GSMA | GTI

Mobile AI

面向智能体网络的信任范式演进

Trust Paradigm Evolution for Agentic Networks

© GSMA 2026。保留所有权利。

免责声明

本文件并非“行业规范”（Industry Specification），亦非由 GSMA 按照《GSMA AA.35 - 行业规范制定程序》（Procedures for Industry Specifications）的相关规定制定或维护。

本文件不代表 GSMA 的官方立场。尽管 GSMA 是本文件的发布方及所有者，但报告中所表达的观点和意见可能仅代表作者本人的立场，未必反映 GSMA 的观点。

本文件按“现状”提供，仅供参考。对于本文件所含信息的准确性、完整性或及时性，GSMA 不作任何明示或暗示的陈述、保证或承诺，亦不承担任何责任。用户使用本文件所含信息需自行承担风险；若因使用该信息而引发任何第三方索赔，由用户自行承担相应责任。对于因使用或依赖本文件而产生的任何直接、间接、附带、特殊、后果性或惩罚性损害，以及任何利润、收入、数据或商业机会的损失，GSMA 概不承担任何责任。

本文件未通过暗示、禁止反言或其他方式授予 GSMA 或任何第三方的任何知识产权许可。未经事先书面许可，本文件中的任何内容均不得被视为授予了使用 GSMA 任何商标的许可或权利。本文件中的任何内容均无意向任何第三方授予任何利益或权利。

GSMA 没有义务更新、修订或补充本文件。GSMA 可随时撤回或修改本文件，恕不另行通知。

反垄断声明

本文件所含信息系根据 GSMA《反垄断政策》（Antitrust Policy）编制：https://www.gsma.com/about-us/wp-content/uploads/2023/10/Antitrust_Policy_October_2023.pdf

摘要

在 AI 智能体快速发展的推动下，下一代智能网络正从连接人与物，逐步走向同时连接分布式智能。随着网络架构和业务范式的持续演进，网络环境中将越来越多地纳入分布式、智能化和异构的要素。这些发展在释放新能力的同时，也带来了安全、可信与治理方面的新挑战。零信任原则已在多种传统网络环境中得到应用，为网络安全架构的演进提供了有益参考；然而，随着自主实体越来越多地执行复杂任务、委托操作、调用网络能力，并在不同上下文和管理域之间开展交互，可能出现传统的以身份和访问为核心的实现方式所未能覆盖的额外信任与授权需求。

本白皮书重点关注两类场景：一是外部 AI 智能体（第三方 AI 智能体）调用运营商开放网络能力的场景；二是运营商内部 AI 赋能网络（AI for Networks）的场景，即网络 AI 智能体和 AI 赋能的网络功能参与网络运行、管理和编排的场景。

自智网络框架虽已支持意图驱动运行和闭环自动化，但智能体交互带来了新的要求，即确保被委托和不断演变的操作始终可信，并处于授权目标范围之内。为应对上述挑战，本白皮书面向智能体网络提出一种新的信任框架：MAIC-Trust 框架（以下简称 M-Trust）。该框架从三个相互补充的维度构建可信的智能体网络环境：

多方信任 Multi-party Trust	支持涉及多个相关实体和信任证据来源的信任评估，并可根据运行场景采用不同的信任建立方式。它为协同信任评估与治理提供基础，同时保留相关运营商及管理域的安全与策略权限。
智能体意图感知信任 Agentic Intent-aware Trust	聚焦智能体自身的可信性。它将传统身份验证机制扩展为身份验证与意图感知授权相结合的一体化模型，在授权决策中综合考虑授权目标、执行上下文、资源请求和风险状况，实现自适应授权。这一方式旨在增强安全性，同时避免不必要的运行开销。
跨域信任 Cross-domain Trust	面向跨异构网络和管理域的交互，在适用的运营商策略和安全要求下，支持信任证据的受控交换与评估。参与各方可据此为跨域交互建立和评估信任，同时保留对自身信任与授权决策的权限。

M-Trust 并非旨在取代零信任或现有的移动网络安全机制。它以相关零信任原则为基础，探讨如何对其加以补充，以应对未来移动网络中日益自主的智能体交互。

M-Trust 定位为面向智能体网络的参考框架和研究方向，而非标准规范或强制性实现。

目录

1 未来网络演进与新兴信任需求 …… 02
1.1 从连接人与物到连接智能 02
1.2 技术驱动：新架构带来新的信任需求 03
1.3 业务驱动：新兴业务带来新的信任要求 04
1.4 智能体网络演进中的信任考量 04
1.5 从传统信任到零信任架构 05
1.6 零信任架构的适用性与局限性 06

2 核心概念 …… 07
2.1 多方信任：多方参与和上下文感知的信任建立 08
2.2 智能体意图感知信任：意图感知授权与自适应策略管理 09
2.3 跨域信任：跨域信任与异构信任根 10
2.4 与零信任的关系 11

3 总体架构 …… 12
3.1 M-Trust 框架的安全性与韧性 12
3.2 架构概述 12
3.3 信任采集与评估层：数据基础与信任感知 13
3.4 策略决策层：策略评估与自适应调整 15
3.5 策略执行层：策略执行与响应 16
3.6 跨层协同与信任闭环 17

4 M-Trust 技术考量 …… 18
4.1 与现有运营商安全机制的关系 18
4.2 信任证据的保护与保障 19
4.3 信任评估与策略决策技术 19
4.4 智能体身份、委托与安全调用 20
4.5 跨域信任证据交换 20
4.6 新兴技术与特定用例技术 21

5 结论与未来展望 …… 22
5.1 结论 22
5.2 未来展望 22

6 缩略语 …… 24

7 术语定义 …… 25

8 参考文献 …… 26

GSMA

前言



Alex Sinclair
GSMA 首席技术官

1865 年，英国颁布了《机车法》，即广为人知的“红旗法案”。该法案规定，任何自行驱动的道路车辆行驶时，须有一人手持红旗在车前步行，提醒他人车辆驶近。立法初衷是管控一项新技术带来的风险，但这部法案也成为一个历久弥新的提醒：治理必须与创新同步演进。规则跟不上发展，就会阻碍进步；创新缺乏有效保障，就会削弱其规模化发展所需的信心。

人工智能正走到一个相似的转折点。生成式 AI 的风险主要在于它“说了什么”，而智能体 AI 的风险则越来越多地在于它“做了什么”。随着智能体开始规划任务、调用工具和 API、访问业务系统，并跨越组织与技术边界委派工作，信任已无法仅在单一模型或单一时间点的层面进行评估。

2026 年 3 月，GSMA 与 GTI 联合发布了《移动 AI 白皮书》，从 AI 赋能网络、网络赋能 AI、移动 AI 终端与智能体、移动 AI 应用四个维度，阐述了业界对移动 AI 的共同愿景，并将安全可信作为核心价值。本白皮书在此基础上更进一步，聚焦一个日益重要的问题：当网络不仅连接人与物，还开始连接能够自主采取行动的智能体时，信任应当如何演进？

现有的身份、认证与访问控制机制依然不可或缺。但仅仅知道智能体“是谁”或“是什么”已经不够。一个可信的智能体环境还必须能够判断：谁授权了某项活动，智能体被允许做什么，委派出去的行动是否仍与授权目标保持一致，以及随着情况变化，相关权限应当维持、收窄还是撤回。这并不意味着将运营商的权力移交给 AI，而是为运营商及其他获授权方提供更好的机制，以验证和管控 AI 在其环境中的行为。

本白皮书提出的 MAIC-Trust 框架，从多方信任、意图感知信任和跨域信任三个相互补充的维度应对这一挑战。该框架提出一种闭环机制：随着证据、行为和上下文的变化，持续重新评估信任与风险；同时，授权始终受运营商策略、监管要求以及适当的人工监督约束。

移动行业为这项工作奠定了坚实基础。SIM 卡在全球范围内建立了可信的身份与认证体系。漫游证明了信任可以跨越运营商边界延伸，同时每张网络仍保有对自身域的控制权。GSMA Open Gateway 正在为开发者打造一种通用、可编程的网络能力调用方式，使这些能力能够融入日益智能化、自动化的服务之中。随着智能体成为网络化服务的一部分，这些都是行业可以借鉴和延续的宝贵经验。

任何一家机构都无法独自构建可信的智能体环境。智能体将跨越网络、云、终端和应用运行。要避免碎片化，同时确保各个域对自身的信任决策保有自主权，开放、可互操作的方法至关重要。这需要运营商、科技企业、标准组织、政府以及更广泛的 AI 生态紧密协作。

信任不应成为挡在创新前面的那面红旗，创新也不应在缺乏有效保障的情况下贸然前行。我们的任务，是建立相应的框架、标准和共同实践，推动智能体技术从孤立的试验走向可信、可互操作、可规模化的部署。

在此，我谨向为本白皮书作出贡献的所有机构和专家致以诚挚的感谢。我也鼓励移动通信和 AI 领域的同仁以本白皮书提出的建议为基础，结合真实的运营需求加以检验，携手为下一代智能网络构建可信基石。

1 未来网络演进与新兴信任需求

1.1 从连接人与物到连接智能

通信网络的演进不断拓展信息交互和系统能力的边界。从历史上看，这一演进可分为三个主要阶段：



连接人

在早期几代移动通信中，网络主要承担信息传输基础设施的角色，其使命是实现个人之间的语音、文本和多媒体通信，打破地理阻隔，支撑人与人之间的交互。



连接物

随着 5G 和物联网（IoT）的兴起，网络逐步向连接设备和物理环境演进。传感器、工业系统和智能终端实现互联，使物理实体能够实时映射到数字系统中，支撑大规模态势感知。



连接智能

随着产业迈向 6G 和 AI 原生时代，网络与 AI 之间的交互可能沿两个相互补充的维度演进。GSMA 发布的《Mobile AI 白皮书》同样将 AI 赋能网络（AI for Network）和网络赋能 AI（Network for AI）列为移动 AI 的关键维度，并将安全可信作为移动 AI 发展的核心价值之一 [19]。

其一，网络赋能 AI（Networks for AI）使分布在云、边、端环境中的计算资源、AI 模型和自主智能体等分布式智能能够相互通信与协作。在这一角色中，网络为日益分布式的 AI 工作负载提供所需的连接和服务能力。

其二，AI 赋能网络（AI for Networks）是指在网络自身的设计、运行、管理和编排中越来越多地使用 AI 能力。在这一语境下，智能成为网络运维、演进的能力组成部分，而不仅仅是运行在网络之上的应用或服务。

这两个维度带来既有区别又相互关联的信任需求。对于网络赋能 AI，信任需要从传统的身份和通信信道，延伸到分布式模型、智能体、数据和计算资源之间的交互；对于 AI 赋能网络，信任还需要涵盖 AI 在网络运行和决策中的使用。因此，本文提出的框架探讨信任机制如何演进，以同时支撑网络之上的 AI 业务和网络内部的 AI 能力。

具体而言，本白皮书主要关注以下两类场景：一是外部 AI 智能体调用运营商网络能力的场景，例如第三方 AI 智能体通过 GSMA Open Gateway 等开放接口请求访问运营商开放的网络能力；二是运营商内部 AI 赋能网络的场景，即网络 AI 智能体和 AI 赋能的网络功能参与网络的运行、管理和编排。前者是网络赋能 AI 维度下智能体与运营商网络交互的典型形态，后者对应 AI 赋能网络维度。后续各章的信任需求分析和框架设计均围绕这两类场景展开。

1.2 技术驱动：新架构带来新的信任需求

未来通信网络预计将在拓扑结构、运行智能化和部署范围上经历重大结构性变革。三个相关趋势分别是部署日益分布化、智能化应用不断深入以及异构融合。这些发展共同挑战了依赖固定边界和静态身份验证的传统安全假设。

分布式云与边缘架构

随着计算能力越来越多地分布于云和边缘环境 [1]，安全与信任边界的位置和性质也可能随之变化。然而，去中心化程度因网络层级和部署场景而异，在网络互联等领域，清晰界定的边界依然重要。因此，信任机制需要根据架构和用例，同时支持既有的基于边界的安全控制，和更加分布式、能够持续自适应的安全控制方式。

智能化架构

智能体预计将成为网络功能和用户设备的重要组成部分 [2]。网络实体将从单纯被动执行的单元，演进为具备不同程度感知、推理、协作和自主决策能力的智能实体。在这一环境中，身份验证依然必要，但可能需要辅以对智能体行为、授权决策、执行上下文、计算完整性和多智能体协作的评估。

异构融合网络

未来陆地、空中、卫星和海洋一体化网络将融合多样化的通信系统、协议、治理模式和信任域。异构的安全策略、动态的连接条件和跨域交互，使这类环境的复杂性显著提升。因此，信任架构可能需要支持信任证据在允许的管理边界之间受控交换与评估，同时在多变的运行条件下保持连续性和韧性。

综上所述，架构演进在提升网络能力的同时，也暴露出现有安全框架的局限性。现有信任与安全机制可能需要加以补充，以应对日益自主、分布式和跨域的交互。未来的信任框架应在支撑这些交互的同时，保留既有的运营商安全控制、管理权限和监管边界。

1.3 业务驱动：新兴业务带来新的信任要求

除架构演进外，新兴业务场景也在重塑信任要求。ITU 为 IMT-2030 定义了六大应用场景 [3]，其中三个是对现有 IMT-2020 场景的延伸，另外三个是面向未来的全新场景。其中，以下三个尤为重要的未来业务领域，预计将催生新的信任需求：

人工智能与通信

随着 AI 深度融入通信系统，信任关系将不再局限于人与设备，而是越来越多地延伸至 AI 赋能的网络功能、服务和自主智能体，包括自主智能体之间以及人与智能体之间的交互。由于越来越多的决策由智能体自主完成，系统需要在无需人工介入每次交互的情况下，支持异构智能体之间的身份识别和意图对齐。鉴于 AI 模型可能存在不透明性，需要建立适当机制，使关键的自主决策能够被追溯、评估，并在必要时由相关方进行审查。

通感一体化

通感一体化系统使网络不仅能够传输信息，还能够观察、理解物理环境并与之交互 [4]。这在显著拓展网络能力的同时，也带来了需要妥善应对的额外隐私与安全问题。未来的信任框架必须为感知数据的全生命周期提供保障，包括采集、存储、处理、共享和销毁。通感系统应支持适当的授权、目的限定、访问控制和数据治理机制，使数据能够在多个相关方之间安全使用，同时保护敏感信息 [15]。

泛在连接

未来通信环境需要支持陆地、卫星、空中、海洋和专用网络之间的无缝交互。用户、设备和智能体可能跨越组织、技术和地理边界移动。这些场景可能需要相应机制，使相关凭证和信任证据能够在允许的域边界之间安全传递和评估。在一个域中建立的证据可以为另一个域的决策提供参考，但是否采纳仍取决于接收域的策略、安全控制和监管义务。基于 SIM 和 eSIM 凭证以及网络认证的运营商锚定身份，为信任的可移植性和跨域协作提供了可信基础。这一基础可通过 GSMA Open Gateway API 等标准化接口加以扩展，并在适当情况下辅以联邦身份框架。

1.4 智能体网络演进中的信任考量

自智网络（autonomous networks）的演进，已经引入了意图驱动运行、AI 辅助决策和闭环自动化，以改进网络和业务管理。M-Trust 无意取代或重复这些能力，而是着眼于信任与授权挑战，这一挑战随着自智网络功能向智能体化运行演进而日益突出。

在智能体网络中，一个授权目标可能需要通过多个自主操作来实现，包括任务分解、委托给其他智能体、调用网络能力，以及在不断变化的执行上下文中进行交互。因此，安全问题不再仅限于自智系统能否达成预期的运行结果。运营商还需要判断所涉及的实体是否始终可信，以及执行过程中所选择的操作是否始终处于授权目标、适用的运营商策略和已授予权限的范围之内。

因此，M-Trust 通过支持持续评估智能体操作在目标分解、委托和执行过程中是否始终可信且经过授权，对自智网络运行形成补充。信任、风险或上下文的变化，可能引发在现有运营商安全与管理权限范围内的有限调整、额外验证或由运营商控制的干预。

1.5 从传统信任到零信任架构

传统网络安全通常较多依赖基于边界的信任模型。该模型通过划分网络安全域，并利用防火墙、虚拟专用网络、网络分段和接入控制等机制，对跨越安全边界的访问进行保护和限制。在这类模型中，网络位置和边界通常具有较高的信任权重，已经进入可信网络域的实体可能被赋予一定程度的隐式信任。

在移动通信网络中，信任关系也长期建立在明确的身份、凭证、预先配置的安全关系和运营商管理边界之上，例如以订阅关系、身份凭证和接入认证机制为基础的用户与设备信任，运营商之间基于漫游和互联关系建立的跨域信任，以及不同网络功能之间依据既定安全关系和运营商策略所建立的信任。在网络架构相对封闭、管理边界较为明确的环境中，这些机制为移动通信网络提供了有效的安全基础。

然而，随着网络云化、服务化、能力开放以及多方协作的发展，传统网络边界逐渐变得更加复杂，单纯依赖网络位置或预先建立的信任关系已难以充分应对不断变化的安全风险。一旦攻击者突破边界或获得合法身份凭证，可能进一步尝试访问其他内部资源或进行横向移动。同时，传统安全模型往往更加依赖初始接入或连接建立阶段的认证与授权，对会话建立之后主体行为、执行上下文和风险状态的持续变化考虑相对有限。


Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

零信任正是在这一背景下发展起来的一种安全范式。

零信任概念由 Forrester Research 分析师 John Kindervag 于 2010 年系统提出。2020 年，美国国家标准与技术研究院（NIST）发布了 SP 800-207《零信任架构》[5]，定义了抽象的零信任架构，并描述了其逻辑组件和部署模型。基于 NIST SP 800-207 及后续研究，零信任可概括为以下三项基本原则：

以身份为中心的安全

零信任将身份置于安全控制的核心。访问决策需要对相关主体及设备或工作负载进行适当的认证和授权，并结合适用的上下文信息。

在运营商网络中，这一原则同样适用于网络自身，而不仅限于使用网络的实体。在 5G 服务化架构中，网络功能之间的通信通过既有的认证、授权和接口安全机制加以保护，用户凭证和接入认证则通过相关 3GPP 流程加以保护。将以身份为中心的控制延伸至运营商间互联、网络管理与运维访问以及网络设备保障，可使运营商在其提供的服务和承载服务的基础设施上一致地应用零信任。

最小权限

最小权限原则确保实体仅被授予完成特定任务所需的最低权限。通过限制访问权限的范围，零信任降低了“横向移动”的可能性，并将安全事件的潜在影响降至最低。风险和上下文可用于收缩权限或施加附加条件。任何控制的放宽都应保持在明确定义的策略和授权边界之内。

持续监测

零信任持续监测系统行为、流量模式和运行状态，以识别异常和新出现的威胁。通过实时监测和自适应访问控制，该架构能够持续评估和缓解安全风险，支撑及时的安全响应和运行韧性。

通过上述机制，零信任将安全从传统的基于边界的防护，转变为由身份和行为验证驱动的持续防护。其原则已应用于多种云原生架构、虚拟化环境和多租户平台。

1.6 零信任架构的适用性与局限性

零信任在电信网络中的适用性已得到广泛探讨。例如，3GPP TR 33.894 研究了部分零信任安全原则在移动网络中的适用性 [6]，TR 33.794 则研究了相关使能技术，包括如何开放数据以支持安全评估与监测，以及动态策略的执行机制 [7]。这些研究表明，零信任原则对于加强电信网络安全具有现实意义。然而，相关工作主要停留在研究和使能机制层面，零信任尚未成为 5G 系统全面的规范性安全架构。

尽管具备上述优势，现有零信任架构主要是面向用户、设备、工作负载和资源访问而设计的。随着网络向以智能体为中心的环境演进，呈现出自主决策、动态协作、工具调用、权限委托、持久记忆、概率推理和跨域交互等特征，零信任的若干局限性逐渐显现。

持续信任评估的可扩展性与效率

零信任支持持续监测和策略评估，并基于最小权限原则，在策略和上下文要求时进行重新认证或重新授权。这些原则在 AI 智能体环境中依然重要，因为自主智能体可能与多个服务、工具和其他智能体动态交互。然而，对智能体的每一次高频交互统一采用传统的验证和策略评估机制，可能带来计算和通信开销，且在时延敏感场景中难以高效扩展。因此，挑战不在于放宽最小权限或验证要求，而在于使信任评估更具自适应性、上下文感知能力和风险感知能力，从而能够根据身份、授权目标、执行上下文、所请求的网络能力及相关风险，动态施加适当的安全控制。

对概率性的智能体行为施加确定性安全控制

AI 智能体依赖概率推理，受模型特性、可用数据、任务上下文以及与外部工具和环境交互的影响，其具体决策和执行路径往往无法事先预测。这种不确定性并未降低对确定性安全控制的需求，反而凸显了清晰界定的授权边界、最小权限访问以及对智能体行为的“可约束能力”的重要性。然而，仅基于身份和预定义访问条件的静态规则，可能缺乏足够的上下文来评估动态生成的操作和不断变化的风险状况。因此，挑战在于将确定性的策略执行与持续的、可感知上下文、意图、风险的信任评估相结合。在这种方式下，自适应信任信号可用于判断访问是被授予、受限、上报以待额外审批，还是被拒绝；而最终的安全决策始终可执行、可审计，并受预定义治理边界的约束。

跨移动网络信任域的适应能力有限

未来移动网络预计将支持越来越多的自主 AI 智能体，在网络功能、边缘与云环境、服务平台以及多个管理域之间运行。对运营商而言，此类交互必须在清晰界定的安全、策略、监管和管理边界内进行。传统零信任方法通常应用于既定的组织或信任域内，策略决策由负责该域的权威机构管理。随着智能体能力日益分布化，并在运营商、企业、云和服务提供商环境之间交互，跨越这些边界建立和评估信任变得愈发复杂。因此，未来移动网络需要相应机制，能够在允许的域边界之间建立和传递可验证的信任上下文，同时保留各参与域的策略权限、监管义务和安全控制。

2 核心概念

传统零信任架构建立在三项基础原则之上：以身份为中心的安全、最小权限和持续监测。这些原则为现代网络安全奠定了坚实基础 [8]。然而，在未来电信网络中引入智能体能力，可能带来更高程度的网络运行自主性、更加动态的业务交互、分布式协作以及跨域协调。鉴于电信网络作为关键基础设施的地位，这种自主性必须在清晰界定的安全、策略和治理边界内运行。GSMA 的安全工作还将生成式人工智能（Generative AI）和智能体人工智能（Agentic AI）确定为移动生态系统中需要持续关注安全问题的新兴领域 [16]。由此产生了额外的信任需求，包括在保持确定性授权边界、最小权限访问、可归责性和运营商控制的同时，持续评估智能体的身份、意图、上下文和风险。

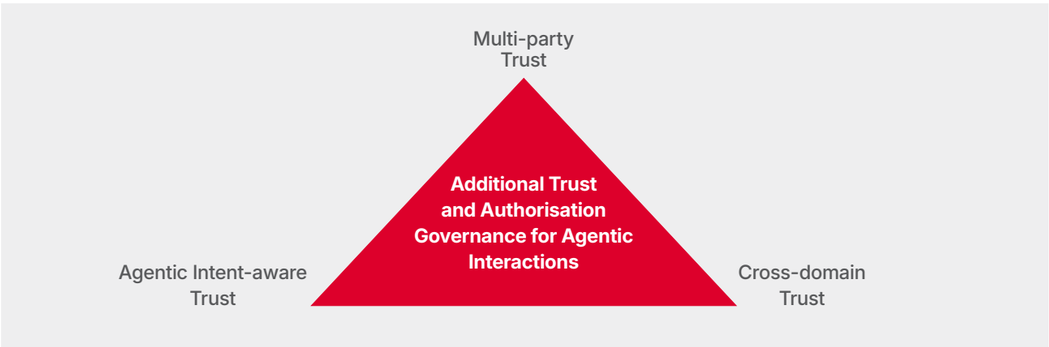


图 1：M-Trust 对零信任的扩展

如图 1 所示，MAIC-Trust（以下简称 M-Trust）对零信任的基础原则进行了扩展，引入了三个新的维度：

多方信任：支持相关的多方证据和与上下文相适应的信任建立。

智能体意图感知信任：支持意图感知授权和有限制的策略自适应。

跨域信任：支持信任锚与信任证据，以及在允许的管理边界之间受控交换证据。

这三大维度协同作用，为下一代智能通信网络提供可扩展、自适应、协同的信任保障。

2.1 多方信任：多方参与和上下文感知的信任建立

多方信任面向以下场景：相关信任证据由多个获授权方分别持有，或任何单一参与方都无法掌控完整的信任关系。它支持多方共同提供证据，并采用与上下文相适应的信任建立方式，同时保留各运营商的策略与授权权限。

在本白皮书中，多方信任是指联邦式多方信任证据与评估，以及上下文感知的信任建立 [9] 二者的结合，为分布式协作提供基础。

联邦式多方信任证据与评估

在多运营商和跨域的电信环境中，相关信任证据可能分布于运营商、漫游与互联合作伙伴、边缘服务提供商、应用提供商、企业客户以及其他获授权的参与方。例如，归属运营商（Home MNO）可能持有身份及签约相关证据，拜访运营商（Visited MNO）可能观察到本地网络行为，边缘提供商可能提供工作负载或平台证明（attestation），应用提供商则可能提供有关智能体软件完整性、受委托权限及所执行任务的信息。

多方信任评估的目的，并不是要求所有参与实体得出相同的信任判断，也不是用一个全局聚合的单一信任结果取代单一信任权威。相反，获授权方可以提供可独立验证、限定用途且有时效约束的信任证据。各运营商保留对自身信任与授权决策的控制权，并根据其业务上下文、安全策略、监管义务、风险偏好以及与请求方的关系，对可用证据进行评估。

因此，外部证据应被视为运营商本地策略决策的输入，而非替代。证据可根据其来源、完整性、时效性、相关性、独立性及其来源的保障等级进行验证和加权。根据所请求操作的风险，证据也可能触发受限访问、额外验证、人工或运营商审批、隔离或拒绝。

然而，增加更多的证据提供者也会带来额外的风险，包括评估者受损、针对信任证据进行协同或串通操纵、证据相关性、信息滞后以及对聚合机制的操纵。相关实现方案应保障所提供证据的真实性、完整性、时效性与独立性，支持撤销机制与可审计性，并保留安全可靠的本地策略执行能力。在独立的市场参与者之间交换信任证据时，还应采取适当的保障措施，防止交换具有竞争敏感性的信息，或利用共享的信任机制不公平地排斥第三方。

在参与方、故障假设、决策范围和治理规则均已明确确立的情况下，共识机制可能适用。但不应假定共识机制能够在所有运营商或业务之间产生普遍适用的信任结果。

上下文感知的信任建立

未来移动网络中的不同交互，可能需要采用不同的信任建立方式。例如，在单一运营商管理域内，AI 智能体与网络功能之间的交互，可主要依赖运营商控制的身份、策略和授权机制。当第三方 AI 智能体请求访问开放的网络能力时，可能需要获授权外部方提供额外的信任证据或背书，并须满足运营商的安全、策略和监管要求。在多运营商或其他联邦场景中，由于没有任何单一运营商掌控完整的信任关系，可能需要联邦式或分布式信任机制，以在参与域之间建立可验证的信任。因此，上下文感知的信任建立并不意味着动态替换底层的运营商安全架构，而是根据所涉实体、管理边界、风险等级以及适用的策略和监管要求，采用相应的信任建立机制。

2.2 智能体意图感知信任：意图感知授权与自适应策略管理

智能体意图感知信任面向下一代智能体网络架构而设计，以身份验证与意图感知授权作为其基础机制。通过综合考虑任务目标、执行上下文、资源请求和风险状况，智能体意图感知信任能够实现动态安全决策。在该框架中，“意图”是指明确表达的目标或任务预期，涵盖了相关的目标设定和约束条件。智能体为实现该意图而衍生出的操作，仍需单独接受授权和策略限制。该框架通过两项相互补充的能力，应对智能体自主、动态的交互特征。该框架并不假定智能体未来的操作能够被完全预测，而是持续评估可观测的信任信号、所声明的意图、执行上下文和风险状况，为安全决策提供依据。智能体操作始终受预定义且可执行的安全与策略边界约束；当信任证据不足或风险超出可接受阈值时，将施加额外验证、权限收缩、上报或拒绝等措施。

意图感知授权

现有访问控制机制能够支持动态的、基于策略的决策。智能体意图感知信任还会考虑智能体特定的上下文，包括授权目标、委托链与调用链、执行上下文以及观测到的行为。

在多智能体环境中，智能体会根据任务条件的变化调整计划、提出不同操作，其行为因而可能是动态的。然而，这种调整绝不意味着智能体可以自主扩大其授权范围。在电信网络中，尤其是当操作可能影响敏感数据或关键网络功能时，任何超出智能体现有授权范围的“拟定”操作，都应在执行前接受额外的策略评估，并在必要时获得批准方可执行。因此，授权决策应持续评估授权目标、所请求操作、执行上下文与实际资源使用之间的一致性，并根据不断变化的信任和风险状况动态调整授权。智能体可以调整其执行计划，其有效权限也可在预定义的策略、任务、风险边界内自动调整，但智能体本身不应能够自主将其权限扩大到这些边界之外。

该框架持续评估任务上下文、调用链、资源请求、可观测的行为特征和风险信号，以判断所请求的操作是否仍与授权目标及适用的安全策略保持一致。对于处于预授权策略范围内的低风险操作，系统可自动授予执行所需的、在时间和范围上均有限定的最小权限。随着信任或风险状况的变化，这些权限也可能被收缩、撤销或附加额外验证。

对于超出预定义授权范围的操作，尤其是跨域访问敏感数据、核心网配置变更或其他高影响操作，应触发新的授权决策。根据适用的运营商策略和风险等级，可能需要明确批准、附加约束，或予以拒绝。

自动化与自适应策略管理

自动化与自适应策略管理聚焦于在运营商定义的治理、安全和监管边界内，实现信任策略执行的自动化和动态调整。它并非让整个策略生命周期完全自治，而是使策略及相关控制措施能够根据不断变化的信任、风险和运行状况进行选择、应用和调整，而策略权限和治理始终由运营商掌控。

传统策略管理方式高度依赖人工配置和定期更新。与之不同，智能体意图感知信任会持续采集环境信息（包括风险状况、数据敏感等级和任务紧迫程度），以及智能体行为信息（如合规历史、任务完成记录、任务执行表现、历史行为一致性、异常活动频次和网络资源使用模式）。这些输入被汇聚形成动态的信任与风险评估。基于这些评估，并结合授权目标、执行上下文、网络能力与资源敏感度以及运营商定义的策略约束，系统可在预定义的策略边界内自动选择、应用或调整

访问控制条件和风险缓解措施。在满足适用的基线安全和授权要求的前提下，较低风险的操作可采用简化的验证流程；而涉及敏感网络能力与资源或跨域交互的高风险操作，则可能触发增强验证、细粒度授权和持续审计，或在必要时触发由运营商控制的额外审批。

策略并非一成不变。当环境条件变化、风险上升或出现异常行为时，系统可在运营商定义的约束范围内，自动加强监测、收窄授权范围并触发额外保障措施。通过风险状况与策略执行之间的这种动态同步，智能体意图感知信任能够提升对运行条件变化的响应能力，同时保留运营商的策略权限、安全控制和适用的监管要求。

2.3 跨域信任：跨域信任与异构信任根

跨域信任面向在允许范围内的，跨越管理域或安全域边界的智能体交互。它支持信任证据的受控交换与评估，同时保留各参与域的信任锚、策略权限、安全控制和监管义务。

异构信任锚与信任证据

信任锚是在移动网络中建立信任的重要基础。现有的基于硬件的、由运营商控制的信任机制，包括基于 UICC/eUICC 的凭证、安全元件、硬件信任根和基于 PKI 的机制，仍然是移动网络安全的根本。智能体网络并不会消除对这些机制的需求。相反，网络 AI 智能体、AI 赋能的网络功能、第三方 AI 智能体与外部管理域之间日益多样的交互，可能要求运营商在既有的认证、授权和安全控制之外，评估更多形式的信任证据。

因此，M-Trust 支持异构的信任基础，即根据参与实体、管理域、所需保障等级、风险、运营商策略和适用的监管要求，由不同的信任锚、凭证和验证机制共同为信任评估提供支撑。硬件支撑的信任锚可为凭证及其他安全关键资产提供强有力的保护；在运营商策略允许使用的场景和保障等级下，具备适当保障的软件机制可提供补充，但在需要硬件级保护的情况下，不应将其作为硬件保护的替代方案。包括数字签名、完整性保护及其他密码学证明在内的密码学机制，为验证身份声明、数据完整性、来源或其他信任证据提供了手段，但不应将其视为可脱离底层硬件或软件信任基础而独立存在的替代方案，因为其凭证和执行环境可能依赖于这些信任基础。

在跨多个管理域的交互中，如果没有任何单一参与运营商掌控完整的信任关系，可考虑采用额外的联邦式或分布式信任机制。其作用是支持信任证据在允许的域边界之间交换或验证，而非取代各参与运营商既有的信任锚、PKI、认证机制或安全权限。任何此类机制均须满足各相关域的策略、安全、管理和监管要求。

例如，网络 AI 智能体与单一运营商域内网络功能之间的交互，可主要依赖运营商控制的身份、凭证、授权，并在需要时依赖硬件支撑的信任机制。请求访问开放网络能力的第三方 AI 智能体，可能还需提供运营商认可的可验证信任证据。当交互跨越多个运营商或管理域时，各参与域可建立交换或验证信任证据的机制，同时各自保留对自身网络能力和安全策略的权限。因此，适用的信任基础由运营商的安全架构和交互要求决定，而不是由 AI 智能体自主选择或替换。

跨域信任建立

未来移动网络中的智能体交互可能跨越多个管理域和安全域，例如第三方 AI 智能体与运营商开放的网络能力交互，或网络 AI 智能体和网络功能在运营商域或服务提供商域之间交互。跨越此类边界，并不意味着各域无需再施加自身的信任、安全和授权控制。真正的挑战在于，使相关的信任与授权上下文或声明能够在允许的域边界之间安全传递和评估，而无需每个域从头重建全部信任上下文。

因此，跨域信任建立可依托以下三项相互补充的能力：

可互操作的信任凭证与证据

跨域信任验证机制

信任与授权上下文的连续性

在运营商场景中，请求访问开放网络能力的第三方 AI 智能体，可出示由另一可信域签发或背书的可验证身份、信任、授权或合规证据。同样，运营商域之间的交互可能需要将相关的信任和调用上下文跨管理边界传递。接收方运营商在授予网络能力或资源访问权限之前，依据自身的运营商策略、安全控制、风险评估、授权要求和适用的监管义务对这些证据进行评估。

跨域机制可在交互跨越允许的域的过程中保留相关的信任与授权上下文，在保持域间隔离的同时减少不必要的重复信任建立。因此，在一个域中建立的信任不会被另一个域自动继承，跨域信任也不意味着授权可以在全局范围内转移。各参与运营商或管理域对接受哪些外部信任证据、如何评估这些证据以及授权哪些网络能力（如有）保留决定权。

2.4 与零信任的关系

M-Trust 并非旨在取代零信任或现有的移动网络安全机制。它以相关零信任原则为基础，包括摒弃隐式信任、遵循最小权限访问、实施持续验证和基于策略的授权，并探讨如何针对未来移动网络中日益自主的智能体交互对这些原则加以补充。

引入网络 AI 智能体、AI 赋能的网络功能和第三方 AI 智能体，并不会取代现有的用户、设备、应用或网络功能，而是带来了新的交互模式：智能体可能规划和执行操作、委托任务、调用其他智能体、代表用户或应用行事，并在不断变化的执行上下文中请求访问网络能力。这些特征可能要求运营商不仅评估身份、设备和资源访问信息，还要评估授权目标、委托链与调用链、所请求的网络能力、观测到的执行行为、信任证据及相关风险。

因此，M-Trust 在以下三个方面对零信任方法形成补充：

01

将持续评估延伸至判断智能体所请求和所执行的操作，在可能包含多个步骤的调用链中，判断这些操作是否始终与授权目标保持一致。

02

基于智能体特定上下文、信任证据、观测到的行为和风险，支持自适应授权和策略执行，同时保持最小权限和运营商定义的策略约束。

03

支持信任证据在允许的管理边界之间以受控的方式交换和评估，同时各参与运营商或管理域保留对自身信任决策、网络能力和安全控制的权限。

M-Trust 中的跨域信任并不意味着普遍信任、将授权决策从一个域转移到另一个域，或依赖单一信任权威。从另一个域获得的信任证据可以为本地决策提供参考，但仍须依据接收域的策略、分层安全控制、保障要求和适用的监管义务，接受独立的验证和评估。

因此，应将 M-Trust 理解为一种拟议框架，旨在通过引入额外的信任上下文、证据、评估和治理机制，增强现有的身份、认证、授权及策略机制，从而支持未来移动网络在许可边界内、与外部及跨边界进行的自主交互。

3 总体架构

3.1 M-Trust 框架的安全性与韧性

M-Trust 旨在增强而非取代或集中化现有的运营商认证、授权、策略执行和特定域安全控制。因此，不应将其逻辑功能理解为需要一个单一的集中式信任权威，或一个关乎整个网络安全的单一决策点。信任评估和执行可按照网络、业务和管理边界进行部署，而在每个域内，相关的运营商安全控制和策略权限始终具有最终决定权。

M-Trust 功能及其处理的信任信息本身就是安全关键资产。因此，其实现应考虑：保护信任证据和策略信息免遭未经授权的修改，M-Trust 功能之间适当的认证与授权，职责分离与最小权限，安全的接口与通信，可审计性，以及在单个组件被攻破或不可用时的韧性。一个 M-Trust 功能或信任域被攻破，不应自动导致对其他网络域的信任或访问授权。此外，实现时应考虑适当的故障隔离与影响范围控制，使单个智能体或 M-Trust 功能的异常、失效或被攻破能够被限制在有限范围内，避免引发跨功能或跨域的级联故障。

上述原则使 M-Trust 能够为智能体交互提供额外的信任上下文和评估，而不会形成通用信任权威机构，也不会削弱底层移动网络的分层安全控制 [13]。

3.2 架构概述

M-Trust 旨在为未来智能通信网络建立一个可演进、可验证、可互操作的信任框架。传统信任模型主要关注身份验证和访问控制，与之不同，M-Trust 将信任评估视为依赖于上下文的过程，并针对相关的智能体交互进行持续的重新评估。信任评估结果作为可计算、持续演进且自适应的系统属性进行管理，可为智能安全决策提供支撑。

为实现这一目标，该框架依据以下三项基本架构原则进行设计：

分层协同 —— 不同信任功能独立运行，同时在整个架构中保持紧密协调。

有边界的自动化 —— 信任评估和策略调整可在预定义的运营商治理、安全和授权边界内实现自动化。

闭环反馈 —— 在运营商定义的治理和安全边界内，信任评估与策略执行通过监测和基于风险的调整持续互动。在运营商策略允许的情况下，常规调整可以自动完成；而较高风险、异常或涉及策略敏感性的决策，则可能需要额外验证，或上报至由运营商控制的监督或人工监督。人工监督应基于风险进行设置：对于预定义策略边界内的常规操作，不宜在每次交互中引入同步的人工审批，而可通过异步监测、审计和抽查等方式实施监督；人工或运营商审批主要设置在策略边界变更以及高影响或异常操作等关键节点，以避免人工环节成为智能体交互的性能瓶颈。在需要时，始终保留人工干预能力，用于审查、否决、暂停或批准与安全相关的决策。

基于上述原则，M-Trust 架构划分为三个功能层：

信任采集与评估层

数据信任指标采集（DTIC） 分布式信任评估（DTE）

策略决策层

策略智能体（PA，策略决策与验证功能）

策略执行层

策略执行智能体（PEA）

三个层级通过定义的接口交换信任信息。为支持在网络功能、网络 AI 智能体和管理域之间实现可互操作的部署，可能需要制定标准化的接口定义和信任信息交换格式，以及统一的信任证据分类体系与语义定义。任何关于信任信息的交换均须遵守适用的法律、法规及政策要求，包括有关数据保护、数据传输和竞争法的要求。这些交互共同支撑端到端的信任管理生命周期：DTIC 负责采集和保护信任相关数据；DTE 执行信任评估和风险分析；策略决策功能根据信任和上下文信息，确定并验证适用的策略和授权条件；PEA 则根据策略决策执行安全控制和执行动作。通过这一架构，M-Trust 能够在高度分布式、不确定且动态变化的环境中支持持续的信任管理。

3.3 信任采集与评估层：数据基础与信任感知

信任采集与评估层是整个 M-Trust 架构的基础，其目的是采集与信任相关的证据，建立可信的观测，并生成信任评估结果，为上层的策略决策提供支撑。

数据信任指标采集（DTIC） DTIC 是该框架的信任感知组件，主要负责从异构来源采集信任相关信息，包括：

- 智能体行为记录
- 系统运行状态
- 策略执行日志
- 安全事件与异常报告

M-Trust 决策的可靠性取决于评估中所使用的信任证据的质量和完整性。因此，DTIC 应确保所采集的信任证据经过适当认证、受到完整性保护、在需要时可追溯至其来源，并对相关信任决策而言有足够的时效性。这些要求同时适用于单一运营商部署和多域部署。根据部署环境和所需的保障等级，现有的运营商控制安全机制可辅以硬件支撑的保护、远程证明、数字签名和密码学验证等机制。

当信任证据在管理域之间交换时，DTIC 还应支持对其来源以及生成该证据所依据的权限进行验证。不应仅因来自另一个域的证据可通过密码学验证就将其视为可信；该证据是否可被接受，仍取决于接收方运营商的信任策略、安全控制和适用的授权要求。

信任证据可能包含敏感信息，包括身份属性、观测到的智能体行为以及访问或执行信息。因此，DTIC 应依据运营商策略和适用的监管要求，采取适当的数据保护、数据最小化、访问控制和隐私保护措施 [15]。对于某些特定应用场景，如果其安全与隐私方面的收益足以抵消相应的运营开销，则可考虑采用计算密集度更高的隐私增强技术；但这些技术并非 M-Trust 架构的普遍要求。

分布式信任评估（DTE）

分布式信任评估对与某一智能体交互相关的信任证据进行评估，并生成上下文相关的信任与风险评估结果，供运营商控制的策略和授权功能使用。根据交互的不同，这些证据可能包括身份和凭证状态、证明或保障信息、授权目标、委托链与调用链、所请求的网络能力、执行上下文、观测到的行为以及相关风险指标。DTE 是对现有运营商信任锚、认证、授权、策略和安全控制的补充，而非替代。

“分布式”仅指证据采集或评估功能可能采用分布式部署。运营商可根据架构、保障、时延、韧性和管理方面的要求，采用集中式、分层式、分布式或联邦式部署。不应假定分布式部署本身就能提升安全性。

在单一运营商管理域内，信任评估可主要依赖运营商控制的信任锚、凭证、受保护的数据源以及现有的安全和策略机制。在时延、可扩展性、可用性、本地数据处理或故障隔离等需求合理的情况下，可采用分布式的评估功能，但不应假定其本身就能提升安全性。所有参与的功能、接口、证据流和评估逻辑都必须得到保护，防范被攻破、被操纵、未经授权的访问以及策略应用不一致等风险。

当信任证据或评估结果在允许的管理边界之间交换时，每个接收域仍负责依据自身策略，验证这些信息的来源、出处、时效性、范围和相关性。在一个域中生成的证据或评估结果，不会自动在另一个域中建立信任或授予访问权限。对于参与方、治理安排、故障假设、决策范围和运行收益均已明确界定的特定多域用例，可考虑采用联邦式或分布式验证机制。

人工智能、统计方法和基于规则的技术均可为信任评估提供支撑，但评估方法的选择取决于具体实现。所选方法应与相关运营商场景所需的保障等级、可解释性、鲁棒性、响应能力和运行约束相匹配。M-Trust 不强制要求将分布式账本技术（DLT）、联邦学习、去中心化共识或任何特定机器学习模型作为 DTE 的组成部分。

3.4 策略决策层：策略评估与自适应调整

策略决策层在运营商定义的治理、安全和监管约束内，将信任与风险评估结果转化为策略和授权决策。它是 M-Trust 架构中的一项逻辑功能，不应被理解为取代现有运营商策略、认证、授权或安全控制功能的集中式权威。其作用是利用 M-Trust 提供的额外信任上下文，支撑策略决策和调整，同时保留运营商的策略权限。

该层提供两项相互补充的能力：

上下文感知的策略决策 + **策略验证与监督**

上下文感知的策略决策

上下文感知的策略决策在预定义的运营商策略范围内，确定智能体交互适用的授权范围和安全条件。相关输入可能包括授权目标、身份和凭证状态、信任与风险评估结果、委托链或调用链、所请求的网络能力和资源、执行上下文、观测到的行为、管理域以及适用的策略约束。

随着信任和风险上下文的变化，这些输入可支撑对授权范围、验证要求、监测条件或其他安全控制的动态调整。在运营商策略允许的情况下，较低风险的操作可采用简化的控制措施；而访问敏感网络能力、较高风险的操作或跨域交互，则可能需要增强验证、额外的信任证据、更严格的授权条件或由运营商控制的审批。此类调整不允许 AI 智能体自行授予额外权限，也不允许其在预定义的治理边界之外修改底层的运营商安全策略。

基于规则的技术、分析技术或 AI 辅助技术均可为这些决策提供支撑，但 M-Trust 并不规定特定的决策算法。在使用 AI 技术的情况下，其输出仍须受运营商定义的策略约束以及所需的安全和保障控制的约束。

策略验证与监督

在执行新的或经过实质性修改的策略决策之前，应进行策略验证。验证过程检查拟议决策是否符合授权目标、适用的运营商策略、授权约束、安全要求和相关监管义务。不满足这些条件的决策不应被执行，而可能被拒绝、受限、附加额外验证，或在需要时上报以供运营商控制的审查或人工审查。

执行之后，运行时监测会就信任、风险、执行行为、资源使用或其他相关上下文的变化提供反馈。当这些变化影响到原授权决策的依据时，策略决策层可重新评估该决策，并在预定义的策略边界内加强验证、收缩或撤销授权、附加条件或触发上报。较高风险或异常的变更在实施前，可能需要额外测试、运营商控制的审批或人工干预。

策略决策、验证结果、授权变更及相关干预措施应可审计，并依据运营商的安全与合规要求，防止未经授权的修改。这一闭环过程使 M-Trust 能够根据不断变化的信任和风险状况调整策略执行，而不会将策略权限从运营商转移给自主智能体或 M-Trust 框架本身。

3.5 策略执行层：策略执行与响应

策略执行层在相关执行点上实施由策略决策层确定的授权决策和安全控制。它是对现有运营商安全与执行机制的补充，而非替代。执行遵循“设计即安全”、最小权限和默认拒绝原则：只有在适用的运营商策略明确授权的情况下，才允许访问网络能力或资源。

策略执行智能体（PEA）是逻辑上的执行功能，可部署在适当的网络或业务执行点。PEA 依据来自策略决策层且经过验证的策略和授权决策行事，在实施这些决策时可利用相关的本地上下文。PEA 不会自行扩大授权范围或制定安全策略。任何自动化的执行动作均保持在运营商定义的策略、安全和治理边界之内。

自适应策略执行

在运营商策略允许的情况下，M-Trust 支持基于风险对执行控制进行调整。信任、风险、执行行为或上下文的变化，可能促使策略决策层要求额外验证、收窄授权范围、暂停或撤销访问，或施加额外的安全条件。PEA 在相应的执行点上执行由此产生的决策。

例如，当观测到智能体的执行明显偏离其授权目标，或相关信任和风险状况发生变化时，可对现有授权进行收缩或暂停。敏感网络能力在授予或继续授予访问之前，可能需要更强的认证、额外的信任证据或运营商控制的审批。在底层网络安全架构支持的情况下，可依据运营商策略和已识别的威胁，采用现有的隔离控制措施（包括在相关虚拟化 5G 核心网部署场景中采用微隔离 [14]）。自动化响应应与其潜在的运行影响相称。常规动作可在预定义的策略边界内自动执行，而可能显著影响网络可用性、特权管理或关键网络功能的动作，则可能需要额外的保障措施、上报，或由人工 / 运营商进行干预。从限制性措施中恢复，须经重新评估并遵循适用的运营商策略；不应仅因某一信任或风险指标恢复到先前状态，就默认恢复之前的授权。

在设计失效处理机制时，应区分智能体对网络能力的访问控制与网络本身承载的业务。当 M-Trust 相关功能出现异常或不可用时，对智能体新增或扩大的网络能力访问请求应遵循默认拒绝原则（fail-closed）；与此同时，已有的网络服务，尤其是承载公众通信的连接，应在既有运营商安全机制和策略的保障下保持连续性（fail-safe），而不应仅因 M-Trust 这一附加信任功能的失效而中断。

针对智能体异常的循环调用或类似拒绝服务的异常流量，可采用限流、熔断等自动化保护措施。此类措施的触发阈值应审慎设定并持续校准，并可结合智能体的授权目标、行为表现和信任信号，而不仅依赖原始流量指标，以避免因误触发导致自身服务中断，或使运营商管理人员失去对关键系统的访问能力。

执行反馈与重新评估

执行结果可为后续的信任和风险评估提供额外证据，包括预期控制措施是否成功实施、执行行为的相关变化、运行影响以及其他与安全相关的观测结果。此类反馈可支撑对现有授权决策的重新评估，并在适当时调整其范围或条件。

在经过适当验证、变更控制和运营商治理的前提下，反馈还可用于离线改进评估模型、策略或运行基线。但不应将其理解为允许策略执行层或 AI 智能体自主修改底层的运营商安全策略。由此形成的闭环如下：

信任证据采集 → 信任与风险评估 → 策略与授权决策 → 执行前验证 → 执行 → 监测与反馈 → 重新评估

这使得自适应执行成为可能，同时保留现有的运营商安全控制、分层防御 [13]、运营商权限以及适当的人工监督。

3.6 跨层协同与信任闭环

M-Trust 的多层架构，即信任采集与评估层、策略决策层和策略执行层，并非以一组相互孤立的模块形式运行。在 M-Trust 框架内，这些层级通过信息流和控制流的协同交互，共同实现上文定义的闭环。各层在履行各自不同职能的同时，与其他层交换相关信息，在运营商定义的治理、安全和授权边界内，支撑闭环的信任评估和策略执行。

当信任采集与评估层中的 DTIC 收到表明存在异常行为或数据可能被操纵的信任证据或外部告警时，无需等待常规评估周期，即可直接触发跨层告警信号。异常数据特征（如伪造凭证的签名痕迹或异常行为的时间序列模式）被实时推送至 DTE，触发 DTE 启动应急重新评估流程，基于异常数据优先重新评估主体的信任状态和风险等级，并生成更新后的信任与风险评估结果。

基于该评估结果，策略决策层在运营商定义的策略约束范围内，判断是否应调整适用的授权范围或安全条件。任何新的或经过实质性修改的策略决策，都须在执行前依据授权目标、适用的运营商策略、授权约束和安全要求进行验证。验证通过后，策略执行智能体（PEA）依据运营商策略实施相应的执行动作，监测相关执行结果，并为后续的信任和风险评估提供反馈。在适当情况下，并经过验证、变更控制和运营商管控，此类反馈还可用于离线改进评估模型或策略配置。

通过跨层的信息流与控制流交互，M-Trust 实现了跨层的协调运行，并支撑策略执行随信任和风险状况的变化进行调整。这一闭环过程是对现有运营商安全控制的补充，使信任和授权决策能够随着相关证据和上下文的变化而重新评估，同时保留运营商的策略权限以及适当的人工或运营商监督。

4 M-Trust 技术考量

M-Trust 是一个技术中立的框架，旨在增强而非取代现有的运营商认证、授权、策略执行、信任锚和特定域安全控制 [10]。其实现可借助成熟技术和新兴技术，用于信任证据保护、信任与风险评估、智能体身份与授权、安全调用以及跨管理域的受控交互。然而，没有任何单一技术、部署模式或信任建立机制是所有 M-Trust 场景必须采用的。

技术选择应考虑参与实体、部署位置、管理边界、所需保障等级、运行风险、性能约束、运营商策略和适用的监管要求。现有的运营商控制机制，包括适用情况下基于 UICC/eUICC 的凭证、PKI、认证与授权机制、网络功能安全以及分层安全控制，仍然是根本。M-Trust 为未来移动网络内部、与网络之间以及跨越其许可边界的日益自主的交互，提供额外的信任上下文、证据、评估和治理能力。

因此，本章阐述的是实现层面的考量，而非规定固定的技术栈。新兴技术可以支撑 M-Trust 的特定需求，但其适用性应对照相关运营商场景的运行、安全、治理和性能要求进行评估。

4.1 与现有运营商安全机制的关系

M-Trust 应作为更广泛的运营商安全架构中一项额外的信任评估与治理能力来实现。它不应建立一套替代性的身份体系或通用的信任权威，也不应要求替换现有的接入安全、网络功能安全、凭证管理或策略控制机制。

对于单一运营商管理域内的交互，信任可主要依赖运营商控制的身份、凭证、认证、授权、策略和安全机制。在适用情况下，硬件支撑的信任锚、安全元件、基于 UICC/eUICC 的凭证以及成熟的 PKI 机制，可为身份、凭证、密钥、工作负载和网络功能的保护提供支撑。GSMA 的相关指南已将 SIM 确定为相关物联网设备到云安全场景中的标准化硬件信任根 [12]；因此，M-Trust 应建立在此类成熟机制之上，而非取而代之。

当智能体交互带来更长的调用链、智能体之间的委托、不断变化的执行上下文、对开放网络能力的访问或跨多个管理域的交互时，M-Trust 的附加能力便具有了现实意义。在这些情况下，现有安全机制可辅以有关授权目标、智能体角色、委托范围、调用链、执行行为、平台状态及相关风险的额外证据。

集中式、分层式、分布式和联邦式部署模式在不同条件下均可能适用。不应假定分布式部署本身就能提升安全性，因为额外的节点、接口、凭证和同步安排也可能扩大攻击面。所选部署模式应支撑所需的规模、时延、韧性、保障和故障隔离目标，同时保留相关运营商的策略与安全权限。

4.2 信任证据的保护与保障

M-Trust 决策的可靠性取决于评估所用信任证据的质量和完整性。因此，信任证据应经过适当认证、受到完整性保护、在需要时可追溯至其来源，并对所作决策而言具备足够时效性且相关。

根据所需的保障等级和部署环境，成熟的运营商控制机制可辅以硬件支撑的密钥保护、安全执行环境、远程证明、数字签名、受保护的日志记录及其他密码学验证机制。这些机制提供不同形式的保障，不应被视为可相互替换的信任根。例如，证明（attestation）可以提供有关平台或工作负载状态的证据，但依赖该机制的运营商仍需判断签发方、证据、度量值及相关声明是否符合其策略要求。

信任证据可能包含敏感信息，包括身份和凭证属性、智能体行为、调用历史、执行上下文和访问记录。拥有交换信任信息的技术权限，本身并不意味着此类信息的交换在法律上是允许的。因此，应根据运营方政策以及适用的法律法规要求（包括数据保护、数据传输及竞争法相关要求），采取适当的数据最小化、访问控制、数据留存、保密及隐私保护措施 [15]。

如考虑采用计算开销较大的隐私增强技术，应以明确界定的需求为依据，并结合时延、可扩展性、复杂度和运行开销进行评估。此类技术是针对特定用例的可选方案，而非 M-Trust 架构的通用要求。

信任证据和策略信息本身就是安全关键资产。采集、交换、评估和使用这些信息的功能，应通过最小权限、职责分离、适当的信息防火墙，以限制未经授权或不当的信息流动、安全的接口与通信、可审计性、韧性以及适当的生命周期管理加以保护。一个 M-Trust 功能或信任域被攻破，不应自动导致对另一网络域的信任或访问授权。

4.3 信任评估与策略决策技术

M-Trust 可采用基于规则的技术、统计技术、分析技术或 AI 辅助技术来评估信任证据，并为策略和授权决策提供支撑。技术的选择取决于具体实现，应与相关运营商场景的保障、鲁棒性、可解释性、响应能力和运行约束相匹配。

信任评估的输出应为运营商控制的策略和授权提供参考，而非取而代之。信任评估结果或风险指标本身并不构成授权。策略决策层应将可用的信任和风险信息，与授权目标、所请求的网络能力、委托链与调用链、执行上下文、管理域、运营商策略以及适用的安全和监管约束一并进行评估。

将 AI 辅助技术应用于信任评估或策略决策时，其输出应始终受运营商定义的规则和治理约束。适当的控制措施可包括输入与输出验证、策略约束、测试、监测、可审计性、回退机制，以及在需要时的人工或运营商监督。AI 辅助技术不应自主扩大授权范围、重新定义运营商策略或授予智能体额外权限。

新的或经过实质性修改的策略和授权决策，应在执行前进行验证。随后，运行时监测应判断支撑原决策的信任、风险、执行行为或上下文是否发生了实质性变化。必要时，可收缩授权范围或条件、要求提供额外证据或进行额外验证，或暂停、撤销访问。这些机制的实现应与第 3 章所述的安全、验证、可审计性和变更控制原则保持一致。

4.4 智能体身份、委托与安全调用

M-Trust 应区分移动网络接入认证，与在网络内部运行、代表网络行事或与网络交互的 AI 智能体的身份和授权。现有的或 3GPP 定义的接入安全机制及其未来演进，将继续保护网络接入关系。智能体身份、委托和调用安全属于额外的考量，不意味着 5G-AKA、网络功能安全或成熟的 PKI 机制等已经过时。

网络 AI 智能体应纳入由运营商控制的生命周期管理，涵盖创建或部署智能体的授权、入网（onboarding）、身份和凭证分配、允许的功能、授权范围、相关的软件或模型变更、监测以及权限撤销或停用。代表用户、应用、网络功能或其他智能体行事的智能体，应具有可验证的委托关系和明确的授权范围。受委托智能体的身份和权限，不应仅根据原始请求方的身份推断得出。

请求访问开放网络能力的第三方 AI 智能体，应通过运营商认可的机制进行认证和授权。访问应遵循设计即安全、最小权限和默认拒绝原则：只有在适用的运营商策略明确授权的情况下，才开放网络能力。较高风险的请求可能需要额外的信任证据、更强的验证、更严格的授权条件或运营商控制的审批。

智能体之间以及智能体与网络功能之间的交互，可能涉及多步调用链。因此，安全控制应支持保证请求完整性、识别调用实体和受委托实体、验证授权目标和相关授权范围，以及对安全相关操作进行审计。每个接收方网络功能或管理域仍负责判断所请求的操作是否已获授权。

可归责性（Accountability）是智能体网络信任与授权治理的重要组成部分。GSMA 发布的负责任 AI 成熟度路线图将可归责性与人的自主与监督、透明度等一并纳入负责任 AI 的重要原则 [17]。在 M-Trust 中，可归责性意味着与安全、授权或网络资源相关的重要智能体操作应能够追溯至明确的责任和授权主体，例如部署网络 AI 智能体的运营商、提供第三方 AI 智能体的服务方，以及发起或授权任务的用户、应用或其他主体。为此，应以防篡改和可审计的方式记录授权目标、委托链与调用链、相关信任证据、策略决策及执行结果，使运营商能够在事后重建关键决策过程、明确相关参与方的责任，并在必要时采取纠正、回滚、权限撤销或其他补救措施。在出现异常时，这些记录还应支持运营商较快地开展根因分析，判断异常源于模型推理错误、输入数据异常、错误的工具或跨域能力调用，还是其他因素。智能体的自主性不应造成责任真空：智能体可以在授权边界内自主执行操作，但相应的责任和治理义务仍应由明确的人或组织承担。

未来的智能体通信协议可能为智能体发现、能力描述、委托、调用和证据交换提供标准化支持，但这一领域仍在发展之中。当前 3GPP 的工作将涉及基于 UE 的智能体、网络 AI 智能体、第三方 AI 智能体以及 6G 核心网内部智能体的通信列为相关研究领域，而非已完成的规范性协议框架。因此，M-Trust 应保持协议中立，并支持与现有 5G 系统、未来 6G 系统以及多代混合部署共存。

4.5 跨域信任证据交换

跨域 M-Trust 交互可能涉及运营商、企业环境、云或边缘提供商、服务提供商以及第三方 AI 智能体。这些交互跨越允许的管理边界进行，并须满足各参与域的安全、策略、授权和监管要求。跨域信任应支持相关信任证据的受控交换和验证。此类证据可能包括凭证、证明、授权声明、来源信息或其他与安全相关的断言。密码学验证可以证明证据由特定来源签发且未被篡改，但并不要求接收方运营商必须接受该证据或授予访问权限。

每个接收域应独立评估：

- 签发方身份、权限、来源、实效性和完整性；
- 范围、主体、目标、能力和保障等级；
- 是否符合接收域的策略、授权、安全和监管要求。

因此，在适用的法律法规约束之下，信任证据可以在允许的边界之间交换，但信任决策和授权权限仍归属于各自的域。一个域作出的授权决策，不应自动授权访问由另一个域控制的能力或资源。这保留了分层防御，并防止跨域合作形成通用信任权威机构或单点安全故障。

当多个管理域需要交换或验证证据，且没有任何单一参与方掌控完整关系时，可考虑采用联邦式或分布式验证机制。此类机制的应用应基于明确界定的参与方、治理安排、故障假设、证据语义、决策范围及运营效益。它们是对各参与域既有信任锚点及安全权威的补充，而非替代。

4.6 新兴技术与特定用例技术

一系列新兴技术可为未来的 M-Trust 实现作出贡献，例如机密计算、先进的隐私增强技术、后量子密码、分布式或基于账本的证据记录、联邦评估以及 AI 辅助安全技术。这些技术并非 M-Trust 的必选组件，也不应假定其适用于所有运营商场景。

其适用性应结合具体的运营商用例，从与现有安全架构的兼容性、保障收益、性能与运行开销、攻击面、治理要求、成熟度、互操作性以及适用法规等方面进行评估。

因此，M-Trust 不依赖于任何特定的新兴技术。该框架定义了智能体交互的信任、授权、治理和证据要求；各运营商及参与域在各自的安全架构和权限边界内，确定适当的实现技术。

5 结论与未来展望

5.1 结论

M-Trust 并非旨在取代零信任、现有的运营商安全机制或当前的自智网络运行方式。它以显式授权、最小权限、持续验证、分层安全和基于策略的控制等成熟原则为基础，探讨随着移动网络向日益自主的智能体化运行演进，可能产生的额外信任与授权需求。

自智网络已经通过使用意图驱动的运营、AI 辅助决策和闭环自动化来改进网络和业务管理。M-Trust 着眼于一个互补性的问题：当自主智能体分解任务、委托操作、调用网络能力并在不断变化的上下文中交互时，运营商如何持续判断所涉及的实体是否始终可信，以及其操作是否始终处于授权目标的范围之内？

通过多方信任、智能体意图感知信任和跨域信任，M-Trust 提供了一个概念框架，用于考量信任证据与评估、上下文感知授权、委托链与调用链、自适应策略执行，以及信任证据在允许的管理边界之间的受控交换。这些能力旨在增强现有的由运营商控制的身份、认证、授权、策略和安全机制。运营商策略、安全控制、管理权限和适用的监管要求始终具有最终决定权。

M-Trust 定位为参考框架和研究方向，而非标准规范、强制性架构或规定的技术栈。本白皮书提出的概念，还需要通过有代表性的运营商用例、架构分析、原型验证、安全评估、监管要求以及相关产业和标准化活动加以进一步验证。

5.2 未来展望

将智能体能力融入未来移动网络，仍是产业界和标准化研究中不断发展的领域。当前 3GPP 正在研究如何在 6G 中支持 AI 和智能体能力，包括涉及网络 AI 智能体、第三方 AI 智能体和 AI 赋能的网络功能的交互。相应的架构、协议、安全机制和部署模式仍在发展之中。因此，M-Trust 应与这些工作同步演进，而不是预设某种特定的未来网络架构。

以下几个方面值得进一步研究。

01 M-Trust 需要更精确地映射到移动网络架构和现有安全机制

未来工作应明确信任证据在何处生成和评估，M-Trust 功能如何与现有的认证、授权和策略控制交互，以及对网络 AI 智能体和第三方智能体如何进行全生命周期管理。应特别关注与现有 5G 部署的兼容性以及向未来 6G 能力的演进，而不是假定现有安全架构将被替换。

02 智能体交互的信任与授权治理需要进一步研究

自智网络框架已支持意图驱动和闭环运行；M-Trust 应聚焦于智能体在追求授权目标的过程中分解任务、委托权限、调用其他智能体或网络能力、改变执行路径时所带来的额外要求。还需进一步研究如何在无需预测智能体未来所有可能操作的前提下，表示和评估授权范围、委托、调用链和信任证据。例如，以结构化、机器可读的方式表达意图及其对应的授权范围，使策略执行能够基于明确界定的约束条件，而不依赖于 AI 模型对意图的主观解释。TM Forum 已将意图驱动决策和闭环管理定位为 L4 级自智网络的能力，这进一步说明 M-Trust 应聚焦于信任与授权治理维度，而非重复网络自动化工作 [11]。

03 跨域信任需要清晰界定的管理边界和安全边界

未来工作应研究信任证据如何在运营商、企业、云或边缘提供商以及第三方 AI 服务之间交换和验证，同时使各参与域保留对自身网络能力和授权决策的权限。跨域信任不应假定信任可以普遍传播，或授权可以在域之间自动转移。

04 M-Trust 自身的安全性和韧性需要进一步验证

信任证据、评估功能、策略决策和接口都可能成为安全关键资产。因此，未来工作应评估攻击面、入侵遏制、可用性、职责分离、可审计性，以及信任评估结果出错或被操纵所带来的后果。应根据具体运营商场景的需求，对集中式、分层式、分布式和联邦式部署模式进行评估，而不是假定某种模式天然更安全。

05 安全保障、响应能力与运行复杂度之间的平衡需要进一步验证

信任评估和授权控制应与其所保护的网络能力相匹配，同时应从性能开销、成熟度、互操作性以及与现有运营商安全机制的兼容性等方面，对新兴的实现技术进行评估。

随着智能体网络概念及相关标准的演进，M-Trust 可以为产业界探讨信任与授权治理如何随网络自治程度的提升而演进，提供一个结构化的讨论基础。未来工作应结合具体的运营商场景和新兴标准，逐步验证该框架，细化其功能边界，并明确哪些方面需要新的机制、哪些方面现有的移动网络安全机制已经足够。

6 缩略语

缩略语	英文全称	中文名称
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G-AKA	5G Authentication and Key Agreement	5G 认证与密钥协商
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用程序编程接口
DLT	Distributed Ledger Technology	分布式账本技术
DTE	Distributed Trust Evaluation	分布式信任评估
DTIC	Data Trust Indicator Collection	数据信任指标采集
eSIM	Embedded SIM	嵌入式 SIM
eUICC	Embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
GSMA	GSM Association	全球移动通信系统协会
IMT	International Mobile Telecommunications	国际移动通信
IoT	Internet of Things	物联网
ITU	International Telecommunication Union	国际电信联盟
ITU-R	ITU Radiocommunication Sector	国际电信联盟无线电通信部门
M-Trust	MAIC-Trust Framework	MAIC-Trust 框架（简称 M-Trust）
MNO	Mobile Network Operator	移动网络运营商
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
PA	Policy Agent (Policy Decision and Validation Function)	策略智能体（策略决策与验证功能）
PEA	Policy Enforcement Agent	策略执行智能体
PKI	Public Key Infrastructure	公钥基础设施
SIM	Subscriber Identity Module	用户身份识别模块
SLA	Service Level Agreement	服务等级协议
SP	Special Publication (NIST)	（NIST）特别出版物
TR	Technical Report	技术报告
TS	Technical Specification	技术规范
UE	User Equipment	用户设备
UICC	Universal Integrated Circuit Card	通用集成电路卡

7 术语定义

术语	定义
AI 智能体 AI Agent	能够感知或获取相关环境与上下文信息，通过推理、规划和决策，自主或与其他智能体协作执行任务，以实现特定目标的智能实体（参见 3GPP TR 22.870[18]）。
智能体网络 Agentic Network	网络功能、网络 AI 智能体与第三方智能体在其中自主协作，并通过目标分解、委托和能力调用实现授权目标的未来网络形态。
自智网络 Autonomous Networks	通过意图驱动运行、AI 辅助决策和闭环自动化提升网络与业务管理水平的网络，参见 TM Forum 的相关定义。
零信任 Zero Trust	不基于网络位置默认授予信任的安全模型，以身份为中心的安全、最小权限和持续监测为核心原则（参见 NIST SP 800-207）。
M-Trust MAIC-Trust 框架	本白皮书提出的面向智能体网络的信任框架，在零信任基础上扩展了多方信任、智能体意图感知信任和跨域信任三个维度。M-Trust 定位为参考框架和研究方向，而非标准规范或强制性实现架构。
多方信任 Multi-party Trust	由多个获授权方提供可独立验证、限定用途且有时效约束的信任证据，并结合与上下文相适应的信任建立方式进行的信任评估。外部证据是运营商本地策略决策的输入，而非替代。
智能体意图感知信任 Agentic Intent-aware Trust	以身份验证与意图感知授权为基础建立的智能体信任，并可根据风险和上下文，在运营商定义的边界内对策略进行有限制的自适应调整。
跨域信任 Cross-domain Trust	在允许的管理域或安全域边界之间对信任证据进行受控交换与评估，同时保留各参与域的信任锚、策略权限、安全控制和监管义务。
意图感知授权 Intent-aware Authorization	在身份验证之外，进一步评估所请求的操作是否仍与授权目标、委托链与调用链、执行上下文及适用策略保持一致的授权方式。超出预授权范围的操作应触发新的授权决策。
授权目标 Authorized Objective	智能体被允许实现的任务目标及其权限边界。
委托链与调用链 Delegation and Invocation Chain	任务在智能体之间逐级委托，以及智能体调用其他智能体、工具或网络能力所形成的链路，是意图感知授权需要评估的上下文之一。
信任证据 Trust Evidence	用于支撑信任评估的可验证信息，例如身份及签约数据、观测到的网络行为、工作负载或平台证明（attestation）、软件完整性以及受委托权限等。
信任锚 Trust Anchor	建立信任的根基础，凭证和信任证据依据其进行验证，例如基于 UICC/eUICC 的凭证、安全元件、硬件信任根和 PKI 机制。
管理域 Administrative Domain	由单一实体（如运营商或服务提供商）对其行使策略、安全和管理权限的网络或系统范围。
网络 AI 智能体 Network AI Agent	部署于运营商网络内或代表运营商网络行事、并遵循运营商控制的生命周期进行管理的 AI 智能体。
第三方 AI 智能体 Third-party AI Agent	由运营商以外的主体提供、与移动网络交互的 AI 智能体，例如通过 API 访问运营商开放的网络能力。

8 参考文献

[1]. 3GPP, TR 23.801-01, “Study on Architecture for 6G System; Stage 2,” Release 20, work in progress.

[2]. M. Chen, Z. Yang, T. Qiu, J. Zhang, M. Shikh-Bahaei, and T. Ohtsuki, “AI-Native Networking: A Vision and Survey,” *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 1–34, 2024.

[3]. ITU-R, Recommendation M.2160-0, “Framework and overall objectives of the future development of IMT for 2030 and beyond,” November 2023.

[4]. Z. Xiao, X. Song, W. Ni, X. Tao, and G. Li, “Integrated Sensing and Communication: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 790–823, 2023.

[5]. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, August 2020.

[6]. 3GPP, TR 33.894 V18.0.0, “Study on applicability of the Zero Trust Security principles in mobile networks,” Release 18, September 2023.

[7]. 3GPP, TR 33.794 V19.1.0, “Study on enablers for Zero Trust Security,” Release 19, March 2025.

[8]. Y. Wang, X. Kang, T. Li, H. Wang, C.-C. Kang, and Z. Lei, “SIX Trust for 6G: Towards a Secure and Trustworthy 6G Network,” *IEEE Access*, vol. 11, pp. 107657–107668, 2023.

[9]. Y. Wang, X. Kang, and T. Li, “Towards an Open Trust Establishment Infrastructure for Future Network: Motivations, Models and Technologies,” *IEEE Access*, vol. 12, pp. 111196–111205, 2024.

[10]. 3GPP, TS 33.501 V18.8.0, “Security Architecture and Procedures for 5G System,” Release 18, January 2025.

[11]. TM Forum, “Autonomous Networks: Level 4 Industry Blueprint,” June 2024.

[12]. GSMA, “IoT SAFE: Robust IoT Security at Scale: The Why, What and How of Securing IoT Applications and Data,” June 2021.

[13]. GSMA, “GSMA Mobile Telecommunications Security Landscape 2025,” February 2025.

[14]. GSMA, FS.61 Version 1.0, “Micro-Segmentation in 5G Core Network Resource Pool Guidelines,” April 2025.

[15]. GSMA, “Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem,” February 2016.

[16]. GSMA, “GSMA Mobile Telecommunications Security Landscape 2026,” February 2026.

[17]. GSMA, “The GSMA Responsible AI Maturity Roadmap,” September 2024.

[18]. 3GPP, TR 22.870 V20.0.0, “Study on 6G Use Cases and Service Requirements,” Release 20, March 2026.

[19]. GSMA, “The Mobile AI whitepaper,” March 2026.

编制单位：

华为技术有限公司
中国电信集团有限公司
中国联合网络通信有限公司
中国移动通信集团公司
中国电信股份有限公司研究院
北京邮电大学
国家信息中心
中国移动通信有限公司研究院
中国移动通信集团设计院有限公司
北京神州绿盟科技有限公司

支持单位：

中广电移动网络有限公司
中移（杭州）信息技术有限公司

编制组：

李铁岩｜刘　鸿｜魏　凯｜石　霖｜谷红勋｜武姗姗
常力元｜郑　直｜陶　冶｜王晓晴｜杨　凯｜王　勇
静　静｜国志宏｜程崇浩｜康　鑫｜张云峰｜范晓继
邵　萌｜张　晨｜张　熙｜张　昆｜刘文懋｜徐孟珺
杜　刚｜李　岩｜王　越｜吴　超



GSMA 总部
1 Angel Lane
London
EC4R 3AB
United Kingdom

电话: +44(0)20 7356 0600
传真: +44(0)20 7356 0601