面向城市数字化转型的数字信任体系建设

Building Digital Trust System for City Digital Transformation

上海市数字证书认证中心有限公司

SICSI CYBER RESEARCH INSTITUTE 赛博研究院

— 版权声明 —

COPYRIGHT STATEMENT

出品方

上海市数字证书认证中心有限公司

上海赛博网络安全产业创新研究院

编写组

崔久强	上海市数字证书认证中心有限公司总经理
郑　宁	上海市数字证书认证中心有限公司行业研究员
惠志斌	上海社会科学院互联网研究中心主任、研究员 上海赛博网络安全产业创新研究院首席研究员
石英村	上海赛博网络安全产业创新研究院研究员

咨询专家

周亚超	安恒信息（上海）首席科学家、工程师
朱易翔	第五空间研究院理事长、翼盾（上海）智能科技有限公司 CEO

FOREWORD | 前言

当前，新一轮科技革命和产业变革深入发展，经济生产、政府治理、公共服务、人民生活等各领域的数字化转型全面开启，“泛在网络实体互联、异构数据实时流通、智能应用层叠涌现”的万物智联世界加速形成，人与人、人与物、物与物之间全面依托数字化方式交互的各类经济和社会活动的信任关系和模式面临数字化重塑。日益严峻的网络安全风险挑战对经济社会信任体系带来深刻挑战，如何构建面向数字化转型的新型数字信任体系是网络安全的核心使命。

基于上述背景和目标，本报告分析了信任、网络信任、数字信任等概念的源起和特点，提出数字信任的概念内涵、核心特征和主要意义，并对主要国家的数字信任相关的法律政策、前沿技术进行梳理。在此基础上，报告提出以可信数字身份验证识别和可信数据流通为核心，针对新型网络安全风险和数字治理难题，以身份信任、算法信任、数据信任、能力信任、规则信任五大愿景为建设目标，包括制度标准、技术创新、产业生态等多维度的数字信任体系框架，以及重点场景的数字信任技术解决方案，为我国城市数字化转型和数字中国建设提供参考和帮助。

CORE IDEA | 核心观点

● 信任关系受到行为主体、社会关系和安全风险三种因素的影响。数字时代的到来使得这三种约束条件都发生了颠覆性变化，传统的人际信任、制度信任必然演变为数字技术深度内嵌的新型数字信任。

● 数字信任是指一切链入 / 映射到数字空间的泛在网络实体，基于数字身份识别、可信数据流通和网络安全能力验证形成的正向预期，以及由此产生稳定数字交互关系的活动。

● 数字信任体系是网络安全体系建设的高级形态，是以可信数字身份验证和可信数据流通为核心，聚焦新型网络安全风险和数字治理难题，通过制度标准、技术创新、产业生态等多维度建设，最终实现身份信任、数据信任、算法信任、能力信任、规则信任等五大建设目标的数字时代信任治理模式。

● 泛在网络实体之间构建数字信任关系通常需要“建立数字身份 - 形成交互规则 - 明确安全能力 - 实现识别验证 - 持续正向反馈”五个步骤，数字信任建设者能够为信任的每个环节提供支撑和服务，在数字信任体系建设中发挥着重要作用。

● 数字信任的实践高度依赖于数字身份、PKI 架构、隐私计算、人工智能、区块链等各种数字技术的创新和应用。随着数字化转型发展，数字信任解决方案将在电子政务、数据流通、物联网、金融科技、在线医疗等领域有着广泛的应用前景。

CONTENTS | 目录

CONTENTS | 目录

PART 1
从信任到数字信任

一 | 信任的概念及内涵

信任（Trust）理论的研究是一个多学科交叉综合的复杂议题。最早的信任理论是在哲学和政治学领域作为道德和政治关系的组成，20 世纪以来，信任被各国学者广泛引入到社会学、经济学、心理学、博弈论和国际关系等多个学科中，形成不同范式的信任理论模型并在政府的公共治理实践和企业的市场商业行为中大量应用。

在社会学领域，信任被理解为一种社会运作的高级机制和共同体内部关系的成熟状态，比如 19 世纪现代社会学创始人之一韦伯（Max Weber）将信任分为普遍信任和特殊信任，其中普遍信任主要集中在既定的权威规范（法理、契约）范围，而特殊信任则主要建立在共同的亲缘和宗族等基础之上。德国社会学家卢曼（Niklas Luhmann）认为信任是人类简化复杂性生存策略的机制之一，即信任是为了简化人与人之间的合作关系。**在经济学领域，信任被认为是市场经济重要的润滑剂，是企业在与消费者交互时追求的理想关系。**美国经济学家阿罗（Kenneth Joseph Arrow）认为信任是市场经济非常重要的组成部分，将信任视为市场经济的润滑剂，是企业很难买到的一种独特的商品。**在政治学领域，信任被认为是国家发展和政府统治的重要积极因素**，日本政治学家福山（Francis Fukuyama）认为建立在宗教、传统、历史习惯等文化机制之上的信任程度构成一个国家的社会资本，一个国家的信任度高低直接影响企业的规模，进而影响该国在全球经济中的竞争力。20 世纪著名思想家哈贝马斯（Jürgen Habermas）更是明确指出，“一个统治制度的合法性，是以被统治者对合法性的信任为尺度的，包括对于国家制度、官僚、道德和治理方式的普遍信任。**在心理学领域，信任被理解为个体心理与外界环境持续正向互动后的一种情绪**，美国社会心理学家罗素 (Denise M.Rousseau) 认为，信任是个体建立在对另一方意图和行为的正向估计基础之上的不设防的心理状态。尽管在不同专业中信任的理论和模型存在相当大的差异甚至冲突，但总体而言，各学科的信任理论仍具备以下的基本共识：

- **信任是一种多主体之间的双向关系。**无论是公民个体，还是政府、企业或是其他组织，信任一定是在具备决策、选择和行为能力的社会主体之间形成的双向关系。
- **信任的构建是一个持续正向反馈的动态过程。**主体间信任的并不是凭空存在的，而是一个双方通过预期、行为和反馈等多个环节交互的持续性构建过程。
- **信任存在的约束条件是社会依存关系和风险。**人类社会普遍存在的依存关系使得每个社会主体都无法单独存在，必须与其他主体保持联系和分工，而风险的绝对存在使得这种依存关系面临各种复杂不确定的挑战，信任的价值和意义正是为了控制和承担风险，减少风险对于社会依存关系的破坏以及交互成本的增加。
- **信任的成立和维护需要一定的机制和成本。**无论是社会性信任，还是人际信任，信任的成立和维护都需要相对稳定的社会机制以及成本付出。包括基于心理和情感的信任，基于理性认知和计算博弈的信任，基于社会性权威（法律、契约）和道德规范的信任等。
- **信任关系能够带来边际递增的效益和价值。**在大量的政治学、经济学和社会学研究中，信任都具备重要的社会性价值。包括在市场经济中降低双方交易和分工的成本，在新技术发展和普及中减少怀疑和抵制，在政府治理中提高政策的理解度和执行力等。

二 | 数字信任的源起及定义

根据信任理论共识，信任关系会受到行为主体、社会依存关系和安全风险的影响。因此，当人类文明进入以数字技术和数字经济为基础的数字文明时代时，这三种约束条件都发生了颠覆性变化，传统社会的信任关系必然演变为新特点、新内涵的数字信任（Digital Trust）关系。

表 1：人类文明形态发展下的信任关系演变

	农业文明	工业文明	数字文明
主要信任模式	人际信任：基于人际关系构建的信任关系，具备较强的情感性，信任传递性较低	制度信任：基于政府监管和市场契约形成的信任关系，稳定性较强，信任传递性有限	数字信任：基于数字技术在虚拟数字空间形成的信任关系，高度依赖于数字技术和数字应用
行为主体类型	社会个体	企业、各种社会组织	企业、各种社会组织 所有链接 / 映射到数字空间的组织、人和物
信息沟通机制	通过熟人关系网络（宗族、村落）和书信进行信息传递	通过印刷术、电报、电话进行信息传递	通过互联网、移动设备进行信息传递
社会依存关系	依自给自足的农业生产为主，商业化水平、社会分工和依存度整体较低	以社会化工业生产为主，依靠高商业化水平下和发达市场经济形成社会化分工，社会依存关系较高	依靠互联网平台企业和跨国互联网公司形成了基于数字经济的精细化社会分工，社会依存关系极高
社会主要风险	以重大自然灾害、战争、瘟疫、社会动乱为主，带有典型的不可抗力	除了不可抗力风险外，因人类活动对自然深度介入产生的环境污染、生态破坏影响巨大，还包括犯罪、工程灾害等	实体世界与数字世界的风险深度交织泛化，高频网络攻击、数据泄露、数据滥用、隐私侵害等网络安全风险对整体社会影响越来越大

从上表可以看出，随着以 5G、物联网等为代表的新型数字基础设施的大规模普及，数据日益成为信息知识传递的主要载体和核心生产要素，数字产业化和产业数字化深度发展，政府治理、公共服务、人民生活各个领域都在加快数字化转型，数字时代的到来使得信任关系产生和维系的社会情境发生了根本性变化。

在行为主体上，以政府、企业 / 其他组织和公民个体的人类网络实体，和以智能终端 / 设备（包括各种传感器节点）、算法程序（包括各种

在线应用）为代表的机器网络实体共同链接在一个广泛的数字空间中。**从关系上看**，政府和企业通过数字化转型形成了高度相关的大规模社会化的协作和分工关系，基于数字技术进行的海量信息流动规模庞大且已经成为人类沟通的主要方式。**从风险上看**，常态化的高能网络攻击、数据泄露滥用等网络安全风险对人类社会的外溢影响日益深刻，已经上升到国家安全的高度。

在此背景下，“网络信任（Internet trust）”和“数字信任（Digital Trust）”概念迅速成为最前沿的研究方向，各国研究机构、咨询公司和专业学者基于此开展了一系列研究。

在互联网发展的初期，政府、企业和公民个体通过数字身份链入到网络空间中，并通过互联网进行信息交互和经济互动，以身份欺诈、虚假账号、网络攻击和虚假信息内容为主要特征的网络安全风险开始影响正常的网络互动。因此各国政府和研究者普遍采用网络信任或者可信的表述，主要内容聚焦在电子商务领域的公民 / 法人身份认证、电子合同、在线支付等商业风险的规制，以及在网络新媒体环境下政府、企业和媒体在信息传播领域的信任建设，核心特征是传统信任体系在网络空间的映射和适用。比如我国在 2006 年 2 月国务院办公厅转发的《关于网络信任体系建设的若干意见》中，将网络信任体系定义为“是以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系”。

随着新一轮数字化转型浪潮开启，外延更大的数字信任逐步覆盖了网络信任概念。2017 年 Gartner 在《数字信任 - 重新定义数字时代的信任》（Digital Trust — Redefining Trust for the Digital Era: A Gartner Trend Insight Report）报告中认为，“数字信任是传统信任模型的演变，它通过得出可测度的高水平信任来做出基于风险的决策，从而支撑了（主体）数字业务的所有要求。”普华永道（PWC）在《2019 年数字信任洞察之中国报告》认为，“科技企业发展和传统企业数字化转型的关键要点在于要使网络安全规划与业务发展目标相匹配，共同构建数字信任。”美国知名科技公司 TechTarget 认为，“数字信任是用户对人类、技术和制度共同创建安全数字世界能力的信心，企业和组织通过向用户表明他们可以确保在线程序或设备的安全性、隐私性、可靠性和数据道德性来获取用户的数字信任。”2020 年 3 月美国网络安全公司 SUBEX 在研究报告中，将数字信任定义为“一种使用户能够以安全、合乎道德和可靠的方式进行业务交易的概念。”并认为数字信任必须包括“隐私、安全性、数字身份、可预测性、缓解风险、数据完整性”等六个方面。

本报告在各学科信任理论共识的基础上，基于网络安全学科视域将数字信任（Digital Trust）定义为：**指一切链入 / 映射到数字空间的网络实体，基于数字身份识别、可信数据流通和网络安全能力验证形成的正向预期，以及由此产生稳定数字交互关系的活动。**

其中，**数字身份（Digital Identification）是数字信任的基本内核，数字信任是数字身份的拓展延伸。**身份是行为主体背后的职业、能力、责任、义务等信息交叉凝结后，形成的代表其在社会关系网络结构中节点位置的表征，对身份的识别和验证在传统社会就是建立信任关系的基础。在数字时代，行为体必须通过数字身份这一代理方式链入数字空间，使得数字身份对于数字信任更加关键和重要。2019 年 4 月麦肯锡在《数字身份：包容性增长的关键》（Digital Identification: A Key to Inclusive Growth）报告中将数字身份定义为“指可以通过数字通道进行远程身份识别、验证的一个系统过程和标识体系，包括政府、公共部门、企业、非盈利组织或个人实体颁发的，基于数字签名、口令、生物特征数据、密码、二维码、嵌入身份信息的智能设备、安全令牌等任何数字技术的数字化身份。”本报告将数字身份定义为任何链入 / 映射到数字空间的网络实体的可识别、可验证、具

备系统唯一性的标识体系，它是在数字空间辨识不同网络实体身份和行为的基础，也是构建数字信任关系的基石。

可信数据流通是数字信任的必要条件，数字信任是可信数据流通的必然要求。数字时代，数据成为信息沟通和知识交流的主要载体，隐私保护和数据安全则成为行为体数字交互时最主要的担忧。2020 年 11 月，德国马歇尔基金会（GMF）发布《数字民主理念》（Ideas for Digital Democracy）报告认为，缺乏对隐私保护的信任将会破坏数字技术为改善人们生活而做出的承诺，必须通过隐私规则和问责制来实现人民对技术的数字信任。因此，通过密码学、区块链、隐私计算等技术实现数据在不同数字环境下的可信任流通，并通过完备的数据安全法律标准体系来规制数据的开放、流通、利用等全链条活动，是构建数字信任关系最关键的必要条件。

网络安全能力是数字信任的重要关切，数字信任是网络安全能力建设的高级形态。数字时代，高频复杂的网络安全攻击已经成为数字空间的常态。随着新型技术设施的大规模部署建设，实体社会在数字空间的暴露面极速扩大。因此，对于行为体是否具备抵御网络攻击和确保数据、隐私安全的能力，成为双方成功实现数字信任的重要关切。另一方面，随着“泛在网络实体互联、异构数据实时流通、智能应用层叠涌现”的虚拟数字孪生空间加速形成，大量的数字交互关系必须在网络边界日趋模糊、通用信任机制普遍缺失的环境进行，数字化活动的风险投入和交易成本大幅上升，行为体不仅要投入高额的安全成本以及进行复杂的安全流程管控，还要面临投入边际产出低、效果不明显问题，因此，数字信任可以通过对不同行为体网络安全能力的测量和验证，以实现更加快捷、低成本的访问控制和交互认证，从而提高行为体网络安全投入的正向收益。数字信任必将成为未来网络安全能力建设的发展方向。

三 | 数字信任的核心特征

1. 数字信任主体包括复杂多元的各种泛在网络实体

移动互联网和物联网的发展使得网络实体的类型和数量爆发式增长，以智能终端 / 设备（包括各种传感器节点）、算法程序（包括各种在线应用）和数据为代表的机器网络实体已经远远超过以政府、企业 / 组织和公民个体的人类网络实体数量。比如智能设备，根据权威市场统计公司 Statista 的数据，2020 年底全球物联网设备数量将超过 307.3 亿台。在算法程序上，我国工信部统计数据显示到 2019 年底全国可在线下载的手机 APP 数量接近 449 万，同年度美国谷歌和苹果商城上也有近 350 万和 210 万个应用。在数据领域，根据国际数据公司（IDC）的报告，2018 年全球数据量达到 33ZB，预计 2025 年将达到 175ZB。可以说，**随着未来物联网和人工智能技术的快速发展，数字信任主体将极大拓展到各种机器网络实体，而非传统实体信任关系中的单一人类主体。**

2. 数字信任议题聚焦网络安全风险和数字治理难题

在数字化转型的大背景下，社会风险相较于传统工业社会发生了重大转变。传统社会信任所关注的风险主要在于商业契约执行、虚假内容宣传、恶意市场行为、违法犯罪活动以及不可控的自然灾害等。而数字空间普遍存在的网络攻击、网络犯罪和黑灰产，以及近年来数据泄露、滥用事件的高频爆发，使得网络安全和数据安全成为

现代数字社会的重要风险。波耐蒙研究所（Ponemon Institute）发布的《2020 数据泄露事件损失报告》揭示，2020 年平均每起数据安全事件对企业造成的损失高达 386 万美元，且大部分原因在于恶意攻击导致的访问身份凭证被盗。因此，**能否有效抵御网络攻击、保障系统和数据安全、保护用户隐私，成为数字信任关注的主要问题。**

另一方面，随着教育、养老、医疗、交通等各类公共服务数字化转型加速深化，越来越多的社会机遇和公共福利以数字化方式提供，信息弱势群体面临的数字鸿沟问题更加凸显。借助安全可信、弹性扩展的数字身份服务能力，为各类人群提供便捷的身份服务，能够降低老人、残疾人等群体在数字接入上的技能要求和流程成本，减少因数字身份欺诈、多次重复认证产生的安全风险，更好地分享城市数字化转型发展的红利。

3. 数字信任实践具有高度技术依赖性和场景差异性

相较于传统信任关系对于社会制度、经验知识和个体情感等因素的依赖，数字信任的构建更强调技术。一方面，数字信任的构建极大依赖于数字身份、密码学、隐私计算等安全技术的创新发展。另一方面，以人工智能、物联网、区块链和量子计算等为代表的数字技术仍在不断创新发展的进程中，将会重塑未来数字空间的规则和风险，因此数字信任体系必须确保对新兴数字发展的兼容性和敏捷性。同时，数字信任也是高度场景化的关系，数字时代的交互关系类型既包括传统的人与人、人与组织之间的关系，也包括人与物联设备、人与机器算法的交互。不同场景下的交互关系和规则差异性极大，因此高度场景化的数字信任并不具备通用的传导性，需要特殊的“信任通道”机制来实现数字信任的跨域传递。

四 | 数字信任关系的建立

1. 多主体类型的数字信任关系

传统网络信任模型中，信任主体主要包括政府及公共部门、企业 / 其他组织、个体用户三大类，他们通过数字身份链入数字空间中，并基于身份认证和规则在数字交互中形成信任。而在数字化转型进程中，行为主体普遍出现了大量数字代理情况，即政府和企业掌握的 IoT 设备、算法程序、数据甚至是各种终端接口和传感器成为网络实体，并在数字空间中运行，这类网络实体同样需要“数字身份”来确保其可验证和可信任。

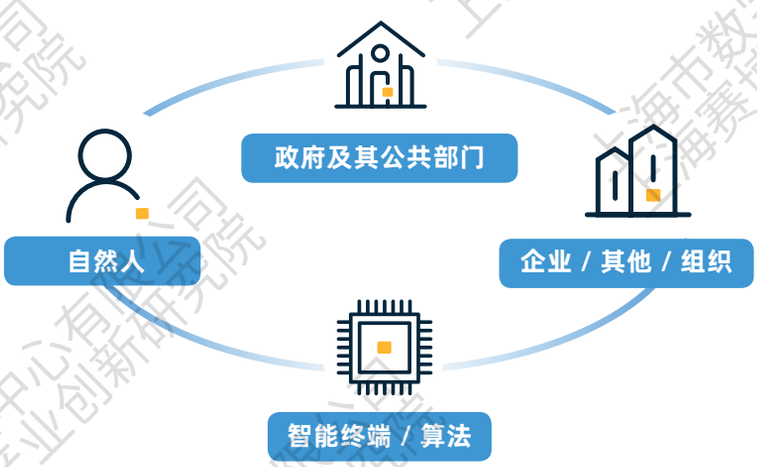

图 1：多主体类型的数字信任关系

- **“政府及公共部门 - 企业 / 其他组织”的数字信任关系：**主要表现为政府对企业落实相关法律政策规定的信任，包括对企业在电子认证、数字签名、网络安全、隐私保护、供应链安全等各领域合规性的信任。企业 / 其他组织对于政府及公共部门的数字信任，主要表现为能够形成对政府在数字监管领域法律、政策制定和执法过程的公正、透明上的稳定预期，包括政府在网络安全和数据安全领域的法律制定情况、执法数据调取等。

● **“政府及公共部门 - 自然人”的数字信任关系：**主要表现为政府及公共部门对于个体用户数字身份与现实身份关联的真实性和有效性。而个体对于政府的数字信任，则更多是对于政府数字监管和数字公共服务的认同和理解，包括政府对其个人信息的采集是否合理合法、以及对其个人信息是否存在滥用等问题。

● **“企业 / 其他组织 - 个体用户”的数字信任关系：**主要表现为个体用户对于企业数字产品和服务的信任，以及对企业网络安全和隐私保护能力的信任。

● **“人 - 机交互和机器交互”的数字信任关系：**在物联网和人工智能场景中，会产生大量 IoT 设备、算法程序、数据以及终端接口和传感器机器等机器网络实体之间的数字交互或机器网络实体与人类网络实体之间的数字交互。“人 - 机”与“机 - 机”之间的数字信任可能极大地依赖于自动化技术进行的身份识别和认证。

2. 数字信任建设者和数字信任关系建立

由于数字空间的虚拟性，复杂的技术和规则门槛使得数字信任必须要通过第三方来实现。同时，在随着以 IoT 设备、算法程序和数据等非人类网络实体大量进入数字代理和数字业务领域，同样需要提供可信支撑服务的专业第三方来深度支撑各类主体的数字信任关系。2019 年 11 月，全球著名科技媒体哈佛商业评论（Harvard Business Review）在《数字信任的四大维度：覆盖 42 个国家 / 地区的数字信任图表》（The 4 Dimensions of Digital Trust,Charted Across 42 Countries）报告中提出“信任担保人（Trust Guarantors）”概念，认为**“信任担保人能提供广泛的信任支撑机制，来解决政府、企业和消费者在网络空间的信任问题。”**

本报告将所有为数字信任关系提供支撑服务的主体定义为“数字信任建设者（Digital Trust Builder）”，包括提供数字空间链入设施的电信运营商，提供数字身份管理和认证的权威机构，提供网络安全和数据安全技术和服务的网络安全厂商，提供网络安全产品和能力认证的测评认证机构，提供数字规则咨询和合规的专业法律机构，提供网络安全保险和风控的金融机构等等。数字信任建设者作为第三方参与到各种网络实体的数字信任关系中，能够有效地降低信任关系构建的成本，提供更为权威和专业的第三方信任服务，帮助网络实体构建数字信任关系。

2020 年 2 月，法国国家网络安全局（ANSSI）发布了《控制数字风险—信任优势》（Controlling digital risk —Trust advantage）报告，为组织管理者和风险管理者提供了包括 11 个步骤的数字信任构建和风险管理策略。本报告在上述研究的基础上，构建了微观层面上网络实体建立数字信任的过程，主要包括以下步骤：

● **建立数字身份：**即网络实体通过电子验证、数字签名等技术建立并维护数字身份，以实现数字链接。同时确保数字身份的可验证和安全性，以及识别物理实体的唯一性（即每个数字身份标识只能识别到唯一实体）。

● **形成交互规则：**即网络实体对于数字交互的场景或系统所必须遵守的法律、法规、标准、商业契约和技术逻辑上形成共同的认知和理解，以确保双方对于数字信任过程中遵守一致的规则。

● **明确安全能力：**安全能力是网络实体在数字空间中控制和规避风险的能力。即网络实体通过一系列安全制度建设、技术研发和产品服务采购，确保自身能够抵御网络攻击、保证数据安全和用户隐私以及维持系统和业务连续性，可以通过一系列指标进行测度甚至量化。

● **实现识别验证：**即网络实体对双方数字身份的真实性、安全能力以及遵守数字规则的意愿进行充分地信息共享和验证，以确保对方是其声称的

代理身份，能够合法、完全地代表数字身份所标识的实体，并有能力在遵守规则的前提下参与数字业务交互。

● **持续正向反馈：**即网络实体在特定场景下的数字业务交互中，对对方和环境的数字信任产生的持续性正向反馈，能够使得参与交互的实体能够形成对对方信任的认知和经验。必须看到的是，即使在进行充分的网络安全部署和可信能力建设的情况下，网络实体仍旧可能面临网络安全的各种不可预期的风险。因此，正向反馈的一个重要内容是网络实体在网络安全事件爆发后的应对情况，包括能否及时响应并采取补救措施，能否在最大限度上减少损失，以及是否通过保险等方式进行风险控制或者对冲。

在上述构建数字信任关系的五个步骤中，数字信任建设者都将会深度参与并提供专业的支撑服务（详见下表 2）。

表 2：数字信任建设者在不同环节提供的信任支撑

环节	数字信任建设者类别	信任产品 / 服务
数字身份	数字身份和电子认证的第三方服务机构（如 CA 中心等）	身份标识 、身份验证与证明、身份鉴别与授权、电子签名秘钥发布和统一管理等
交互规则	电子认证第三方服务机构、律师事务所、法律咨询机构	电子合同、电子签名、隐私计算、可信环境、网络安全合规咨询等
安全能力	网络安全厂商、电子认证第三方服务	访问权限控制、漏洞监测、风险监测、态势感知、安全运营等
识别验证	测评认证机构、电子认证第三方服务、网络安全厂商	身份验证、电子认证、反渗透测试、网络安全评级认定、数据安全能力测评、网络安全的可信度测量和尽职调查等
正向反馈	网络安全厂商、网络安全保险公司、风控金融机构	网络安全事件的响应和救济，网络安全损失的控制和理赔等

五 | 数字信任的重大意义

数字信任已经成为数字化转型的重要议程。在数字技术发展和数字经济变革的背景下，政府和企业的数字化转型将长时间处于持续发展状态，随着底层技术逻辑和外部风险环境的变化，数字信任成为整体数字化转型规划中必须思考的重要议程。在国家层面上，政府必须要整体思考数字化转型中可能产生的各种非传统安全风险和治理问题，包括数字技术应用带来的公共安全风险、数字技术对社会伦理道德产生的冲击和颠覆、数字经济业态创新带来的治理监管挑战、数字鸿沟带来的地域 / 人群分化等等。构建数字信任体系，不仅能够使国家很好地适应当下激增的网络安全和数据安全问题，也能够充分发挥信任的社会功能和经济功能，实现国家和社会整体的数字化转型。在企业层面上，无论是为了更好地应对政府和公众对于其数据开发和技术创新的担忧和质疑，还是在数字经济市场上形成具备差异化优势的品牌竞争力，企业都必须将数字信任纳入到数字化转型规划的重点议题中。

1. 数字信任是数字经济良性发展的关键机制

经济学信任理论中，信任是良好、成熟的市场经济发展所必须具备的重要机制组成，对于构建优质的营商环境和稳定的市场秩序具有重大意义。在数字经济时代，数字信任的经济功能将继续放大。

微观层面上，**数字信任已经成为科技企业发展和传统企业数字化转型的关键。**普华永道2019年的市场分析数据显示，消费者对于信息类产品以及科技企业的数字信任，已经成为他们下载应用和购买产品/服务的核心影响因素。近21%的消费者表示，他们对于企业及其产品/服务在网络安全和数据安全方面的关注，已经超过了对产品/服务价格和质量的关注。Gartner的研究报告显示，具备高数字信任度的企业在品牌影响力和市场竞争力具备明显的差异化优势。

在宏观层面上，**数字信任成为支撑数字经济高质量发展的重要机制环境。**数字经济发展必然要求数据要素的便利、高效化流通以及最大化分析利用，但是，数据确权定价不清晰、数据流通来源和链条复杂且难以溯源、数据滥用和泄露风险依然严峻等数据治理和安全问题，使得数据要素在市场化配置上一直举步维艰，加快数字信任在数据流通交易中的服务支撑，能够很好地促进数据要素市场培育，推动数字经济发展。同时，数字经济发展带来了平台经济业态的快速崛起，也产生了数据垄断、大数据杀熟、算法歧视等各种平台数字治理难题。构建“用户-平台-企业”之间稳定的数字信任关系网络，能够极大地降低数字经济活动中的营销成本、交易成本、沟通成本和分工成本，避免因信息不对称导致的过度保护行为，减少市场纠纷和不正当竞争行为，推动数字经济进入良性竞争和稳定发展的状态。

2. 数字信任是数字政府公共治理的底座支撑

政治学和社会学信任理论中，信任是公共治理的重要社会资本。随着政府及公共部门数字化转型的加速，基于数字技术履行政府监管职能和提供公共服务将成为未来公共治理的重要方式，数字信任的治理功能将持续凸显。

在政府数字化转型上，**数字信任是解决政府信息化建设割裂和网络安全问题的重要支撑。**由于政府部门在信息化建设初期的阶段性和分散性，各国的数字政府建设大多都存在内部系统割裂、技术标准不统一、应用重复建设和数据信息沟通不畅等共性问题，导致政府内部的网络安全建设始终存在协调成本过高的困难。因此，随着各国逐步将网络安全纳入到政府数字化转型的统一规划中，打造基于统一数字身份认证和管理，聚焦解决网络安全和数据安全的数字信任体系，将成为各国政府数字化转型的重要政策发力点和有效支撑。

在政府数字治理上，**数字信任是构建政府数字治理合法性的重要组成。**政府数字治理是指政府及其公共部门利用新兴数字技术履行法定职责并提供公共服务的过程。构建“政府-企业”和“政府-公民”之间的数字信任，能够有效提高企业和公民对于国家在数字经济领域的法律、政策的理解认同，使得政府监管和执法过程变得更为顺畅和高效，推动企业和公民获得政府数字化公共服务的平等机会，构建政府数字治理的合法性组成。

3. 数字信任是应对网络安全风险的重要策略

当下，高能复杂的网络攻击已经成为数字空间的常态，无论是政府还是企业都面临着日益严峻的网络安全和数据安全风险，而开展网络安全

工作不仅需要越来越多的资金和人力投入，更是会对数字交互和应用的便捷性和创新产生负面影响。**构建基于数字身份应对网络安全和数据安全的数字信任能够很好地平衡安全与发展的关系。**

一方面，传统基于信息系统边界构建的防护方式越来越难以应对当下的安全挑战，**基于身份认证和访问控制开展网络安全实践越来越成为共识和趋势。**各大科技公司和网络公司在零信任领域的普遍加快布局证明了这一点。零信任通过对数字身份的认证和访问控制，来应对网络边界模糊化带来的权限控制颗粒度粗、有效性差的问题，以此达到保护系统网络安全和数据安全的目的。可以说，**零信任架构是用对身份的信任取代了对边界的信任，是基于数字身份的数字信任体系在新型网络安全风险环境下的理念革新。**

另一方面，未来的数字信任体系能够使得交互双方通过对对方数字身份的认证和识别，获得关于其网络安全能力的信息，并通过数字身份实现持续性的安全信任评估，使得安全产品 / 服务实现更高的集约化，安全防护更加精准化，**降低政府和企业因网络安全工作而对数字业务产生的负面影响。**

4. 数字信任是推动技术创新普及的基础路径

新兴数字技术的发展具有鲜明的“双刃剑”特征，在赋能经济社会发展的同时，也会带来复杂的风险挑战，而政府和公众对于网络犯罪和网络安全风险的担忧、对于新兴技术的迟疑以及对企业保障隐私的怀疑将极大地影响技术创新，构建围绕技术的数字信任关系则能够较好地解决这个问题。Gartner 的研究报告显示，**数字信任能够有效地测度和控制安全风险和隐私问题，高数字信任度的技术的发展将更快地进入技术成熟期，创新和应用成本更低。**

比如对于人工智能技术而言，人工智能决策的“算法黑箱”和“算法歧视”问题被广为讨论，各国在人工智能发展战略和社会倡议上都明确表示“可信性”在人工智能发展的重要性，构建可信人工智能能够减少企业和用户的后顾之忧。在物联网发展中，大量 IoT 设备链入所带来的身份管理、关键基础设施安全、工业互联网安全、供应链等问题也需要数字信任来应对。在数据保护方面，2020 年 11 月德国马歇尔基金会发布《数字民主理念》显示，81%的用户认为对公司收集的个人数据几乎没有控制权，79%的用户担心公司可能不当使用其个人数据，超过一半的美国人（占比约为 52%） 基于隐私的担忧而决定不使用互联网产品或服务，围绕数据的确权、流通、交易、开放和利用中的数据安全和隐私保护问题，数字信任能够很好地解决支撑机制，在区块链和量子计算创新中，同样需要通过加强安全和隐私保护、提高技术逻辑的可解释性和透明度等方式构建数字信任。总之，**基于身份、聚焦安全的数字信任，能够在提高技术创新、普及和应用时发挥“润滑剂”般的作用，增进开发者与用户的信息沟通和共识基础，减少因安全担忧和缺乏理解带来的质疑和阻力。**

5. 数字信任是实现数字包容普惠的有效方式

数字鸿沟是指在全球数字化进程中，不同国家、地区、行业、人群、社区之间，由于对数字技术的拥有程度、应用程度以及创新能力的差别而造成的发展不平衡甚至不平等加剧的趋势。2000 年 7 月，世界经济论坛组织（WEF）在《从全球数字鸿沟到全球数字机遇》（From the Global Digital Divide to the Global Digital Opportunity）报告中认为，信息和网络技术发展带来的“数字鸿沟”已经成为全球不平等的重要因素。

数字信任在实现数字技术普惠式应用、数字经济包容性发展和解决“数字鸿沟”问题上能够发挥极大的作用。2019 年 4 月麦肯锡在《数字身份：包容性增长的关键》报告中认为，数字技术的发展使得越来越多的社会机遇和公共福利被用数字化方式

提供，推广可信任的数字身份能够推动更多落后地区和代际人群分享数字化红利。2020 年 4 月，联合国贸易与发展会议（UNCIAD）在《COVID-19 危机：重视亟需弥合的数字鸿沟》（The COVID-19 Crisis:Accentuating the Need to Bridge Digital Divides）报告中更是明确指出，全球数字化准备程度的巨大差异阻碍了世界上大部分国家利用数字化技术来应对疫情危机的能力，而政府、企业和公众在数据采集和应用开发中的互信度，则是全球数字化准备程度的关键要素之一。总之，无论是对一个国家或地区，还是全球而言，通过打造可信的数字身份体系，应对技术发展的网络安全和数据安全问题，构建各方的数字信任关系，能够确保数字机遇更加便捷、平等地提供给每个社会主体，弥合数字鸿沟。

PART 2
全球数字信任的发展现状及趋势

一 | 主要国家数字信任的法律 / 政策

基于数字身份在数字信任中的核心地位，报告在政策研究中重点聚焦美国、欧盟和中国三个全球最主要经济体对于电子签名、电子身份、电子认证等广义数字身份所包括各类领域的战略和法律。同时，由于网络安全和数据安全是数字信任聚焦的主要风险，报告也将选取其中对数字信任有较大影响法律或政策。

1. 美国

（1）通过“联邦 - 州”法律明确电子签名的效力

1995 年，自美国犹他州出台了全世界范围内第一部《数字签名法》（Utah Digiatl Signature Act）以来，在接下来五年时间内，美国各州纷纷出台了规制电子签名的地方法律或相关政策。**2000 年 6 月，美国联邦层级的《国际与国内商务电子签名法》（The Electronic Signature in Gobal and National Commerce Act, 即“E-Sign Act”）正式生效，法案协调了州法中关于概念和标准的差异，明确赋予了电子签名、电子记录与手写签名、印章等同的法律地位，同时不在电子签名技术上做特定的障碍性条款，确保市场能够自由决定哪种技术最为安全，允许企业自由地构建自己的安全方法与安全程序以从事电子交易，极大地扫除了使用电子技术制定、签署合同，收集和储存文件以及发送通知的法律障碍。**

（2）基于网络安全视域下的联邦可信身份战略

2009 年 5 月，美国白宫发布《网络空间政策评估》（Cyber Space Policy Review）报告，高度强调网络空间的战略地位和美国当前网络安全形势的严峻性。报告同时配套了美国网络安全近期和中期行动计划，在近期计划第 10 项和中期计划第 13 项中，明确要建立基于网络安全的身份管理战略。2011 年 4 月，美国总统奥巴马签署发布了《网络空间可信身份国家战略》（National Strategy for Trusted Identities in Cyberspace，NSTIC），**NSTIC 作为美国在数字身份领域长达十年的国家宏观战略，基本成为美国政府数字化转型过程中的数字身份体系发展和管理的基础。**

NSTIC 旨在通过政府、企业界和社会团体的共同努力，用 10 年时间构建一个以用户为中心的网络空间可信身份生态系统，促使个人和组织

遵循协商一致的标准和流程来鉴别和认证数字身份，从而实现相互信任。NSTIC 明确了可信身份生态体系的四项原则，即身份解决方案应当是：1）增强隐私且基于公众自愿应用；2）安全、可扩展；3）具备互操作性；4）高效且易于应用。同时 NSTIC 提出了四项任务目标：1）研究形成一个完整的身份生态系统框架，包括一套可互操作的标准、风险模型、隐私保护政策以及对该系统进行管控的问责机制；2）建立和实现可互操作的身份生态系统，联邦政府将与私营机构和各级政府合作，组织、协调、促进和参与实现身份生态系统的、可跨部门操作的试验计划；3）扩大宣传和教育，提升身份生态系统中各参与方的信心与意愿；4）政府和私营机构长期参与维护，确保身份生态系统的持续正常运行。最终达到“使个人和机构能够在提高信心、隐私性、选择性和创新性的情况下，运用安全、有效、易用、可互操作的身份解决方案进行在线服务”的愿景。**在 NSTIC 框架下，联邦政府在各个领域的数字身份工作均取得较大进展。**NIST 在 2011 年、2013 年和 2017 年对《电子身份指南》（SP 800-63 系列）进行三次更新，确保联邦通用标准能够适应技术和风险。2016 年底美国国防部认证中心（DoD CA）、国家安全局认证中心（NSS CA）和联邦调查局认证中心（FBI CA）基于 PKI 框架共同主导的“联邦身份凭证和访问管理”（FICAM）体系基本完成建设和互通互认。同时，在地方政府电子政务、医疗健康、智能汽车和儿童在线服务等方面，NSTIC 也有大量数字身份管理项目落地。甚至在项目落地最多的美国弗吉尼亚州，促成了其在 2015 年和 2017 年分别通过了《电子身份管理法案》和《电子凭证法案》。

（3）体系庞杂的网络安全和数据安全法律

美国是全球范围内网络安全立法最早的国家，自上世纪 70 年代伊始至今，已经形成全面乃至庞杂的网络安全法律体系，为美国构建数字信任提供了坚实的法律性支撑。根据本报告不完全统计，美国联邦层级涉及到广义网络安全或信息安全领域的国家法律超过 25 项，同时还有大量的总统行政令、州法律、技术标准和行业自律规范。**其中，以 2002 年《联邦信息安全管理法》（Federal Information Security Management Act）和 2009 年《网络安全法》（Cybersecurity Act）为主，基本确立了美国目前在联邦信息系统安全的总体制度框架**，明确了各联邦部门的管理权限和网络安全责任。同时，以克林顿政府的 63 号总统令、小布什总统的第 13231 号总统令以及奥巴马政府的《国家基础设施保护计划》为核心，确立了美国在联邦关键基础设施网络安全保护的基本制度基础。

在数据安全领域，**美国立法现状是基于公民隐私权和具体行业领域进行规制。**包括 1974 年《隐私权法》（The Privacy Act）、1986 年《电子通信隐私法》（Electronic Communications Privacy Act）、1996 年《健康保险流通和责任法》(Health Insurance Portability and Accountability Act)、2000 年《儿童在线隐私保护法》(Children's Online Privacy Protection Act) 和 2010 年《多德 - 弗兰克华尔街改革和消费者保护法》(Dodd-Frank Wall Street Reform and Consumer Protection Act) 等，都涉及到不同行业领域的数据安全进行规制，**但美国始终缺乏真正适应数字时代的国家数据安全统一立法。**在此背景下，近年来美国国会密集讨论了诸多联邦层面的数据安全提案，包括 2019 年 2 月的《数据隐私法案》(Digital Accountability and Transparency to Advance Privacy Act)，2019 年 4 月的《隐私权利法案》(Privacy Bill of Rights Act)、2019 年 11 月的《国家安全和个人数据保护法案》(National Security and Personal Data Protection Act) 和 2020 年 2 月《数据保护法案》(Data Protection Act) 等，试图推动一部全面的联邦数据保护法律和并建立一个专项的联邦数据监管机构。

在联邦层面上缺乏统一数据立法的情况，美国的州立法在实践中发挥了重要作用。目前美国 50 个州

都有不同完备程度的法律规制，主要集中在公民隐私保护和数据泄露通知等方面。其中以加州 2020 年 1 月生效的《加利福尼亚消费者法》(California Consumer Privacy Act,CCPA) 最为引人瞩目。这个被外界喻为美国史上最严格的隐私保护法案，因其能直接规制监管到像谷歌、脸书、易趣和推特等总部在加州的美国著名数字企业，因此在美国应对数字经济时代的数据安全方面影响巨大。

2. 欧盟

（1）“电子政府”和“单一市场”下的数字身份计划

欧盟的电子身份源于欧盟的“单一市场”和“电子政府”计划。1999 年 12 月，欧盟发布政府和社会的信息化战略《电子欧洲：所有人的信息社会》（eEurope: An Information Society for All），明确提出“电子欧洲”的战略总目标，欧盟在 2000 年、2002 年、2005 年和 2006 年的年度电子欧洲计划或电子政府计划中，不断强调建立安全、扩展、有效和共通数字身份的重要性。**2006 年 6 月，欧盟发布专项数字身份战略——《2010 泛欧洲电子身份标识（eID）管理框架路线图》（A Roadmap for a pan-European eIDM Framework by 2010），从欧盟层面统筹规划各成员国电子身份证（eID）的实施，**并制定了为期 5 年的推进 eID 行动计划，要求各成员国要共同建立能在欧盟全境范围适用的 eID 基础设施，使得成员国公民持有电子标识即可在欧盟内的任一国家享受求职、医疗、保险等一系列公共和数字化服务。**2015 年 5 月，欧盟发布《欧洲数字单一市场战略》（A Digital Single Market Strategy for Europey），提出要构建“可以被消费者和企业所信任的跨境电子商务规则”和“在数字服务和个人数据处理中强化信任和安全”两项目标，并具体拆解为数字身份、网络安全、隐私保护等多项具体举措。**

在法律层面上，1999 年 12 月，欧盟发布《建立电子签名共同法律框架的指令》（EU Directive on a Community Frameworke for Electronic Signatures），首次明确了电子签名的法律效力等同于手写签名，同时“禁止成员国限制源自另一成员国提供的认证服务。”旨在为统一的欧洲电子商务和数字市场服务。2014 年，欧盟发布《电子身份认证与签名条例》（EU Regulation on Electronic Identity Authentication and Signature，即 eIDAS 条例）取代了 1999 年《电子签名指令》。**eIDAS 条例将电子签名、电子认证以及其他一系列身份服务统一作为信任服务进行规制，作为欧盟层面关于数字身份的统一立法，无需成员国国内立法配套而直接生效，成为欧盟规制数字身份乃至数字信任最核心的法律。**

eIDAS 条例的核心目的在于通过实现欧盟层级的各成员国安全、高效的跨境身份认证，促进欧洲区域内可信电子服务和数字经济的流通和发展，实现欧洲“单一数字市场”。eIDAS 条例的主要内容包括重申“禁止成员国限制从另一成员国向本国提供信息社会服务的自由”的“内部市场条款”，将电子身份划分为标准电子签名（Standard Electronic Signature，ES）、高级电子签名（Advanced Electronic Signatures，AdES) 和可信电子签名（Qualified Electronic Signatures，QES），并根据等级确定对应电子签名的认证、安全要求和法律效力，同时对各成

员国关于电子签名的颁发、管理、认证、合作和互操作性设计了一整套制度体系。

eIDAS 条例还提出欧盟要打造包括电子身份证（eID）、电子签名（eSignature）、电子印章（eSeal）、时间戳（eTimeStamp）、可信电子数据送达（eDelivery）和网站认证（Web Authentication）在内的可信电子服务（Electronic Trust Services），最大限度地确保数字经济发展的高效和安全。同时根据报告不完全统计，在 eIDAS 条例框架下，欧盟层面发布的数字身份管理相关技术标准已达 120 余项，包括电子签名算法、签名设备、签名生成等基础技术标准，时间戳服务、验证服务等可信服务标准，以及跨境互操作相关标准。

（2）数字欧洲战略下的数字信任建设

2020 年以来，欧盟密集发布了三份欧洲整体数字化转型的宏观战略报告，高度强调信任和安全在其中的关键作用。2020 年 2 月，欧盟委员会发布《塑造欧洲数字未来》（Shaping Europe's Digital Future）战略报告，提出要以根植于欧洲共同价值理念的整体数字化解决方案，推动欧洲成为数字化转型的全球领导者。战略认为**“为了实现这一目标，需要一个清晰的框架来促进的可信任的、数字化的人和经济的社会互动。如果缺少了对信任的关注，数字化转型的关键过程将无法成功”**，并“信任”明确列入九个愿景关键词中。

在欧盟与战略同期发布的两份报告中，数字信任的意义更具体的表述。2020 年 2 月，欧盟委员会在《面向卓越和信任的欧洲人工智能发展之道》（On Artificial Intelligence - A European approach to excellence and trust）报告中，明确未来欧洲人工智能监管政策选择是必须构建一个独特的**“卓越和信任的生态系统”**。该系统必须确保人工智能可以遵守欧盟规则，包括保护公民基本权利和数据权利，特别是在欧盟运行的、构成高风险的人工智能系统。生态系统将促进公民有信心接受人工智能应用，赋予企业和公共组织利用人工智能进行创新的法律确定性，**建立政府、企业、公民和社会组织在人工智能领域的信任交流，助力欧洲成为可信人工智能领域的全球领导者**。在同月发布的《欧洲数据战略》（A European Strategy for data）中，明确提出了欧洲“单一数据空间”目标，即一个真正的数据单一市场且面向世界开放，其中个人和非个人数据（包括敏感的业务数据）都是安全的，**企业和公民能够以可信的数字身份轻松访问无限的高质量数据，并利用数据创造价值**。同时在此数据空间中，欧盟法律可以有效执行，所有数据驱动型产品和服务都应符合欧盟数据单一市场的相关规范。

（3）统一高标准的网络安全和数据安全要求

欧盟在网络安全和数据安全领域采取“双轨制”立法，一方面通过欧盟指令来明确统一的立法原则和框架，由各成员国制定国内法进行具体实现；另一方面则通过欧盟条例，直接形成在欧盟区域内具有强制力和最高效力的统一法律。同时，欧盟和各成员国层面也通过大量的行政令、技术标准和实践指南来配套支撑法律的落实。

在网络安全领域，**欧盟目前最重要的法律是 2016 年 8 月生效的《网络和信息系统的安全指令》（The Directive on Security of Network and Information Systems，NISD）和 2019 年 6 月生效的《欧盟网络安全法》(EU Cybersecurity Act)**。前者旨在加强基础服务运营者、数字服务提供者的网络与信息系统的安全，并明确要求这两者履行网络风险管理、网络安全事故应对与通知等义务。此外，该法要求成员国 21 个月内制定网络安全国家战略，同时加强成员国间合作与国际合作，在网络安全技术研发方面加大资金投入与支持力度等。后者在法条第一款明确表示其目的是“**旨在实现欧盟内部的高水平网络安全、网络弹性和信任，确保欧洲内部市场的正常运作**”，主要内容包括对欧盟网络和信息安全局 (European Network and Information Security Agency，ENISA) 职责的

重新定义和授权，以及启动欧洲覆盖所有的 ICT 产品和服务的统一网络安全认证机制。

在数据安全领域，2016 年 4 月欧洲议会投票通过了商讨四年的《通用数据保护条例》(General Data Protection Regulation,GDPR) 以替代 1995 年的欧盟《个人数据保护指令》，并于 2018 年 4 月正式生效。**作为欧盟数据保护立法的集大成者，GDPR 旨在协调欧盟各成员国的数据安全和隐私法律，建立完备的用户数据权利清单和完备的数据问责体系，并基于此形成了一整套系统的数据安全治理制度，对于全球各国数据规则制定都有着极大影响。**此外，2017 年通过的《电子隐私权指令》修订案（ePD 修正案）和 2018 年 11 月欧盟发布的《非个人数据自由流动条例》(Regulation on the Free Flow of Non-personal Data,RFFND) 也对与数据安全和数字信任有不小影响。

3. 中国

（1）构建基于数字身份的网络信任体系

2006 年 2 月，国务院办公厅转发了国家网络与信息安全协调小组的《关于网络信任体系建设的若干意见》（国办发 [2006]11 号文件，以下简称《意见》），成为我国在国家层面高度重视并加快推进网络信任体系建设的起点。《意见》将网络信任体系定义为“是以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系”，并进一步界定“身份认证是通过技术手段确认网络信息系统中主、客体真实身份的过程和方法；授权管理是综合利用身份认证、访问控制、权限管理等技术措施解决访问者合理使用网络信息资源的过程和方法；责任认定是应用数据保留、证据保全、行为审计、取证分析等技术，记录、保留、审计网络事件，确定网络行为主体责任的过程和方法。”

《意见》认为“网络信任体系建设是实施国家信息化战略的重要保障，是信息安全保障体系建设的重要组成部分。加快网络信任体系建设，保障国家、企业和个人信息安全可控，维护网络活动中有关各方的合法权益，对于有效打击网络犯罪，增强网络信息系统的防泄密、抗侵入、拒黑客、识真伪、保安全能力，为信息化建设提供安全保障，具有十分重要的现实和长远意义”。同时，《意见》还对国家加快整个电子认证工作提出了总体要求，明确由国家密码管理局会同有关部门做好电子政务中电子认证工作的规划和管理，实现电子政务电子认证的安全可控、互通互认。同时，网络信任体系也被列为《国家中长期科学和技术发展规划纲要》（2006—2020）的重点领域优先主题。

在《意见》的框架下，国家密码管理局密集发布了一系列政策文件和部门规章，包括 2007 年的《电子政务电子认证体系建设总体规划》（国密局联〔2007〕2 号）、2009 年的《电子政务电子认证服务管理办法》（国密局联〔2009〕7 号）和 2009 年修订的《电子认证服务密码管理办法》（国密局 17 号公告）等。同时，北京、浙江、江苏等地方省市也纷纷出台了相关的具体实施计划和政策。

（2）制定支撑数字信任的多项国家法律政策

2004 年 8 月，全国人大常委会正式审议通过了国家《电子签名法》，并在 2015 年 4 月和 2019 年 4 月进行了两次修订。**修订后的《电子签名法》明确了数据电文和电子签名的定义、格式、适用范围和法律效力，并对提供电子签名认证的第三方服务的准入、责任和行为规范做了详细规定，有力地支撑了基于我国基于数字身份的网络信任体系建设。**

2019 年 1 月，我国《电子商务法》正式生效，

成为规范我国电子商务经济活动的顶层法律。该法在第三章对电子合同的订立、履行、效力以及电子支付的相关签名、指令和认证等内容进行了规制。

2020 年 1 月，我国《密码法》正式生效。对于密码的分类、管理、认证、使用和安全责任等做了全面规定。在第二十九条明确规定“国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理”。在《密码法》框架下，2020 年 8 月国家密码管理局发布了《商用密码管理条例（修订草案征求意见稿）》，根据新形势的发展对 1999 年的《商用密码管理条例》进行大幅度修订，包括在第四章对基于商用密码的电子认证服务的资质、准入、管理、技术规范和法律责任进行全面规定，并在第二十九条明确提出**“国家建立统一的电子认证信任机制，推动电子认证服务互信互认”**。

（3）加快推进网络安全和数据安全立法

2016 年 11 月全国人大正式审议通了国家《网络安全法》。作为我国在网络安全领域的顶层立法，《网络安全法》明确了网络安全等级保护、关键信息基础设施保护、重要数据保护和网络安全监测预警等一系列重要制度，对我国网络运营者的网络安全义务和责任作出了全面规定。在《网络安全法》第二十四条第二款再次明确规定，**“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”**。同时，在《网络安全法》框架下，国家各部委还出台一系列部门规章政策，包括 2017 年的《关键信息基础设施安全保护条例（征求意见稿）》、2018 年的《网络安全等级保护条例（征求意见稿）》、2019 年的《网络安全审查办法（试行）》等，对数字经济市场主体的具体网络安全义务和责任做了更细化的要求。

在数据安全领域，我国数据立法起步较晚，但近年来进展迅速。包括 2019 年 5 月的《数据安全管理办法（意见征求稿）》、2019 年 6 月的《个人信息出境安全评估办法（征求意见稿）》和 2019 年 8 月《儿童个人信息网络保护规定》一系列部门规章的密集出台。2020 年 5 月，全国人大会正式通过了《中华人民共和国民法典》，确立了数据和虚拟财产依法受到保护、公民个人信息和隐私权保护的基本原则。《法典》第四编“人格权”的第六章“隐私权和个人信息保护”中，对自然人的隐私权，侵犯隐私的行为方式，自然人的个人信息定义，收集、处理自然人个人信息的原则、方式和限制，自然人的个人信息权利，信息收集、控制者的责任、义务和豁免等进行了明确规定。2020 年 7 月，全国人大常委会正式对外发布国家《数据安全法（草案）》，《草案》作为我国数据安全领域的顶层立法，对国家数据安全制度和各主体数据安全保护义务进行了全面规定，为我国加快数据安全制度坚实提供坚实的上位法基础。2020 年 10 月，全国人大常委会正式对外发布国家《个人信息保护法（草案）》，对个人信息处理原则、处理者义务、数据主体权益做了全面规定。

二 | 全球数字信任的关键技术方向

数字信任与数字技术发展和应用高度相关。**数字技术的发展不仅能够极大地提高政府和企业的安全能力，也会对现行的数字身份和网络安全架构产生冲击甚至底层性的颠覆。**对此，本报告重点对当前数字身份中的密码学和生物特征识别技术、数据安全中的隐私计算技术、网络安全中的零信任框架、区块链技术、量子计算技术的理论和趋势进行介绍。

1.PKI 架构及密码学

目前，各国通行的数字签名、数字身份标识以及验证应用中，核心的底层技术都基于密码学。自上世

纪 70 年代开始，欧美等国就率先开始密码技术的研究与应用，取得了大量先进成果，有利支撑了数字身份验证应用的发展，其中主流的密码算法有三大类：对称加密算法（Symmetrical Encryption）、非对称加密算法（Asymmetric Cryptographic Algorithm）和哈希算法系列（Hash）。

● **对称加密算法**：对称加密算法即采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。同一个密钥使得对称加密具备使用较为简单，加解密迅速的优势，但存密钥分发和存储的安全性问题，因此这类算法通常运用在一般大规模数据加密传输的场景。目前，对称加密算法主要包括 DES、3DES、TDEA、Blowfish 和 AES 等算法模型。IBM 公司在上世纪 70 年代首先提出 DES 算法，该算法成为之后的美国 FIPS-46 标准。但 DES 算法自推出以来，其安全性一直广受质疑，20 世纪末不断有研究机构成功攻破 DES 算法。随后，美国 NIST 开始征集开发 AES 算法，欧洲也开始启动 NESSIE 工程，最后确定 AES 算法可根据所需安全强度设定密钥长度为 128/192/256 位。鉴于 AES 算法具有加解密运算速度极快的优点，该算法成为使用最为广泛的对称密码算法。

● **非对称加密算法**：非对称加密算法是采用双钥密码系统的加密方法，公钥用于加密而用户的私钥用于解密。由于非对称加密算法使得用户最终不需要相互交换秘钥，且现有计算能力从公钥推导出私钥十分困难，因此实现了更高的安全性，但非对称加密算法的算法强度复杂，因此在成本和效率上需要做出平衡。目前，全球大部分数字签名、可信通信与加密信息传输均是通过基于非对称加密的 PKI（Public Key Infrastructure，即“公钥基础设施”）架构实现。美国在 1978 年首次提出基于大整数素因子分解的 RSA 算法，1985 又提出了基于离散对数问题的 ELGamal 算法，其中 RSA 算法是目前应用较为广泛。RSA 算法的强度与其算法密钥长度有关，RSA1024 已经在 2012 年被美国密码学家攻破，目前最新版本为 RSA4096。由于过长的 RSA 密钥会导致运算效率大大下降，美国 NIST 和欧洲 NESSIE 的专家又提出了椭圆曲线和超椭圆曲线密码 ECC，该算法只需 282bit 的密钥长度即可媲美 RSA4096 的加密强度，运算效率大大提高，是目前非对称密码技术研究的热点。

● **哈希算法**：哈希算法又称为杂凑算法或摘要算法，即能够将任意长度的数据压缩成固定长度的标识，能够赋予每个数据唯一的“数字指纹”。对称 / 非对称加密算法主要解决的是防止数据被窃取的问题，而哈希算法主要用于证明数据信息的完整性，即防止数据被篡改，广泛应用于数字签名、数据质量治理和数据安全保护领域。哈希算法的典型代表是美国 NIST 发布的 SHA 系列，1995 年 SHA-1 正式发布，经过二十余年的发展 SHA-1 算法逐渐成为互联网最基础的数字签名算法。由于 SHA 家族算法本身的问题存在“碰撞”破解的可能性，SHA 算法被攻破的时间仅依赖于所使用的计算能力，所以，欧美密码学家不断调整改进 SHA 算法，既 SHA-1 后推出 SHA-224、SHA-256、SHA-384 和 SHA-512。

2. 区块链

区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在数字经济时代应用模式的集成创新。提核心原

理是通过在互联网上建立一个点对点的公共账本，由区块链网络的参与者按照共识算法规则共同添加、核验、认定账本数据。网络中每个参与者都拥有一个内容相同的独立账本，且账本数据是公开透明的。目前区块链应用主要有三种模式：1）公有链是运行在互联网的完全分布式区块链；2）联盟链则是由多个关联机构共同发起和运营，带有准入机制；3）私有链是公有链的私有化部署，往往由单个机构主持运行。由于区块链具备中心化、开放性、自治性、不可篡改性、匿名性等诸多优势，目前已经成为数字经济最具颠覆性和研究热度的技术方向。

区块链在数字信任体系中的应用前景广泛。区块链在数字身份认证中应用相较于传统 PKI 体系具备明显优势，包括身份信息更难篡改和身份信息分布式存放带来安全性和便捷性的提升，以及区块链激励机制的存在能够促使用户积极维护整个区块链，使系统在良性、高稳定性长期运作下维护成本更低。目前，不少区块链初创企业已经通过与科技企业、传统企业合作进行分布式数字身份（Decentralized ID）产品试验。比如区块链企业 ShoCard 与航空服务商 SITA 合作开发了 SITA Digital Traveler Identity App 的身份认证应用，该应用融合了基于区块链的数据和面部识别技术，致力于简化航空公司乘客身份验证流程，以及实现机场实时数据流；微软与 Blockstack Labs、ConsenSys 合作，推出了基于区块链技术的身份识别系统，实现人、产品、应用和服务的深度交互。IBM 与法国国民互助信贷银行（CréditMutuelArkéa）合作完成了一个基于区块链技术的身份认证系统，该系统采用超级账本区块链框架（Hyperledger）引导客户向第三方（比如本地公共部门或零售商）提供身份证明。

3. 隐私计算

在当下的安全实践中，隐私计算通常是指在**数据全程保密或无接触的情况下，确保合作双方能够对数据进行计算、比对、运行等并读取和利用结果，并保证任何一方均无法得到除应得的计算结果之外的其他任何信息。**目前，隐私计算包括同态加密（Homomorphic Encryption，FHE）、多方安全计算（Secure Multi-Party Computation，sMPC）、 差分隐私（Differential Privacy）、联邦学习（Federated Learning）、零知识证明（Zero-knowledge Proof）等多种技术方向。

● **同态加密：同态加密是指对加密数据进行处理得到一个输出，将此输出进行解密，其结果与用同一方法处理未加密原始数据得到的结果一致。**在同态映射下，先运算后加密和先加密后运算，得到的结果相同。同态加密算法从功能上可分为部分同态算法和全同态算法。1）部分同态是指支持加法同态或者乘法同态或者两者都支持但是操作次数受限；2）全同态算法则可简单理解为能不受限制地同时支持加法和乘法操作，从而完成各种加密后的运算（如加减乘除、多项式求值、指数、对数、三角函数等）。

● **多方安全计算：**多方安全计算主要针对无可信第三方情况，安全地进行多方协同计算问题。即**在一个分布式网络中，多个参与实体各自持有秘钥输入，各方希望共同完成对某函数的计算，而要求每个参与实体除计算结果外均不能得到其他用户的任何输入信息。**从计算场景上，可以将安全多方计算分为特定场景和通用场景。特定场景是指针对特定的计算逻辑，比如比较大小，确定双方交集等。具体场景可以采用多种不同的密码学技术设计协议。通用场景是指安全多方协议的设计要具有完备性，可以理论上支持任何计算场景。目前采用的方法主要是加密电路，不经意传输以及同态加密。通用的两方计算已经具备了商用的条件。多方计算在某些特定场景下也已经没有太多的性能瓶颈，而通用计算协议在可扩展性层面依然不成熟，这也是学术界一直在探索的方向。

当前，多方安全计算的主要适用场景包括：1）数据安全查询。使用安全多方计算技术，能保证数据

查询方仅得到查询结果，但对数据库其他记录信息不可知。同时，拥有数据库的一方，不知道用户具体的查询请求。2）联合数据分析。改进已有的数据分析算法，通过多方数据源协同分析计算，使得敏感数据不被泄露。

● **差分隐私：**差分隐私是一种被广泛认可的隐私保护技术，通过对数据添加干扰噪声的方式保护数据中的隐私信息。当对用户数据进行训练时，差分隐私技术能够提供强大的数学保证，保证模型不会学习或记住任何特定用户的细节。在许多场景下机器学习涉及基于敏感数据进行学习和训练，例如个人照片、电子邮件等。理想情况下，经过训练的机器学习模型的参数代表的应该是一般模式，而不是关于特定训练示例的事实。为了确保训练数据中的隐私得到有效的保护，可以使用差分隐私技术。2016 年，研究者提出基于差分隐私的深度学习算法，利用随机梯度下降过程中对梯度增加扰动来保护训练敏感数据。但在某些情况下，由于添加了噪声，差分隐私技术可能会导致精度受到影响。

● **联邦学习：联邦学习是指本地进行 AI 模型训练，然后仅将模型更新的部分加密上传到数据交换区域，并与其他各方数据的进行整合。**其技术特点包括：1）数据隔离：数据不会泄露到外部，满足用户隐私保护和数据安全的需求；2）模型质量无损：不会出现负迁移，保证联邦模型比割裂的独立模型效果好；3）地位对等：合作过程中，合作双方是对等的，不存在一方主导另外一方；4）共同获益：无论数据源方，还是数据应用方，都能获取相应的价值。

当前，联邦学习技术的主要类型包括：1）横向联邦学习：数据集共享相同特征空间但样本不同。例如，两个区域银行可能具有与其各自区域不同的用户组，并且它们的用户的交集非常小。但是，它们的业务非常相似，因此要素空间相同；2）纵向联邦学习：两个数据集共享相同的样本 ID 空间但特征空间不同；3）迁移联邦学习：两个数据集不仅在样本上而且在特征空间上都不同的情况。考虑两个机构，一个是位于中国的银行，另一个是位于美国的电子商务公司。由于地理位置的限制，两个机构的用户群体之间的交叉点很小。另一方面，由于业务不同，双方的特征空间只有一小部分重叠。目前，联邦学习主要应用于 AI 联合训练。通过利用联邦学习的特征，为多方构建机器学习模型而无需导出企业数据，不仅可以充分保护数据隐私和数据安全，还可以获得到更好的训练模型，从而实现互惠互利。

4. 生物特征识别

随着人工智能技术的发展，基于生物特征识别（Biometric Identification Technology）的数字身份认证将在未来获得更多的应用。生物特征识别技术是指通过数字技术将人类具备唯一性标识的生物特征进行数字化采集、提取并形成特征模板，并通过与已有数据库或特征模板进行比对来实现数字身份的标识和认证。随着以自然语言识别为代表的人工智能技术发展，生物特征识别在数字身份领域的应用日益广泛，包括指纹识别、声纹识别、虹膜识别、人脸识别、行为识别甚至基因识别等。生物特征识别技术在识别准确率、应用便捷性上具备密码学不可比拟的优势，但也面临众多安全性的风险。2013 年，FIDO 联盟（Fast Identity Online Alliance）提出的一个开放的标准协议——FIDO 线上快速身份验证标准，通过集成生物识别与非对称加密两大技术来完成用户身份验证，试图解决多年来用户必须记忆并使用大量复杂密码的烦恼，为企业和用户提供一个高安全性、跨平台兼容性、极佳用户体验

与用户隐私保护的在线身份验证技术架构。在 2015 年的 FIDO 标准 1.0 版本中，用户可以选择 U2F 与 UAF 两种用户在线身份验证协议。其中 U2F 协议兼容现有密码验证体系，在用户进行高安全属性的在线操作时，需提供一个符合 U2F 协议的验证设备作为第二身份验证因素，即可保证交易足够安全。而 UAF 则充分地吸收了移动智能设备所具有的新技术，更加符合移动用户的使用习惯。在需要验证身份时，智能设备利用生物识别技术（如指纹识别、面部识别、虹膜识别等）取得用户授权，然后通过非对称加密技术生成加密的认证数据供后台服务器进行用户身份验证操作。整个过程可完全不需要密码，真正意义上实现了“终结密码”。根据 UAF 协议，用户所有的个人生物数据与私有密钥都只存储在用户设备中，无需经网络传送到网站服务器，而服务器只需存储有用户的公钥即可完成用户身份验证。这样就大大降低了用户验证信息暴露的风险。即使网站服务器被黑客攻击，他们也得不到用户验证信息进而伪造交易，也消除了传统密码数据泄露后的连锁式反应。目前，谷歌、微软、Egistec 等科技公司纷纷基于 FIDO 标准开发自身的基于密码学和生物特征识别的联合数字身份认证体系。

5. 零信任架构

零信任（Zero Trust）的最早雏形源于 2004 年成立的耶利哥论坛（Jericho Forum），其核心理念是为了应对信息系统边界日益模糊趋势下的网络安全问题。2010 年，Forrester 的分析师金德维格（John Kindervag）正式提出“零信任”概念，在其研究报告中指出，**基于目前互联网空间下的安全风险常态化，必须假定所有的网络流量都是不可信的，从而通过对访问任何资源的任何请求进行控制来实现安全。**2019 年 10 月，美国防创新委员会（DIB）发布《通往零信任安全之路》白皮书，敦促军方尽快实施零信任架构（ZTA）。2020 年 8 月，美国国家标准技术研究院（NIST）发布了《零信任架构》（SP800-207）的最终版，将零信任定义“为将网络防御从广泛的网络边界缩小到最小的微隔离区，针对每一个用户访问的每一个应用，建立一对一的封闭的安全隧道，通过策略决策引擎（Policy Decision Point，PDP）和策略管理引擎（Policy Enforcement Point，PEP）对全交互过程进行严格验证和授权，才允许其访问资源，从而实现应用访问的封闭系统。”Evan Gilman 和 Doug Barth 在《零信任网络：在不可信网络中构建安全系统》专著中，总结了零信任的五大前提条件，即“网络无时无刻不处于危险的环境中；网络中自始至终存在外部或内部威胁；网络的位置不足以决定网络的可信程度；所有的设备、用户和网络流量都应当经过认证和授权；安全策略必须是动态的，并基于尽可能多的数据源计算而来。”

随着移动互联网和云计算的发展，软件定义边界（Software Defined Perimeter，SDP）的趋势成为现实，“**零信任”通过对数字身份的认证和访问控制，来应对网络边界模糊化带来的权限控制粒度粗、有效性差的问题，以此达到保护系统网络安全和数据安全的目的，**具备更细粒度的控制、更灵活的扩展和更高的可靠性优势，现已成为目前国际上公认的解决云访问安全的最新趋势，也日趋成为当下网络安全防护的重要模型。

当前，全球产业界围绕零信任纷纷布局。微软、谷歌、Cisco、Symantec 等在内的国际巨头均已进军此领域，国内众多安全厂商也纷纷推出自己的零信任方案。2020 年 6 月，Gartner 在《零信任网络接入市场指南》报告中预测，到 2022 年，面向生态系统合作伙伴开放的 80% 的新数字业务应用程序将通过零信任网络（Zero Trust，ZTNA）进行访问。到 2023 年，60% 的企业将淘汰大部分远程访问虚拟专用网络（VPN），转而使用 ZTNA。

6. 量子计算

量子计算(Quantum Computation)是指一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式，包括量子计算架构、量子算法、量子计算机等软硬件研究的技术体系。量子计算是一种完全不同于传统二进制的计算操作，其最小数据单位是基于量子力学的量子比特（Quantum Qubit，又译量子位元），其将0或1显示出一种叠加状态或是两种状态的某种组合，这可以使量子计算机能够同时（而不是按顺序）执行涉及许多量子位的操作。这种架构的量子计算机在进行数据分解、离散对数解析和数据库算法检索计算时具备巨大的优势，而上述算法正是当下非对称加密算法的核心数学基础。**因此从理论上讲，量子计算机可以通过计算能力绕过现行的防御，直接暴力破解用于保护现有几乎所有网络通信的秘钥体系，使现有通信的身份验证和访问控制完全失去安全性。**2020年4月，兰德公司（RAND Corporation）在《量子计算时代的通信安全》报告指出，“量子计算能够用于破解现有的加密系统，可能会现有的通信基础架构产生颠覆性影响，身份验证的安全与通信隐私将难以保证，军事情报系统、金融交易系统乃至全球经济的支持系统都将面临潜在的巨大风险。

尽管经过多年的研究和大量的投资，以及美国、欧盟在量子计算方面的部署和推进，学术界和产业界在关于实现量子计算机基本架构的最佳方法仍未达成基础共识。目前正在探索可能实现的量子比特架构，包括超导量子比特、捕获离子量子比特、自旋量子比特、光子量子比特和拓扑量子比特等。2019年10月，谷歌宣称其制造出了53量子比特的量子计算机，能够在200秒内完成目前最先进的传统超级计算机需要1万年完成的特定计算任务。未来，围绕后量子时代的加密体系（即“后量子密码”Post Quantum Cryptography,PQC）的技术研究和标准制定，可能成为未来十到二十年数字信任发展的关键。

PART 3
城市数字化转型下的数字信任体系

随着全球科技革命和产业变革蓬勃兴起，人工智能、大数据、区块链、物联网等新兴数字技术加速演进融合，创新活力、集聚效应和应用潜能裂变式释放，城市作为人类文明的主要物理载体，正在经济、生活、治理等全领域开启“整体性转变、全方位赋能、革命性重塑”的新一轮数字化转型进程。同时，物联网安全、数据安全、算法安全等网络安全风险与技术伦理、数字鸿沟等治理问题深度交织泛化，城市数字化转型成为了数字信任体系建设的重大需求牵引。

一 | 城市数字化转型的数字信任需求

1. 城市基础设施数字化转型的数字信任需求

随着以工业互联网、物联网、云计算等为代表的新型基础设施大规模部署，由智能终端、物联设备等类型的城市神经元设备爆发式增长，远远超过个人或组织的联网数量。在以城市各类基础设施和终端为主要网络节点的数字拓扑和层叠应用环境下，城市在数字空间暴露面极速扩大，

用户交互触点急剧增多，时刻面临着日趋复杂高能的物联网攻击。通过部署适应于物联网环境下的低成本、快捷的身份识别验证设备和访问控制，能够在网络边界日趋模糊、网络拓扑日益复杂的环境下构建“人 - 物、物 - 物”的可信数字交互关系，能够在平衡物联网安全投入的同时，更好地保障数字城市感知和运行的平稳安全。

2. 城市数据要素市场化配置的数字信任需求

2020 年 4 月，中共中央和国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，首次明确将数据列为与土地、劳动力、资本和技术等并列的一种新型生产要素，强调要加快培育数据要素市场。自中央明确定调以来，深圳、天津、北京、广东等省市纷纷制定推动数据要素市场发展的规划政策，数据要素便利高效化的流通和最大化的分析利用成为城市数字化转型的关键。同时，数据确权定价不清晰、数据流通来源和链条复杂且难以溯源、数据滥用和泄露风险依然严峻等数据治理和安全问题，成为了培育数据要素市场的重要瓶颈。通过部署数据全生命周期安全防护体系，利用区块链、隐私计算等技术，实现数据要素在共享、开放和利用等全链条的可信流通，从而构建双方的数字信任关系，能够极大地支撑数据要素市场发展。

3. 城市经济生产数字化转型的数字信任需求

随着数字产业化和产业数字化的深入融合发展，传统人际信任和制度信任在数字时代下越来越难以适应。消费互联网端兴起较早，围绕用户的个人信息和数字轨迹形成的信用数字化治理模式，以及“用户评论 - 平台治理 - 商家反馈”等机制，实现了传统信任关系的重构。随着产业互联网发展，工业互联网、智能制造不断深度渗透的背景下，企业内部、企业与供应链、人与机器之间亟需数字技术深度内嵌的新型数字信任体系，以解决数字化的经济社会活动的风险投入和交易成本大幅上升的问题。同时，合规驱动仍是企业网络安全投入的主要原因，企业网络安全能力仍未成为数字时代差异化竞争的关键因素。通过构建数字信任体系，构建基于主体网络安全能力认证的数字信任测度量化机制，形成市场与合规双驱动下网络安全能力建设的良性循环。

4. 城市治理和公共服务数字化转型的数字信任需求

随着“一网通办”“一网统管”的持续建设，政府数字化转型在加速推进，越来越多的政务服务、教育养老、医疗健康、交通出行等各类民生公共服务以数字化方式提供，信息弱势群体面临的数字鸿沟问题更加凸显。借助安全可信、弹性扩展的数字身份服务能力，为各类人群提供便捷的身份服务，能够降低老人、残疾人等群体在数字接入上的技能要求和流程成本，减少因数字身份欺诈、多次重复认证产生的安全风险，更好地分享城市数字化转型发展的红利。

二 | 面向城市数字化转型的数字信任体系

在 2006 年 2 月国务院办公厅转发的《关于网络信任体系建设的若干意见》中，网络信任体系被定义为“是以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系”。本报告在上述研究的基础上，将**数字信任体系（Digital Trust System）定义为“是以可信数字身份验证和可信数据流通为核心，聚焦新型网络安全风险和数字治理难题，通过制度标准、技术创新、产业生态等多维度建设，最终实现身份信任、数据信任、算法信任、能力信任、规则信任等五大建设目标的数字时代信任治理模式”**

图 2：数字信任体系框架

其中，数字信任体系被期待或应当实现的功能和未来愿景，主要包括：

● **身份信任：**即基于系统内参与网络实体的数字身份的真实性、安全性和可验证形成数字信任关系。随着以智能工厂、无人机、智能网联汽车、智慧家居为代表的全球物联网产业发展，海量的机器设备甚至单独的传感器单元链入到数字空间中。身份信任将覆盖如何构建对于 IoT 设备数字信任，包括确保 IoT 设备具备安全可验证的数字身份，IoT 设备通过云计算或者边缘计算运行时的网络安全，以及 IoT 设备采集的数据在后续开发利用的合规性。

● **算法信任：**即对人工智能算法形成数字信任。包括确保算法本身设计的正义性和合理性（包括非歧视、合乎伦理道德），算法在训练和运行时所输入数据的质量（包括数据的代表性是否科学、数据是否被投毒污染等），算法运行时的安全性（能否抵御逆向还原攻击和数据泄露），以及算法在实体决策中的参与深度和终结机制（即人类对自动算法决策的拒绝选项）。

● **数据信任：**数据信任包括确保数据来源的合法性与必要性、数据质量的完整性和可用性、数据流动中的防泄漏和防窃取、数据控制者的数据活动的合法性和不被滥用等等。随着全球范围内数据要素市场的探索，数据交易中的数据确权定价、收益分配等制度设计也将会成为数据信任的重要机制。

● **能力信任：**即网络实体对发生数字交互各方的网络安全和数据安全能力实现信任。包括其安全产品 / 服务的部署和有效性、安全制度和流程的设计、安全管理人员的专业素质、应对安全事件的能力、供应链的持续性和可靠性等，以及在能够达成共识的标准下对网络安全能力和数据安全能力的评级认定。

● **规则信任：**即网络实体对规制数字交互的法律、政策、标准制定及其执行实现信任。包括规则制定的权威性、科学性和稳定性，规则规制范围的明确边界和效力，规则执行的公正性和透

明性等，以及网络实体在对数字规则的认知和理解上是否能够达成共识等。

1. 制度标准

● **国家战略：**即国家围绕数字信任体系发布的宏观战略和总体规划，包括政府各部门和地方政府配套的行动计划和政策等。国家数字信任战略通常包括在数字化转型战略中关于“信任”的制度和机制设计，以及在可信数字身份和网络安全领域的相关战略和规划。

● **法律法规：**即国家在数字身份、网络安全和数据安全领域制定的法律法规体系，通常还会包括互联网、物联网领域的标识管理以及人工智能算法可信任的要求。

● **社会倡议：**即行业协会、企业联盟、研究机构和科技企业围绕数字信任主题发布的各种社会倡议，包括各种技术伦理、行业公约和行为规范等。

● **行业标准：**即国家标准化部门围绕数字身份领域形成行业技术标准和建设指南，也会包括一系列具备约束力的国际标准。

2. 技术创新

即为网络实体在构建数字信任关系提供主要支撑和工具的技术体系。包括管理和维护数字身份的技术、实现网络安全和数据安全的技术，以及支撑和确保数字交互和数字应用中安全性、适用性的广泛技术领域。主要包括：

● **PKI 及密码学：**包括对称加密、非对称加密和哈希加密等三种主要密码算法类别。虽然面临人工智能和量子计算可能带来的冲击，但是 PKI 架构依旧是目前全球数字身份认证最核心的底层技术支撑。

● **隐私计算：**包括全同态加密、多方安全计算、差分隐私、联邦学习、零知识证明、安全沙箱等多种计算模型。隐私计算主要为网络实体在数字交互中提供数据 / 算法传输、共享和应用的安全性保证。

● **人工智能：**以生物特征识别和自然语言识别为代表的人工智能技术主要应用于数字身份领域，同时机器学习和深度学习模型在漏洞检测、态势感知、风险评估等网络安全防护领域也有广泛的应用。

● **区块链：**区块链在分布式数字身份、局域网络架构、信息记录方面均有应用。智能合约则能够为具体行业中的数字交互提供去中心化的信任结构。

3. 信任生态

● **数字信任规则制定者：**主要包括政府中负责数字化转型和信息化建设、数字经济发展、国家网络安全和数据安全保护、密码管理等一系列职责部门。同时，还包括标准制定部门、行业自律协会等能够发布具备一定约束力的公共部门和社会组织。

● **数字信任建设者：**即所有为数字信任关系提供支撑服务的机构，包括提供数字空间链入设施的电信运营商，提供数字身份管理和认证的权威机构，提供网络安全和数据安全技术和服务的网络安全厂商，提供网络安全产品和能力认证的测评认证机构，提供数字规则咨询和合规的专业法律机构，提供网络安全保险和风控的金融机构等。

● **数字信任用户：**主要包括通过数字化方式开展业务的企业 / 其他组织和个体用户，同时包括物联网、人工智能发展带来的各种数字代理。

三 | 相关建议

1. 加快完善数字信任制度规则

完善《网络安全法》的配套支撑措施，加快推动《数据安全法（草案）》、《个人信息保护法（草案）》的正式出台。研究制定可信数字身份战略和管理办法，统一规划非对称加密、生物特征识别、分布式等数字身份的认证、发展和应用，在物联网、人工智能、区

块链等“人 - 机”复杂交互的重点行业领域，制定用户数字身份和设备数字标识相互识别验证、数据可信传输流通的管理办法、指导意见或标准规范，为各主体建立数字信任关系提供体系完备的治理规则。

2. 前瞻部署数字信任技术方向

聚焦数字技术的前沿应用方向，加快新兴技术在数字信任方向的融合创新应用。围绕区块链技术，加快推动区块链与电子认证技术的融合发展，打造新一代分布式智能化可信身份技术体系。围绕人工智能技术，加快生物特征识别在数字身份领域的应用。围绕隐私计算方向，重点关注同态加密、零知识证明、联邦学习等方向，探索数据共享、数据流动和数据交易中数字信任关系构建。围绕零信任架构，关注企业、组织在零信任架构改造进程中对于身份访问控制的需求，探索构建零信任环境的数字信任交互架构。围绕 PKI 及密码学，加快密码法算法、商业密码应用的技术攻关，密切关注量子计算、量子加密的技术演进动态。

3. 培育壮大数字信任产业集群

通过建立行业性组织，充分打通软硬件提供商、电子认证第三方服务机构、网络安全厂商、安全合规律所、网络安全保险和咨询企业，形成综合性的数字信任第三方支撑服务能力。围绕数字信任认证、中介、担保等业务，深化数字信任增值服务的集成式开发。围绕解决方案培育、行业应用创新和支撑体系构建等方面，征集遴选一批掌握关键技术、具备创新能力和应用推广能力的机构开展应用示范工作，在金融、政务、司法、工业等培育一批解决方案和应用新模式，为数字信任服务协同发展树立标杆和方向。

4. 形成场景化数字信任解决方案

聚焦电子政务服务领域，搭建全市数字身份统一认证平台，重点围绕在线教育和在线医疗等数字化民生服务领域，形成统一的用户身份识别、电子合同签署、数据可信传输、责任溯源等服务。聚焦工业互联网领域，探索基于区块链的分布式工业设备识别框架，培育覆盖企业身份认证、设备身份认证的分布式设备标识服务能力和工业 SaaS 平台、APP 身份认证服务新场景。聚焦数据流通交易领域，利用区块链、数字标识、数据溯源等技术，建设数据要素线上登记、全链条确权和第三方科学估价的统一平台，支持数据购买、数据互换、协议转让、数据与其他要素置换等多种交易模式。

5. 构建区域 / 国际的数字信任生态

依托长三角、粤港澳等国家区域一体化战略，打破我国现在数字身份和电子签名在地区性、行业性交叉认证过程中存在“各自为政”的分散甚至割裂情况。加强区域内在数字身份、电子签署、数据流通、数据安全方面的标准对接和技术认证。依托我国数字“一带一路”倡议、国际自由贸易谈判和自由贸易区建设，加强与主要贸易伙伴的电子认证服务机构的交流合作，创新数字贸易中的国际电子认证和签署服务。

PART 4

重点场景的数字信任解决方案

一 | 电子政务的数字信任解决方案

随着政府治理能力的数字化转型，各地以“一网通办”为核心的电子政务平台在持续建设，通过数字化方式提供审批、备案、办事等政务公共服务成为大势所趋。同时，困扰基层群众的“办证多、办事难”现象仍然大量存在，其核心仍是在于办事人身份及相关资质信息如何证明的问题。

电子政务的数字信任解决方案以数字身份、电子签名为核心，通过区块链、生物特征识别等技术，实现数字身份的多渠道、多终端的无密码认证和鉴证证明，提供 PC 端、移动端等多种接口。同时，通过区块链、隐私计算技术，实现后台数据的匿名化访问、加密共享传输和隐私保护，旨在实现群众办事的多次认证、隐私保护、数据安全传输等问题。系统主要架构包括：

● **PKI/CA 安全支撑平台：**为在线政务服务平台提供本地签名验签、数据加密、时间同步、移动认证、日志审计等基础密码服务支撑，以及与多元可信身份认证管理服务云平台、电子签名 / 签章公共服务云平台的连接。

● **多元可信身份认证管理云服务平台：**基于数字证书、生物特征识别等技术，覆盖 PC 端、网页、移动 APP、小程序等各种界面，为不同网络身份标识的用户提供可信、方便的身份鉴别和身份认证服务，同时为政务系统提供统一的用户访问与权限管理功能。

● **电子签名签章云服务平台：**为政府、企事业单位以及个人提供形态多样、便捷可靠的电子签名 / 签章云服务，包括文档签名签章、审批签章、电子证照盖章、移动签名、批量签章等等。通过公有云或私有云部署，为各级电子政务应用提供。

● **统一认证和单点登录系统：**以服务方式，可以利用多元可信身份认证管理服务云平台包含的统一认证和单点登录系统；以产品方式，可以在各级电子政务门户独立建设统一认证和单点登录系统，也可接第三方统一认证和单点登录系统。

● **门户及业务集成系统：**为各级电子政务门户使用多元可信身份认证管理服务云平台功能提供服务接口和对接工具，为各级电子政务应用提供使用电子签名签章公共服务云平台（电子印章中心）功能提供服务接口和对接工具。

● **CA 证书与电子印章的管理机制：**企业一证通证书用户以及其他已经具备 CA 证书的企业用户利用 CA 证书关联注册，同时发放并关联电子印章；已有企业证书但不用关联注册的企业用户，按照标准流程方式注册，经过实名鉴别后，自动检索证书库关联已发放的证书和电子印章；个人用户或没有 CA 证书的企业，按照标准流程方式注册，经过实名鉴别后，个人用户自动发放手证通手机证书并开通手写签名（个人印章），企业用户自动发放云证书并发放和关联企业电子印章。

● **运维和运营机制：**所有用户一旦注册完成，都可全部免费使用证书和印章。按照“通过政府购买服务，鼓励社会力量参与政务服务平台建设”的原则由各级政务部门购买服务，不向使用人收费。服务内容包括面向所有用户的全生命周期的数字证书服务、电子印章服务、实名验证服务、业务端运维服务、业务端支撑服务、终端咨询及支持服务。

二 | 数据流通的数字信任解决方案

随着今年来中央明确将数据列为生产要素，提出要加快培育数据要素市场，各地都在加快探索数据要素市场化流通交易的机制模式，但是，当下数据确权定价、交易模式、收益分配、安全保护等基础规则仍然未形成真正清晰、可落地的路径，成为阻碍数据要素市场化流通交易的关键瓶颈。

数据流通交易的数字信任解决方案，旨在通过区块链、隐私计算、数据标识、数字身份等技术，搭建“数据要素可信交易平台”，以实现数据要素可信、安全、便捷的市场化流通交易。平台核心功能包括：

● **数据要素资源登记管理平台：**通过区块链、数据标识、数据溯源等技术，形成数据要素来源审核、数据要素线上登记、数据要素全链条确权等核心功能，形成统一、规范、合法、可信的数据要素资源标的。

● **数据要素多方交易磋商平台：**构建数据交易多方主体的数字身份识别和认证服务，提供数据购买、数据呼唤、协议转让、数据与其他要素置换等多种交易模式的电子签署文本。通过隐私计算、区块链、数据标签等技术，确保买方对数据价值的可信查验，以及卖方对数据安全保障和防止数据泄露的要求。依托数字身份、电子签署、数据溯源等技术，确保在线的报价、询价、竞价、定价和挂牌机制符合相关规定并具有法律效力，支持数据要素市场的交易纠纷仲裁和市场管理。

● **数据要素流通交易服务平台：**提供数据安全能力认证服务，确保数据买方的数据安全和隐私合规能力与其购买额度挂钩。引入数据担保、数据中介、数据资产质押融资、数据资产保险等服务，打造提供数据确权、数据估值、数据清洗、法律咨询、市场分析、尽职调查、安全审计等服务的第三方支撑生态。

三 | 物联网的数字信任解决方案

随着物联网的快速发展，在智能家居、智能工厂、可穿戴设备等各种场景下，海量的物联网智能设备在大规模部署和上云联网，网络边界的日趋模糊，针对物联设备的攻击和非法访问、非法控制成为重要的安全风险，同时，物联网设备的资源有限性放大了这些安全挑战，以及一些合法用户的不正当访问、使用。物联网环境下的身份验证、访问控制逐步成为物联网安全保障的关键。

物联网的数字信任方案，针对物联网设备计算能力、联网能力碎片化的特点，旨在通过多方式、跨域的物联网设备访问控制，以实现对物联网环境下设备每次访问流程控制，构建物联网环境下的数字信任。

● **基于 CMOS 芯片技术的 PUF 芯片：**利用 CMOS 技术设计、生产的 PUF 芯片具备随机性、唯一性、可验证性、一一对应性、防入侵特征等优势，能够在物联网设备的 ID 自动生成、密钥的生产与管理、设备识别验证等场景下带来很好的安全应用。

● **物联终端访问实时监控：**可对大量物联网设备进行快速监测与扫描，实现对物联网设备安

全状态的实时监控，及时发现其中的在线、离线、故障等状态异常情况。包括物联网终端脆弱性监测、终端异常接入安全监测等，通过形成硬件信息库，通过设备指纹识别与对比分析技术，一旦发现其中存在身份仿冒、非法接入等情况，可以快速进行预警，为用户分析、取证、管控提供技术支撑。

● **基于信任评估的动态访问控制：**通过对用户进行信任评估，确定用户的信任度并进行分组，进而即可根据其信任度和获得的角色对用户进行访问授权，能够更好地适应物联网分散、动态的环境。包括身份识别验证、权限授权审核、上下文监测、用户会话监控、用户信任度评估、根据用户信任度对用户角色进行权限指派等功能。

四 | 供应链金融的数字信任解决方案

供应链金融是指以核心企业为依托，以真实贸易为前提，运用自偿性贸易融资的方式，通过应收账款质押、货权质押等手段封闭资金流或者控制物权，对供应链上下游企业提供的综合性金融产品和服务。供应链金融对实体经济有着强大的赋能作用，这在改善中小微企业生存困境方面尤为明显。同时，由于供应链上下游数据共享、流通不足，以及中小企业数字化程度不高，使得传统金融机构的供应链金融业务，主要还是依赖核心企业的承诺或担保开展业务，占用核心企业授信额度。

供应链金融的数字信任解决方案以搭建“产业供应链普惠金融数字信任服务平台”为核心，主要通过大数据、人工智能、区块链、数字身份、电子签署等技术，打造支撑供应链金融的数字信任体系，旨在解决供应链金融企业间的信任和风控安全问题与中小企业融资难、成本高的困境，让金融机构能够更高效、便捷、稳健地服务于中小企业客户，确保借贷资金基于真实交易，同时依托核心企业的付款，使得整个产业链条上的企业都能融资，且是安全的融资。

● **云平台 + 数字身份：**通过云计算技术，将产业端的数据、文件等流程数字化，实现全线上 / 线上与线下混合的供应链管理平台，将供应链金融能力与服务嵌入进区块链产业供应链普惠金融服务平台中，实现供应链全流程随时、随地、按需获得供应链金融服务。由此通过科技手段，赋能、连接金融与产业端，并为两端进行匹配。同时，为供应链核心企业、上下游供应商、各类金融机构，匹配形成平台唯一的数字身份体系，由平台统一发放 CA 证书并进行更新服务，以确保各类主体的资格认证和访问控制。

● **区块链 + 电子签署：**通过连接产业端中的核心企业及其上下游供应商，以及多元化金融机构，包括银行、非银金融机构（信托、资管公司、保理公司、融资租赁公司等）、保险公司等。针对产业端实际的业务场景，与金融机构联合设计、开发“数字信任票据”金融产品，提供给供应链上的企业。同时，通过电子签署和数字签名技术，确保数字信任票据的时间效力和法律效力。

● **平台核心功能：**主要为产业核心企业作为系统核心通过金融机构（多方）合作获得授信后，将授信额度分配给产业链内核心企业成员单位，成员单位获得相应额度即可开具数字信任额度，数字信任票据用于向上游供应商进行业务结算；供应商收到数字信任票据后，如果不继续流转，账款到期日平台向供应商结算还款；同时，任何

一级持有者需要对其上游供应商进行支付账款，数字信任票据可以进行逐级转让，即债权转让，同时电子信票支持拆分部分转让；第三，任何一个持有方可以在平台发起融资，即反向保理业务。保理公司买入资产后，如果资金短缺，可将资产进一步卖出至金融机构，如银行、证券公司等，即再保理、ABS、ABN 业务。基于信用保证，核心企业一旦开具数字信任票据，到期刚性兑付。如果成员单位到期未还款，所属集团需为其垫款、代偿。整个系统基于此模式开展业务，底层具有系统化的区块链协议、数字身份确责、电子签署确保法律效力支撑。

五 | 医疗健康的数字信任解决方案

随着医疗健康行业的数字化转型，各类在线医疗 App 和应用蓬勃发展，由于医疗健康行业中患者疾患信息、医院诊疗信息、电子病历、电子健康档案、疫情信息等数据会涉及大量个人敏感信息，数据仿冒、篡改、泄露和滥用的风险日益加剧，并由此产生了患者个人权益侵害、互联网医疗的医生资格身份审核、在线处方效力确认、医患纠纷责任溯源等各种现实问题，对医疗健康行业的数字化转型带来了严峻威胁和挑战。

医疗健康的数字信任解决方案以“统一可信身份认证 + 数据全流程安全保护”为核心，通过数字技术解决在线医疗诊断主体的身份核实和医疗数据的完整性、机密性问题，以保障电子病历、电子健康档案等医疗数据全生命周期过程中的法律效力，以及在线医疗服务行为责任可追溯等问题，重构“医 - 患”在数字环境下的信任关系，形成支撑医疗健康数字化转型的数字信任体系。

- **可信身份认证：**医务人员可使用数字证书 USBKey、手机移动证书或人脸识别等多种方式登录医疗机构信息系统，获得对电子病历、电子处方等医疗数据的编辑、调取等权限。患者可通过移动终端查阅、手写签名等方式，对相应的医疗信息内容进行确认。此外，还可通过为医疗设备发放证书的方式，实现对各类医疗设备的身份认证。最终实现医院各类行为主体基于数字证书的身份认证服务、权限管理和访问控制等。签名和签章核心都是将医疗数据进行数字签名，以保证数据的不可抵赖性和完整性需求，并在查询相关数据时，实现用户对于所查询数据真实性的验证。
- **可信时间戳：**通过集成部署时间戳服务，可以证明各类医疗数据的有效性及产生时间，其核心是将经数字签名的一个可信赖的时间与特定医疗数据绑定在一起，实现两者时间保持一致。
- **数据安全共享：**医疗机构之间、医疗机构与全民健康信息平台间通过数据共享，以实现跨区域业务协同，实现远程医疗、分级诊疗等医疗服务。

PART 5
参考文献

[1][德] 尼古拉斯 • 卢曼 . 信任: 一个社会复杂性的简化机制 [M]. 瞿铁鹏 , 李强译 . 上海 : 上海人民出版社 ,2005 年 .

[2][美] 弗朗西斯 • 福山 . 信任: 社会美德与创造经济繁荣 [M]. 彭志华译 . 海口 : 海南出版社 ,2001 年 .

[3][法] 佩雷菲特 • 阿兰 . 信任社会 [M],. 邱海婴译 . 商务印书馆 ,2005 年 .

[4][美] 尤斯拉纳 • 埃里克 . 信任的道德基础 [M]. 张敦敏译 . 北京: 中国社会科学出版社 ,2006 年 .

[5][德] 马克斯 • 韦伯 . 儒教与道教 [M], 王容芬译 . 商务印书馆 ,2004 年 .

[6][德] 哈贝马 • 斯尤尔根 : 交往与社会进化 [M]. 张博树译 . 重庆出版社 ,1989 年 .

[7] 梁克 . 社会关系多样化实现的创造性空间——对信任问题的社会学思考 [J]. 社会学研究 ,2002(03):P.1-10.

[8] 蒋典阳 . “陌生人社会” 背景下社会信任的困境及重构 [J]. 甘肃理论学刊 .2018, 第 3 卷第 3 期 :P.112.

[9] 郭慧云 . 论信任 [D]. 浙江 : 浙江大学 ,2013 年 .

[10] 吴新慧 . 数字信任与数字社会信任重构 [J]. 学习与实践 .2020 年第 10 期 :P.87-96.

[11] 吕尧 , 周鸣爱 , 李东格 . 国际电子认证服务现状分析 [J]. 网络空间安全 ,2019,010(010):P.33-37.

[12] 胡传平 , 陈兵 , 方滨兴 , 邹翔 . 全球主要国家和地区网络电子身份管理发展与应用 [J]. 中国工程科学 ,18(6):P.99-103.

[13] 刘劲彤 , 吴勇 . 欧盟 eID 项目与面向未来的身份服务战略 [J]. 信息安全与通信保密 ,2012,000(011):P.124-127.

[14] 祝磊 . 美国电子签名法律制度研究 [D]. 湖南师范大学 .

[15] 陈徽 . 欧盟与美国电子身份管理立法比较研究 [D]. 暨南大学 .

[16] 周晓斌 . 电子政务电子认证关键技术研究 [D]. 华南理工大学 .

[17] 宋宪荣 , 张猛 . 国外网络可信身份认证技术发展现状、趋势及对我国的启示 [J]. 网络空间安全 ,2018,02(09):P.06-11.

[18] 田青 , 宋建彬 . 探讨生物特征识别在身份认证的应用安全 [J]. 中国信息安全 ,2019,No.110(02):P.86-87.

[19] 全国信息安全标准化技术委员会鉴别与授权工作组 . 电子认证 2.0 白皮书 (2018 版)[R].https://www.tc260.org.cn/front/postDetail.html?id=20180415235648.

[20] 中国信息通信院等 . 隐私保护计算发展报告 (2020 版)[R]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202011/t20201110_361696.htm.

[21] 公安部第三研究所 .eID 数字身份体系白皮书 (2018 版)[R]. https://eid.cn/eid2018.pdf.

[22] 亿欧智库 . 第三方电子合同行业研究报告 [R].http://pdf.dfcfw.com/pdf/H3_AP202007071390029775_1.pdf.

[23] 中国电子信息行业联合会等 . 电子签名与可信服务研究报告 (2019 版)[R].

[24]Gartner.Digital Trust — Redefining Trust for the Digital Era: A Gartner Trend Insight Report[R].May 31,2017.

[25]IDC.2020 China ICT market predictions to help Future Enterprises navigate digital transformation[EB/OL].Dec 16,2019.https://www.idc.com/getdoc.jsp?containerId=prCHE45745219.

[26]IDC.ICT Market Opportunities Arise Amid Headwinds as Digital Transformation Becomes New Normal[EB/OL].Apr 24,2020.https://www.idc.com/getdoc.jsp?containerId=prCHE46240020.

[27]Bhaskar Chakravorti,Ajay Bhalla &Ravi Shankar Chaturvedi.The 4 Dimensions of Digital Trust,Charted Across 42 Countries. Harvard Business Review.[EB/OL].February 19,2018.https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries.

[28]McKinsey.Digital Identification:A Key to Inclusive Growth[R].17 April,2019.https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#.

[29]German Marshall Fund of the United States.Ideas for Digital Democracy[R].November 19,2020.https://www.gmfus.org/sites/default/files/Tech2021%20Report%20Final.pdf.

上海市数字证书
认证中心有限公司

SICSI
CYBER RESEARCH INSTITUTE
赛 博 研 究 院

面向城市数字化转型的数字信任体系建设

出品方：上海数字证书认证中心有限公司
赛博研究院

2020.12