

附件 2

团体标准《5G 核心网信令数据的采集、处理、传输与隐私保护技术规范》编制说明

一、工作简况

（一）任务来源：2024 年 12 月，由重庆邮电大学牵头开始本标准的工作，于 2025 年 3 月广东省质量检验协会发布立项。广东省质量检验协会提出和归口，重庆邮电大学等单位共同起草，完成期限为 18 个月。

（二）协作单位：本标准由广东省质量检验协会提出并归口，参与起草单位有重庆邮电大学、深圳北理莫斯科大学、香港大学、澳门科技大学、广州波奇亚标准及检测技术有限公司、中国检验检疫科学研究院粤港澳大湾区研究院、中山市信裕科技有限公司、中山亿联智能科技有限公司、OrionAI Limited、中山市政达企业管理有限公司。

（三）具体分工：广东省质量检验协会作为本标准的牵头指导单位，主要负责本标准的总体工作方向、实施方案与基本框架的确认，重庆邮电大学作为本标准的主导起草单位，负责标准项目的策划组织和实施推进，按照标准制定程序实施标准研制，论证标准关

键内容，开展标准宣传推广普及等。深圳北理莫斯科大学、香港大学、澳门科技大学、广州波奇亚标准及检测技术有限公司、中国检验检疫科学研究院粤港澳大湾区研究院、中山市信裕科技有限公司、中山亿联智能科技有限公司、OrionAI Limited、中山市政达企业管理服务有限公司作为本标准的主要参与单位，负责组织行业专家开展标准的调研、起草、编制与论证工作，各协作单位利用各方发挥自身专业优势、人员优势，形成专业+标准的工作模式，全面确保标准的科学性、准确性、完整性与应用性。

二、立项的必要性

随着 5G 通信网络的广泛部署，信令数据在网络控制与管理中起到关键作用，但其隐私保护与安全共享面临严峻挑战。传统的加密与共享方法难以满足 5G 网络高并发、低时延、大规模数据处理的需求，且存在隐私泄露与数据篡改风险。本标准的制定旨在通过先进的加密技术与区块链分布式存储方案，统一信令数据隐私保护与共享的关键指标与技术规范，推动通信行业构建安全、高效、可控的数据管理体系，为 5G 网络安全与数据应用赋能。

三、标准框架和内容的确定

（一）标准框架

本标准结合我国现有政策、法规与标准，遵循和按照国家标准 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结

构和起草规则》的要求统一和规范标准的结构、表述规则、编排格式和制定程序，坚持市场导向原则，鼓励企业参与制定标准，提高标准的适用性；坚持国际化原则，积极采用国际标准，保持与国际并行的步伐；坚持科学严谨的原则，系统深入研究 5G 数据保护与共享的科学性。

（二）主要内容

本文件主要包括以下方面内容：

1. 范围。

本文件规定了面向 5G 通信网络的信令数据隐私保护与数据共享的技术要求、实验方法及技术规范。具体涵盖信令数据隐私保护技术、数据共享方法、加密与解密算法、数据存储与检索技术等方面内容。

本文件适用于面向 5G 通信网络的信令数据隐私保护与数据共享技术。包括针对信令数据的加密、解密、存储、传输及共享机制的实现与验证，也适用于通信设备制造商、网络运营商、安全服务提供商及相关研究机构在 5G 核心网信令数据处理系统设计、部署与验证中的技术研究。

2. 规范性引用文件。

规范性引用文件中列示了本标准引用的相关标准。本标准中引用了 9 个国家标准，均为推荐性标准。

3. 术语和定义。

为便于对本标准的理解和适用，本部分对标准中涉及的主要术语进行了定义。同时指明 GB/T 25069-2022、GB/T 22239-2020、ISO/IEC 27001:2013、3GPP TS 29.501 5G、Hyperledger Fabric、RFC 5246 TLS、ITU-T X.805、T/CCSA 20004-2018、RFC 8705 OAuth 2.0 界定的术语同样适用于本文件。

4. 信令数据保护与共享方法。

给出 5G 通信网络的信令数据保护和共享的技术方法，包括数据保护和数据共享的加密机制、技术流程和实现方法。确保信令数据在 5G 网络中进行加密保护的同时，也能够安全地进行共享与访问。

5. 技术要求。

给出 5G 通信网络的信令数据隐私保护与数据共享的技术要求。对主要基本要求、采集数据要求、隐私保护模型要求、共享模型要求、设备与系统要求做出规定。

6. 信令数据保护与共享流程。

给出信令数据保护与共享的操作流程，包括共享环境初始化、数据全生命周期保护流程以及数据共享协同流程，确保流程的可操作性与规范性。

四、与现行法律法规、强制性标准等上位标准关系

本文件符合国家现行法律、法规、规章和强制性国家标准的要求，本标准有助于国内相关法律、法规、规章和强制性国家标准的实施。

五、标准有何先进性或特色性

本标准在充分研究 5G 通信网络相关法律法规和标准化政策方向的基础上，在信令数据隐私保护与数据共享方面具有重大创新。一是**高效非侵入式加密**，结合同态加密与区块链技术，降低数据泄露风险，提升大规模数据处理场景下的安全性。二是**多层次保护**，支持从多维度实现数据加密与访问控制，以更全面地保障数据的隐私性和完整性。三是**多场景、多通道共享**，利用联盟链与分布式存储技术，提升数据共享的精度和效率。四是**高扩展性设计**，系统能够在多样化的网络环境中有效运行，显著增强数据保护与共享的适应性，提高系统在复杂场景中的适用性。

六、标准调研、研讨、征求意见情况

（一）项目启动。2024 年 12 月重庆邮电大学受委托承担了本标准的制定工作，联合深圳北理莫斯科大学、香港大学、澳门科技大学、广州波奇亚标准及检测技术有限公司、中国检验检疫科学研究院粤港澳大湾区研究院、中山市信裕科技有限公司、中山亿联智能科技有限公司、OrionAI Limited、中山市政达企业管理服务有限公司等高校及企业，成立标准编制工作组（以下简称工作组）。工

工作组明确了工作组的责任和要求，讨论和确定了详细的人员分工和工作计划，包括时间计划和流程规划。工作组开始广泛调研相关的法律法规和整理思路。

（二）广泛调研。2024 年 12 月，工作组广泛搜集、整理和分析相关的法律法规，国家、行业和地方标准，调研相关的技术文献，整理标准制定思路，形成标准的基本框架。

（三）形成征求意见稿。2024 年 12 月至 2025 年 1 月，各参编单位根据自身优势参与标准草案的不同部分编制工作，编制组召开 3 次标准讨论会，会上对标准草案的基本架构、主要内容和技术要求等内容进行反复讨论和修改。

（四）征求意见。2025 年 1 月，经过前期多次修改讨论，形成征求意见稿。征求意见稿在具有通信、安全相关领域研究和应用经验的高校、企业、行业协会和标准相关部门发送。截至 2025 年 3 月，收集汇总相关的意见 23 条，经主编单位分析后，采纳意见 21 条，部分采纳意见 1 条，未采纳意见 1 条。其中，未采纳意见主要包括与其它意见冲突等原因。“部分采纳”和“不采纳”的处理结果向意见提出单位进行反馈，最终达成一致。

七、技术指标设置的科学性和可行性

本文件的指标科学性和可行性体现为：一是**技术指标设置科学合理**。本标准是在充分分析国家标准、行业标准对数据隐私保护、共享

技术等相关要求的基础上提出 5G 信令数据保护与共享规范，并在此基础上开展了大量的加密算法与分布式存储技术的调研，结合相关数据得出的技术指标，不仅满足法律法规和标准要求，还结合通信行业实际，具有科学性。二是技术指标具有及时性和前瞻性。本标准从技术要求和数据共享的多个细节规范方面提出了适应当前网络安全需求和未来技术发展的技术指标，有助于引导 5G 信令数据隐私保护与共享技术的规范化发展，具有可行性。

八、与国际、国家、行业、其他省同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况。采标情况，以及是否合规引用或采用国际国外标准

截至目前，还没有面向 5G 通信网络的信令数据隐私保护与数据共享技术规范相关的国际、国家、行业、其他省同类标准。

九、涉及专利的有关说明

无。

十、专家审定会情况

/

十一、标准名称变更应详细说明理由并单独拟文申请

无。

十二、编制单位增减应予说明增减原因并单独拟文申请

无。

十三、其他应当说明的事项

无。

标准编制工作组

2025 年 3 月 10 日