且费力。在以机构为中心的身份管理中，一个机构（企业或者政府部门）利用一个集中的身份管理系统管理其用户的身份，用户利用该身份登录所有的机构内部应用或者服务，实现单点登录。

当一个用户使用多个机构的服务时，仍旧需要使用多套账户，机构与机构之间的跨机构访问，以机构为中心的身份管理也难以应对。目前，身份管理已经打破应用或者机构边界，逐步形成以用户为中心的身份管理。以用户为中心的身份管理能够确保用户用少量的身份，使用跨机构、跨地域、甚至跨国界的服务。业界已涌现出一系列标准，用于不同的网络身份认证系统之间的互联互通，以及跨域进行访问授权。如，OpenID、SAML、OAuth、FIDO 等国际标准已得到广泛应用，被大量国内外主流的互联网企业所采用。

在网络应用和身份大规模增长的现状下，身份管理系统共享共用在为个体提供选择和便利、为应用节省成本的同时，也能更好的保护用户的个人信息。在共享共用的身份管理系统里，作为身份管理服务企业，通过身份入口掌握用户信息，同时通过提供身份服务获取商业利益；作为应用提供商，可选择不同的身份管理系统，自己不需要管理用户。作为个人，可自由选择身份管理系统，其个人信息放在较安全的身份管理系统，有利于身份信息的管理和隐私保护。

在身份管理系统中加强身份信息的安全与隐私保护，实现身份管理方与应用服务提供方的分离、不同类型身份管理系统之间的互联互通，以达到最大范围的单点登录、单点注销。

4.5 基于大数据的行为追溯可加强网络实体的可信管理

在目前的身份管理技术发展趋势下，个体的身份、行为信息存储在身份管理机构，随着大数据在各行各业的应用和发展，可通过构建网络身份与行为数据中心，实现对用户在不同身份管理机构的身份关联，从而完成用户行为预测和网络可信感知。

通过与身份管理机构进行用户身份与行为数据的交换，利用不断积累起来的历史元数据，可以获得用户身份关联、行为预测、网络可信感知等能力，建立用户网络活动信用档案，提高追溯能力。通过对用户行为大数据的监控与预测，可以发现异常行为提前预警，实现快速追踪；还可实现网络可信感知和网络宏观状态发现，包括上网流量分析、网络关注度分析、异常分析和报警等等。

利用大数据技术对用户行为技术进行关联，可通过分析和整合还原用户的网络行为记录。当个体用户在网上犯罪后，可以通过数据取证，快速获取犯罪目标的身份信息和网络活动历史，并获得犯罪目标的多种通讯定位手段，如电话、QQ、微信、交际圈等，及犯罪目标下一步的行动预测，实现对个体用户的追溯，大幅提高网络犯罪追踪、取证、溯源能力。

第五章　电子认证 2.0 发展面临诸多问题

5.1　身份管理相关法律法规体系仍有待完善

《中华人民共和国网络安全法》的颁布，奠定了我国在网络空间安全治理的法治化的基础。全国人大常务委员会于 2004 年通过了《中国人民共和国电子签名法》，并于 2015 年进行了修正；为了加强对个人信息的保护，第十一届全国人大常委会于 2012 年通过了《关于加强网络信息保护的决定》，工信部于 2013 年发布了《电信和互联网用户个人信息保护规定》；中央网信办于 2014 年发布实施了《即时通信工具公众信息服务发展管理暂行规定》；为规范互联网群组信息服务，国家互联网信息办公室于 2017 年 9 月印发了《互联网群组信息服务管理规定》。

可以看出，我国网络信息安全的法律体系已经成形，尤其侧重在服务提供商和服务使用者的管理方面，同时也涉及对用户信息收集、保护以及个人信息泄露的惩处等方面，但是在身份服务相关的责任和担保相关法律和个人信息泄露赔偿等方面的法律尚有所欠缺。虽然目前的多条法律法规中提到，在使用网络服务注册时，用户需要将个人真实信息提交给网络服务提供者，且服务提供者应当建立健全用户隐私保护制度，但是对于个人信息泄露受害用户的赔偿问题，目前还没有相应的法律法规给出赔偿的处理方法。此外，利用大数据对用户行为进行追溯，其中涉及诸多法律问题，

尚缺乏对应的法律法规予以解决。

5.2 传统电子认证服务安全程度单一

我国电子认证服务取得了长足的发展，形成了覆盖 40 多家第三方 CA 机构的全国统一信任关系，基本建立了全国电子认证行业监管体系，制定了多项电子认证相关技术标准，初步形成覆盖全国的电子认证运营服务体系，形成了丰富的电子认证应用模式服务。目前，电子认证服务已经改变了以前信任关系孤立、基础设施多样、服务标准各异的散乱局面，基本形成了一个信任关系互联互通、基础设施安全可靠、服务规范有章可循的全国统一的第三方电子认证服务体系，在各行各业信息化建设中发挥了重要作用。

但是，我国电子认证服务安全程度仍较为单一，无法全面支撑我国网络可信的应用需求。目前，我国 CA 机构提供的电子认证服务，均是基于数字证书，相对于用户名、口令之类的简单身份验证方式，安全程度高，主要适用于电子政务、电子商务、电子支付等重要的网络应用。在互联网应用环境中，诸如社交网络、论坛、视频服务、新闻浏览等网络应用，无需对用户进行过于严格的身份信息验证，目前电子认证的成本和易用性都不满足这些简单的应用需求；而另一方面，超大额电子交易、不动产交易等对身份服务有更高安全要求。部分第三方电子认证机构由于缺乏评估保障和赔偿保障，其安全程度也无法满足上述高安全应用需求。

电子认证行业缺乏统一的评价体系，电子认证服务互联互通仍存在一定困难，限制了电子认证行业发展。目前我国的 CA 机构大都根据自身的技

术及安全能力可以为用户提供若干安全等级的身份认证服务，但是各 CA 机构对于电子认证服务的安全等级划分、证书策略制定等都各不相同，而且我国 CA 机构对用户承诺的赔偿额也远小于国际 CA 机构的标准。由于我国未建立对于 CA 机构服务能力的统一评价体系，我国 CA 机构之间的互联互通也存在障碍，无法有效对 CA 机构的安全等级、服务能力、业务范围、身份服务的可信度、赔偿能力等进行评价。用户及互联网应用无法通过有效途径获取具有权威性评价信息，极大地限制了我国电子认证行业的发展。

5.3 专业身份服务应用范围有限

目前，诸多应用接入方式已经不仅限于使用应用提供商本身的账号，开始加入开放平台并接受外部提供的身份服务。这些应用不需要对用户身份信息进行管理，用户身份管理完全由开放平台进行维护。应用加入一个或几个平台，通过接受由开放平台提供的外部身份服务，在拓展自己应用市场的过程中降低了维护用户的成本，同时具备了更高效的推广能力，使得其用户数量大幅提升且获得了更多收益。

互联网用户也已经广泛接受使用互联网身份服务，如互联登录。互联登录是指采用某个网络身份登录其他互联网应用。目前，普遍使用的是 OAuth 授权技术，身份管理系统可在用户授权的基础上将用户部分信息提供给需要登录的应用。互联登录可以帮助用户免去注册的麻烦，同时用户将账户只交给可信的开放平台提供商管理，降低身份信息泄露的风险。

但是，目前我国互联网身份服务的应用范围还非常有限。首先，互联登录范围还只局限于互联网中的商业应用，还没有涉及到电子政务、金融等

领域。例如，在电子认证服务行业，跨地区、跨行业的网络应用需求旺盛。其次，在互联网行业，互联登录也只局限在一些有业务关系的企业之间，对专业身份提供商的鼓励机制还不足。开放平台提供商只限于一些大型的互联网公司，也还没有形成专业的身份服务提供商，因此互联登录推广的内生动力还需要加强，行业标准和规范还待制定。

5.4 身份服务互联互通仍有待改善

目前，已经有一些身份服务标准从技术上初步解决了不同系统间身份服务的互联互通问题。OpenID、SAML、OAuth 是几个主要的标准，这些标准可以提供互通的身份认证、跨域授权登录、属性控制等服务。其中，SAML 标准已被我国采纳为国家标准，并且已经发布。

但是，不同系统间身份管理的安全要求和责任追溯，缺乏统一认可的标准。目前不同企业或机构对于用户身份、属性、可信度、权限管理、责任追溯等的方面的关注不完全相同，身份管理服务大多处于各自为战的状态，人力物力重复投入很大。机构间信任孤岛问题很严重，由于机构间对身份管理的需求、技术水平等因素的不同，机构间普遍存在彼此不信任的情况。跨行业、跨领域身份服务安全要求缺乏统一的标准和体系。很多机构都采取单一的技术路线，对不同身份服务互通标准之间的安全性兼容互通支持不足。

第六章　鉴别与授权标准体系建设

6.1　鉴别与授权标准体系框架

为适应电子认证 2.0 的发展，需要结合我国网络发展趋势，重新构建和完善鉴别与授权标准体系框架。身份服务技术是电子认证 2.0 形势下网络可信身份生态体系形成的重要保障，鉴别与授权标准体系是身份服务技术的主要内容。在电子认证 2.0 的时代背景下，鉴别与授权技术正在发生重要变革，多方位呈现新特点，其标准的制定就尤为重要。

在电子认证 2.0 的推动下，鉴别与授权标准体系要注重解决身份服务中的重要技术的标准化问题，特别是要解决网络实体快速膨胀，相互关系复杂多变形势下的统一标识问题；要解决应用发展迅速，安全需求多样化形势下身份证明和多种身份凭证发放与管理问题；要解决攻击手段不断演进，易用成为重要需求情形下的风险可控的安全身份鉴别问题；要解决大规模用户参与下的的细粒度授权和基于身份的授权管理问题；要解决不安全环境下身份管理系统中的个人信息保护要求以及互联互通问题。

图 6-1 是在分析国内外鉴别与授权标准化需求、技术发展和应用现状的基础上提出的。该标准体系框架由五个类别的技术标准组成，分别为：标识类标准、验证与证明类标准、鉴别类标准、授权类标准和集成应用与身份管理类标准。

图 6-1 鉴别与授权标准体系框架

6.2 标识类标准

标识是实体对象（如人员、设备、数据、服务、应用）身份的标志，在新形势下，应强调具有全局的可区分性和可辨识性，同时注重实体间的关联性。标识类技术标准要扩展关注的领域，要关注包括人员、设备、数据、服务、应用软件以及各种实物。现有的相关标准包括对象标识符（Object Identifier，OID）、唯一可辨识名（Distinguished Name，DN）、国内身份证号码等。标识类标准的目标是实现标识技术的统一，为其他技术应用及互操作奠定基础。

截至目前，我国标识类的标准研制情况如附录 A.1 所示。

未来重点研制工作：加强对规模巨大、变化迅速、关系复杂的网络实

体标识标准的研制，支持未来关系复杂、快速漂移的网络管理需求。

6.3 验证与证明类标准

验证与证明类标准是指在用户鉴别前为用户登记验证证明并发放凭证的相关标准，电子凭证相关技术标准是验证与证明类标准规范的主要内容。通过验明正身，根据安全需求可以为人员、设备、数据、服务、应用等网络实体颁发数字证书、数字令牌、实体令牌、登录口令、秘密密钥等凭证。该类标准主要包括：

1）**凭证语法与格式：**主要规范化、标准化电子签名、数字证书、产品证明、电子证照、数字货币、软件可信凭证、服务可信凭证、令牌等电子凭证的语法规范、格式要求。

2）**验证与证明机制与方法：**主要规范电子凭证的生成机制、生成方法以及生成技术要求等。

3）**凭证颁发安全技术要求：**对电子凭证的安全技术要求、颁发系统安全要求以及颁发管理安全要求进行规范：

a）**凭证安全机制：**根据不同的凭证强度，规定凭证的安全技术要求，实施不同的保密性、完整性保护，以及发布、管理和验证措施等。

b）**证明与凭证颁发系统安全要求：**针对凭证的生命周期进行管理，与身份绑定的唯一标识、凭证的创建、加密密钥生成、凭证传输、凭证更新、更换、撤销、停用、状态维护、记录管理等要求。

c）**证明与凭证颁发管理安全要求：**对实体证明或凭证的管理要求，包括登记要求，验明正身的过程要求以及全生命周期服务的质量

保障要求。

截至目前，我国验证和证明类的标准研制情况如附录 A.2 所示。凭证的语法与格式方面，主要是针对数字证书凭证相关的语法与格式规范，以及相关策略、分级规范等；验证与证明机制与方法方面，主要是针对电子签名、数字签名相关的生成机制与方法；凭证颁发安全技术要求方面，主要是基于数字证书的分级规范以及数字证书的管理。

未来重点研制工作：当前形势下，要加强对物体、数据、软件、服务等不同类型实体的电子凭证标准研究，如产品防伪证明、电子证照、软件可信凭证、服务可信凭证等，以支持网络制造、网络交易全程自动化的发展；要重点研制电子凭证的互操作、基于生物特征的电子凭证、基于移动终端的电子凭证以及基于可信环境或安全芯片的电子凭证等标准，以满足电子认证 2.0 的需求。

6.4 鉴别类标准

鉴别主要是指利用电子签名、数字证书、令牌、口令、秘密密钥等电子凭证完成对实体（如人员、设备、数据、服务、应用）的身份属性进行验证的过程，确保待鉴别实体身份属性的真实性。该类标准主要包括：

1) **鉴别机制：**包括对运行代码、网络服务、数字防伪、数字货币、实名/匿名实体、消息等身份属性的真实性，如数据源的真实性的验证方法和机制进行标准化。

2) **鉴别框架与协议：**对基于生物特征识别、基于行为、基于凭证安全等级以及基于多因素的鉴别交互过程进行规范化、标准化。基于常

见的生物特征识别（如人脸识别、指纹识别、虹膜识别、步态识别、红外温谱图识别等）的身份鉴别框架与协议；基于实体行为特征的身份鉴别框架与协议；分级实现身份鉴别的标准和要求。

3）**系统实现与安全要求：**对实现鉴别技术的系统、接口等开展系统框架、接口规范、技术/实施要求和系统安全要求方面的技术标准研制。

截至目前，我国鉴别类的标准研制情况如附录 A.3 所示。鉴别机制方面，主要是实体/匿名实体鉴别、消息鉴别码、可鉴别的加密机制；鉴别框架与协议方面，主要是基于生物特征识别的鉴别协议；系统实现与安全要求方面，主要是基于 SAML 的接口规范，以及基于生物特征识别的系统安全技术要求。

未来重点研制工作：在当前形势下，要加强对物体、数据、虚拟资产、软件、服务等不同类型实体的鉴别标准研究，如基于产品防伪证明、电子证照、软件可信凭证、服务可信凭证等的鉴别；要重点研发基于生物特征识别的身份鉴别标准，特别是基于人脸的身份鉴别标准，加快研制基于风险控制的身份鉴别标准，确保基于风险的鉴别具有应用可识别性和互操作性。

6.5 授权类标准

授权主要是指在完成实体身份鉴别的基础上，通过访问控制技术来限制实体对某些信息项的访问，防止对任何资源的非授权访问。该类标准主要包括：

1）**授权机制：**对基于角色、基于密码、基于属性的访问控制机制进行

规范化、标准化。

2）**授权框架与协议：**在目录访问控制、第三方资源授权、家庭网络授权和受限环境中的授权等方面开展技术标准研制。

3）**系统实现与安全要求：**对采用或实现授权技术的接口、访问控制系统等开展系统框架、接口规范、技术/实施要求和系统安全要求方面的技术标准研制。

截至目前，我国授权类的标准研制情况如附录 A.4 所示。授权机制方面，主要对轻量级鉴别与访问控制、基于角色的访问控制进行规范；授权框架与协议方面未开展相关研究；系统实现与安全要求方面，制定了程序接口规范与置标语言。

未来重点研制工作：在当前形势下，要重点研制针对的多级鉴别结构实施多级的细粒度授权的标准，研制互联互通的授权协议，加大针对物联网授权标准的研制力度，推动物联网、智慧家庭等的发展。

6.6 集成应用与身份管理类标准

我国在基于 PKI 技术的集成应用类标准，如电子签名、数字证书、PKI 系统及其互操作等方面已发展成体系，但身份管理和访问控制仍然是当今网络空间安全面临的最大挑战之一。

为促进新型网络身份服务业及网络空间身份管理的发展，进一步推动网络空间可信身份体系建设，统一互联网用户身份认证管理，构建互联网应用健康发展的环境，有必要对可信身份管理技术架构进行设计和论证，定义和规范身份管理框架、身份互联互通要求、安全策略分级要求、安全

服务要求、个人信息保护要求以及行为追踪取证要求等，确保网络身份在认证、鉴别、授权、使用过程中的个人信息保护，支持对网络行为的追踪和溯源。该类标准主要包括：

1）**总体类**：规定身份管理中的基本概念、术语及定义，数字身份格式以及数据模型；

2）**应用实例及要求**：针对身份管理的应用实例及获取、处理、存储、传输以及用于识别或鉴别实体等目的的实体标识符或个人可识别信息的身份管理系统进行规范；

3）**身份管理框架及结构**：规范信息系统身份管理的通用框架及运行体系架构，以使信息系统能满足相关业务、合同、法律法规要求进行定义；

4）**接口及协议**：针对身份管理互操作以及身份管理系统等的交互接口及协议进行规范；

5）**安全机制及身份信息管理**：针对身份管理中的安全技术及安全机制以及个人身份信息管理进行规范；

6）**互操作规范**：对身份管理中涉及的数据模型和接口、身份管理框架及结构、安全技术与机制以及基于身份的 Web 服务之间的互操作进行统一规范；

7）**开发及应用规范**：针对身份管理相关的互联网应用、社交服务的开发等进行规范。

截至目前，我国在集成应用与身份管理方面的标准研制情况如附录 A.5 所示，主要针对可信身份管理框架、身份分级规范开展了相关研究，并发

布了在 PKI 互操作方面的相关标准。

未来重点研制工作：面向电子认证 2.0，我们要加强身份管理和服务的安全性以及互操作性标准的研制，重点研发身份信息管理的隐私保护类标准，身份服务的互联互通标准，包括服务语法、交互协议、以及风险判定标准，身份管理系统的抗风险能力评估标准等。

第七章　电子认证 2.0 发展建议

推动电子认证 2.0 的全面实施，用简单易用的安全认证技术保证身份真实、可靠，解决普通百姓因网络安全意识薄弱容易遭受网络欺诈的问题；通过在线身份服务的共用共享和安全性的增强，大幅提升个人信息保护能力；利用大数据分析技术强化身份和行为的可追溯，使大部分网络应用无需登记实名，在一定程度上消灭网络身份黑市的存在基础；基于风险控制的身份管理，持续提升身份管理和服务企业自身的服务能力，确保任何单一技术的漏洞不会造成巨大损失。我们期望政、产、学、研、用共同努力，协同推动电子认证 2.0 发展，推进我国网络可信身份战略的制定和实施，让百姓享受安全易用且能保护隐私的电子认证成果。

7.1　推动网络可信身份战略的制定

2016 年发布的《中华人民共和国网络安全法》中明确规定“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认”。我们要以网络安全法为指引，顺应电子认证技术新的发展趋势，研究和推动我国网络可信身份战略，努力建立符合世情、国情，体现国家意志，促进产业发展的可信网络身份管理体制与机制。我们要把握好新形势下电子认证的发展方向和战略，为确立和强化

我国对网络的管辖范围、提升我国管控网络空间的能力、推进网络经济发展、加强网络治理、实现网络强国和经济强国做出贡献。

7.2 鼓励理论创新和技术创新

电子认证是富有创新活力的技术领域，新理论、新技术、新应用层出不穷，对网络空间安全形势和竞争格局的改变起着重要作用。应鼓励科研机构和产业集中攻关，研究先进的身份鉴别、授权和身份管理技术，不断完善基于生物特征识别的身份鉴别技术，提升基于风险控制的多因素身份鉴别系统安全能力，探讨共享共用的身份管理服务业态，研究多模式多安全等级的电子认证新技术等，并采用先进的管理技术推进落实实名制要求，减少甚至不在公共互联网上存储个人信息，为我国网络可信身份战略做好科技创新支撑。

7.3 推动身份服务产业生态的形成

鼓励电子认证服务企业、研究机构以及相关事业单位加强合作，促进网络可信身份管理和服务的创新和升级，促进网络可信身份服务产业生态的形成，不断提升我国网络可信身份管理技术和服务能力。促进电子认证服务产业内部各企业在技术、产品、服务、应用等方面的合作，推进企业间电子认证的互联互通，促进企业间资源的共享，打破不同企业间相互孤立的局面，提升产业群体竞争力。加强政、企、研的合作，强化标准规范的评估评价体系建设，推进行业发展进步和市场共识的形成，推动技术、标准、服务及评估评价等各个环节的共同进步。

基于“互联网+政务服务”统一身份认证、统一电子印章、电子证照共享等迫切需求，通过整合政府和互联网身份认证资源，由国家主导，联合社会力量，构建互联网身份认证服务体系，在电子政务网络上开展示范应用，向社会提供可控、可管、权威的身份管理和身份认证服务。以此为抓手，带动国家网络可信身份生态体系的建立。

7.4 鼓励企业采用新技术新模式积极参与实践

鼓励网络服务和应用企业积极参与网络可信身份实践，适应电子认证新技术、新模式的发展。鼓励现有国有大企业、大型事业单位、通信运营商、电子认证企业等充分利用其管理的用户资源，积极参与在线身份管理服务市场开发。政府部门和国有企业，在有条件的情况下要购买和使用具备安全能力的优秀身份服务企业的身份管理服务，更好地实现先进的身份服务技术的应用推广。鼓励电子商务、文化娱乐等企业接受第三方提供的身份服务，支持互联登录。

7.5 推进鉴别与授权标准体系建设

针对上网人员、联网设备、网络数据、网络服务和应用，应建立和完善相关鉴别与授权技术标准体系，加快相关标准的统筹与实施，加快推动安全的基于生物特征识别的身份鉴别标准、基于行为和风险控制的身份鉴别方法标准、具备隐私保护身份管理和服务标准以及相关的互联互通标准等的研制，加快建立与《网络安全法》实施相配套的，引导我国身份服务产业创新发展的标准体系。

附录 A 已发布及在研国家标准清单

A.1 标识类标准

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 网站可信标识技术指南（GB/T 35287-2017）	已发布	服务标识

A.2 验证与证明类标准

A.2.1 凭证语法与格式类

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 公钥基础设施 桥 CA 体系证书分级规范（GB/T 29767-2013）	已发布	凭证语法与格式
2.	信息安全技术 公钥基础设施 数字证书策略分类分级规范（GB/T 31508-2015）	已发布	
3.	信息安全技术 数字证书代理认证路径构造和代理验证规范（GB/T 29243-2012）	已发布	
4.	信息安全技术 公钥基础设施 证书策略与认证业务声明框架（GB/T 26855-2011）	已发布	
5.	信息安全技术 公钥基础设施 数字证书格式（GB/T 20518-2006，正在修订中）	已发布	
6.	信息技术 安全技术 公钥基础设施 证书管理协议（GB/T 19714-2005）	已发布	
7.	信息技术 安全技术 公钥基础设施 在线证书状态协	已发布	

	议（GB/T 19713-2005）		
8.	信息安全技术 公民网络电子身份标识格式规范（20120532-T-469）	在研	

A.2.2 验证与证明机制与方法类

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 公钥基础设施 签名生成应用程序的安全要求（GB/T 25065-2010）	已发布	验证与证明机制与方法
2.	信息安全技术 公钥基础设施 电子签名格式规范（GB/T 25064-2010）	已发布	
3.	信息安全技术 公钥基础设施 XML 数字签名语法与处理规范（GB/T 25061-2010）	已发布	
4.	信息技术 安全技术 带附录的数字签名 第 1 部分:概述（GB/T 17902.1-1999）	已发布	
5.	信息技术 安全技术 带附录的数字签名 第 2 部分：基于身份的机制（GB/T 17902.2-2005）	已发布	
6.	信息技术 安全技术 带附录的数字签名 第 3 部分：基于证书的机制（GB/T 17902.3-2005）	已发布	
7.	信息技术 安全技术 带消息恢复的数字签名方案（GB 15851-1995，修订中）	已发布	
8.	信息技术 安全技术 抗抵赖 第 1 部分： 概述（GB/T 17903.1-2008）	已发布	
9.	信息技术 安全技术 抗抵赖 第 2 部分： 采用对称技术的机制（GB/T 17903.2-2008）	已发布	
10.	信息技术 安全技术 抗抵赖 第 3 部分： 采用非对称技术的机制（GB/T 17903.3-2008）	已发布	
11.	信息安全技术 公钥基础设施 特定权限管理中心技术规范（GB/T 20519-2006）	已发布	

12.	信息安全技术 基于数字证书的可靠电子签名生成及验证技术要求（GB/T 35285-2017）	已发布	
13.	信息安全技术 数字签名应用安全证明获取方法（20111616-T-469）	在研	
14.	信息安全技术 移动签名通用技术规范（20120543-T-469）	在研	
15.	信息技术 安全技术 匿名签名服务第 1 部分：总则（20141157-T-469）	在研	
16.	信息安全技术 匿名签名服务 第 2 部分：采用群组公钥的机制（20173855-T-469）	在研	
17.	基于 SM2 的证书撤销列表格式（20151828-T-469）	在研	
18.	信息安全技术 公民网络电子身份标识安全技术要求第 1 部分：读写机具安全技术要求（20152009-T-469）	在研	
19.	信息安全技术 公民网络电子身份标识安全技术要求第 2 部分：载体安全技术要求（20152008-T-469）	在研	
20.	信息安全技术 公民网络电子身份标识安全技术要求第 3 部分：验证服务协议（20151829-T-469）	在研	

A.2.3 凭证颁发安全技术要求

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求（GB/T 21053-2007）	已发布	凭证颁发安全技术要求
2.	信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则（GB/T 21054-2007）	已发布	
3.	信息安全技术 鉴别与授权 认证中间件框架与接口规范（GB/T 30275-2013）	已发布	
4.	信息技术 开放系统互连 目录 第 8 部分：公钥和属性	已发布	

	证书框架（GB/T 16264.8-2005）		
5.	信息安全技术 公钥基础设施 时间戳规范（GB/T 20520-2006）	已发布	
6.	信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范（GB/T 32213-2015）	已发布	
7.	信息安全技术 公钥基础设施 标准一致性测试评价指南（GB/T 30272-2013）	已发布	
8.	信息安全技术 时间戳策略和时间戳业务操作规则（20111613-T-469）	在研	
9.	基于多用途互联网邮件扩展（MIME）的安全报文交换（GB/Z 19717-2005）	已发布	

A.3 鉴别类标准

A.3.1 鉴别机制类

序号	名称/标准号/计划号	当前状态	类别
1.	信息技术 安全技术 实体鉴别 第 1 部分：概述（GB/T 15843.1-2017）	已发布	鉴别机制
2.	信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制（GB/T 15843.2-2017）	已发布	
3.	信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制（GB/T 15843.3-2008）	已发布	
4.	信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制（补篇）（GB/T 15843.3-2016）	已发布	
5.	信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的机制（GB/T 15843.4-2008）	已发布	
6.	信息技术 安全技术 实体鉴别 第 5 部分：使用零知识技术的机制（GB/T 15843.5-2005）	已发布	

7.	信息技术 安全技术 实体鉴别 第 6 部分 采用人工数据传递的机制（20160648-T-469）	在研	
8.	引入可信第三方的实体鉴别及接入架构规范（GB/T 28455-2012）	已发布	
9.	信息技术 安全技术 匿名实体鉴别 第 1 部分 总则（GB/T 34953.1-2017）	已发布	
10.	信息安全技术 匿名实体鉴别 第 2 部分：基于群组公钥签名的机制（20130349-T-469）	在研	
11.	信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制（20170562-T-469）	在研	
12.	信息技术 安全技术 可鉴别的加密机制(20170580-T-469）	在研	
13.	信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制（GB/T 15852.1-2008）	已发布	
14.	信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制（GB/T 15852.2-2008）	已发布	
15.	信息技术 安全技术 消息鉴别码 第 3 部分 采用泛杂凑函数的机制（20170564-T-469）	在研	

A.3.2 基于生物特征识别的鉴别框架与协议类

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架（20170565-T-469）	在研	鉴别框架与协议
2.	信息安全技术 基于生物特征识别的移动终端身份鉴别技术框架（20173598-T-469）	在研	鉴别框架与协议

A.3.3 基于生物特征识别的系统安全技术要求类

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 人脸识别认证系统安全技术要求（20160783-T-469）	在研	系统实现与安全要求
2.	信息安全技术 虹膜识别系统技术要求（20160781-T-469）	标准修订-在研	
3.	信息安全技术 指纹识别系统技术要求（20111598-T-469）	在研	
4.	手指静脉技术安全规范	标准研究-在研	

A.4 授权类标准

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 轻量级鉴别与访问控制机制（20130328-T-469）	在研	授权机制
2.	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范（GB/T 25062-2010）	已发布	
3.	信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言（GB/T 30280-2013）	已发布	系统实现与安全要求
4.	信息安全技术 鉴别与授权 安全断言标记语言（GB/T 29242-2012）	已发布	
5.	信息安全技术 鉴别与授权 可扩展访问控制标记语言（GB/T 30281-2013）	已发布	
6.	信息安全技术 鉴别与授权 授权应用程序判定接口规范（GB/T 31501-2015）	已发布	
7.	信息技术 安全技术 校验字符系统（GB/T 17710-	已发布	

	2008）		
8.	信息安全技术 鉴别与授权 访问控制中间件框架与接口（20120529-T-469）	在研	

A.5 集成应用与身份管理类标准

序号	名称/标准号/计划号	当前状态	类别
1.	信息安全技术 网络可信身份分级规范	标准研究-结题	概述类
2.	信息安全技术 鉴别与授权 数字身份信息服务框架规范（GB/T 31504-2015）	已发布	身份管理框架及结构
3.	信息安全技术 鉴别与授权 可信身份管理框架规范	标准研究-结题	
4.	信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范（GB/T 19771-2005）	已发布	互操作规范
5.	信息安全技术 公钥基础设施 PKI 互操作性评估准则（GB/T 29241-2012）	已发布	