

号码认证 相关协议



腾讯云

【 版权声明 】

©2013–2025 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 】



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

相关协议

SDK 个人信息保护规则

SDK 合规使用指南

相关协议

SDK 个人信息保护规则

最近更新时间：2024-12-27 15:19:32

更新说明

我们对《号码认证 SDK 隐私保护指引》进行了更新：

- 2024年12月26日更新说明：

更新内容主要为：

- 1.1. 新增号码认证SDK（Harmony）收集的个人信息和获取的权限信息。
- 1.2. 更新了号码认证 SDK（Android、iOS）获取的权限信息。

- 2024年01月05日更新说明：

更新内容主要为：

- 1.1. 细化说明 SDK 的基本业务功能和扩展业务功能。
- 1.2. 更新了号码认证 SDK 收集的个人信息，并细化说明 SDK 收集的可选、必选个人信息。
- 1.3. 更新了号码认证 SDK 获取的权限信息。
- 1.4. 添加了 Cookie 使用指南。
- 1.5. 更新了关于个人信息共享、转让、披露的相关描述。
- 1.6. 添加了未成年人保护规则。

- 2023年10月09日更新说明：

更新内容主要为：

- 1.1 增加了号码认证 SDK 收集的个人信息“手机型号”。
- 1.2 增加了第三方 SDK 以及第三方 SDK 处理的个人信息“手机型号”。

- 2022年03月23日更新说明：

更新内容主要为：

- 1.1 名称修改为《号码认证 SDK 个人信息保护规则》。
- 1.2 整理和重述了 App 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。
- 1.3 对 SDK 使用第三方 SDK 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。
- 1.4 增加对 SDK 可能具有的推送功能的处理规则。
- 1.5 因不涉及未成年人信息处理，删除了处理未成人个人信息的规则。
- 1.6 根据《个人信息保护法》更新了相关术语和表述。
- 1.7 更新了号码认证 SDK 收集的个人信息。
- 1.8 更新了号码认证 SDK 使用的第三方 SDK 的相关信息。
- 1.9 更新了号码认证 SDK 获取的权限信息。
- 1.10 因不涉及 Cookie 技术的应用，删除了关于 Cookie 的相关描述。
- 1.11 更新了关于信息共享的相关描述。

腾讯严格遵守法律法规，按照业界成熟的安全与隐私标准，保护第三方开发者和其终端用户的个人信息。

腾讯云号码认证 SDK 是一款由腾讯云计算（北京）有限责任公司（以下简称“我们”）提供服务的产品，号码认证区别于传统的短信下发验证，集成了三大运营商特有的网关取号、验证能力，通过运营商底层数据网关和短信网关识别本机号码，从源头规避数据泄漏风险，安全、快速地验证用户身份，实现一键免密注册、登录、校验，提升用户使用体验。我们的注册地为北京市海淀区知春路49号3层西部309。腾讯云号码认证产品对接方式包括【SDK】，由于目前相关法律法规、政策及标准中主要对 SDK 产品的应用提供相关指引，以下将统一以 SDK 视角描述相关内容，如果您是集成、调用API能力或H5页面的第三方开发者，本指引中的内容同样适用于您。

《腾讯云号码认证 SDK 个人信息保护规则》主要向第三方开发者和其终端用户说明我们如何处理个人信息（处理包括“收集、存储、使用、加工、传输、提供、公开等”）。在注册、接入、使用腾讯云号码认证 SDK（以下简称“本SDK”）产品和/或服务前，请第三方开发者和终端用户务必仔细阅读本声明。同时，请第三方开发者将本声明提供给第三方的终端用户，以便最终用户了解本声明相关内容并获得用户同意。如果第三方开发者或终端用户不同意本声明，应立即停止接入及使用本 SDK 产品和/或服务。在获得终端用户的同意前，除非法律法规另行允许，不应收集终端用户的任何个人信息，不应启用本 SDK 产品及/或服务。

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. 告知终端用户 SDK 产品收集、使用和处理终端用户个人信息的情况，并依法征得终端用户同意，在征得终端用户同意后初始化SDK产品；
3. 在征得终端用户的同意前、以及在用户触发相应功能场景前，除非法律法规另有规定，不应收集任何终端用户的个人信息；
4. 应按您的应用的具体功能场景，在用户触发具体功能场景时调用SDK的相应功能、调用相应权限或处理终端用户的个人信息，未到具体功能场景时不应调用相应的SDK功能、调用相应权限或处理终端用户的个人信息；
5. 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；
6. 遵守本规则的要求，并详细阅读《SDK 合规使用指南》查看详细操作指引。

我们对个人敏感信息采用“加黑”的书写方式进行特别提醒。如对本声明内容有任何疑问、意见或建议，可随时通过本声明 [第九条](#) 提供的方式与我们联系。

一、如何收集和使用第三方开发者和/或终端用户的个人信息

我们遵循正当、合法、必要的原则，基于本声明所述的以下目的，收集和使用：

1. 第三方开发者和/或终端用户主动提供或我们直接收集的个人信息。
2. 第三方终端用户在使用本 SDK 产品和/或服务过程中产生的个人信息。
3. 从第三方开发者或者其他第三方获取的第三方开发者和/或终端用户的个人信息。

我们通常会在征得第三方开发者和/或终端用户同意后收集个人信息。我们会在本声明中载明收集的个人信息用途，如果我们要将收集个人信息用于本声明未载明的其它用途，我们会以合理的方式向第三方开发者和/或终端用户告知，并在使用前再次征得第三方开发者和/或终端用户的同意。

（一）第三方开发者和/或终端用户主动提供或我们直接收集的个人信息

为实现 SDK 产品的基本业务功能所必须，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。SDK 目前不涉及提供其他扩展业务功能，如后续提供其他扩展业务功能，将通过本隐私政策进行说明并通过《SDK 合规使用指南》为开发者提供扩展功能的配置方式和示例。

关于腾讯云号码认证 SDK 所收集的个人信息清单如下表所示（Android 、iOS 及Harmony相同）：

服务方案	收集的个人信息类型	使用目的及功能场景	处理方式	敏感个人信息处理的必要性说明
一键登录能力	【必选】网络类型	【基本业务功能】采集用于判断当前网络是 WI-FI 还是数据，用于精确取号	1. 采用 SSL 协议加密及 HTTPS 传输加密技术保障安全 2. 采取加密、去标识化等安全措施脱敏处理	无
	【必选】IP地址	【基本业务功能】调用SDK预取号接口、获取一键登录或验证 Token 接口时使用		无
	【必选】运营商类型	【基本业务功能】采集用于判断运营商归属		无
	【必选】手机型号	【基本业务功能】用于对不同型号的设备做个性化的适配，分析当前设备的风险等级，可有效识别作弊行为，剔除作弊设备，识别恶意刷量、恶意程序、保护用户账号安全等		无
	【必选】手机操作系统	【基本业务功能】采集用于判断终端类型，用于确定一键登录的终端适配方案		无
	【必选】硬件厂商	【基本业务功能】采集用于判断终端类型，用于确定一键登录的终端适配方案		无
	【必选】SIM卡状态	【基本业务功能】采集用于判断SIM卡的状态，用于一键获取您的手机号码		无

本 SDK 除自身提供相关服务并需收集相关信息外，还会集成其他可供第三方开发者选择是否接入的第三方 SDK ，此部分第三方 SDK 所收集的个人信息请开发者和终端用户查看第三方 SDK 的隐私政策或类似文件。

本 SDK 接入的第三方 SDK 以及第三方 SDK 的个人信息处理清单具体如下：

第三方 SDK 名称	第三方 SDK 提供方的公司名称	集成第三方 SDK 使用目的	收集的个人信息类型	使用目的及功能场景	处理方式	第三方 SDK 信息保护规则
移动认证	中移互联网有限公司	实现一键登录	【必选】网络类型	【基本业务功能】采集用于判断当前网络是 WI-FI 还是数据，用于精确取号	1. 采用 SSL 协议加密及 HTTPS 传输加密技术保障安全。 2. 采取加密、去标识化等安全措施脱敏处理。	中国移动认证隐私政策
			【必选】IP 地址	【基本业务功能】调用 SDK 预取号接口、获取一键登录或验证 Token 接口时使用		
			【必选】运营商类型	【基本业务功能】采集用于判断运营商归属		
			【必选】手机型号	【基本业务功能】用于对不同型号的设备做个性化的适配，分析当前设备的风险等级，可有效识别作弊行为，剔除作弊设备，识别恶意刷量、恶意程序、保护用户账号安全等		
			【必选】手机操作系统	【基本业务功能】采集用于判断终端类型，用于确定一键登录的终端适配方案		
				【基本业务功能】采集用于判		

			【必选】硬件厂商	断终端类型，用于确定一键登录的终端适配方案		
			【必选】本机号码信息	【基本业务功能】用于一键获取您的手机号码		
			【必选】SIM卡状态	【基本业务功能】采集用于判断SIM卡的状态，用于一键获取您的手机号码		

（二）我们从第三方获得的第三方开发者和/或终端用户的个人信息

我们可能从第三方开发者授权同意的第三方（我们的合作方）处间接获取第三方开发者和/或终端用户的个人信息，获取的个人信息是为实现本 SDK 产品和/或服务必要功能所必需的最少数量。

我们会在收集前要求第三方对个人信息来源的合法性作出承诺，如基于取得终端用户同意处理个人信息时，我们会要求第三方向开发者和/或终端用户告知共享的目的、信息等内容，在依法取得开发者和/或终端用户同意后收集个人信息，确保在已获得的个人信息处理的授权同意范围内进行共享。

如第三方有违反法律法规要求或约定的行为，我们会立即停止从该方收集信息、停止合作并采取相应的补救措施将损失减少到最小；同时，我们会使用不低于对自身用户个人信息同等的保护水平对间接获取的个人信息进行保护，在间接获取个人敏感信息时，我们会采用更加严格的（例如传输加密等）安全保障措施。

（三）相关系统权限申请

根据开发者和终端用户使用本 SDK 功能范围的不同，我们可能在第三方开发者使用本 SDK 过程中申请使用终端用户的系统权限，具体使用场景、申请的权限及申请目的如下表：

Android 系统获权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】 android.permission.INTERNET	网络访问	正常请求时用到	使用 SDK 时用到
【必选】 android.permission.ACCESS_NETWORK_STATE	检查网络状态	请求前判断网络状态是否正常	调用功能接口的前置检查
【必选】 android.permission.CHANGE_NETWORK_STATE	切换网络通道	Wi-Fi 和蜂窝网络双开时需要切换到蜂窝网络通道	Wi-Fi 和蜂窝网络双开且需要使用功能接口时

iOS 系统权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】蜂窝网络权限	使用 SDK 功能的必需信息	调用预取号接口	正常调用预取号接口时使用

Harmony 系统获权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】 ohos.permission.INTERNET	允许应用程序联网，用于访问网关和认证服务器	正常请求时用到	调用sdk业务功能时申请
【必选】 ohos.permission.GET_NETWORK_INFO	检查网络状态	请求前判断网络状态是否正常	调用功能接口的前置检查

注：

1. 本 SDK 不会为实现 SDK 产品功能而申请敏感权限，且不存在其他可选配置权限。
2. 仅在 SDK 使用者使用具体业务功能时，申请对应系统权限。
3. 最终用户拒绝相关权限申请，SDK 不应拒绝提供其他与该权限无关业务功能使用，或频繁弹窗向最终用户申请该权限。

（四）如何使用 Cookie

为实现 SDK 产品功能所必须，我们会使用 Cookie 来收集和储存终端用户的手机号缓存信息，以便下次快速获取。我们不会将 Cookie 用于本政策所述目的之外的任何用途。

1. 如您是终端用户，您可根据自己的偏好清除手机缓存。
2. 如您是开发者，您应当向终端用户告知与 SDK 产品相关的 Cookie 使用情况，包括但不限于 Cookie 的类型、收集的个人信息、使用目的、使用场景，征得终端用户的同意，并向终端用户提供管理和删除 Cookie 的机制（Android 清除缓存 API：public void Descript(Context context)；iOS 清除缓存 API：delectScrip）

（五）以下情形中，我们收集、使用个人信息无需征得第三方开发者和/或终端用户的授权同意：

1. 为订立、履行合同所必需；
2. 为履行法定职责或者法定义务所必需；
3. 为应对突发公共卫生事件，或者紧急情况下为保护自然人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个人信息；
5. 依照《个人信息保护法》规定在合理的范围内处理个人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。

⚠ 注意

如我们收集的信息无法单独或结合其他信息识别到第三方开发者和/或终端用户的个人身份，其不属于法律意义上的个人信息。

（六）个人信息的使用规则

1. 我们会根据本声明和/或与第三方开发者的合同约定，并仅为实现本 SDK 产品和服务功能，对所收集的个人信息进行处理。若需要将收集的个人信息用于其他目的，我们会以合理方式告知第三方开发者和/或终端用户，并在第三方开发者获得终端用户同意后和/或单独获得终端用户同意后使用。
2. 我们向第三方开发者提供的 SDK 产品和服务停止运营后，或者第三方开发者和/或终端用户撤回个人信息的授权后，或者在第三方开发者和/或终端用户注销账号后，我们将会于合理的时间内销毁或匿名化处理从第三方开发者和/或终端用户处接收的所有个人信息，除非法律另有规定。

二、第三方终端用户的授权同意

第三方开发者将本 SDK 产品和服务集成到其第三方中，为向终端用户提供本 SDK 产品和服务，我们会以合法合规的方式收集、存储、加工来自于第三方开发者和/或终端用户的个人信息。

开发者在使用本 SDK 前，应当仔细阅读我们在官网公示的相关服务协议、本指引及第三方开发者合规指南（或同样性质的类似法律文件），并依据您的产品收集使用个人信息的情况进行合规自查。请您注意，我们向您提供本 SDK 产品和服务的前提是：

1. 第三方开发者已经遵守并将持续遵守适用的法律、法规和监管要求收集、使用和处理第三方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声明或隐私政策等。
2. 第三方开发者已经告知第三方终端用户并且已经获得终端用户充分、必要且明确的授权、同意和许可，尤其是涉及到敏感个人信息时的明示、单独同意和许可（若您的产品是针对不满十四周岁的儿童设计和开发的，您应已采取必要的技术措施，保证已获得其服务或者其他监护人的同意）、为提供本 SDK 产品和服务以及与第三方功能对应的目的，我们会收集和共享以及如何使用（包括允许我们根据本声明的规定收集和处理）第三方终端用户的个人信息。
3. 除非适用法律另有规定，第三方开发者已经告知终端用户并且依法获得终端用户充分必要的授权、同意和许可，允许我们对已经收集的个人信息进行去标识化处理，并且在符合相关法律法规的前提下，可以将收集、处理的信息用于本声明第一条列明的用途。
4. 第三方开发者已经向终端用户提供了易于操作的用户权利实现机制，并说明了终端用户可以如何以及何时行使选择权、如何访问、更正其个人信息，以及行使删除权、更改其授权同意的范围等操作。

三、如何共享、转让、公开披露第三方开发者和/或终端用户的个人信息

（一）共享

一般情况下，我们不会与我们的关联公司、合作伙伴及第三方共享第三方开发者和/或终端用户的必要的个人信息，除非为实现本声明第一条中所提及目的的需要。

如存在分享的行为，我们会单独征得第三方开发者和/或终端用户的同意，并要求关联公司、合作伙伴及第三方提供数据安全能力和信息安全资质（如等级保护测评、信息安全管理体系等）证明。在个人敏感信息的处理上，我们会要

求第三方采用数据脱敏加密技术，从而更好地保护个人信息。如果第三方开发者和/或终端用户对第三方处理个人信息有异议或发现这些第三方存在风险时，请按照本声明 [第九条](#) 所述方式联系我们。

我们的关联公司、合作伙伴及第三方如要改变个人信息的处理目的，我们会再次征求第三方开发者和/或终端用户的同意。

（二）转让

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：

- 1.事先告知终端用户转移个人信息的种类、目的、方式和范围，并征得终端用户的单独同意；
- 2.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。

（三）公开披露

我们不会公开披露终端用户的个人信息，但以下情况除外：

- 1.告知终端用户公开披露的个人信息的种类、目的、方式和范围并征得终端用户的单独同意后；
- 2.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。

四、如何存储第三方开发者和/或终端用户的个人信息

（一）存储方式和期限

我们会通过安全的方式存储第三方开发者和/或终端用户的信息，包括本地存储、数据库和服务器日志。

一般情况下，我们只会为实现本声明所述目的所必需的最短时间内或法律法规规定或个人信息主体另行授权同意的条件/范围内存储第三方开发者和/或终端用户的个人信息。但在下列情况下，且仅出于下列情况相关的目的，我们有可能需要较长时间保留第三方开发者和/或终端用户的个人信息：

1. 遵守适用的法律法规等有关规定。
2. 遵守法院判决、裁定或其他法律程序的要求。
3. 遵守相关政府机关或其他有权机关的要求。
4. 为执行相关服务协议或本声明、维护社会公共利益、处理投诉/纠纷，保护我们的客户、我们或我们的关联公司、其他用户或雇员的人身和财产安全或合法权益所合理必需的用途。

（二）存储地域

我们会按照法律法规规定，将境内收集的个人信息存储于中国境内。

目前，我们不会跨境传输或存储第三方开发者和/或终端用户的个人信息。将来如需跨境传输或存储的，我们会向开发者和/或终端用户告知个人信息出境的目的、接收方、安全保证措施和安全风险，并征得开发者的同意和/或终端用户的单独同意，并满足法律法规所规定的其他条件。

五、如何保护第三方开发者和/或终端用户的个人信息安全

（一）安全保护措施

1. 我们已使用符合业界标准的安全防护措施保护第三方开发者和/或终端用户提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损毁、泄漏或丢失。
2. 我们采用业界领先的技术保护措施。我们使用的技术手段包括但不限于防火墙、加密（例如 SSL）、去标识化或匿名化处理、访问控制措施等。此外，我们还会不断加强将 SDK 集成到第三方上的安全能力。
3. 我们建立了专门保障个人信息安全的管理制度、流程和组织。我们也会审查该管理制度、流程和组织，以防未经授权的人员擅自访问、使用或披露用户的信息。

（二）安全事件处置措施

若发生个人信息泄露、损毁、丢失等安全事件，我们会启动应急预案，阻止安全事件扩大。安全事件发生后，我们会及时以推送通知、邮件等形式向第三方开发者和/或终端用户告知安全事件的基本情况、我们即将或已经采取的处置措施和补救措施，以及我们对第三方开发者和/或终端用户的应对建议。

六、第三方开发者和/或终端用户如何管理其个人信息

我们非常重视第三方开发者和/或终端用户对个人信息的管理，并尽全力提供对个人信息的查询、复制、修改、删除、撤回同意、注销账号、投诉举报以及设置隐私功能等的相关权利，以使第三方开发者和/或终端用户有能力保障自身的隐私和信息安全。

（一）针对第三方开发者

1. 第三方开发者实现终端用户查询、复制、修改、删除个人信息等权利的范围和方式将取决于第三方开发者使用的腾讯 SDK 的具体功能。
2. 第三方开发者在使用本 SDK 的过程中，如果终端用户根据第三方开发者与我们的约定提出了个人信息相关的行权请求，并且第三方开发者已确定该等行权请求涉及到了第三方开发者向本 SDK 提供的个人信息时，请及时通过本指引 [第九条](#) 所述方式联系我们，并附上必要的书面证明材料。我们将及时核验相关材料，并按照相关法律法规，以及本指引等法律文本中明确的规则，为第三方开发者提供相应的支持与配合。
3. 我们已向第三方开发者提供关闭本 SDK 服务的能力，第三方开发者可以通过【本指引 [第九条](#) 所述方式联系我们停止收集和处理终端用户的个人信息】来停止收集和处理终端用户的个人信息。
4. 如第三方开发者希望注销本 SDK 服务，也可以通过本指引 [第九条](#) 所述方式联系我们进行服务注销。我们将采取合理的步骤注销账户，我们将根据法律法规的要求删除个人信息。除非我们因法律原因而需保存该等资料，我们将仅限于法律法规所规定的范围进行处理，不会将其用于日常业务活动中。

请知悉：第三方开发者账户一旦注销完成，将无法恢复，请谨慎操作。在进行注销操作之前，请确保与第三方开发者账户相关的服务均已妥善处理。

（二）针对第三方终端用户

由于第三方终端用户不是我们的直接用户，我们建议：

终端用户有权查阅、复制、修改、删除、撤回同意其相关的个人信息，如希望行使以上权利，可以按照本声明 [第九条](#) 所述方式与我们联系。

当终端用户直接向我们主张个人信息主体权利时，应提供必要的证明文件，我们还会对终端用户进行身份验证。我们会向第三方开发者核实终端用户身份以保障终端用户第三方账号安全的情况下，响应终端用户的相关请求。

当终端用户直接向我们主张个人信息主体权利时，根据第三方开发者的隐私政策或个人信息保护声明，我们还可能将与终端用户个人信息相关的请求直接发送给该第三方开发者，要求其处理和/或寻求帮助。

（1）查阅、复制和修改个人信息

当终端用户所使用的第三方中某项功能由本 SDK 产品和服务提供，终端用户可以在使用我们服务的过程中，向开发者查阅、复制、修改其在使用开发者产品中处理的个人信息，也可按照本声明 [第九条](#) 所述方式与我们联系。

（2）删除个人信息

符合下列情形之一的，第三方开发者或终端用户可以请求我们删除其有关个人信息：

- a.处理目的已实现、无法实现或者为实现处理目的不再必要；
- b.我们停止提供服务，或者信息保存期限已届满；
- c.终端用户撤回同意；
- d.认为我们的处理违反法律、行政法规或者违反约定处理个人信息；
- e.法律、行政法规规定的其他情形。

我们将会根据第三方开发者或终端用户的删除请求进行评估，若满足相应规定，我们将会采取包括技术手段在内的相应步骤进行处理。

（3）撤回同意

基于终端用户的同意而进行的个人信息处理活动，终端用户有权撤回该同意。我们已向开发者提供关闭 SDK 服务的能力，第三方开发者可以通过【本指引 [第九条](#) 所述方式联系我们停止收集和处理终端用户的个人信息】来停止收集和删除终端用户的个人信息。由于我们与终端用户无直接的交互对话界面，终端用户可以直接向第三方开发者主张撤回同意的权利，也可以通过第三方开发者提供的开发者平台功能设置主张撤回同意的权利。如开发者需要我们协助终端用户的权利请求，可按照本指引 [第九条](#) 所述方式向我们提出协助请求。

当终端用户撤回个人信息处理的同意并关闭 SDK 服务时，我们无法继续为终端用户提供撤回同意所对应的功能和服务，也不再处理终端用户对应的个人信息。但终端用户撤回同意的决定，不会影响撤回前基于终端用户同意已进行的个人信息处理活动的效力。

（4）注销服务

如终端用户希望注销具体产品或服务，且具体产品或服务的隐私政策中有明确指明，终端用户可通过该方式申请注销相应服务。

（三）响应第三方开发者和/或终端用户的合理请求

我们会响应第三方开发者和/或终端用户上述的合理请求，如无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁盘上存放的信息）的请求，我们可能会予以拒绝。

在以下情形中，我们将无法响应第三方开发者和/或终端用户的请求：

1. 与我们履行法律法规规定的义务相关的。
2. 与国家安全、国防安全直接相关的。
3. 与公共安全、公共卫生、重大公共利益直接相关的。
4. 与犯罪侦查、起诉、审判和执行判决等直接相关的。
5. 我们有充分证据表明第三方开发者和/或终端用户存在主观恶意或滥用权利的。
6. 出于维护第三方开发者和/或终端用户或其他个人的生命、财产等重大合法权益但又很难得到本人同意的。
7. 响应第三方开发者和/或终端用户的请求将导致第三方开发者或其他个人、组织的合法权益受到严重损害的。

8. 涉及商业秘密的。

如第三方开发者和/或终端用户的对上述权利实现存在疑问，可以根据本声明 [第九条](#) 所述方式与我们联系。

七、未成年人保护

本SDK产品主要面向成年人。

若您开发者，如果终端用户是未满14周岁的未成年人（“儿童”），您应当向儿童的父母或其他监护人告知本规则，并在征得儿童的父母或其他监护人同意的前提下处理儿童个人信息。如果我们发现开发者未征得儿童监护人同意向我们提供儿童个人信息的，我们将会采取措施尽快删除。

若您儿童监护人，当您对您所监护儿童个人信息保护有相关疑问或权利请求时，您可以联系开发者，或通过本规则 [第九条](#) 提供的方式与我们联系。

八、如何变更与更新本声明

为给第三方开发者提供更好的服务以及随着本平台产品和/或服务的不断发展与变化，我们可能会适时对本声明进行修订。

当本声明的条款发生变更时，我们会在版本更新时以弹窗、红点提示、网站公告等方式进行提示，并说明生效日期。此外，如果更新后的本声明对第三方终端用户的权利有所影响，还需要请第三方开发者适时更新第三方的隐私政策。对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，我们会通过电子邮件或站内信形式或公告形式发送通知，说明本声明的具体变更内容）。因此，请随时查看和了解本声明内容。如果第三方开发者和/或终端用户不同意接受本声明，请停止接入和使用我们的服务。

本声明所指的重大变更包括但不限于：

1. 我们的服务模式发生重大变化。如处理个人信息的目的、类型、个人信息的使用方式等。
2. 我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产、并购等引起的所有者变更等。
3. 个人信息共享、转让或公开披露的主要对象发生变化。
4. 个人信息处理方面的权利及其行使方式发生重大变化。
5. 负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化。
6. 个人信息安全影响评估报告表明存在高风险。

本声明是腾讯各 SDK 开发者平台服务协议的重要组成部分。我们还会将本声明的旧版本存档，供第三方开发者和/或终端用户查阅。

九、如何联系我们

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，如果第三方开发者和/或终端用户对本隐私政策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 [客服](#) 与我们联系进行在线咨询；（ii）发送邮件至 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。

十、其它

我们请第三方开发者特别注意：当第三方开发者进行个人信息的处理活动，如果符合以下任何一项条件，请第三方开发者注意同时遵守《欧盟通用数据保护条例》（General Data Protection Regulation，以下简

称“GDPR”)：

- 第三方开发者在欧盟经济区域（“EEA”），无论该处理活动是否在欧盟进行。
- 向在 EEA 的个人提供商品或服务（不论是否有偿），或者监视其在 EEA 内的行为。
- 不在 EEA 内，但根据国际公法适用欧盟成员国法律（例如 EEA 成员国的使馆或领事馆）。

如果第三方开发者和/或终端用户来自 EEA，我们收集和使用上述个人信息的法律依据将取决于相关个人信息以及我们收集信息的具体背景。

对于 EEA 中的第三方开发者和/或终端用户，有权根据适用的数据保护法律向主管数据保护机构投诉或向具有管辖权的法院提起诉讼。

如果第三方开发者和/或终端用户对我们收集和使用个人信息的法律依据有疑问或需要进一步信息的，请根据本声明 [第九条](#) 所述方式与我们联系。

SDK 合规使用指南

最近更新时间：2024-12-26 16:48:43

为帮助使用腾讯云号码认证 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，腾讯云计算（北京）有限责任公司（以下简称“我们”）特制定《腾讯云号码认证 SDK 接入使用说明文档》（以下简称“文档”），便于您使用腾讯云号码认证 SDK 过程中符合相应的合规要求。请您在接入、使用腾讯云号码认证 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、站内信、邮件、短信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。

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。您应在 App 登录注册页面及 App 首次运行时，通过弹窗、文本链接及附件等简洁明显且易于访问的方式，应当以清晰易懂的语言告知用户《隐私政策》，由用户在充分知情的前提下，作出自愿明确的意思表示。

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：腾讯云号码认证 SDK（Android）
第三方 SDK 提供方的公司名称：腾讯云计算（北京）有限责任公司
使用目的及功能场景：用户使用号码认证一键登录能力实现注册登录校验
处理的个人信息类型：运营商类型、网络类型、IP地址、硬件厂商、手机型号、手机操作系统、SIM卡状态
实现 SDK 产品功能所需的权限：INTERNET、ACCESS_NETWORK_STATE、CHANGE_NETWORK_STATE
第三方 SDK 隐私政策链接：[号码认证 SDK 个人信息保护规则-相关协议-文档中心-腾讯云](#)

仅 iOS 参考示例：

第三方 SDK 名称：腾讯云号码认证 SDK（iOS）
第三方 SDK 提供方的公司名称：腾讯云计算（北京）有限责任公司
使用目的及功能场景：用户使用号码认证一键登录能力实现注册登录校验
处理的个人信息类型：运营商类型、网络类型、IP地址、硬件厂商、手机型号、手机操作系统、SIM卡状态

实现 SDK 产品功能所需的权限：蜂窝网络权限

第三方 SDK 隐私政策链接：[号码认证 SDK 个人信息保护规则-相关协议-文档中心-腾讯云](#)

仅 Harmony 参考示例：

第三方 SDK 名称：腾讯云号码认证 SDK（Harmony）

第三方 SDK 提供方的公司名称：腾讯云计算（北京）有限责任公司

使用目的及功能场景：用户使用号码认证一键登录能力实现注册登录校验

处理的个人信息类型：运营商类型、网络类型、IP地址、硬件厂商、手机型号、手机操作系统、SIM卡状态

实现 SDK 产品功能所需的权限：INTERNET、GET_NETWORK_INFO

第三方 SDK 隐私政策链接：[号码认证 SDK 个人信息保护规则-相关协议-文档中心-腾讯云](#)

关于腾讯云号码认证 SDK 所收集的个人信息清单如下表所示（Android 和 iOS 相同）：

注：本SDK目前所收集的个人信息都是为实现基本业务功能所收集的必选信息，暂无可选信息，且不涉及提供其他扩展业务功能。

服务方案	收集的个人信息类型	使用目的及功能场景	处理方式	敏感个人信息处理的必要性说明
一键登录能力	【必选】网络类型	【基本业务功能】采集用于判断当前网络是 Wi-Fi 还是数据，用于精确取号	1. 采用 SSL 协议加密及 HTTPS 传输加密技术保障安全 2. 采取加密、去标识化等安全措施脱敏处理	无
	【必选】IP地址	【基本业务功能】调用 SDK 预取号接口、获取一键登录或验证 Token 接口时使用		无
	【必选】运营商类型	【基本业务功能】采集用于判断运营商归属		无
	【必选】手机型号	【基本业务功能】用于对不同型号的设备做个性化的适配，分析当前设备的风险等级，可有效识别作弊行为，剔除作弊设备，识别恶意刷量、恶意程序、保护用户账号安全等		无
	【必选】手机操	【基本业务功能】采集用于判断终端类		无

	作系统	型，用于确定一键登录的终端适配方案	
	【必选】硬件厂商	【基本业务功能】采集用于判断终端类型，用于确定一键登录的终端适配方案	无
	【必选】SIM卡状态	【基本业务功能】采集用于判断SIM卡的状态，用于一键获取您的手机号码	无

关于本SDK申请使用终端用户的系统权限，具体使用场景及申请目的如下表：

注：本 SDK 不会为实现 SDK 产品功能而申请敏感权限，且不存在其他可选配置权限。

Android 系统获权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】 android.permission.INTERNET	网络访问	正常请求时用到	使用 SDK 时用到
【必选】 android.permission.ACCESS_NETWORK_STATE	检查网络状态	请求前判断网络状态是否正常	调用功能接口的前置检查
【必选】 android.permission.CHANGE_NETWORK_STATE	切换网络通道	Wi-Fi 和蜂窝网络双开时需要切换到蜂窝网络通道	Wi-Fi 和蜂窝网络双开且需要使用功能接口时

IOS 系统获权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】蜂窝网络权限	使用 SDK 功能的必需信息	调用预取号接口	正常调用预取号接口时使用

Harmony 系统获权限申请表

权限名称	获取目的	使用场景	调用频率
【必选】 ohos.permission.INTERNET	允许应用程序联网，用于访问网关和认证服务器	正常请求时用到	调用sdk业务功能时申请
【必选】 ohos.permission.GET_NETWORK_INFO	检查网络状态	请求前判断网络状态是否正常	调用功能接口的前置检查

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。

1. 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init()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。该接口仅进行初始化，不会获取个人信息。
2. 请勿在用户同意隐私政策之前动态申请涉及用户个人信息的敏感设备权限；请勿在用户同意隐私政策前私自采集和上报个人信息（尤其注意 Android_ID、OAID、IMEI、MAC地址、硬件序列号、应用安装列表等用户信息）。请勿在 App 处于未激活状态时（例如 App 在后台运行），请求 SDK 相关服务。

四、可选信息配置开关

1. 本 SDK 不存在可选配置权限和可选配置个人信息。所获取的权限（网络权限、获取联网状态权限、获取 Wi-Fi 状态权限以及切换网络通道权限）和获取运营商信息均为 SDK 业务必不可少的权限或信息。
2. 本 SDK 不存在按照不同频次、精度收集个人信息的业务功能。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。
3. 指导建议：

请您重点关注，在 App 安装、运行和使用相关功能时，您应遵守国家相关法律法规、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、SDK 扩展业务功能配置方式

本 SDK 不存在自启动、启动其他应用、自动修复及广告推荐等扩展业务功能，只专注提供手机号码认证。

六、Demo 的使用说明

为了帮助您快速了解、体验 SDK 功能，我们向您提供 SDK Demo，仅供您参考，不作为正式产品。请您理解，由于 Demo 运行方式与正式 App 运行方式有所差异，为实现 Demo 正常运行以便向您提供尽可能全面的 SDK 功能体验，我们在 Demo 中引用了部分依赖库，且仅限于在 Demo 场景下使用。当您接入正式 SDK 产品时请按照 SDK 正式集成文档进行操作。

七、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:

- 通过 [腾讯客服](#) 或 [填写工单](#) 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。

八、注意事项

1. 您接入腾讯云号码认证 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,我们建议您在接入腾讯云号码认证 SDK 前进行合规自查。

- 1.1 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。
- 1.2. 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。
- 1.3. 当腾讯云号码认证 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 集成的腾讯云号码认证 SDK 升级到最新版本。
- 1.4. 其他国家相关法律法规、监管政策及标准的要求。

2. 腾讯云号码认证 SDK 对您的合规审查

您应遵守个人信息保护相关的法律法规、监管政策及标准,并确保合规使用腾讯云号码认证 SDK 服务。请您知悉,为确保您切实获得终端用户的授权,且您已满足个人信息保护相关合规要求,腾讯云号码认证 SDK 可能视具体情况,在双方订立协议、开展合作前或合作过程中,对您进行必要的个人信息保护合规审查。在该等合规审查过程中,您应当提供必要的配合,包括但不限于:

- 2.1. 要求您提供所共享的个人信息合法来源证明及相关文件;
- 2.2. 查阅您官网及其他公开渠道可获取的隐私政策文本;
- 2.3. 试用您的 App 以审查同意授权告知机制及其他合规机制。

例如腾讯云号码认证 SDK 发现存在不合规情形,您可能会被要求增加或补充相关合规措施,如您未按时增加或补充,腾讯云号码认证 SDK 有权拒绝您使用服务。请您知悉,该等合规审查仅属于我们内部必要的合规程序,不构成任何形式的承诺与保证,不具有法律效力。

3. 以下合规文件供开发者参考

- [《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》](#)
- [《个人信息保护法》](#)
- [《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》](#)
- [《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》](#)
- [《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》](#)
- [《App违法违规收集使用个人信息行为认定方法》](#)
- [《网络安全标准实践指南—移动互联网应用程序\(App\)收集使用个人信息自评估指南》](#)
- [《常见类型移动互联网应用程序必要个人信息范围规定》](#)
- [《GB/T 35273-2020信息安全技术 个人信息安全规范》](#)

- 《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》
- 《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》