基于零信任和可信身份技术的个人信息保护方法探索

目前，相比欧美我国对个人隐私保护立法和监管更为严格，行业企业在监管要求和不同经营背景下，采用“各自为战”的个人信息采集和存储方式，带来了更大的信息安全风险和监管难度，运营商也面临同样困境。本文创新性地基于零信任模型和可信身份技术，结合我国实名制实施基础，设计并部分实现了在通信场景下的个人信息保护方法。

文丨**方宇 刘长波 景晓晨** 中国电信股份有限公司网络安全产品运营中心　　**曲子夜** 天翼安全科技有限公司

引言

信息技术快速发展，互联网已渗透到日常生活的各个方面，大量数据被记录，其中包含了丰富的个人信息，这些数据有助于理解用户需求和行为，提供个性化服务，数据要素参与经济运营已成为趋势。但个人信息的收集、存储、处理和使用面临诸多安全风险，一旦发生信息泄露、不当处理等情况，将侵害用户权益，破坏社会信任。

因此，如何在保障个人信息隐私和数据安全的前提下，实现个人信息的有效管理和使用，成为数字中国建设中面临的重要问题。

发展现状

实名制形成完备的治理体系

2012 年 12 月，《关于加强网络信息保护的决定》颁布，电话用户真实身份信息登记工作启动。2015 年 9 月，工信部、公安部、国家工商总局联合开展电话“黑卡”治理专项行动，实名制全面落实。2016 年 9 月，工信部等六部门联合下发《关于防范和打击电信网络诈骗犯罪的通告》，实名制向“实名 + 实人”迈进。我国实名制在“人用卡”领域已基本实现 100% 落实，形成了完备的治理体系；在物联网卡领域，也逐步扩展落实。

个人信息保护相关法律相继出台

相较其他国家和地区，我国对于个人信息保护与数据共享秉持更为谨慎的立法态度。近年来相继发布及更新 20 余部法律法规，形成了全面的个人信息保护监管体系。2022 年 12 月起执行的《中华人民共和国反电信网络诈骗法》规定：电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任，建立反电信网络诈骗内

部控制机制和安全责任制度，加强新业务涉诈风险安全评估。

零信任模型逐步应用

零信任模型是一种新兴的、具有前瞻性的信息安全架构理念，其设计核心是建立一种动态的、基于策略的、细粒度的访问控制机制，对每一次请求进行认证和授权。旨在通过消除信任前提、限制攻击面和强化检测响应能力来提高信息安全。零信任模型正被国内外企业、组织、政府机构及科研团队广泛研究和应用。

可信身份及可信通信技术逐步应用

可信通信是指在通信过程中，保障通信双方信息交换的可信性、保密性、完整性和可用性的一种通信方式。通信双方需要依靠多种技术手段进行身份认证、授权和加密解密等操作，以确保通信过程中参与者身份以及通信信息的安全和可靠性。近年来，可信通信研究与应用备受重视，已成为网络安全领域保障信息安全的重要手段。

问题

个人信息保护面临多项挑战

政府和企业因为拥有的大量数据成为网络攻击者攻击和窃取的目标，同时给监管也带来了更大的工作量和难度。为提高潜在竞争力，个别企业存在采取不当手段非法收集、无授权披露或出售个人信息等情形。个人信息安全意识不足，缺乏必要的防范措施和技能，使其更容易成为个人信息泄露的受害者。上述问题随着互联网、产业数据化的高速发展变得日益严峻。

电信业务经营者风险防控责任难以全面落实

关键基础设施运营者承担着保障社会公共利益和公民合法权益的责任，同时面临重大挑战：业务种类繁多，场景复杂，需求多样，如采取以业务条线的应对方式，资源需求大、管理成本高。此外，电信技术迭代迅速，新技术和新业务不断涌现，伴生新的风险，需持续制定配套的风险防控措施，保障业务的安全和稳定。

分析

基于零信任模型的通信模型

参考零信任模型，对通信行为进行分析，其本质是主体基于一定规则，通过系统对数据资源的访问。人与人之间的通信行为，可参考零信任模型，构建通信场景下的个人隐私保护方法。

电信通信场景分析

电信通信是指利用电子技术在不同的地点之间传递信息。在电信通信场景中，绝大部分场景以人作为通信主体，电话号码是参与电信通信的核心标识。根据《反电信网络诈骗法》的规定，电信业务用户必须提供真实身份信息。目前在我国电信通信场景中，电话号码本质是个人主体身份标识的强烈、清晰的映射，并且具备在短信、电话、网络电话、网络等系列通信场景中作为通用认证手段的良好基础。

电信网络诈骗的根因分析

《反电信网络诈骗法》指出：电信网

络诈骗是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。电信网络诈骗行为的本质是在主体间发生远程或非接触方式的电信通信场景下，利用参与通信主体之间对于对方身份无法进行直接确认，而被不法分子利用，进行身份的冒用欺骗，从而致使参与电信通信的另外一方或多方主体基于对其身份错误的认知，继而造成系列经济、声誉等方面的损失。因此，对于电信网络诈骗行为的预防和治理，根本在于基于通信主体和内容的、必要的、具有公信力与安全性的通信主体身份展示。

措施

总体思路

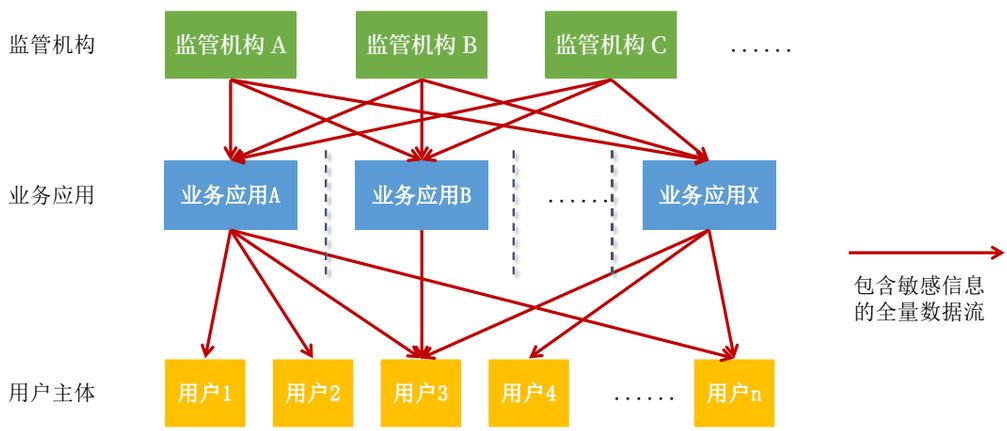
本文提出的电信通信场景下的个人隐私保护方法的总体思路：依托国家、各部门及电信业务经营者构建的实名制基础，在相关主管部门指导下采用可信身份技术手段及分段认证 + 集约管理的零信任模型机制，联合构建新型电信网络通信安全认证和身份展示架构，组织电信、互联网、金融等业务服务提供者，在电话、网络应用等场景全面应用。从架构角度进行优化设计，同时通过技术手段加强管理，以高效、高质量的方式和手段，进一步提高我国电信通信场景下的个人信息保护综合治理水平（仅讨论技术架构设计思路）。

方案设计

区别于目前各业务应用离散的“烟囱”式架构，提出“分层解耦”式通信场景个人隐私保护方法。

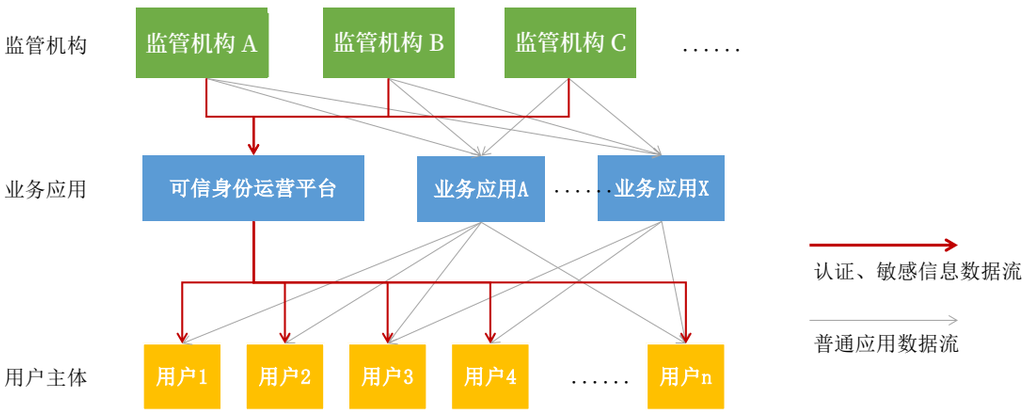
“烟囱”式架构：业务应用根据监管要求，各自负责实施实名制注册管理，全量个人信息数据的采集、保存、处理及数据安全保护职责。个人信息安全暴露面大，各条线监管机构工作触点多，难以实施高效管理（如图 1 所示）。

改进的“分层解耦”式架构：新建统一个人数字身份信息管理平台，一点对接公安、金融等数据，面向应用不直接



来源：中国电信股份有限公司网络安全产品运营中心

图 1 现行的“烟囱”式架构



来源：中国电信股份有限公司网络安全产品运营中心

图 2 改进的“分层解耦”式架构

提供个人信息，仅提供个人信息核验结果，以及向通信参与主体提供必要身份信息展示。各业务应用平台与可信身份平台对接，采用零信任架构，通过可信身份平台进行实名制注册及核验等。业务应用平台内仅使用应用身份标识进行管理和服务，不直接留存个人身份信息及个人影像等信息。监管工作相应地集中至可信身份平台的个人信息保护和数据安全管理，以及平台与业务应用单位的规范和审计，降低监管成本，提升监管效率（如图 2 所示）。

中国电信应用探索

中国电信积极探索，基于国密算法，在端到端通信场景下，研发推出“可信通信”产品。基于国密算法，提供端到端的可信身份录入、授权、认证、验证、展示及注销全流程能力，解决电信通信场景下的身份信任问题。参编 GB/T 43779-2024《信息安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范》国家标准（第二编制单位）。该实践已在广东 96110 反诈中心等千余家政府和企业客户商用验证，有效提高 B 端辨识度，降低采信成本，杜绝通信中身份伪造和骚扰泛滥，提升国家通信安全综合治理水平。

结论

本文创新性地基于零信任模型和可信身份技术，结合我国实名制实施基础，设计提出了“分层解耦”式模型架构，收缩个人信息暴露面，降低个人信息安全风险，提升监管效率，压降治理成本，经过理论分析与实践探索，印证了本方案的有效性。本方案在以下几方面有待进一步完善和细化：可信身份平台的数据安全保护，平台对接公安、金融、民政等各监管机关的数据，可结合联邦计算、数据加密等手段实现更全面的数据安全保障；探索对匿名服务等场景进行安全保护，需要联合用户和生态进一步结合场景进行方案的完善；相关监管部门的管理职责尚需国家及各部门联合逐步推进，完成国家级可信身份平台的建立和持续运营。

责任编辑：孙姗姗 zhouhl@staff.ccidnet.com