实时音视频

协议与策略

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

协议与策略
安全合规认证
信息安全说明
安全白皮书
服务等级协议
实时音视频 TRTC SDK 个人信息保护规则
苹果隐私策略：PrivacyInfo.xcprivacy
合规使用指南

协议与策略
安全合规认证

最近更新时间：2023-01-31 15:31:25

合规性是腾讯云实时音视频发展的基础，腾讯云实时音视频遵从不同国家和行业的合规性要求，除了保证所提供服务的安全性、合规性、可用性、保密性和隐私性之外，还可以为使用实时音视频的客户提供相关支持，满足企业及其客户的多项合规监管需求，降低公司及客户在审计工作上的重复投入，提高审计与管理效率。
实时音视频已通过 SOC 系列审计报告（包括 SOC 1、SOC 2、SOC 3）、网络安全等级保护2.0、ISO 系列认证（包括 ISO 9001、ISO 20000、ISO27001、ISO27017、ISO27018、ISO27701、ISO29151）、CSA STAR、NIST CSF、BS10012 和 K-ISMS 认证。

SOC 1 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 320 针对腾讯云云服务体系的控制环境出具的报告

SOC 2 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 205 以及 TSP section 100 2017版，针对云服务体系的安全性、可用性、机密性出具的报告

SOC 3 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 205 以及 TSP section 100 2017版，针对云服务体系的安全性、可用性、机密性报告出具的一般控制报告

网络安全等级保护2.0

腾讯金融云通过了等级保护四级备案和测评，公有云通过了等级保护三级备案和测评

ISO 9001 质量管理体系认证

腾讯云是国内首家在云计算领域获得 ISO 9001 CNAS 和 ANAB 双认可的云计算服务商，实施有效的质量控制流程交付优质的云服务

ISO 20000 IT 服务管理体系认证

腾讯云是国内首家通过 ISO 20000-1:2018 新版标准认证的云计算服务商，建立并严格执行标准的 IT 服务管理流程

ISO 27001 信息安全管理体系认证

ISO/IEC 27001:2015 是 ISO/IEC 27002:2013 的补充，腾讯云通过 ISO 27001指导证书，证明腾讯云实施了有效设计和实施云计算信息安全控制

ISO 27017 云服务信息安全控制实施指引

ISO/IEC 27017:2015 是 ISO/IEC 27002:2013 的补充，腾讯云通过 ISO 27017指导证书，证明腾讯云实施了有效设计和实施云计算信息安全控制

ISO 27018 公有云个人信息保护认证

腾讯云致力于保护每个客户的个人信息，构建完善的个人信息管理体系，采用各种技术手段保护用户个人信息

ISO 27701 个人信息管理体系国际标准

腾讯云是全球首家通过 ISO/IEC 27701认证的云服务提供商，建立和实施了隐私信息管理体系，并具备持续改进的能力

ISO 29151 个人身份信息保护实践指南

腾讯云提供了恰当的信息安全风险管理环境用于个人身份信息的保护，同时满足行业最佳实践，具备持续改进的能力

CSA STAR 云安全管理体系认证

CSA STAR 是针对云安全特性的一项国际性认证，腾讯云以金牌等级通过了 STAR 认证，强化云安全技术管控

NIST 网络安全框架

NIST CSF 是美国国家标准技术研究所根据行政命令(EO) 13636“改进关键基础设施网络安全”开发，该框架侧重于使用业务驱动因素来指导网络安全活动

KISMS 认证

腾讯云是中国首家通过 KISMS 认证的云计算服务商，证明腾讯云建立的信息安全管理体系和能力满足相关韩国法律和标准合规性要求

BS 10012

英国标准协会发布的个人信息管理体系标准

信息安全说明

最近更新时间：2023-02-09 17:52:41

特对本文做如下声明：

- 本文档意在向客户介绍腾讯云实时音视频（TRTC）产品、服务的安全概况，阐述如何进行信息管理和保护客户及终端用户数据安全。如您对此有强制要求，建议您与腾讯云以书面商业合同（SLA）进行约定。否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。
- 安全特性范围较广，本文仅涉及“部分”技术安全要点。
- 本文档不作为国家或行业信息安全相关标准、要求参考文档。
- 本文经过可阅读性加工，若存在描述不准确的地方请参考第1点。
- 文档解释权归腾讯云所有。

1. 概述

腾讯云实时音视频库通过下列认证并符合下列认证的安全要求：

- ISO 9001认证
- ISO 20000认证
- ISO 27001认证
- ISO 27017认证
- 网络安全等级保护2.0
- 信息安全等级保护（三级）
- CSA STAR 认证，更多安全合规认证。

2. 信息安全保障说明

腾讯云实时音视频的管理安全与技术安全要求符合国家信息安全等级保护（三级），部分要求达到金融行业信息安全（四级）标准。

2.1 信息数据安全

用户与实时音视频服务器间的通讯将受到腾讯云私有传输协议、安全传输层协议和 Web Socket Secure 等协议的保护。实时音视频在传输过程中没有任何可对传输的信息进行解密的密钥。通话内容信息只能在终端设备上（如客户端 App 和本地服务端录制服务器）通过客户授权密钥才能解密。

2.2 数据可用性

- **海量数据中心**：腾讯云实时音视频在全球区域有多个机房共同提供服务。任一机房遭受攻击，都不会影响其他机房的正常运转、不影响整体服务，具有分区隔离保障机制。
- **故障隔离修复**：数据中心若遭遇拒绝服务（DoS）等难以防范的恶意攻击导致服务故障，腾讯云实时音视频会将

故障机器做合理处理，确保整体服务稳定可用。

- **DDoS 攻击防护**：腾讯云实时音视频在使用的数据中心配置了反 DDoS 防火墙，具备足够的能力和资源控制 DDoS 的风险。

2.3 数据分类存储

数据类别	类型说明
个人与企业用户数据	指实时音视频提供产品或服务过程中直接或间接采集的，以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息，以及企业用户 (如政府机关、企事业单位、社会团体、民间组织等)的相关数据，例如企业基本资料、公司经营资质、交易记录等。
终端用户数据	指经客户收集的与终端个人用户设备、网络相关的信息，包括麦克风和摄像头信息、CPU状态、内存状态、电池状态、系统版本、手机型号、手机信号等级、接收的信号强度指示（RSSI）、网络类型、用户属性、房间属性等。
音视频通话数据	客户在通话过程中通过录制产生的音视频数据。
系统运行与安全数据	指控制台功能服务配置、网络和信息系统运维及网络安全数据（不包括个人用户数据）。例如访问TRTC服务器时产生的网络性能数据、网络日志数据、网络监测预警信息等。

实时音视频为客户提供本地化录制和云端录制功能，客户可以对部分或全部通话内容进行录制。在使用云端录制服务时，所有音视频通话录音/录像均存放在客户提供的云存储服务中，实时音视频不会对您的音视频文件进行存储。
实时音视频将对国内站客户数据存储与中国大陆和国际站点，以符合数据安全合规存储的要求。

2.4 访问授权

终端用户进入实时音视频房间时，需要进行动态签名身份认证，阻止恶意攻击盗用您的云服务使用权，详情请参见 安全保护签名 UserSig 说明 。

2.5 访问控制

实时音视频对内部的所有系统实行严格的访问控制管理，所有用户拥有独立内部账号和授权体系，且必须经过二步验证，任何访问记录都会有备案。
所有涉及用户数据服务的机器，均受到严格的审计和保护。实时音视频在非必要情况下不会访问用户的服务器；如因安全等必须访问用户服务器的场景下，实时音视频也会在获取临时授权后访问用户服务器，且这一过程将全程录屏，并保留所有操作记录。

2.6 内部安全审核

腾讯云实时音视频严格进行全面的安全审计和风控管理，审计范围覆盖到服务器上的每个房间和主播观众数据；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；审计记录保存1年以上，且存储在安全等级更高的位置，避免受到未预期的删除、修改或覆盖等。

- **数据库安全审核：**对实时音视频所有业务数据库和数据库所有操作均经过安全审计。
- **管理系统操作审计：**腾讯云实时音视频对内外管理系统的操作均记录详细操作日志，以便于风险追溯。
- **定期风险评估：**腾讯云实时音视频定期对服务器运维管理进行安全评估，进行多地容灾演戏。

2.7 员工安全意识培训

腾讯云实时音视频对所有员工均定期开展信息安全意识及安全合规培训，并所有员工每年定期接受信息保密意识的讲座和培训。

2.8 违规处理

腾讯云实时音视频员工需按要求遵守保密协议及内部安全制度。若员工违反上述要求，会视情况严重程度采取相应的违规处理措施，包括但不限于加强培训教育、解除劳动关系以及追究其他法律责任等。

2.9 潜在安全漏洞

如果您发现实时音视频平台有潜在安全漏洞，请您直接提交工单反馈，我们的技术专家会在第一时间处理并反馈，非常感谢。
为便于验证和定位漏洞，请您提交以下相关内容：

- 您的联系方式。
- 您发现的潜在漏洞功能描述。
- 请结合提供必要的定位方法、问题重现的步骤。

安全白皮书

最近更新时间：2023-07-12 10:28:01

1. 概述

腾讯实时音视频（Tencent Real-Time Communication，TRTC），将腾讯多年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者提供统一、标准化的应用程序接口（Application Programming Interface，API），并为不同行业和场景提供主流操作系统和平台下适配的软件开发工具包（Software Development Kit，SDK）解决方案，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
作为实时音视频 PaaS 云服务行业引领者，数据安全和用户隐私安全是腾讯云实时音视频立身之本的问题。实时音视频始终将数据和用户隐私安全作为首要安全原则，充分将其体现在日常安全能力建设当中。为帮助开发者了解腾讯云实时音视频产品服务的安全保障能力，以下将介绍腾讯云实时音视频 PaaS 服务的安全建设及安全合规审计说明。

2. 安全合规与隐私保护

安全合规性是腾讯云实时音视频发展的基础，腾讯云实时音视频满足不同行业的合规性要求，除了保证所提供服务的安全性、合规性、可用性、保密性和隐私性之外，还可以为使用实时音视频的客户提供相关支持，满足企业及其客户的多项合规监管需求，降低公司及客户在审计工作上的重复投入，提高审计与管理效率。
实时音视频已通过 SOC 系列审计报告（包括 SOC 1、SOC 2、SOC 3）、网络安全等级保护2.0、ISO 系列认证（包括 ISO 9001、ISO 20000、ISO27001、ISO27017、ISO27018、ISO27701、ISO29151）、CSA STAR、NIST CSF、BS10012 和 K-ISMS 认证。

安全合规与隐私保护	说明
ISO/IEC 27001: 2013 信息安全管理标准	ISO/IEC 27001: 2013 是最基础的、获得国际最广泛认可的信息安全管理体系标准。腾讯云实时音视频通过 ISO 27001:2013认证，更能体现企业对安全的承诺，表明企业信息安全管理已建立起一套科学有效的管理体系，能够为用户提供可靠的信息服务。
ISO/IEC 27017: 2015 提供云服务信息安全控制实施指引	ISO/IEC 27017: 2015 是专门针对云服务信息安全的实用标准，为云服务提供商和云服务客户提供特定的安全控制及其实施指南。ISO 27017是基于 ISO 27002延伸的标准，主要目的在于提供云厂商一个云端建设与运维的安全规范，腾讯云实时音视频通过ISO/IEC 27017 认证，证明我们的云服务具有充分的信息安全管理和保障能力。
ISO/IEC 27018: 2019 提供公有云中的个人信息的保护指南	ISO/IEC 27018: 2019 是专注于保护公有云中个人信息的指导标准。它基于信息安全标准 ISO/IEC 27001，提供了适用于公共云中的个人信息保护的补充控制措施，加强对公有云层面的个人信息保护能力。腾讯云实时音视频通过 ISO 27018认证可证明企业在保护企业数据、知识产权、文档和云端 IT 系统安全等方面达到了高标准的行业最佳实践。

CSA STAR 认证	CSA STAR 云安全评估基于国际权威的非盈利组织云安全联盟（Cloud Security Alliance）推出的云控制矩阵 CCM（Cloud Control Matrix），满足云计算安全领域的特定要求，针对云计算安全特性的一项国际性认证；同时它也是 ISO/IEC 27001信息安全管理体系的增强版本，将云安全的特有问题可视化，为云服务商的安全管控能力提供了直观的评估框架。腾讯云实时音视频通过 CSA STAR 认证可证明具有云服务安全的保障能力。
SOC 审计	SOC 报告（System and Organization Controls Reports）是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列报告。 腾讯云作为领先的云服务提供商，在2017年 SOC 审计过程中已经使用了2017版的信托服务标准，是国内率先遵循了2017版信托服务标准的云服务提供商。实时音视频获得此服务鉴证报告，证明我们建立和实施了有效的内部控制，同时会定期接受第三方审核，确保各产品服务均符合鉴证报告要求。
网络安全等级保护认证	网络安全等级保护2.0（简称等保2.0）于2019年12月01日正式实施，等保2.0更加注重主动防御，从被动防御到事前、事中、事后全流程的安全可信、动态感知和全面审计，实现了对传统信息系统、基础信息网络、云计算、移动互联、物联网、大数据和工业控制系统等级保护对象的全覆盖。依据网络安全等级保护2.0的标准及有关规定，腾讯公有云实时音视频 PaaS 服务平台通过了三级备案和测评，标志着我们遵循国家在云计算平台安全建设方面的技术保障要求和安全管理要求。为云平台上行业多样、业务繁多的各企业用户提供了助力等保合规的服务。

3. 数据安全

数据安全是腾讯云实时音视频最为关切的问题之一，实时音视频将开发者数据进行了充分必要的合法合规处理，以保证数据的安全，本节将介绍腾讯云和腾讯云实时音视频在数据安全上采取技术控制措施和管控政策。

3.1 数据安全政策

腾讯云实时音视频坚持以数据保密、完整和高可用作为音视频服务的数据安全发展前提，将数据安全管理建设理念融入音视频PaaS服务建设过程中，腾讯云始终坚持确保开发者数据的可用性、保密性、完整性，即：

- **可用性**：通过腾讯云私有网络传输协议保障数据高可用。
- **保密性**：防止在开发者未经授权下的访问和窃听。
- **完整性**：确保开发者数据完整且不被伪造。

腾讯云实时音视频对其所有员工均定期开始数据安全、隐私合规、数据加密保护的安全培训，并与员工签署保密协议，确保内部员工在开展日常工作维护中，确保落实服务数据的可用性、保密性和完整性。

3.2 数据高可用

实时音视频力图为开发者提供高可用的音视频 PaaS 数据服务：

- **海量数据中心**：腾讯云实时音视频在全球区域有多个机房共同提供服务。任一机房遭受攻击，都不会影响其他机房的正常运转、不影响整体服务，具有分区隔离保障机制。

- **故障隔离修复**：数据中心若遭遇拒绝服务（DoS）等难以防范的恶意攻击导致服务故障，腾讯云实时音视频会将故障机器做合理处理，确保整体服务稳定可用。
- **DDoS 攻击防护**：腾讯云实时音视频在使用的数据中心配置了反 DDoS 防火墙，具备足够的能力和资源控制 DDoS 的风险。

3.3 数据采集

腾讯云实时音视频只采集经用户授权同意的，且产品服务所必须的数据字段，严格按照最小必要原则采集数据；而腾讯云实时音视频开发者收集的用户数据，如程序登录信息、身份识别、密码、支付信息、姓名和地址等，均由开发者自身保管，不在实时音视频平台留存。

3.4 数据脱敏

保护开发者数据隐私，腾讯云实时音视频针对官网控制台的企业和个人信息均进行脱敏后的展示，此策略同样也适用于实时音视频内部系统和其他产品，如内部管理平台、日志打印和监控告警等数据展示渠道。

3.5 数据使用和存储

- 针对开发者的个人或企业用户数据、终端用户数据、音视频通话数据和系统运行与安全数据进行分类分级存储，以保证开发者数据合规安全留存。
- 腾讯云实时音视频的研发过程中严格分离生产、测试和开发环境，确保开发者的真实数据不会直接用于开发和测试，同时，对于开发者及用户的机密信息，如密码等，我们会进行加密存储。
- 如果开发者及用户使用腾讯云实时音视频提供的本地服务端录制 SDK 和云端录制功能，开发者及用户可对部分或全部通话内容进行录制，且所有录像/录音内容均直接写入开发者及用户所提供的存储服务器上而非腾讯云实时音视频服务器进行存储。

4. 腾讯云实时音视频 PaaS 服务安全

实现低延时、高质量的实时互动解决方案对腾讯云实时音视频服务有着严苛的要求，腾讯云实时音视频在构建音视频 PaaS 服务的过程中，充分评估架构技术安全风险的同时，最大程度遵循合规标准中的安全风险控制体系，并将其运用落地在音视频 PaaS 各个环节的建设之中，以保证为开发者及用户提供一套高质量、稳定、安全的音视频 PaaS 解决方案。

4.1 腾讯云实时音视频传输网络安全

实时音视频基于腾讯云私有传输网络，打造了具有超低延时、高质量传输以及支持百万人级实时互动音视频平台。私有传输网络是腾讯云实时音视频 PaaS 的核心服务之一， 它为 音视频服务终端信令的接入、身份鉴权、实时调度、音视频数据实时传输等环节提供合规且安全的服务支撑，同时腾讯云私有传输网络在架构设计上，深入考虑当前互联网环境面临的安全不稳定因素，为了给开发者及用户提供安全稳定的服务，会从以下几点控制措施进行实现。

传输网络安全控制措施	说明
加密传输	为了保证音视频数据在传输过程的机密性，腾讯云实时音视频提供内置加密和自定义加

	密两种方式以提供传输链路的加密保证。腾讯云实时音视频服务 PaaS 默认全局开启内置加密，覆盖 全数据链路，以保证数据传输的加密安全性。
资源隔离	腾讯云实时音视频为每一个音视频应用（SdkAppId）分配专有的资源，确保与其他项目资源彼此独立，为实时音视频提供安全可靠的运算资源保证。对开发者及用户而言，在实时音视频控制台正式注册后，只需要在控制台（Console）上进行简单的操作即可新建实时音视频应用（SdkAppId）并分配对应的资源。
房间隔离	腾讯云实时音视频为每种音频、视频或消息数据传输创建了独立的隔离通道，即房间 Roomid。所有房间在逻辑上是分开的，只有当用户使用具有相同 SdkAppid 的音视频互动应用和相同房间名时，用户才能加入同一频道。房间在会话开始时创建，会话结束（最后一个用户离开）后销毁，通过该机制，在房间层面实现了传输隔离。
身份认证	当用户使用实时音视频应用并接入腾讯云实时音视频 PaaS服务时，实时音视频会通过基于 SdkAppid + 密钥生成的鉴权信息进行进房验证，以帮助有需要的开发者及用户对其用户进行强鉴权。

4.2 腾讯云实时音视频 SDK 安全

腾讯云实时音视频提供 iOS、Android、macOS、Windows、Web、小程序等平台的 SDK 方便客户集成，以满足开发者各个终端平台的实时音视频互动开发集成需求。腾讯云实时音视频 SDK 不仅仅为开发者及用户提供简单、易于集成且安全稳定的音视频开发套件。
实时音视频会竭力为开发者及用户打造合规、安全保障的音视频 PaaS 服务，以减少开发者及用户在应对合规监管和应对信源数据安全威胁方面付出的工作。

SDK 安全支持	说明
SDK 安全与合规性	腾讯云实时音视频 SDK 的可信和安全是腾讯云实时音视频基础的能力保障之一。腾讯云实时音视频在功能迭代时，前期会充分评估功能需求在合规隐私的合理性以及在安全上的风险点，确保符合腾讯云合规和隐私政策。 在功能实现时，实时音视频会在进行充分且必要的质量安全测试，在涉及引用或集成第三方 SDK、库文件时进行安全检测，尤其是合规性确认。
SDK 内容加密	腾讯云实时音视频 SDK 支持使用 AES 128 对称密钥对所有音视频数据流和消息进行数据层面的加密，被加密的数据经腾讯云私有传输网络发送至实时音视频房间中的节点，最终由接收的终端来解密音视频数据内容进行渲染，传输过程中保证数据安全保密。
SDK 安全与合规对开发者的帮助	腾讯云实时音视频始终坚持为开发者提供高质量且安全合法的音视频PaaS服务，腾讯云实时音视频 SDK 提供了安全内容内置加密，以协助开发者及用户完善实时音视频数据安全及隐私合规，最大程度满足客户关于安全和隐私方面的需求，减少此方面的开发成本。

4.3 实时音视频基础计算资源安全

腾讯云实时音视频基础计算资源是由遍布全球上百多个自有分布式数据中心（IDC）和腾讯云云服务器组成，以此保证了实时音视频基础计算资源环境的高扩展、高安全、高可用的特性。

计算资源安全	说明
自有 IDC 中设备的安全管理	腾讯云实时音视频基础设施中自有 IDC 中设备的日常管理中，腾讯云实时音视频制定了一套完备的数据中心管理规范，该规范详细定义了管理办法和服务实施标准，充分体现在了数据中心物理环境安全、日常巡视巡检、异常监控上报和电力资源保障等，已达到腾讯云实时音视频安全合规及基础安全建设要求。
主机、数据库、中间件等计算资源安全	腾讯云实时音视频服务运行所依赖的资源，会根据业务负载合理地调度分配 CPU、内存、磁盘等资源来满足，实时音视频在实际安全运营中，通过制定适配的安全基线、漏洞管理规范，并落地纵深威胁检测机制，在基础服务场景下，充分确保基础运算负载资源的安全性。
防 DDoS 攻击	针对分布式拒绝服务攻击 DDos 对腾讯云实时音视频 PssS 服务的系统和业务可用性产生重大影响，实时音视频结合腾讯云公有云能力，在核心服务上部署了 DDoS 防御方案。该方案能够实时检测并防御来自网络层、传输的 DDoS 攻击。防 DDoS 攻击方案会实时监控网络流量，发现攻击立即清洗，为腾讯云实时音视频服务提供秒级开启防护。

4.4 Web API 安全

为方便开发者高效管理开发自己的音视频业务，腾讯云实时音视频将部分控制台的功能以 RESTful API 的方式供开发者调用。RESTful API 在安全方面提供如下保障：

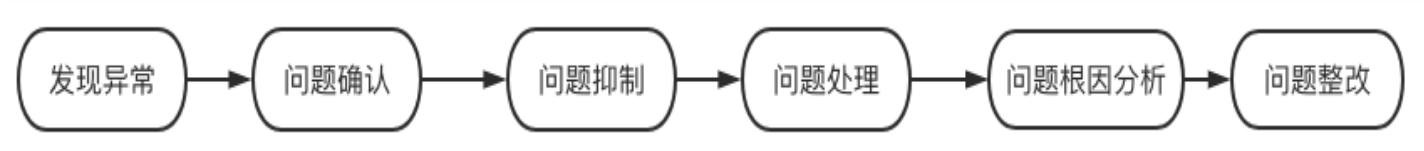
安全保障	说明
身份鉴权	开发者在使用腾讯云实时音视频 RESTful API 前，需先登录腾讯云控制台，创建开发者专属的 SecretId&SecretKey，确保服务者身份唯一性。
输入验证	开发者请求的参数会经过实时音视频服务器后台进行合法性验证，过滤非法参数，以避免一些常见的易受攻击缺陷。
传输安全	RESTful API 仅支持 HTTPS 协议，以确保使用 SSL / TLS 对所有 API 通信进行加密，可以保护 API 凭据和传输的数据。
API 限速	服务端对 API 请求的速率有限制，在保证正常用户请求可以得到响应的同时，限制恶意用户的 API 请求。

5. 安全运营

坚持贯彻合理的安全运营策略，是腾讯云实时音视频实现客户安全、合法合规保障的基础，腾讯云实时音视频基于自身业务特性，通过以下方式保证业务运营安全：

5.1 安全应急响应机制

腾讯云实时音视频基于自身 音视频PaaS业务特性，制定不同的安全事件分类标准，对服务类型进行分类分级，系统性的安全评估和威胁等级，配合完善且高效的处置流程，以确保及时有效地处理安全异常。
简要来说，腾讯云音视频针对功能安全异常会进行如下环节处理：



5.2 业务连续性管理

为了保障腾讯云实时音视频能够 7×24 小时不间断地向开发者及用户提供音视频服务，实现低延时、高品质的音视频服务，产品内部具有专业高效的研发运维团队来负责音视频服务的可用性支撑和管理。

应急响应机制	说明
业务监控与告警	腾讯云实时音视频内部建立了 7×24 小时的高效监控机制，以监测业务服务和系统运行的状态，通过搭建的一套统一完善的监控工具，实现业务服务中涉及的应用、中间件、运算负载、数据库和网络设备等系统组件的运行状态和资源负载等指标进行事件监控和自动化告警，并结合机器人通知值班人员进行第一时间相应处理，确保问题及时发现并恢复服务，保证服务可用性。
灾备与冗余	腾讯云实时音视频在自有核心 IDC 以冗余架构建设上，通过考虑设备的容灾安全性，针对基础设施层，运算负载以及网络结构等方面考虑各种极端业务场景下制定了解决方案。为了进一步保障腾讯云实时音视频基础资源的可用性，结合腾讯云公有云服务器来用于在突发情况下保障音视频服务的高可用。
连续性演练	腾讯云实时音视频为保障音视频重要业务系统持续有效运行，会定期对机房网络、中间件、业务系统等开展安全应急容灾演练，根据每次应急演练的数据进行复盘总结，完善技术架构、运营管理流程和应急预案，以不断完善腾讯云实时音视频服务的稳定性。

5.3 安全监控与反入侵

腾讯云实时音视频 PaaS 服务在落实纵深防御以应对威胁的基础方面，安全团队会在最小权限范围内采集进行安全日志分析。在业务每日产生的日志数据之上，针对识别的安全异常事件，会及时告警，安全运营人员会进一步展开关联以及溯源分析复核；对已核实的潜在风险点，腾讯云实时音视频的应急响应机制会进行处置和追踪，以保障业务系统的安全性和稳定性。

6. 员工安全

保证数据信息安全，腾讯云实时音视频从每一个内部员工出发，在平时运营和管理过程中，严格落实遵守这一准则。腾讯云实时音视频充分认识到人员安全在整体安全层面的重要性，在招聘、入职、培训、离职等流程中，充分考虑员

工的职业道德和基础素养，符合腾讯云的价值观，满足安全合规要求以及业务发展的需要。

流程阶段	说明
招聘	在招聘员工前期阶段，腾讯云实时音视频会通过专业的人力资源专家对候选人的教育学历、过往工作经历进行确认，确保员工专业技能符合条件。
入职	新员工在入职后，会进行学习员工安全行为规范，满足对腾讯云安全合规认知要求。同时，会与每一个员工签署了不同级别的保密协议。针对接触重要数据的岗位员工，会进行更严格的安全合规规范学习并通过考核后才能参与实时音视频日常的建设中。
在职	在职员工，定期参与安全和隐私保护培训并需通过考核。另外腾讯云实时音视频会不定期组织开展内部安全隐私相关的活动，以不断提升全员的安全意识。
离职	离职员工须按照既定离职流程完成交接并关闭访问权限，腾讯云实时音视频将依照该员工签署的保密协议，审计其脱密期的执行情况，告知员工离职后的信息安全保密责任；对于核心关键岗位员工，视情况签署竞业协议。离职员工在完成工作交接、数据清理，并通过审核后，方可离职。

7. 安全责任共担

腾讯云实时音视频作为实时互动音视频 PaaS 云服务平台，实时音视频将对云服务平台和 SDK 的安全进行管控；同时对于开发者作为服务的接入方，需要对自身应用和系统环境的安全进行管控，并根据自身需求，合理使用腾讯云实时音视频提供的安全管控功能，以保障自身信息、平台、程序、系统和网络的安全。

8. 总结

为客户提供安全、合规和稳定的音视频服务PaaS服务是腾讯云实时音视频首要考虑的要素之一，腾讯云实时音视频从人员、技术、管理流程等多个方面系统性推进执行信息安全方案的落地，履行监管合规义务，将其作为日常运营中的规范指导产品服务开发，同时积极研究新技术，以期实现更高效率，高安全自动化的安全保护措施。
保障实时音视频 PaaS 服务的持续高可用，捍卫末端用户的合法权益，腾讯云音视频将竭尽全力打造安全合规的实时互动音视频云服务产品。

服务等级协议

最近更新时间：2023-06-01 14:18:23

详情请参见 实时音视频服务等级协议 。

实时音视频 TRTC SDK 个人信息保护规则

最近更新时间：2024-04-10 09:57:01

更新说明

我们对《腾讯云视立方 SDK 隐私保护指引》进行了更新，更新内容主要为：

- 名称修改为《实时音视频 TRTC SDK 个人信息保护规则》。
- 梳理和重述了开发者使用 SDK 处理个人信息或使用 SDK 构建处理个人信息的 App 的规则。
- 对 SDK 使用第三方 SDK 以及引入第三方服务提供商的披露要求和管理要求做出更新。
- 细化信息主体行使相关权利的机制。
- 删除了处理未成年人个人信息的规则。
- 根据《个人信息保护法》更新了相关术语和表述。

引言

实时音视频 TRTC SDK ，又名 腾讯云视立方 · 实时音视频 SDK （以下简称“ SDK 产品”）由深圳市腾讯计算机系统有限公司（以下简称“我们”）开发，公司注册地为深圳市南山区粤海街道麻岭社区科技中一路腾讯大厦35 层。其中，我们基于原生端实时音视频 TRTC SDK （Android/iOS）设计了跨平台实时音视频 TRTC SDK 产品，包括：实时音视频 TRTC Flutter SDK、实时音视频 TRTC Unity SDK、实时音视频 TRTC ReactNative SDK、实时音视频 TRTC UE4 SDK 4 款跨平台 SDK 产品。上述 4 款跨平台 SDK 隐私保护规则与实时音视频 TRTC SDK 隐私保护规则一致，具体可以参见本规则中适用于实时音视频 TRTC SDK 的内容。《实时音视频 TRTC SDK 个人信息保护规则》（以下简称“本规则”）主要向开发者及其终端用户（“终端用户”）说明，为了实现 SDK 产品的相关功能，SDK 产品将如何处理终端用户的个人信息，“处理”包括收集、存储、使用、加工、传输、提供、公开个人信息等行为。
请开发者及终端用户务必认真阅读本规则。如您是开发者，请您确认充分了解并同意本规则后再集成 SDK 产品，如果您不同意本规则的任何内容，应立即停止接入及使用 SDK 产品。同时，您应仅在获得终端用户的同意后集成 SDK 产品并处理终端用户的个人信息。

特别说明

如您是开发者，您应当：

1. **遵守法律、法规收集、使用和处理终端用户的个人信息，包括但不限于制定和公布有关个人信息保护的隐私政策等。**
2. **在集成 SDK 产品前，告知终端用户 SDK 产品处理终端用户个人信息的情况，并依法获得终端用户同意。**
3. **在获得终端用户的同意前，除非法律法规另有规定，不应收集终端用户的个人信息。**
4. **向终端用户提供易于操作且满足法律法规要求的用户权利实现机制，并告知终端用户如何查阅、复制、修改、删除个人信息，撤回同意，以及限制个人信息处理、转移个人信息、获取个人信息副本和注销账号。**
5. **遵守本规则的所有要求。**

如开发者和终端用户对本规则内容有任何疑问、意见或建议, 可随时通过本规则 第七条 提供的方式与我们联系。

一、我们收集的信息及我们如何使用信息

(一) 为实现 SDK 产品功能所需收集的个人信息

SDK 目前不涉及提供其他扩展业务功能，为实现 SDK 产品的相应功能所必需，我们将向终端用户或开发者收集终端用户在使用与 SDK 产品相关的功能时产生的如下个人信息，如下的个人信息均为必选，无可选个人信息：

个人信息名称	处理目的	使用场景	处理方式	操作系统
Wi-Fi 状态	针对网络类型进行网络优化	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android、iOS
系统属性	针对 Android 兼容性问题进行适配	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android
设备型号	Android/iOS/Windows/Mac 的兼容问题、崩溃问题进行适配和分析	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android、iOS、Windows、MacOS
操作系统	Android/iOS/Windows/Mac的兼容问题、崩溃问题进行适配和分析	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android、iOS、Windows、MacOS
IP 地址	检测网络链连接质量	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android、iOS、Windows、MacOS
相机	**视频通话时采集视频画面**	**在视频通话场景中**	**去标识化、加密传输的安全处理方式**	**Android、iOS**
录音	**音频通话时采集声音**	**在语音通话场景中**	**去标识化、加密传输的安全处理方式**	**Android、iOS**
加速度传感器	获取手机横竖屏状态来适配采集画面的方向	在视频通话场景中	本地处理、不传输不上报	Android、iOS
显卡硬件设备的 PCI ID	将硬编码器初始化 crash 状态写入本地注册表	在视频、语音通话场景中	本地处理、不传输不上报	Windows
CPU 信息	iOS/Mac 的兼容问题、崩溃问题进行适配和分析	在视频、语音通话场景中	本地处理、不传输不上报	iOS、MacOS

为实现 SDK 产品的相应功能所必需，我们会在 SDK 产品中嵌入第三方 SDK ，第三方 SDK 的信息如下：

第三方SDK名称	第三方SDK提供方的公司名称	处理的个人信息类型	使用目的	使用场景	处理方式	第三方SDK个人信息保护规则	操作系统
硬件耳返	华为技术有限公司	音频数据	在华为设备上开启/关闭硬件耳返功能	合唱、K歌中需要听到自己的声音等场景	采集华为设备终端的音频信息并在本终端上进行实时播放（仅限连接有耳机时）	文档	Android

(二) 为实现 SDK 产品功能所需的权限

SDK 目前不涉及提供其他扩展业务功能，为实现 SDK 产品的相应功能所必需，我们可能通过开发者的应用申请开启终端用户设备操作系统的特定权限，如下的权限均为必选，无可选权限：

操作系统	权限名称	使用目的
Android	android.permission.CAMERA	用于采集摄像头画面，与其他使用者进行交互、录制画面
	android.permission.RECORD_AUDIO	用于采集用户声音，与其他使用者进行交互、录制声音
	android.permission.WRITE_EXTERNAL_STORAGE	存储 SDK 配置文件和日志文件
	android.permission.READ_EXTERNAL_STORAGE	读取 SDK 配置文件和日志文件
	android.permission.BLUETOOTH	需要支持蓝牙耳机和耳麦的接入
	android.permission.READ_PHONE_STATE	SDK 需要监听电话的打断，在电话呼入时，停止音频的采集
iOS	NSCameraUsageDescription	使用视频通话功能，需要开启摄像头
	NSMicrophoneUsageDescription	使用视频通话功能，需要开启麦克风

请注意，在不同设备和系统中，权限显示方式及关闭方式可能有所不同，请终端用户参考其使用的设备及操作系统开发方的说明或指引。当终端用户关闭权限即代表其取消了相应的授权，我们和开发者将无法继续收集和使用对应的个人信息，也无法为终端用户提供上述与该等授权所对应的功能。

(三) 根据法律法规的规定，以下是征得用户同意的例外情形

1. 为订立、履行与终端用户的合同所必需。
2. 为履行我们的法定义务所必需。
3. 为应对突发公共卫生事件，或者紧急情况下为保护终端用户的生命健康和财产安全所必需。
4. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理终端用户的个人信息。
5. 依照本法规定在合理的范围内处理终端用户自行公开或者其他已经合法公开的个人信息。
6. 法律行政法规规定的其他情形。

特别提示: 如我们收集的信息无法单独或结合其他信息识别到终端用户的个人身份，其不属于法律意义上的个人信息。

二、第三方数据处理及信息的公开披露

- 我们不会与我们的关联公司、合作伙伴及第三方共享（“接收方”）终端用户的个人信息。
- 我们与第三方合作过程中，将遵守法律规定，按照最小必要原则，安全审慎地处理相关数据。
- 我们将按照法律法规的规定，对数据处理涉及的第三方进行严格的限制，要求其严格遵守我们关于个人信息保护的措施与要求。
- 我们不会将终端用户的个人信息转移给任何公司、组织和个人，但以下情况除外：
  - 事先告知终端用户转移个人信息的种类、目的、方式和范围，并获得终端用户的单独同意。
  - 如涉及合并、分立、解散、被宣告破产等原因需要转移个人信息的，我们会向终端用户告知接收方的名称或者姓名和联系方式，并要求接收方继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，我们会要求接收方重新取得终端用户的同意。
- 我们不会公开披露终端用户的个人信息，但以下情况除外：
  - 告知终端用户公开披露的个人信息的种类、目的、方式和范围并获得终端用户的单独同意后。
  - 在法律法规、法律程序、诉讼或政府主管部门强制要求的情况下。

三、终端用户如何管理自己的信息

我们非常重视终端用户对其个人信息管理的权利，并尽全力帮助终端用户管理其个人信息，包括个人信息查阅、复制、修改、删除、撤回同意、限制个人信息处理、获取个人信息副本、注销账号以及设置隐私功能等，以使终端用户有能力保障自身的隐私和信息安全。
如您是开发者，您应当为终端用户提供并明确其查阅、复制、修改、删除个人信息、撤回同意、转移个人信息、限制个人信息处理、获取个人信息副本和注销账号的方式。
如您是终端用户，由于您不是我们的直接用户，与我们无直接的交互对话界面，为保障您的权利实现，我们已要求开发者提供便于操作的用户权利实现方式。您也可通过本规则 第七条 中的方式与我们取得联系。请您理解，特定的业

务功能和服务将需要您的信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供对应的功能和服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响我们此前基于您的授权而开展的个人信息处理。

四、信息的存储

(一) 存储信息的地点

我们遵守法律法规的规定，将在中华人民共和国境内收集和产生的个人信息存储在境内。

(二) 存储信息的期限

一般而言，我们仅在为实现目的所必需的最短时间内保留终端用户的个人信息，但下列情况除外：

- 为遵守适用的法律法规等有关规定。
- 为遵守法院判决、裁定或其他法律程序的规定。
- 为遵守相关政府机关执法的要求。

五、信息安全

- 我们为终端用户的个人信息提供相应的安全保障，以防止信息的丢失、不当使用、未经授权访问或披露。
- 我们严格遵守法律法规保护终端用户的个人信息。
- 我们将在合理的安全水平内使用各种安全保护措施以保障信息的安全。
  例如，我们使用加密技术、匿名化处理等手段来保护终端用户的个人信息。
- 我们建立专门的管理制度、流程和组织确保信息安全。
  例如，我们严格限制访问信息的人员范围，要求他们遵守保密义务，并进行审查。
- 若发生个人信息泄露等安全事件，我们会启动应急预案，阻止安全事件扩大，并以推送通知、公告等形式告知开发者。

六、变更

我们可能适时修订本规则的内容。
如该等变更会导致终端用户在本规则项下权利的实质减损，我们将在变更生效前，通过网站公告等方式进行提示。如您是开发者，当更新后的本规则对处理终端用户的个人信息情况有重大变化的，您应当适时更新隐私政策，并以弹框形式通知终端用户并且获得其同意，如果终端用户不同意接受本规则，请停止集成 SDK 产品。

七、联系我们

我们设立了专门的个人信息保护团队和个人信息保护负责人，如果开发者和/或终端用户对本规则或个人信息保护相关事宜有任何疑问或投诉、建议时，可以通过以下方式与我们联系：

- 通过 https://kf.qq.com/ 与我们联系。
- 将问题发送至 Dataprivacy@tencent.com。
- 邮寄信件至：中国广东省深圳市南山区海天二路33号腾讯滨海大厦 数据隐私保护部（收）邮编：518054。

我们将尽快审核所涉问题，并在15个工作日或法律法规规定的期限内予以反馈。

苹果隐私策略：PrivacyInfo.xcprivacy

最近更新时间：2024-04-19 19:04:22

根据苹果公司发布的 App Store 提交的隐私更新，自2024年春季开始，上架 App Store 的应用需要同时提供一份 App 的**隐私清单文件**。
当您准备分发 App 时，Xcode 会将 App 使用的所有第三方 SDK 的隐私清单合并为一个简单易用的报告。
这个报告内容全面，总结了 App 中的所有第三方 SDK，让您能够更轻松地创建更准确的隐私标签。
因此嵌入 App 的 SDK 和三方库都需要包含 **PrivacyInfo.xcprivacy** 。

实时音视频 TRTC 的适配

在 **11.7** 及以上版本的 TRTC SDK（包含精简版和全功能版）会默认包含 **PrivacyInfo.xcprivacy** 文件。
在 **2.3.0.920** 及以上版本的 TUICallKit 会默认包含 **PrivacyInfo.xcprivacy** 文件。
在 **2.3.0** 及以上版本的 TUIRoomKit 会默认包含 **PrivacyInfo.xcprivacy** 文件。

- 当您使用 CocoaPod 集成时，我们会通过 Pod 为您添加 **PrivacyInfo.xcprivacy** 到工程内，**您无需为此做额外工作。**
- 当您手动集成时，请注意需要将源代码目录下的 **PrivacyInfo.xcprivacy 拷贝进您的代码工程里。**

> **注意：**
> 由于 TUIKit 方案与 TRTC SDK 的全功能版本（Professional）包含了多个 SDK 产品，**PrivacyInfo.xcprivacy** 的内容上会略有差异，您可以根据需要选择对应的文件版本。

TRTC 相关的 PrivacyInfo.xcprivacy

精简版（TRTC）SDK

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NSPrivacyCollectedDataTypes</key>
  <array>
    <dict>
      <key>NSPrivacyCollectedDataType</key>
      <string>NSPrivacyCollectedDataTypeUserID</string>
      <key>NSPrivacyCollectedDataTypeLinked</key>
      <false/>
      <key>NSPrivacyCollectedDataTypeTracking</key>
```

```
        <false/>
        <key>NSPrivacyCollectedDataTypePurposes</key>
        <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
        </array>
    </dict>
    <dict>
        <key>NSPrivacyCollectedDataType</key>
        <string>NSPrivacyCollectedDataTypeOtherDiagnosticData</string>
        <key>NSPrivacyCollectedDataTypeLinked</key>
        <false/>
        <key>NSPrivacyCollectedDataTypeTracking</key>
        <false/>
        <key>NSPrivacyCollectedDataTypePurposes</key>
        <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
        </array>
    </dict>
    <dict>
        <key>NSPrivacyCollectedDataType</key>
        <string>NSPrivacyCollectedDataTypePhotosorVideos</string>
        <key>NSPrivacyCollectedDataTypeLinked</key>
        <false/>
        <key>NSPrivacyCollectedDataTypeTracking</key>
        <false/>
        <key>NSPrivacyCollectedDataTypePurposes</key>
        <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
        </array>
    </dict>
    <dict>
        <key>NSPrivacyCollectedDataType</key>
        <string>NSPrivacyCollectedDataTypeAudioData</string>
        <key>NSPrivacyCollectedDataTypeLinked</key>
        <false/>
        <key>NSPrivacyCollectedDataTypeTracking</key>
        <false/>
        <key>NSPrivacyCollectedDataTypePurposes</key>
        <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
        </array>
```

```
        </dict>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypePerformanceData</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>C56D.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryFileTimestamp</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>0A2A.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>35F9.1</string>
            </array>
        </dict>
    </array>
</dict>
</plist>
```

全功能版（Professional）SDK

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>NSPrivacyCollectedDataTypes</key>
   <array>
      <dict>
         <key>NSPrivacyCollectedDataType</key>
         <string>NSPrivacyCollectedDataTypeUserID</string>
         <key>NSPrivacyCollectedDataTypeLinked</key>
         <false/>
         <key>NSPrivacyCollectedDataTypeTracking</key>
         <false/>
         <key>NSPrivacyCollectedDataTypePurposes</key>
         <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
         </array>
      </dict>
      <dict>
         <key>NSPrivacyCollectedDataType</key>
         <string>NSPrivacyCollectedDataTypeOtherDiagnosticData</string>
         <key>NSPrivacyCollectedDataTypeLinked</key>
         <false/>
         <key>NSPrivacyCollectedDataTypeTracking</key>
         <false/>
         <key>NSPrivacyCollectedDataTypePurposes</key>
         <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
         </array>
      </dict>
      <dict>
         <key>NSPrivacyCollectedDataType</key>
         <string>NSPrivacyCollectedDataTypePhotosorVideos</string>
         <key>NSPrivacyCollectedDataTypeLinked</key>
         <false/>
         <key>NSPrivacyCollectedDataTypeTracking</key>
```

```
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeAudioData</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypePerformanceData</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>E174.1</string>
            </array>
        </dict>
        <dict>
```

```
        <key>NSPrivacyAccessedAPIType</key>
        <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
        <key>NSPrivacyAccessedAPITypeReasons</key>
        <array>
            <string>C56D.1</string>
        </array>
    </dict>
    <dict>
        <key>NSPrivacyAccessedAPIType</key>
        <string>NSPrivacyAccessedAPICategoryFileTimestamp</string>
        <key>NSPrivacyAccessedAPITypeReasons</key>
        <array>
            <string>0A2A.1</string>
        </array>
    </dict>
    <dict>
        <key>NSPrivacyAccessedAPIType</key>
        <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
        <key>NSPrivacyAccessedAPITypeReasons</key>
        <array>
            <string>35F9.1</string>
        </array>
    </dict>
  </array>
</dict>
</plist>
```

TUICallKit

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NSPrivacyTracking</key>
  <false/>
  <key>NSPrivacyTrackingDomains</key>
  <array/>
  <key>NSPrivacyCollectedDataTypes</key>
  <array>
    <dict>
```

```
        <key>NSPrivacyCollectedDataType</key>
        <string>NSPrivacyCollectedDataTypeUserID</string>
        <key>NSPrivacyCollectedDataTypeLinked</key>
        <false/>
        <key>NSPrivacyCollectedDataTypeTracking</key>
        <false/>
        <key>NSPrivacyCollectedDataTypePurposes</key>
        <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
        </array>
      </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
      <dict>
        <key>NSPrivacyAccessedAPIType</key>
        <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
        <key>NSPrivacyAccessedAPITypeReasons</key>
        <array>
          <string>E174.1</string>
        </array>
      </dict>
      <dict>
        <key>NSPrivacyAccessedAPIType</key>
        <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
        <key>NSPrivacyAccessedAPITypeReasons</key>
        <array>
          <string>CA92.1</string>
        </array>
      </dict>
    </array>
</dict>
</plist>
```

TUIRoomKit

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
    <key>NSPrivacyTracking</key>
    <false/>
    <key>NSPrivacyTrackingDomains</key>
    <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>35F9.1</string>
            </array>
        </dict>
    </array>
</dict>
</plist>
```

手动导入自身 App

除了通过 CocoaPod 自动导入 PrivacyInfo 外，您还可以直接将 TRTC SDK（或相关版本）的 **PrivacyInfo.xcprivacy** 中的条款补全到自身 App 的**PrivacyInfo.xcprivacy** 中。具体补全方式可以参见以下内容：

- 使用 Source Code 方式添加

Xcode 中使用 Source Code方式打开 app 项目下的 **PrivacyInfo.xcprivacy** 。复制腾讯云 **PrivacyInfo.xcprivacy** 中的条目，注意不要重复添加或错行。

- 使用 Property List 的方式添加

  在 Xcode 中双击打开 **PrivacyInfo.xcprivacy** 文件，在其中点击+，Xcode 会提示可选的条款和可设置项，按照需求进行增补即可。

合规使用指南

最近更新时间：2024-03-11 17:32:21

为帮助使用实时音视频 TRTC SDK 的开发运营者（以下简称“您”）在符合个人信息保护相关法律法规、政策及标准的规定下合规接入、使用第三方 SDK，深圳市腾讯计算机系统有限公司（以下简称"我们"）特制定《实时音视频 TRTC SDK 接入使用说明文档》（以下简称“文档”），便于您使用实时音视频 TRTC SDK 过程中符合相应的合规要求。请您在接入、使用实时音视频 TRTC SDK 前，充分阅读和了解本文档内容。

一、接入/升级至满足监管新规的最新 SDK 版本

我们高度重视 SDK 的功能优化、个人信息安全和保护，将适时升级迭代 SDK 版本以提升产品的安全性和稳定性，确保符合相关法律法规及、监管及标准的最新合规要求。强烈建议您升级使用最新版本 SDK，以便保障您正常使用 SDK 最新功能、避免因您更新不及时产生的不利影响（例如 App 被通报或下架等）。

SDK 更新后，我们会及时通过官网公告通知或其他适当的方式提醒您更新的内容，以便您及时了解 SDK 最新版本信息。同时，您可以访问 SDK 最新版本 下载链接 。

二、App 隐私政策中应披露第三方 SDK 相关情况

请您确保您开发或运营的 App 配备了符合监管要求的《隐私政策》文本。请您务必明确告知终端用户您的 App 集成了第三方 SDK 服务。您应在《隐私政策》中添加关于本 SDK 收集使用个人信息的目的、方式和范围等，并显示本 SDK 的开发运营者名称及隐私政策链接。

我们提供以下告知文案示例供您参考，您可以通过文字或表格方式向用户告知。请您理解 SDK 不同版本提供的功能服务及所需的字段信息可能会因开发者的选择或配置不同而存在差异，因此请您参考 SDK 隐私政策及您实际接入使用的 SDK 运行情况向用户进行充分告知并获得用户的同意。

仅 Android 参考示例：

```
第三方 SDK 名称：实时音视频 TRTC SDK
第三方 SDK 提供方的公司名称：深圳市腾讯计算机系统有限公司
使用目的及功能场景：提供实时音视频通信服务，主要场景包括音视频通话、在线会议、在线课
堂、互动直播等等
处理的个人信息类型：Wi-Fi 状态、系统属性、设备型号、操作系统、IP 地址、相机、录音、传感
器信息
实现 SDK 产品功能所需的权限：相机、录音、存储读写、蓝牙、电话状态权限
第三方 SDK 隐私政策链接：实时音视频 TRTC SDK 个人信息保护规则
```

仅 iOS 参考示例：

```
第三方 SDK 名称：实时音视频 TRTC SDK
```

第三方 SDK 提供方的公司名称：深圳市腾讯计算机系统有限公司
使用目的及功能场景：提供实时音视频通信服务，主要场景包括音视频通话、在线会议、在线课堂、互动直播等等
处理的个人信息类型：Wi-Fi 状态、设备型号、操作系统、IP 地址、相机、录音、传感器信息、CPU 信息
实现 SDK 产品功能所需的权限：相机、录音权限
第三方 SDK 隐私政策链接：实时音视频 TRTC SDK 个人信息保护规则

三、获得用户同意后再初始化 SDK

为满足法律法规及监管要求，您应确保在获得用户的同意后再初始化 SDK，并在用户触发 SDK 具体功能服务后通过配置 SDK 的相关参数完成发送请求的调用，此时 SDK 才会按照您设置的配置方式采集功能所需的个人信息或申请功能所需的权限。为了避免您在获取用户同意前，提前启动 SDK 收集使用用户个人信息，SDK 提供了延迟 SDK 初始化调用的 API 接口、合规初始化技术配置方案，点击这里 查看详细操作指引（以 Android 平台为例）。

1、第一步：确保在用户阅读 App 隐私政策并取得用户授权之后，按 App 功能需要在合适时机调用正式初始化函数 `sharedInstance` 初始化 SDK。反之，如果用户不同意《隐私政策》授权，则不能调用正式初始化函数。
2、第二步：按照您 App 功能场景调用 SDK 功能配置参数，在用户触发具体功能场景时完成 SDK 功能的调用。

四、可选信息配置开关

1、配置可选权限

SDK 目前不涉及提供其他扩展业务功能，为实现 SDK 产品的相应功能所必需，我们可能通过开发者的应用申请开启终端用户设备操作系统的特定权限，如下的权限均为必选：

操作系统	权限名称	使用目的
Android	android.permission.CAMERA	用于采集摄像头画面，与其他使用者进行交互、录制画面
	android.permission.RECORD_AUDIO	用于采集用户声音，与其他使用者进行交互、录制声音
	android.permission.WRITE_EXTERNAL_STORAGE	存储 SDK 配置文件和日志文件
	android.permission.READ_EXTERNAL_STORAGE	读取 SDK 配置文件和日志文件
	android.permission.BLUETOOTH	需要支持蓝牙耳机和耳麦的接入

	android.permission.READ_PHONE_STATE	SDK 需要监听电话的打断，在电话呼入时，停止音频的采集
iOS	NSCameraUsageDescription	使用视频通话功能，需要开启摄像头
	NSMicrophoneUsageDescription	使用视频通话功能，需要开启麦克风

请注意，在不同设备和系统中，权限显示方式及关闭方式可能有所不同，请终端用户参考其使用的设备及操作系统开发方的说明或指引。当终端用户关闭权限即代表其取消了相应的授权，我们和开发者将无法继续收集和使用对应的个人信息，也无法为终端用户提供上述与该等授权所对应的功能。

2、配置可选个人信息

SDK 目前不涉及提供其他扩展业务功能，所需个人信息均为实现业务功能所需的必须个人信息，暂无可选个人信息。

3、配置可按照不同频次、精度收集个人信息

SDK 的数据采集仅在 App 调用/最终用户触发相关功能时触发，不涉及定时逻辑等频次控制选项。

4、指导建议

请您重点关注，在 APP 安装、运行和使用相关功能时，您应遵从国家相关法律法规、监管政策及标准的要求，收集用户个人信息或申请敏感权限，不得存在以下违规行为：
（1）未经用户同意不得收集任何个人信息。
（2）非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用不得自动退出或关闭。
（3）在用户明确拒绝权限申请后，APP 不应向用户频繁弹窗或反复申请开启与当前服务场景无关的权限、影响用户正常使用，建议掌握合适时机申请敏感权限，不得影响其他功能可用。
（4）不得未明确告知用户索取权限的目的和用途。
（5）APP 首次打开或运行中，未见使用权限对应的相关功能或服务时，不应提前向用户弹窗申请开启敏感权限。
（6）不得超出业务功能实际需要过度收集个人信息。

五、用户权利保障机制

本 SDK 提供以下接口配置，以便您帮助终端用户实现个人信息主体权利请求。
1、终端用户撤销同意处理其个人信息的授权时，您可通过调用 `destroySharedInstance` 接口停止使用 SDK 功能并停止采集与关闭功能相应的用户数据，点击 此处 查看接口使用的操作指导。
2、如果您需要我们协助来实现您最终用户的其他个人信息主体权利请求，您可以通过“联系方式”来申请协助。

六、联系方式

我们设立了专门的个人信息保护团队和个人信息保护负责人，如果您和/或终端用户对本规则或个人信息保护相关事宜有任何疑问或投诉、建议时，可以通过以下方式与我们联系：
(i)通过 腾讯客服（ https://kf.qq.com/ ）或 填写工单 与我们联系

(ii)将问题发送至 Dataprivacy@tencent.com；
(iii)邮寄信件至: 中国广东省深圳市南山区海天二路33号腾讯滨海大厦 数据隐私保护部(收)邮编: 518054。
我们将尽快审核所涉问题, 并在15个工作日或法律法规规定的期限内予以反馈。

七、注意事项

1、您接入实时音视频 TRTC SDK 前的合规自查。
为确保您就本 SDK 的使用获得终端用户的授权，且遵守个人信息保护要求和合规流程，我们建议您在接入实时音视频 TRTC SDK 前进行合规自查。
1）请仔细阅读并按本说明文档提示对您 App 的《隐私政策》进行合规自查。
2）请务必做延迟初始化配置，确保获得用户同意后再初始化 SDK。
3）当实时音视频 TRTC SDK 基于最新的法律法规或监管要求进行更新后，请您在收到版本更新通知时及时将您 App 集成的实时音视频 TRTC SDK 升级到最新版本。
4）其他国家相关法律法规、监管政策及标准的要求。

2、以下合规文件供开发者参考：
（1）《个人信息保护法》
（2）《工业和信息化部关于开展信息通信服务感知提升行动的通知》
（3）《工业和信息化部关于开展纵深推进 App 侵害用户权益专项整治行动的通知》
（4）《工业和信息化部关于开展 App 侵害用户权益专项整治工作的通知》
（5）《App 违法违规收集使用个人信息行为认定方法》
（6）《App 违法违规收集使用个人信息自评估指南》
（7）《常见类型移动互联网应用程序必要个人信息范围规定》
（8）《GB/T 35273-2020信息安全技术 个人信息安全规范》
（9）《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》
（10）《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》