CAICT 中国信通院

集智 专题报告

新通话安全技术研究报告

（2024 年）

中国信息通信研究院技术与标准研究所

2024年11月

版权声明

前　言

近年来，伴随着电信网网络算力与运力的不断增强，电信业务创新基础不断夯实，电信业务向智能、交互、个性化发展的趋势日渐清晰。新通话作为传统通话业务的创新载体，将媒体、数据交互和应用程序功能无缝集成进音视频通话中，提供了趣味化、智能化、多样化的新型实时通信服务，成为运营商转型升级和赋能行业提质增效的重要着力点。

交互式数据通道的引入、基于小程序的业务提供模式，增加了新通话网络、运营及业务管理方面安全风险防范的复杂性。同时，随着用户、设备、业务、平台的多元化发展，新通话网络将面向未来丰富的交互场景提供更灵活的网络开放能力，为话音基础网的复杂性、可靠性、稳定性带来了挑战。另外，新通话业务与行业数字化转型的深度融合正在推动新通话应用场景、业务模式持续拓新，加快了音视频通信到多模态通信的演进，网络安全边界也逐渐趋于模糊化。

本报告着眼于新通话商用业务网络侧安全、终端及应用服务安全，分析介绍了潜在的安全风险及相应的解决方案。另外，本报告前瞻性地系统评估了新通话未来业务潜在的安全风险，包括防诈骗安全，能力开放安全等。最后，本报告从内生安全、衍生安全等方面提出了新通话业务安全发展策略建议，希望能够帮助业务相关方构建更完备高效的业务安全能力体系，助力业务健康持续发展。

目 录

图 目 录

一、新通话业务发展态势

近年来，伴随着电信网网络算力与运力的不断增强，电信业务创新基础不断夯实，电信业务向智能、交互、个性化发展的趋势日渐清晰，通信产业链企业开始围绕语音业务功能提升进行研究。新通话作为运营商基础通话业务的升级，在传统音视频通话业务的基础上，基于 IMS 网络进行系统增强和业务创新，为用户提供了多媒体通话与数据应用深度融合的、智能的、交互式的实时通信服务，能够满足不同用户群体多元化场景下的通信需求。

（一）新通话商用业务场景

新通话作为实时通信领域的重要创新，基于传统音视频通话提供了一系列通话增强服务和创新应用，能够为个人用户提供更可视化、个性化的业务体验，也能够与金融、医疗、教育、政务等产业深度融合，在通话中实现引流、交互、签约的全链条服务闭环，满足千行百业远程服务、即时服务的通信需求。**新通话的商用分为两个阶段，**第一阶段为基于视频通话的新通话业务，第二阶段为基于数据通道的新通话业务。

1.第一阶段：基于视频通话的新通话业务

基于视频通话的新通话业务已经于 2023 年实现商用，包括趣味通话、智能翻译、点亮屏幕等。用户可通过线下签约新通话业务并选择其需要的媒体素材，利用现有 IMS 网络的视频通话能力，体验智能的、交互式的实时通信服务。例如，趣味通话业务支持用户选择系统预置的图片以替换用户在通话时所处的真实通话环境。智能翻译业

务支持自动识别双方对话内容，并实时将对方的语音翻译成设定的目标语言，以字幕的形式叠加在视频通话界面。

2.第二阶段：基于 IMS 数据通道的新通话业务

基于 IMS 数据通道的新通话业务包括:

（1）智能翻译增强

支持签约用户使用 DC（Data Channel，数据通道）终端在通话中操作设置翻译的源语言、目标语言，以及呈现的字幕样式。

（2）趣味通话增强

支持签约用户使用 DC 终端进行通话时实时设置视频通话背景，以及数字人形象。

（3）屏幕共享

支持签约用户使用 DC 终端在通话中向通话对方共享屏幕、摄像头，对共享内容的内容进行标记，辅助双方支持提升沟通效率。

（4）AR 标记

支持签约用户使用 DC 终端在通话中对共享屏幕进行 AR 标记，并对被标记的内容进行位置跟踪。

（5）内容共享

支持签约用户使用 DC 终端在通话中进行内容共享，包括文件、图片、视频、位置等。

（6）智能客服

支持客户系统向使用 DC 终端的签约用户推送菜单等内容，签约

用户可实时触屏互动进行业务查询和办理。

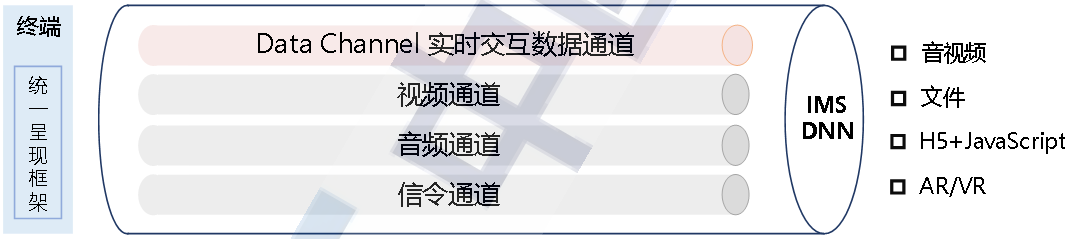
（7）智能家庭终端互动

支持签约用户使用 DC 终端对智能家庭终端进行管理、控制及音视频通话。

（二）新通话网络架构和工作流程

1.标准化网络架构

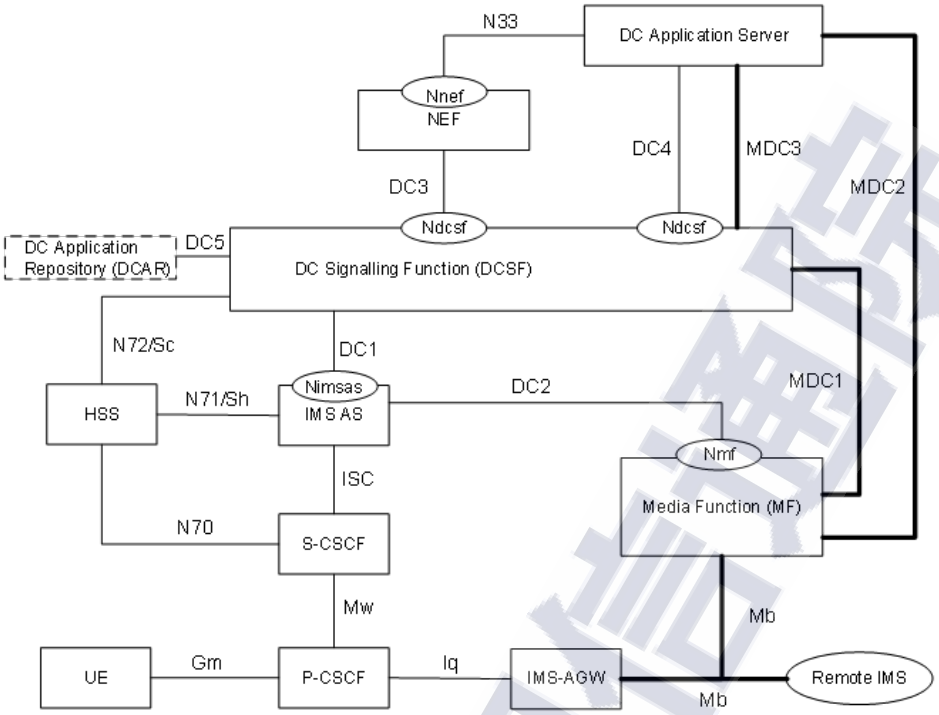
新通话的网络架构，是基于现有 IMS 网络进行增强，在 VoLTE（Voice over LTE）/VoNR（Voice over NR）音视频通道的基础上增加了 IMS 数据通道，用于传输任何类型的应用数据，实现用户在通话时的交互式信息传递。



来源：中国信息通信研究院

图 1 Data Channel 数据通道技术

3GPP TS 23.228 定义了标准化的新通话网络架构，引入了数据通道信令功能（Data Channel Signaling Function，简称 DCSF）和媒体功能（Media Function，简称 MF）两个新的网络功能，并面向未来网络演进引入了服务化接口，旨在支撑交互式多媒体业务的规模发展，实现新通话创新业务体验。



来源：3GPP TS 23.228 R18

图 2 3GPP R18 新通话网络架构

为支持新通话业务，IMS AS（IMS Application Server，IMS 应用服务器）需要升级支持数据通道的连接管理，并可根据指示完成 IMS 会话的媒体协商；DCSF 提供数据通道的控制能力，并向北向第三方 AS（Application Server, 应用服务器）开放；MF 提供数据通道资源管理和 AR 渲染能力；DCAR（Data Channel Application Repository，数据通道应用仓库）用于存储数据通道应用。

2.数据通道工作原理

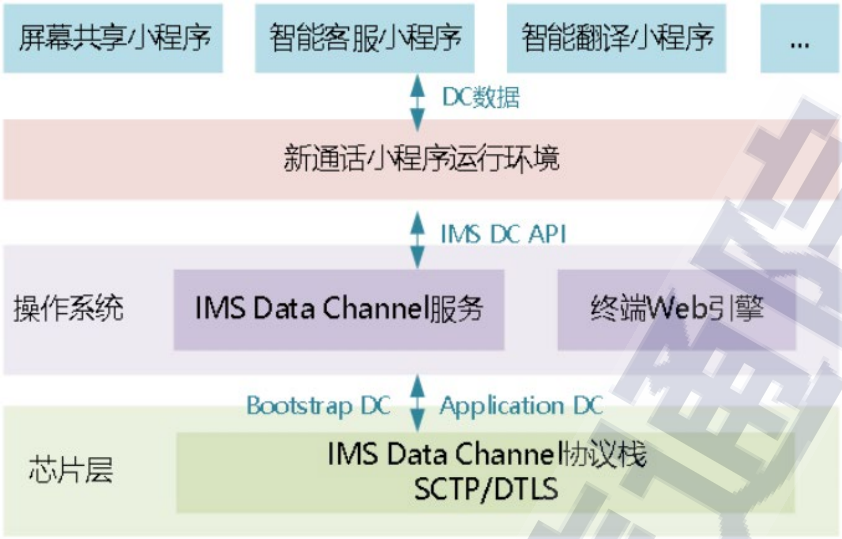
3GPP TS 26.114 定义的 IMS 数据通道分为引导数据通道和应用数据通道两类，终端通过引导数据通道从主叫网络和（或）被叫网络下载数据通道应用程序（即新通话小程序）列表和各种应用程序。应用数据通道可以在终端与终端之间、终端与网络之间建立，用于传递

数据通道应用程序的应用数据。

IMS 数据通道不关注通道中传递的数据内容及其格式，仅需要通信双方对通信格式达成一致，通过 HTML+CSS+JavaScript 脚本等互联网成熟技术在数据通道中传递多样化的应用内容，支撑新通话业务的快速创新、快速部署、快速上线。

3.新通话小程序架构

新通话采用小程序模式构建业务生态，小程序由业务平台提供，在通话过程中，终端可通过 DC 通道从网络侧下载并使用新通话小程序。基于小程序的提供方式，可以屏蔽业务升级对终端的要求，有助于业务的快速迭代和创新，提高用户易用性。现阶段为推动终端产业对新通话能力的支持，芯片厂商提供 DC 基础能力、运营商自主研发终端侧 SDK（Software Development Kit，软件开发套件）提供小程序运行环境、终端厂商在通话应用中集成 SDK，合作实现新通话原生终端方案。其中，新通话运行环境提供小程序运行所需的进程调度、存储管理、安全框架、硬件接口、交互展示等，能够帮助小程序开发者在无需了解技术细节的情况下快速实现业务功能，降低开发成本、缩短开发周期。



来源：中国信息通信研究院

图 3 新通话小程序架构

（三）新通话产业发展情况

前期，我国运营商、终端、芯片等企业与标准化、行业组织已开展了各项关键技术攻关及标准化工作。

1.标准化进展

数据通道的概念源自 W3C WebRTC，并被 IETF 标准化，由 3GPP SA4 工作组在 R16 中引入到 IMS 网络中。3GPP SA2 NG_RTC 项目在 R18 阶段完成了 IMS DC 和 AR 通信架构、接口和流程的标准化工作。2023 年 6 月，GSMA 发布《NG.134 IMS Data Channel》，定义了支持 IMS DC 的 UNI（User Network Interface，用户网络接口）和 NNI（Network to Network Interface，网络节点接口）标准最小集，可支持单运营商 DC 商用。2024 年 7 月，GSMA TSG 发布《TS.66 IMS Data Channel API Specification》，定义了终端面向新通话小程序的 JS API，支持新通话小程序跨终端、跨运营商运行。

在国内标准方面，CCSA TC3/TC11 有多个项目面向基于 IMS DC 方案的新通话业务开展标准化工作，主要聚焦网络架构、业务流程及终端要求等方面，对标国际先进水平，持续推进新通话标准化体系构建和完善。

2.产业发展现状

运营商方面，我国运营商陆续启动了新通话的网络规划、建设和试商用。中国移动已于 2023 年完成基于 DC 方案的技术试点和网络升级，目前已经上线点亮屏幕、趣味通话等 6 款新通话应用；中国电信已于 2023 年第三季度开展新通话业务试点验证工作，后续计划开展双卡双 DC 技术研究以及 AI 类业务研究；中国联通目前已完成基于视频通道的新通话平台建设和业务商用，计划启动基于 DC 方案的表情特效、虚拟形象、位置共享、AR 标记等应用试点。

终端方面，当前 MTK、高通、展锐均已完成 IMS DC 协议栈开发，并完成基础流程功能验证；华为、中兴、小米、VIVO 已完成中国移动新通话 SDK 适配和端到端业务测试，且原生支持新通话能力的华为 Mate 60 Pro 已在 2023 年 10 月中国移动合作伙伴大会上做了正式发布。

垂直行业企业方面，新通话的行业应用目前处在试验阶段，通过能力推介，部分金融行业用户、快速消费品行业对新通话给予厚望，已经开始要求供应商提供测试能力以开展 PoC 验证（Proof of Concept，概念验证）。但是，以目前的网络环境和供应商能力，仍然难以满足日益增长的行业应用需求。

产业链聚合方面，2023 年 11 月，在工业和信息化部的指导下，中国信息通信研究院与中国通信企业协会联合发起成立新通话工作组，旨在搭建企业间、行业间交流平台、凝聚产业链各方力量、更好更快地推动新通话规范发展，共有成员单位 40 余家，覆盖电信运营企业、应用开发企业、终端企业以及垂直行业单位等。

二、新通话安全风险及防护策略

新通话将媒体、数据交互和应用程序功能无缝集成进传统音视频通话中，提供了趣味化、智能化、多样化的新型实时通信服务，成为运营商转型升级和赋能行业提质增效的重要着力点，同时也对新业务网络、运营、业务管理等安全风险防控带来了更大的挑战。

（一）网络侧安全

1.控制面安全

控制面安全风险为 SBA（Service Based Architecture，服务化架构）的网元传递消息篡改、非法接入和服务滥用风险。若 IMS 网元之间缺少机密性和完整性保护，攻击者将能够获取或篡改 IMS 网元之间传递的消息；若在 IMS 的两个网元交换消息前无身份认证，攻击者将能够冒充某个网元，并劫持两个网元之间的消息，实现欺骗攻击和中间人攻击；若没有授权流程，网元可任意请求其他网元的服务并获取未经授权的信息，涉及 IMS 媒体面所有支持服务化的网元。

针对上述安全风险，3GPP TS 33.328 的附录 P 已标准化 IMS 控制面的 SBA/SBI（Service Based Interface，服务化接口）安全。其中，网络传输层的安全由 TLS（Transport Layer Security，传输层安全协议）

实现；IMS 网元之间的认证可分为直接认证和非直接认证。直接认证可通过传输层保护、NDS/IP（Network Domain Security/IP layer security，网络域安全/IP 层安全机制）或物理保护实现，非直接认证可通过传输层保护、CCA（Client Credentials Assertion，客户端凭据断言）、传输层或 NDS/IP 或物理层的多跳保护实现；IMS 网元之间的授权可通过基于网元之间本地策略的静态授权或基于 OAuth 2.0 的动态授权实现。

此外，控制面安全风险还包括传统 IMS 网络的 SIP（Session Initiation Protocol，会话发起协议）信令安全风险，例如非法用户接入、网络拓扑泄露、信令 DoS/DDoS 攻击、SIP 畸形报文攻击、SIP 业务逻辑攻击、用户敏感信息泄露、账号暴力破解。传统 IMS 网络的控制面采用纵深防御策略。接入侧部署防信令 DoS/DDoS 攻击、防止信令畸形报文攻击以及防止账号暴力破解等机制；核心网侧部署 SIP 头域检查、流控、SIP 畸形报文检查和接入认证等机制。具体防护方案可参考 3GPP TS 33.203。

2.媒体面安全

媒体面安全风险为数据通道用户在传递消息时面临的窃听与篡改、非法接入风险。若两个 UE（或 UE 和 IMS 网络）之间的 DC 通道缺少安全防护方案，攻击者将能够窃听或修改基于 DC 通道传输的数据；若在两个 UE（或 UE 和 IMS 网络）交换消息前没有进行身份认证，攻击者将能够冒充某个 UE 或 IMS 网络，并劫持两者之间的消息，实现欺骗攻击和中间人攻击；若仅有 Mb 接口受到保护，即仅有

UE 到 IMS-AGW 的 DC 通道被安全保护，而 IMS-AGW 到外部数据服务器的通道没有安全保护措施，攻击者将能够进行监听、篡改和重放攻击。

针对上述安全风险，3GPP TS 33.328 已标准化 DC 通道安全策略，包括 e2DCe（end to Data Channel edge，即 UE 到 MF）和 e2e（end to end，即 UE 到对端 UE 或 IMS DC AS）架构的安全，即使用 DTLS 保护 IMS DC 的安全。

针对 e2DCe 架构，UE 和 MF 之间通过 DTLS record 协议保护媒体面消息，完成会话密钥的交换和相互认证。其中，证书指纹通过 SDP（Session Description Protocol，会话描述协议）消息经 P-CSCF（Proxy-Call Session Control Function，代理-呼叫会话控制功能网元）、S-CSCF（Serving-Call Session Control Function，服务类型的会话控制功能网元）、IMS AS 在 UE 和 MF 之间传输。

针对 e2e 架构，UE 和对端 UE 或 IMS DC AS 之间通过 DTLS record 协议保护媒体面消息，完成会话密钥的交换和相互认证。其中，证书指纹通过 SDP 消息在 UE 和 P-CSCF（DCSF，IMS AS）之间传输。

传统 IMS 网络的媒体面还使用 RTP（Real-time Transport Protocol，实时传输协议）和 MSRP（Message Session Relay Protocol，消息会话中继协议）。其中 RTP 协议的密钥管理包括 DTLS-SRTP（用于保护 e2ae）、SDES（用于保护 e2ae 和 e2e）、KMS（用于保护 e2e）协议，安全传输协议为 SRTP 协议。MSRP 通过交换证书和传输证书指纹实

现 e2ae 保护的密钥管理，通过与 RTP 相同的 KMS 实现 e2e 的密钥管理，基于生成的密钥建立 TLS-PSK 保护。具体安全防护方案可参考 3GPP TS 33.328。

（二）小程序安全

1.上架安全

小程序的合规和安全问题对新通话业务用户体验和数据安全具有重要影响。频繁弹窗、复杂的外链嵌套等不恰当的交互设计，不仅会严重扰乱用户的通话体验，还可能引入恶意软件、病毒等安全风险，或诱导用户误访问，妨碍通话的顺畅进行。此外，不恰当的权限请求或恶意代码可能导致通话过程中敏感信息泄露。因此，小程序上架前的合规性和安全性审核，是新通话业务健康有序发展的关键前提。

用户安全和隐私保护方面，确保小程序不会对用户的设备、数据或隐私造成威胁，防止小程序包含恶意代码、未经授权的追踪功能、与小程序功能无关的权限请求等，避免存在潜在的安全漏洞，或在未经过用户同意的情况下收集、使用用户的个人数据等情况。

内容合法合规方面，运营平台审核确保小程序的内容符合相关法律法规及平台政策，发现小程序名称、图标、简介存在违法和不良信息，业务类型存在违法违规等情况的，不得为其提供服务。

防欺诈和滥用方面，防止小程序中存在虚假或欺诈性内容，例如冒充其他应用、钓鱼应用、非法链接等，避免小程序诱导用户进行操作而导致财产损失或信息泄露。运营平台可以参考业界成熟的管理规范，严格审核小程序外链的来源和质量、控制外链的数量和变化频率、

确保外链与应用内容高度匹配、定期检查外链的有效性并及时处理失效或被篡改的外链、确保同类服务的展示和访问形式的一致性，保障用户数据安全和良好的用户体验。

2.下载安全

小程序下载是全生命周期安全中的重要环节，小程序在下载过程中可能受到多种网络攻击的威胁，例如中间人攻击，攻击者可能通过不安全的网络恶意篡改小程序下载地址，导致用户下载仿冒小程序；或利用小程序漏洞，注入恶意代码，导致用户信息泄露或者被篡改。

因此，需要制定相关策略，做好小程序下载过程中的安全防范。当前，3GPP TS 33.328 已标准化小程序下载安全机制，采用 DTLS 保护小程序下载时的完整性和机密性，采用基于 SIP 信令完整性保护的证书指纹安全传输实现认证保护，采用 IMS UE 隐式授权网元的方式实现安全保护的授权。基于上述标准化方案，可确保应用数据正常传输、不掉包、传输过程未被篡改以及非授权访问。

3.运行安全

小程序作为一种轻量级、即用即走的应用形式，面临着诸如隐私泄露、数据篡改、恶意攻击等安全风险。风险可能来源于不当的数据管理、不安全的 API 调用、代码逻辑漏洞、以及外部的网络攻击等。

为保障小程序的安全运行，运营平台需要实施相应的安全策略。运行监测方面，新通话小程序需要对运营平台开放监管入口，以使运营平台能够对小程序采取运行状态监测和管理，包括数据监控、日志分析、异常处理等，实时跟踪小程序的各项性能指标，识别和过滤异

常行为、敏感信息、非法言论、恶意攻击、错误信息和潜在的安全威胁。针对过度营销、诱导分享等有损用户利益的行为及时采取应对措施，如下架小程序、通知用户、提供修复指南等，以减少安全事件的影响。对于已经发现的安全问题，平台应提供事后分析工具，帮助开发者追踪问题源头、优化代码逻辑、修复安全漏洞。用户数据保护方面，平台需要确保小程序遵守相关的隐私保护法规，对用户数据的收集、使用和共享进行严格监管。同时建立用户举报机制，在小程序应用内为用户提供举报入口，以便用户向服务提供商或运营商对违规小程序进行举报，并及时响应和处理这些举报。

4.使用安全

新通话应用伴随着音视频通话发生，用户信息及数据有更多的暴露风险，可能存在小程序强制授权、过度收集、违法违规使用个人信息等情况。首先，不恰当的访问权限管理（录音、摄像头、位置、通讯录、存储权限等），可能会导致用户数据泄露的风险。另外，在个人信息存储和使用方面，可能存在数据非法访问、篡改、超范围使用，导致个人信息滥用或不法分子通过获取用户的消费习惯、兴趣爱好等敏感信息，实施更加精准的诈骗和攻击。

新通话小程序可通过加强访问控制权限管理，限制通话双方能够访问的数据和信息，阻止与业务功能不相关的敏感操作。一方面，当新通话小程序访问用户设备及用户数据时，可通过通知推送、弹窗提示等直观方式告知用户所需权限的具体内容，并得到用户的授权许可，尊重用户偏好和选择权。另一方面，小程序应具备细粒度的权限管理，

提供多种授权选项，包括如一次性授权、使用期间授权和永久授权等，例如在趣味通话场景中，用户可选择只允许在发起一次视频聊天、人脸活体认证及其他需要摄像头的信息的合理功能需求时，采集用户的人脸信息。当用户实现了一次功能需求后，拍摄照片及录制视频的行为则不允许在后台继续进行。在文件传输等场景中，用户可选择仅在小程序使用期间具有文件读取的权限，避免频繁的权限请求，影响小程序的使用体验。

（三）终端侧安全

新通话 SDK 作为端侧核心能力套件，实现新通话小程序运行所需的依赖环境，是所有新通话业务的入口和底座，SDK 的合规和安全问题直接影响了新通话业务安全和运行安全。

首先，SDK 自身安全风险通常包括技术层面安全漏洞、利用 SDK 进行违法及非正当恶意行为、以及处理个人信息不当等问题。为了应对这些风险，GB/T 43435-2023《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》中明确了 SDK 的安全要求。在设计开发阶段，SDK 提供方应当通过代码审计、漏洞扫描、隐私合规检测等手段对 SDK 进行全面安全评估及安全测评，避免由于技术方案不合理和代码缺陷导致的数据交互安全漏洞；在发布阶段，SDK 运营者应提供相关的数字签名，保证终端集成 SDK 来源的真实性和开发者身份的合法性；在运营阶段，可通过防御检测、动态行为拦截等手段防范流量劫持、恶意广告、远程控制等恶意行为。同时，SDK 在处理个人信息方面，要遵循合理、最小、必要原则，确保用户

个人信息不被未经授权的访问。

除上述 SDK 本身存在的安全风险外，由于新通话 SDK 承载多个小程序，通过沙箱技术为小程序提供相对隔离的运行环境，可确保它们在执行时不会相互干扰，从而有效防止潜在的恶意代码传播和数据泄露风险，保障各个小程序的安全运行。此外，通过 SDK 监测、精细化控制小程序对资源的访问，确保它们不会进行任何未授权的操作，比如访问或修改其他小程序的数据。通过这种方式，SDK 能够在确保安全的前提下，为小程序提供一个稳定和可靠的运行环境。

（四）数据安全

新通话业务涉及身份信息、人脸识别信息、通话信息、位置信息等个人隐私数据，保障数据收集、存储、使用、传输等环节的安全性，对于新通话小程序稳定运营至关重要。

信息收集方面，在个人信息收集过程中，需要尊重用户的自主意愿，确保用户的知情权和选择权，明确信息收集范围和时限。由国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布的《常见类型移动互联网应用程序必要个人信息范围规定》（下称《规定》)中明确了不同类型小程序个人信息收集范围的要求。新通话小程序能够在通话过程中提供客服咨询、商品购买、家电维修等各种类型等用户服务。因此，新通话小程序同时兼具《规定》中定义的“即时通信”和“支付”、“购物”、“生活服务”、“实用工具”等多种属性，必要个人信息则不仅限于注册用户移动电话号码，根据业务场景还可能包括证件信息、支付信息、位置信息等。不同新通话小

程序需要根据所提供功能和服务的类别，按照最小必要原则，以对个人权益影响最小的方式，收集实现业务功能必要的个人信息，并为提供和未提供个人信息的用户提供平等的服务质量和使用体验。

在信息存储和使用方面，新通话小程序需要严格按照 YD/T 4177.1-2022《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第 1 部分：总则》中的要求执行，存储的个人信息需要经过去标识化处理，采用数据加密、数据脱敏、访问控制等安全措施，确保个人信息在存储过程中不被非法访问或篡改，并按照存储时间最小化原则，在超过实现使用目的的最短存储期限后，及时删除或匿名化处理个人信息。使用个人信息时，应消除明确身份指向性，针对通话习惯、社交行为等个性化的新通话业务用户画像要素，应当建立自主控制机制，保障个人信息主体对个性化展示、推送所依赖的个人信息的自主控制权。

在信息传输方面，新通话小程序可通过哈希摘要校验、数字签名、数据水印、区块链技术、应用程序沙盒等风险防范手段，确保个人信息和应用数据的安全传输，保护用户的合法权益。

（五）互通安全

在新通话网络架构下，运营商或第三方提供的小程序被上载到数据通道服务器中，以应用列表的方式呈现于终端的用户通话界面。用户无需提前下载和安装，即可在通话过程中即时选择，并利用数据通道从网络侧下载所需的新通话小程序。

在市场导入阶段，新通话小程序多为运营商自有应用，并主要服务于与其签约的用户群体，即用户只能下载和使用在其签约运营商平台上架的小程序。为了确保跨运营商网络通话时的服务连续性和用户体验的一致性，各家运营商需要确保所提供的同款小程序版本能够相互兼容。同时，第三方应用开发企业也需要分别对接各家运营商新通话平台，开发适配成本较高。**在业务发展阶段，**市场和用户需求增长，第三方应用开发企业加大投入力度，不断丰富新通话应用生态。随着小程序种类和数量的日益繁多，运营商间支持小程序跨网下载和业务交互将成为新通话广泛推广的必要条件。

运营商间小程序互信是实现小程序跨网使用的前提条件。为此，可采用 CA 认证（Certificate Authority，证书颁发机构）机制实现小程序的身份验证和数据加密，确保用户在不同运营商网络间使用小程序时的安全性和信任度。同时，第三方服务提供方也需要做好安全管理，提升服务自身的安全性，针对行业业务差异化特性做好数据传输与业务交互中的安全机制保障。例如银行客服小程序，在涉及用户敏感信息方面，需要做好身份认证、访问控制、数据加密、防泄露防篡改，通过运营商与第三方协同共建安全机制，确保端到端的数据安全传输。

三、新通话未来业务安全

随着用户、设备、业务、平台的多元化发展，新通话网络将面向未来丰富的交互场景提供更灵活的网络开放能力，为话音基础网的可靠性、稳定性、安全性带来了挑战。同时，新通话业务与行业数字化转型的深度融合正在推动新通话应用场景、业务模式持续拓新，加快

了音视频通信到多模态通信的演进，网络安全边界也逐渐趋于模糊化。系统评估新通话未来业务潜在的安全风险，能够帮助业务相关方构建更加完备高效的业务安全能力体系，助力业务健康持续发展。

（一）防诈骗安全

企业主叫名片业务支持运营商通过对企业号码进行实名认证建立安全可信的商业身份。当认证企业员工开展外呼业务时，员工可以使用企业分配的员工账号（即第三方 ID）接入 IMS 网络发起呼叫。运营商网络识别企业外呼并获取当前企业员工的职位、照片等信息，进一步合成企业名片在振铃阶段推送至被叫客户，提前建立企业与客户的信任关系。

然而，恶意用户可能会利用其他员工的账号或伪造账号发起呼叫，已离职的员工也可能利用原有账号发起不当呼叫。另外，员工账号也可能存在被 IMS 网络篡改的情况，导致客户接收到错误的员工信息，对企业形象和客户信任度构成严重影响。

建议通过如下方案解决上述安全问题。首先，加强企业与 IMS 网络的双向认证机制，企业提供的认证服务器与 IMS 网络提供 EDS（企业数据服务器，IMS 网络内安全联盟的企业级数据中心）利用各自部署的 CA 证书和服务器证书借助 TLS、OAuth2、SAML（Security Assertion Markup Language，安全断言标记语言）等一系列安全协议实现双向认证。其次，企业应当动态更新和发放企业员工数据，避免造成 IMS 网络与企业私网的强耦合，减轻企业员工流动性的影响。最后，考虑到企业名片涉及跨网传递，可引入主叫身份签名及被叫网

络验证技术，分别在主叫侧网络针对主叫的用户身份或企业名片进行签名，在被叫网络对主叫的签名进行验证，以确认主叫身份的未被篡改。

（二）能力开放安全

新通话网络架构基于现有 IMS 网络架构进行增强，新增 DCSF、DCAR、MF、DC AS 等网络功能。其中，DC AS 提供数据通道应用程序的业务逻辑控制，包括呼叫事件订阅、控制应用数据通道建立和维护、数据传输和交互处理等，可以部署在运营商 IMS 网络，也可以由第三方数据通道应用程序开发者提供。DCSF 负责数据通道的管理、控制，以及与数据通道应用服务器的对接，北向对接 DC AS 的管理，通过服务化接口把数据通道控制能力开放给 NEF（Network Exposure Function，网络开放功能）或运营商自己运营的 DC AS。

新通话平台将网络和业务能力向第三方开发者开放，需要能力开放网元明确第三方数据通道安全管控要求和策略，具备一定的监控、审查功能。建议统一提供策略控制功能，如频次、流量控制等，以及安全防护功能，如访问控制、接入认证、传输安全、业务安全、敏感数据保护、内容管控等，限制对外 API 访问格式、限制自定义脚本等灵活操控方式，并使用沙盒、风险评估、合规审核等必要审核手段，保障能力开放的安全。

（三）AI 治理安全

通过网络侧引入 AI 能力，新通话可为各类终端提供虚拟头像、背景替换、智能翻译等全新体验。在虚拟头像等应用场景中，AI 换脸

技术通过替换用户的人脸图像来实现不同的效果，为用户带来更多创意和娱乐效果，然而如果该技术被恶意使用，将会增加人脸信息冒用盗用、虚假身份伪装欺骗等风险，例如不法分子利用 AI 换脸技术冒充熟人实施诈骗或者盗取个人信息等，侵害用户权益。

AI 换脸属于《互联网信息服务深度合成管理规定》中第十七条中“显著改变个人身份特征的编辑服务”，应当在提供服务的过程中对生成合成内容添加显著的提示标识，如“该内容使用 AI 换脸”等，提示用户谨慎评估内容的真实性和安全性。另外，可以加强 AI 内容生成的检测及审核机制，利用深度学习模型、特征提取等检测方法提高 AI 换脸技术识别的精准性。

四、新通话业务安全发展策略建议

围绕新通话商用业务对应的网络侧安全、终端及应用服务安全诉求，当前3GPP/CCSA已制定了相对全面的安全标准体系，同时业界小程序和应用最佳安全实践已完备，具备充分保护个人用户和数据安全的能力，能够为新通话商用业务保驾护航。针对新通话未来业务面临的安全挑战，包括防诈骗安全，能力开放安全等，亟需各产业联合定义，推动标准和生态完备建设。

为进一步促进新通话业务安全发展、稳定运营并最大化保护用户权益，建议从内生安全与衍生安全两方面，重新认识、评估业务风险，相关安全发展策略建议如下。

（一）以标准化手段主动强化业务内生安全风险管控

业务内生安全可以理解为在业务设计、开发、部署及维护过程中

产生的安全风险。新通话业务和传统业务相比，最主要内生安全差异在于传统业务全程全网均部署于运营商网络之中，而新通话基于互联网思维，将不断引入新能力。在此过程中，业务内生安全的评估并不是一次完成的，需要在新能力、新形态设计、开发、部署及维护中投入更大的精力，通过标准化工具形成行业共识，不断认识新型电信业务内生安全的内涵，主动提升业务内容安全风险的识别与管控水平。针对新通话快速迭代的能力提升方式，需要建立更为主动的内生安全风险管控体系。

（二）将动态业务衍生安全风险识别融入日常业务运营

业务衍生安全风险可以理解为在业务使用过程中，由使用对象、通信内容和不同业务类型组合使用所引发的一系列潜在风险。新通话业务和语音、短信等业务一样，存在被不法分子利用，传播非法信息、实施电信网络诈骗等损害群众合法权益的风险。衍生安全风险与内生安全风险不同，更具复杂性和不确定性，特别是在风险评估的初期，很难准确预判所有潜在的使用对象及其业务使用方式。因此，业务衍生安全风险需要在业务实际使用中不断地识别与评估，是一个相对长期、甚至可以认为是伴随业务全生命周期的一项长期工作。针对新通话的衍生安全风险，需要在业务运营中引入风险识别与响应能力，及时发现漏洞、警示用户并采取应急手段予以解决。

（三）向互联网业务学习快速迭代业务的风险管控措施

与互联网服务相比，电信业务的创新速度难以满足用户需求，学习互联网服务快速迭代、灵活调整的能力，是电信行业的重要研究方向。为了丰富应用形态，有必要为新通话业务设计更为开放包容的安全管控措施，在业务应用中，促进电信业务学习、吸收新业务形态，不断满足群众对通信能力的新需求。在商业运营期间，新通话业务应内置用户各类风险举报入口，不断提升业务衍生安全风险的发现、识别及管控能力，形成业务风险群防群治的良好格局。

中国信息通信研究院 技术与标准研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62305103

传真：010-62305161

网址：www.caict.ac.cn