# 人脸核身 其他指引





#### 【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

其他指引

流程指引

三分钟跑通接口

计费调用量统计

数据分析

订阅日报

监控与告警

创建监控视图

创建告警

控制台访问管理

敏感数据加密指引

数据存储服务指引

版权所有: 腾讯云计算(北京)有限责任公司



# 其他指引 流程指引

最近更新时间: 2023-06-07 16:24:38

为了让您更好地了解并使用腾讯云人脸核身,本页面中提供了相关操作、文档说明链接。

### 步骤1: 注册腾讯云账号

如果您已在腾讯云注册,可忽略此步骤。

点击注册腾讯云账号

# 步骤2: 进行企业实名认证

如果您的腾讯云账号已实名,可忽略此步骤,如果您还未进行实名,可查看 企业认证指引 进行企业实名认证。

点击进行企业实名认证

### 步骤3: 申请人脸核身

单击如下链接,按需求正确填写具体业务信息后提交申请,申请即刻通过,无需等待审核。

点击申请人脸核身服务

# 步骤4: 使用服务

人脸核身提供了 SaaS 和 PaaS 两种接入模式,支持多种载体和多种功能的灵活组合,您可以根据项目的需求选择对应的模式进行接入。

#### SaaS 模式

SaaS 模式下,人脸核身提供了 App SDK、微信 H5、小程序、移动 H5 等多种场景的带 UI 页面的服务。使用 SaaS 化模式接入需要先创建 RuleId,用于调用配置的业务流程。创建流程如下:

# ① 说明

创建 RuleId 的过程中,需要确定以下问题:

- 1. 确定使用的场景。其中小程序和微信原生 H5 需要另外再申请一次微信审核(3 5个工作日)。
- 2. 确定使用的功能。人脸核身提供身份证 OCR、活体检测、人脸比对三个功能组合使用,其中 OCR 能力为非必选项,若不需要,可以选择:调用时传入身份信息。
- 3. 确定使用的比对库源。人脸核身支持两种方式:跟权威库比对,跟上传照片比对,计费方式可参阅 计费概述 文档。
- 1. 登录腾讯云人脸核身控制台 > 自助接入,单击创建业务流程。
- 2. 选择应用场景,如:微信 H5(浮层/普通模式)、微信原生 H5、微信小程序或者混合部署 SDK,并根据需求填写相关信息,填写完成后单击**下一步**。
- 3. 开始进入接入配置,根据您业务的需求按提示信息填写相关内容或选择相关功能。
- 4. 业务信息配合完成后,确认您的配置信息然后单击确认并提交审核。
- 5. 流程审核通过后,系统会自动创建流程并分配业务 ID (Ruleld)。

完成 Ruleld 创建后,可以调用 实名核身鉴权接口,换取流程唯一密钥(BizToken)调用您配置的人脸核身验证的流程,在页面中支持身份证拍摄识别、录制视频、调用云端接口做活体检测与核身比对等操作,并将支持在完成验证后跳转回您的业务页面。

#### ⚠ 注意

为了保证用户的隐私,结果信息人脸核身侧仅保留3天,请您及时拉取。

#### PaaS 模式

PaaS 模式下,人脸核身提供了多种场景的 API,服务申请审核通过后,所有的 API 的调用权限自动开通,您可以自助调用。

• 建议您使用 API 3.0 Explorer 工具进行在线测试,我们提供了在线调用、签名验证、SDK 代码生成和快速检索接口等能力,能显著降低使用云 API 3.0 的难度。您可以通过 API 3.0 Explorer 生成**服务端 SDK** 代码,结合腾讯云的已编写好的开发工具集(SDK) 快速调用人脸核身服务。服务端 SDK 已支持多种语言,包括 Python、Java、PHP、Go、NodeJS、.Net 等。您可以在每个服务的文档中下载对应的 SDK,也可以通过 SDK 中心 获取。



• 此外,人脸核身提供了 三分钟跑通接口 教程,并且针对首次开通服务的用户,人脸核身将会赠送一定量的免费体验次数,用于您调试测试,您可以在 控制台 资源包列表页 查看。

# 步骤5: 查看调用

您可以通过查看 计费概述 了解人脸核身的计费与结算方式。 您可以通过访问 腾讯云人脸核身控制台 查看服务调用情况。

① 说明

在开发、产品使用、费用、合同等问题有任何疑问,欢迎您 联系我们 进行询问。



# 三分钟跑通接口

最近更新时间: 2023-06-26 15:29:11

# 操作场景

该任务指导您在购买腾讯云人脸核身服务后,通过 API 3.0 Explorer 在线接口调试页面调用腾讯云人脸核身接口,并将该接口对应语言的 SDK 集成到项目。 您只需要完成以下步骤,即可快速接入腾讯云人脸核身接口。

# 前提条件

在调用人脸核身接口前,您需要先申请开通腾讯云人脸核身服务,并通过审核。 审核成功后,进入腾讯云人脸核身 API 3.0 Explorer 在线接口调试页面,按照下面的操作步骤调用接口。

# 操作步骤

步骤1: 在左侧导航栏,选择需要调用的接口。



步骤2: 输入参数中的必填参数。

版权所有:腾讯云计算(北京)有限责任公司





#### • Region 参数:

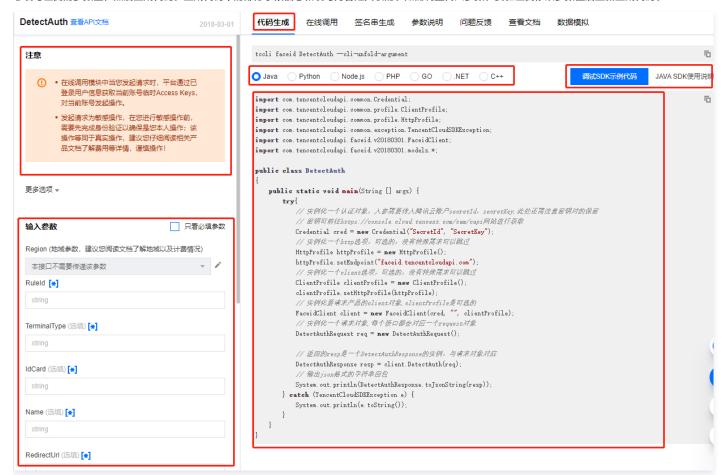
- 域名中的地域信息,该参数决定访问的接入点,例如 faceid.ap-shanghai.tencentcloudapi.com 表示要访问"上海"接入点。
- 公共参数 Region 决定要访问业务资源所在区,例如 Region=ap-beijing 则表示需操作北京区的资源。如果域名中不指定地域信息,则默认就近接入,但由于就近接入可能会存在问题,如果解析不到 IP 最终会默认接入广州地域。
- 域名地域和公共参数 Region 可以不一致,但可能会增加耗时。建议域名和公共参数 Region 选择就近相同的地域。例如,华南地区(广州),ap guangzhou。
- RuleId 参数: 用于细分客户使用场景,申请开通服务后,可以在 腾讯云人脸核身控制台 自助接入里面创建,审核通过后即可调用。如有疑问,点此链接 扫描二维码添加腾讯云人脸核身小助手进行询问。

步骤3:选择语言生成对应代码。

版权所有: 腾讯云计算(北京)有限责任公司



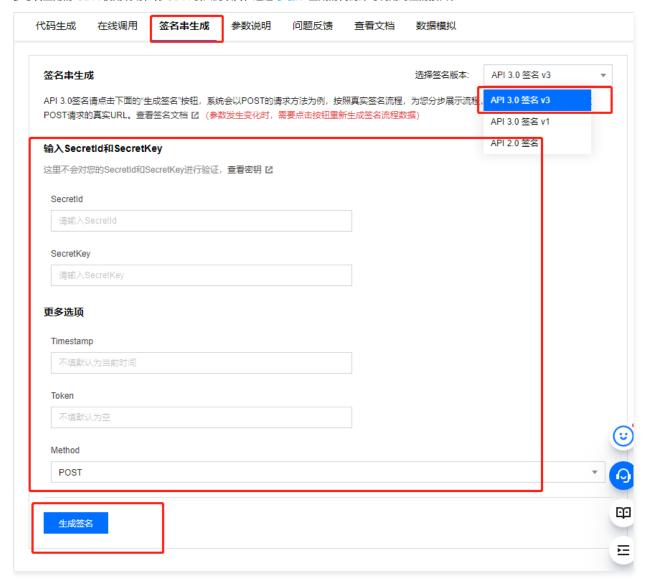
您填写左侧的参数值,然后生成代码,生成代码中的部分字段信息和填写内容是关联的。如需调整传入参数,要在左侧修改参数值后重新生成代码。



步骤4:集成 SDK 到项目。



参考右上角的 SDK 使用说明,将 SDK 引入到项目,通过 步骤3 生成的代码即可调用对应的接口。



### 注意事项

- 使用 SDK 调用人脸核身服务时,公共参数需要关注 Region 字段,建议域名和 Region 统一使用 "ap-guangzhou"。
- SecretId/SecretKey 生成地址: https://console.cloud.tencent.com/cam/capi。
- 图片/视频转 Base64 时,需要去掉相关前缀 data:image/jpg;base64, 和换行符 \n 。
- 如果请求结果提示如下,需要手动设置签名类型:

[TencentCloudSDKException]message:AuthFailure.SignatureFailure-The provided credentials could not be validated because of exceeding request size limit, please use new signature method `TC3-HMAC-SHA256`. requestId:719970d4-5814-4dd9-9757-a3f11ecc9b20

### 设置签名类型:

clientProfile.setSignMethod("TC3-HMAC-SHA256"); // 指定签名算法(默认为 HmacSHA256)

• 如果接口请求内容超过1M,只能使用 V3 鉴权(TC3-HMAC-SHA256),API 3.0 SDK 支持语言: Node、Python、Java、PHP、Go。其他语言如 .net、C# 暂时不支持 SDK 方式调用,需要自行实现接口鉴权V3 进行接口调用,建议使用 API 3.0 Explorer 中签名串生成工具进行核验签名有效



性。





# 计费调用量统计

最近更新时间: 2025-01-15 17:14:53

腾讯云人脸核身提供了计费调用量可视化查询页面,本文档介绍登录腾讯云控制台查看人脸核身产品计费调用量的操作方法及相关注意事项。

# 查询条件

人脸核身数据统计区分人脸核身计费统计支持和实名信息核验计费统计,两者支持的查询条件如下:

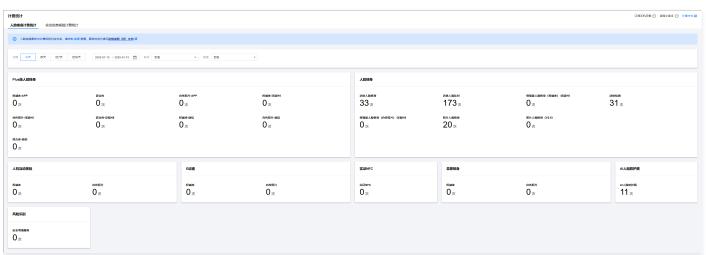
- 按日期查询:可筛选今天、昨天、近7天、近30天,以及90天内指定起止时间的计费调用量。
- 按账号查询:拥有全读写权限或者只读权限的子账号可以查看所有主/子账号的计费次数;拥有自读写权限的子账号,仅可查看自身的计费次数,相关权限说明 请参见控制台访问管理。
- 按产品查询: 可以区分增强版人脸核身、基础版人脸核身、E 证通、实证 NFC 、意愿核身等按产品筛选。
- 按 WBappid 查询: 人脸核身计费统计还支持按 WBappid 查询。

### 功能说明

# 查看人脸核身计费调用量

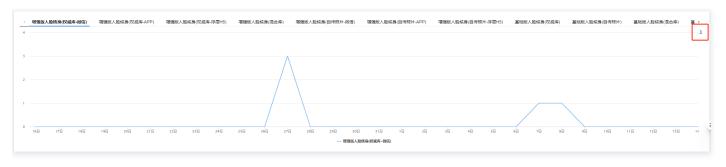
- 1. 进入人脸核身控制台,在左侧菜单栏单击**计费统计**下的 人脸核身计费统计。
- 2. 在人脸核身计费统计页面中,可以查询全渠道的**基础版人脸核身、增强版人脸核身、E 证通、实证 NFC、意愿核身**等产品的计费调用量。

您可以通过筛选日期、账号、渠道等查看产品使用的计费调用量,数据实时更新。调用方式及收费关系请参考 计<mark>费错误码</mark>,如有疑问,联系<mark>我</mark>们 进行询问。



#### 下载人脸核身计费调用量

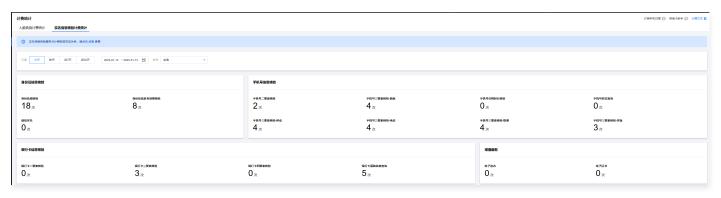
在人脸核身计费统计页面下方,您可根据产品筛选,查看该产品的计费调用量趋势图,在趋势图右上角单击下载标签,可将当前数据下载本地,方便查看调用量明细。



#### 查看实名信息核验调用量

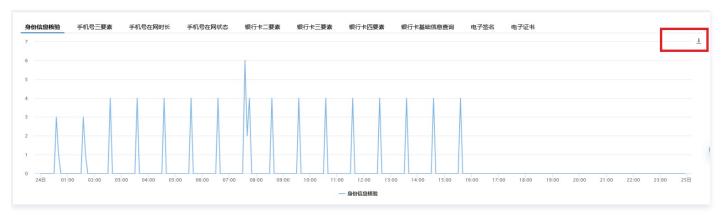
- 1. 进入人脸核身控制台,在左侧导航栏单击**计费统计**列表下的 实名信息核验计费统计。
- 2. 在实名信息核验计费统计页面中,可以查询 PaaS 接入方式的**身份证要素类、手机号要素类、银行卡要素类**等身份实名信息核验相关产品的调用量。 您可以通过筛选日期、账号等查看产品使用的调用量,数据实时更新。调用方式及收费关系请参考 计费错误码,如有疑问可单击页面右上角联系小助手(微信号:faceid001)咨询。





# 下载实名信息核验调用量

在实名信息核验统计页面下方,您可根据产品筛选,查看该产品的调用量趋势图,在趋势图右上角单击下载标签,可将当前数据下载本地,方便查看调用量明细。





# 数据分析

最近更新时间: 2025-01-15 17:14:53

腾讯云人脸核身提供了控制台可视化认证数据分析页面,本文档介绍登录腾讯云控制台查看人脸核身产品认证量数据分析的操作方法及相关注意事项。

① 说明

以下人脸核身数据分析功能是基于您使用的人脸核身服务的日志统计分析,仅作为业务参考,不作为对账使用,对账的计费数据请查看 计费统计 。(数据查询起始时间为2021年9月11日)

# 名词解析

**认证完成次数**: 当前账号下当前人脸核身产品的服务端成功返回验证结果的次数。

**认证通过次数**: 当前账号下当前人脸核身产品的服务端认证通过的次数。

认证通过率:即认证通过总次数/认证完成总次数。

**认证完成总次数**: 当前账号下人脸核身产品全渠道的服务端成功返回验证结果的总次数。

**认证通过总次数**: 当前账号下人脸核身产品全渠道的服务端认证通过的总次数。

# 查询条件

人脸核身数据分析功能目前支持的查询条件如下:



- 按日期查询: 可筛选昨天、近7天、近30天,以及30天内指定起止时间的认证完成次数。
- 按服务查询:可以筛选需要特别关注的服务进行认证完成次数分析。如Plus版App SDK、增强版 App SDK、基础版 App SDK、活体检测 SDK、微信小程序及微信原生H5、微信普通H5、移动 H5 与 PC H5、活体人脸与照片人脸核身 API 和活体人脸比对 API 。
- ▶按账号查询: 拥有全读写权限的子账号可以查看所有主/子账号的计费次数; 拥有自读写权限的子账号, 仅可查看自身的计费次数, 相关权限说明请参见 控制台 访问管理。
- 按 wbappid 查询: 人脸核身认证完成次数分析还支持按 wbappid 查询。

#### 统计分析

#### 查看认证完成次数

- 1. 进入人脸核身控制台,在左侧菜单栏单击数据分析下的\*\* 人脸核身整体看板 \*\*。
- 2. 在人脸核身计费统计页面中,可以查询全渠道的腾讯云慧眼人脸核身产品的认证完成次数。
- 3. 您可以通过筛选日期、账号、渠道等查看当前账号下人脸核身全渠道产品的认证完成次数,及认证通过率。



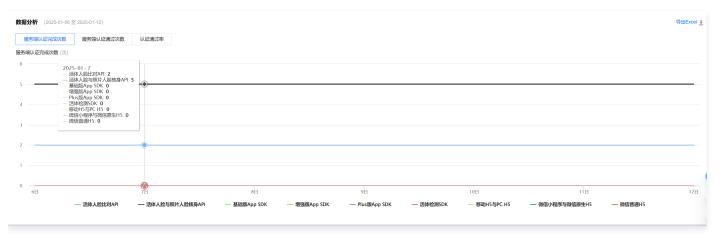
#### 查看认证通过率趋势分析

认证数据分析模块可以直观地查看当前选择的时间区间内的全渠道人脸核身服务认证完成次数,及当前选择的时间区间内认证完成次数趋势图。

- 单击**服务端认证完成次数、服务端认证通过次数**或**认证通过率**可切换视图。
- 单击底部Plus版 App SDK、增强版 App SDK、基础版 App SDK、活体检测 SDK、微信小程序及微信原生H5、微信普通H5、移动 H5与 PC H5、活体人脸与照片人脸核身API和活体人脸比对 API 等可隐藏/显示该服务的数据。



- 如有疑问可单击页面右上角联系小助手(微信号: faceid001)咨询。

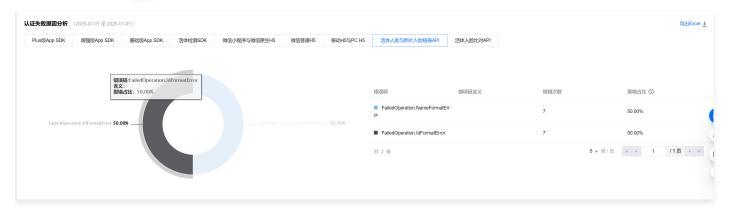


# 分析各服务认证失败原因

认证失败原因分析模块可以直观地查看当前选择的时间区间内的全渠道人脸核身服务认证失败的原因,可供客户定位问题调整业务使用。

- 单击Plus版 App SDK、增强版 App SDK、基础版 App SDK、活体检测 SDK、微信小程序及微信原生H5、微信普通H5、移动 H5与 PC H5、活体人 脸与照片人脸核身 API 和活体人脸比对 API 等可切换各个渠道服务的认证失败原因视图。
- 单击视图右上角,单击 

  → ,可下载查看明细。





# 订阅日报

最近更新时间: 2023-06-29 18:58:03

本文档介绍登录腾讯云控制台关注腾讯云人脸核身获取实名认证日报通知的操作方法及相关注意事项。

# 操作场景

腾讯云人脸核身提供了手机日报订阅功能,通过微信公众号订阅日报后,每天早上10点可以收到昨日的日报数据推送。

# 操作指南

# 管理员订阅

1. 登录腾讯云人脸核身控制台,在订阅日报页面,单击生成订阅链接。



2. 将生成的订阅链接进行复制,发给自己,在微信中打开链接,确认订阅,并关注公众号,即可订阅日报。也可以单击**扫码订阅**,使用手机微信扫码页面二维码 并关注公众号,即可接收每日日报。



版权所有: 腾讯云计算(北京)有限责任公司



3. 手机微信操作完成订阅后,每天上午10点可以收到昨日的日报数据推送,如下图:



日报详情中,可查看**前一天的产品调用量,近7天的调用趋势图**,以及**资源包实时情况**。

#### 多人订阅

人脸核身订阅日报功能还支持多人订阅同一份日报,生成订阅后,单击**复制链接**将链接发送给需要关注这份日报的人,对方使用手机微信打开链接确认授权并关注 公众号,即可接收每日日报。

#### 解除订阅

管理员可以在控制台**订阅日报**页面管理订阅手机日报的用户,单击**解除订阅**可解除不再需要关注的用户订阅 。





# 监控与告警

# 创建监控视图

最近更新时间: 2023-05-23 14:08:10

人脸核身产品已经接入腾讯云可观测平台功能,您可以通过登录 腾讯云可观测平台控制台 配置人脸核身产品下的 API 接口调用量监控视图。

#### 操作场景

通过腾讯云可观测平台,您可以制定针对人脸核身产品下的 API 接口的监控视图。查看 API 接口调用量变化趋势及当前时间总调用量与昨日比例(%)。本文介绍如何配置人脸核身 API 接口监控视图,如需了解更多 Dashboard 相关信息,请参考 Dashboard 相关文档。

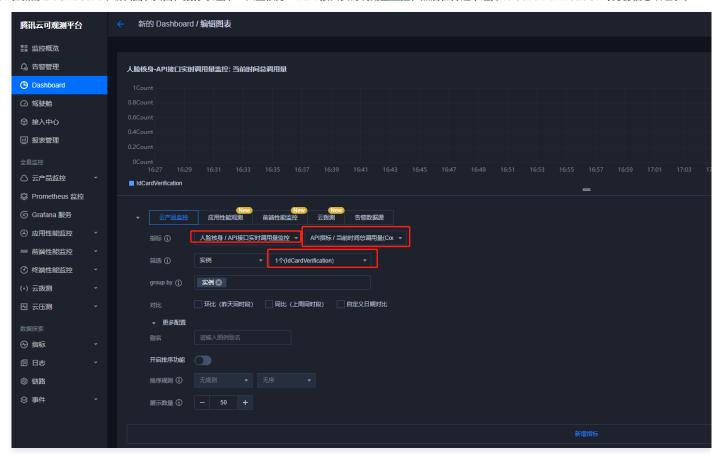
# 视图配置

登录 腾讯云可观测平台控制台 ,在腾讯云可观测平台控制台中,可以配置人脸核身部分 API 接口的调用量实时监控视图,以 IdCardVerification (身份信息 认证 ) 接口为例,具体操作如下:

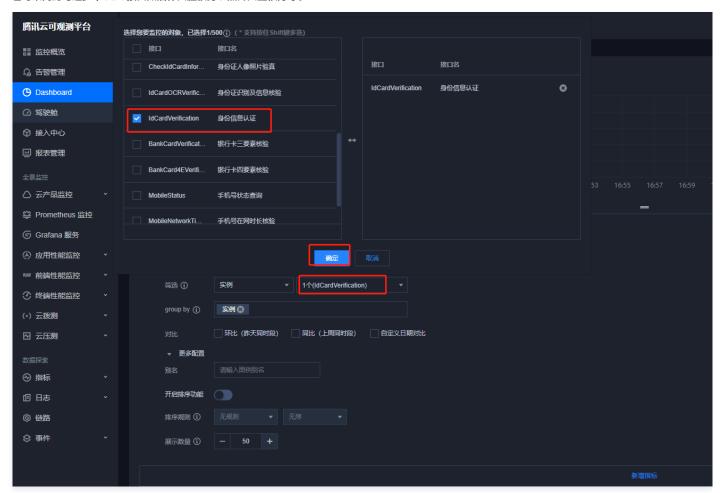
- 1. 单击左侧菜单栏中 Dashboard > Dashboard 列表。
- 2. 在 Dashboard 列表页,单击新建 Dashboard > 新建图表。



3. 在新的 Dashboard / 编辑图表页面,**指标中**选择 > 人脸核身 > API 接口实时调用量监控,然后在**筛选**中选择 IdCardVerification (身份信息认证)。



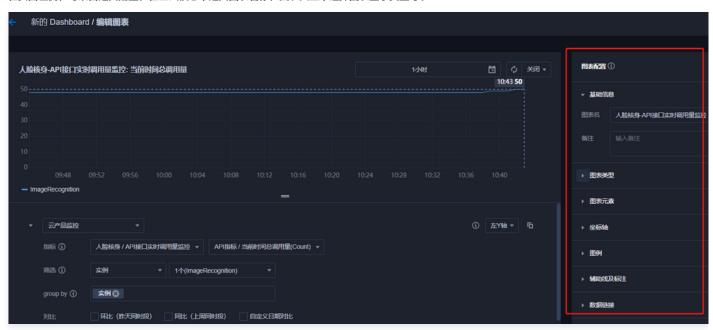
也可以同时勾选多个 API 接口如活体人脸核身、照片人脸核身等。



#### ① 说明

视图监控的指标除了可以选择\*\*当前时间的总量(Count)**外,还可以选择**当前时间总调用量与昨日比例(%)\*\*,可根据您的实际业务需求选择配置。

4. 在页面左侧,可以自定义配置,在**基础信息**中定义图表名称,**图表类型**中选择图表显示类型等。



5. 配置完成后,单击右上角保存,填写 Dashboard 名称和所属文件夹,单击确定即可完成人脸核身监控视图配置。



6. 创建好的人脸核身监控视图,可以在 Dashboard 列表页所属文件夹中找到。





# 创建告警

最近更新时间: 2023-09-05 16:52:07

人脸核身产品已经接入腾讯云可观测平台功能,您可以通过登录 腾讯云可观测平台控制台 配置人脸核身产品下的 API 接口调用量告警策略。

# 操作场景

通过腾讯云可观测平台,您可以制定针对人脸核身产品下的 API 接口的告警规则。在发生异常时会及时通过微信、邮件、短信、电话等渠道通知您,您可以根据 告警信息判断是否采取问题解决措施。适度创建告警能帮助您提高应用程序的健壮性和可靠性。本文介绍如何创建告警,如需了解更多告警相关信息,请参考 新 建告警策略 。

# **企 注意**

请确认您已经设置默认告警接收人,否则腾讯云人脸核身的默认告警策略将无法通知到您。

# 告警配置

#### 1. 新建告警策略

单击左侧菜单栏中**告警管理**,在策略管理页单击**新建策略**。



#### 2. 配置策略基本信息

- 填写策略名称。
- 监控类型选择云产品监控
- 策略类型: 选择**人脸核身>API接口实时调用量监控**



#### 3. 配置告警规则

版权所有: 腾讯云计算(北京)有限责任公司



#### • 选择告警对象

- 若选择**实例 ID**,则该告警策略绑定用户选中的 API 接口,可以勾选 LivenessRecognition (活体人脸核身)或者 ImageRecognition (照片人脸核身)接口等。
- 若选择**全部对象**,则该告警策略绑定当前账号的全部 API 接口。
- 若选择**实例分组**,则该告警策略绑定用户选中的 API 接口分组。若您没有实例组,可以单击新建实例组进行创建。



#### • 配置触发条件

选择以下任意一种方式设置告警触发条件。

#### ○ 选择模板

若选择"选择模板"触发条件,您可以在下拉列表选择已配置的模板。



### (!) 说明

若您没有触发条件模板,请单击新增触发条件模板进行配置,具体配置请参见 配置触发条件模板 。若新建的模板没有显示,请单击右侧的刷新。

#### ○ 手动配置

选择"手动配置"触发条件后,请按需勾选"指标告警"和"事件告警"。

勾选指标告警后,需配置告警触发条件。

例如下图所示,若指定指标为 "调用量" 、"统计粒度1分钟" 、比较关系为 ">" 、阈值为 "1000" 、持续周期为 "持续3个数据点" 、重复通知 为 "每1天警告一次"则表示:每1分钟收集一次调用量数据,若某个 API 接口的调用量连续3次大于1000,则触发告警,且每天警告一次。



#### ① 说明

目前人脸核身服务支持**调用量**与**今日昨日流量比**两种类型维度的告警监控,如果关心每日调用量,可以设置**调用量**大于某个值;如果关心相对昨日的流量,可以设置**今日昨日流量比**大于某个百分比。

若需配置多条告警触发条件,则单击**添加指标**进行配置,当有多条触发条件时,请根据实际选择满足所有条件或任意条件时触发告警。



# 4. 配置告警通知

配置告警通知可设置告警渠道,根据需求配置告警接收组、有效时段、接收对象、接收渠道(邮件、微信)等。 选择以下任意一种方式配置通知模板。

#### 选择模板

若选择"选择模板",您可以在下拉列表选择已配置的模板。



#### 新建模板

若选择"新建模板",则需要在弹窗中填写新建模板信息、配置接收对象及接收渠道。



# 5. 完成告警策略

以上配置信息确认完成后,单击保存即可完成告警策略配置,配置完成的告警策略可以在告警策略列表页管理该条策略。



#### ↑ 注意

由于是实时上报单日调用总量,在单日内会递增。在使用阈值告警时建议设置合理的告警频率,否则告警频率会过高;调用量指当前账号 ID 下接口不区分计费的调用次数。



# 控制台访问管理

最近更新时间: 2025-02-19 16:08:02

访问管理(Cloud Access Management,CAM)是腾讯云提供的一套 Web 服务,它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。通过 CAM,您可以创建、管理和销毁用户(组),并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。

① 说明:

2023年10月18日之前开通人脸核身服务的客户暂不支持使用新版控制台访问管理功能,如有需要请联系我们添加配置。

# 为子账号授予权限

慧眼人脸核身已经接入了 CAM,支持预设策略(推荐)和自定义策略两种方式,您可以根据自身需要,在 访问管理控制台 中为子账号或协作者账号分配合适的 人脸核身访问权限。

在授予子账号权限之后,子账号才能调用人脸核身服务和登录使用人脸核身控制台。

#### 预设策略说明

人脸核身的预设策略分为以下3种,您可以选择其中一种权限授予给子账号,所有预设策略只对人脸核身控制台的功能范围进行区分。

- 1. QcloudFaceIdFullAccess:全读写权限。权限范围最大的预设策略,可以对主账号及主账号下所有子账号的相关项目信息进行查看、修改、停用、人工 审核等管理操作。若您将全读写策略授予子账号,那么它将能够和主账号一样可以管理您所有账号下的项目信息。
- 2. QcloudFaceidReadOnlyAccess: 只读权限。仅可以查看主账号及主账号下所有子账号(包含子账号自身)的相关项目信息,无法进行创建、修改、停用、人工审核等管理操作。
- 3. QcloudFaceidSelfAccountAccess: 自读写权限。仅可以对子账号自己创建的项目信息进行查看、修改、停用、人工审核等操作,无法查看或管理其他子账号创建的项目。

#### 三类预设策略的详细区别:

人脸核身功能	功能细分	全读写	只读	自读写
控制台 > 自助接入	查看自己账号下创建的业务流程信息	$ \emptyset $	€	V
	查看所有主/子账号创建的业务流程信息	$ \mathscr{O} $	V	×
	创建业务流程(仅可在自己账号下创建)	$\checkmark$	×	V
	修改/停用自己创建的业务流程	$ \swarrow $	×	V
	修改/停用其他账号创建的业务流程	$\checkmark$	×	×
控制台 > 计费统计	查看自己的计费数据	$\checkmark$	V	V
IT에다 스 시 팟캐시	查看所有主/子账号的计费数据	$\checkmark$	V	×
控制台 > 数据分析	查看自己的数据分析	$\vee$	$\mathscr{C}$	V
	查看所有主/子账号的数据分析	arphi	V	×
控制台 > 资源包管理	查看所有主/子账号的资源包余量(资源包为所有账号共用)	$\checkmark$	V	V
控制台 > 验证记录	查看自己账号的验证记录	$\swarrow$	V	V
江町日~並加心水	查看所有主/子账号的验证记录	$\checkmark$	V	×
控制台 > 人工审核	查看自己账号的验证记录	$ \swarrow $	$\mathscr{O}$	V
	查看所有主/子账号的验证记录	$ \swarrow $	V	×
	审核自己账号下的验证记录	$ \mathscr{O} $	×	V
	审核所有主/子账号的验证记录	✓	×	×
控制台 > 数据加密服务	查看创建的密钥	$ \emptyset $	V	V

版权所有: 腾讯云计算(北京)有限责任公司



	开通加密服务	✓	×	×
控制台 > 数据存储服务	查看存储路径	V	€	V
	开通存储服务	V	×	×
控制台 > 订阅日报	生成订阅链接	$ \mathscr{O} $	$\checkmark$	V
	解绑订阅的微信	$\checkmark$	€	$\mathscr{O}$
	订阅日报展示自己账号的计费统计	V	€	V
	订阅日报展示所有主/子账号的计费统计	V	<	×
控制台 > 后付费设置	查看后付费配置信息	$ \mathscr{O} $	€	V
	修改后付费设置	$ \mathscr{C} $	×	×
慧眼服务接口	调用慧眼线上服务接口	V	V	V

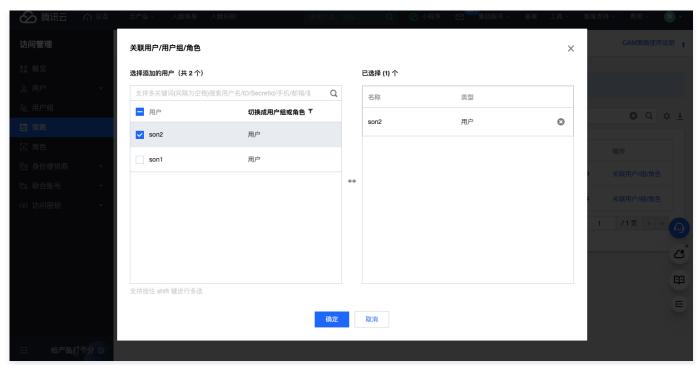
# 预设策略配置方式

预设策略可以在 访问管理控制台 中进行授权。

1. 方式一:如下图所示,进入**访问管理 > 策略**,搜索"QcloudFaceid",可看到人脸核身的三类预设策略:

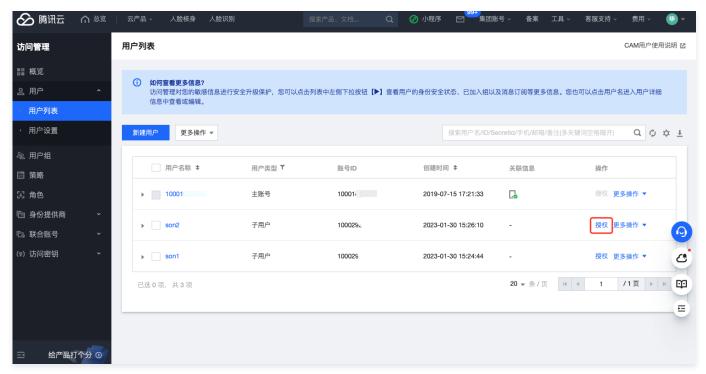


可根据您的自身需要选择对应的预设策略去关联子账号:

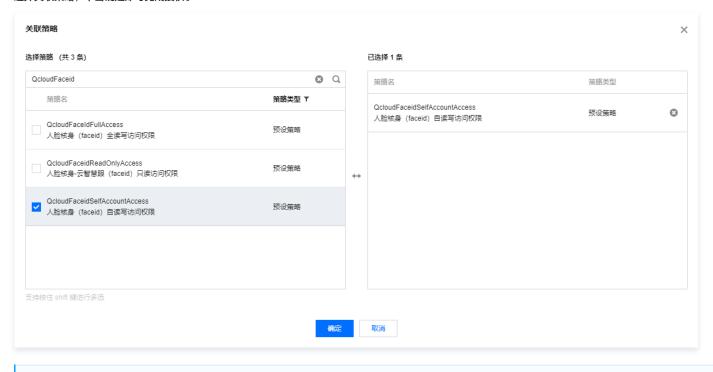




2. 方式二:如图所示,进入**用户 > 用户列表**,可选择子用户,单击**授权**进行关联策略操作。



选择关联策略,单击**确定**即可完成授权。



#### ① 说明

关联策略时,如无特殊的权限需求,我们推荐您使用预设策略。

# 自定义策略说明

若预设策略不能满足您的需求,可自行创建自定义策略。人脸核身的自定义策略目前支持的是接口级授权方式:

接口级授权:您可以在 CAM 控制台中按接口维度给子账户授权,子账户将只能使用您已授权的接口。可参考使用示例中授予单个接口权限的操作。

### 自定义策略配置方式

自定义策略也需要在 访问管理控制台 中进行授权,和预设策略一致。 创建自定义策略的方式请参见 通过策略生成器创建自定义策略。



#### 自定义策略语法

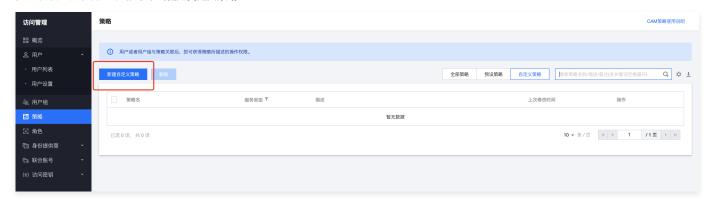
创建自定义策略时,接口级接口均遵循以下规则。

- effect 字段填入"allow",表示当子账号命中该策略时,允许对策略中配置的接口进行访问。
- 由于人脸核身只支持接口级授权方式,所以 resource 字段填入" \* "。
- action 字段用于配置账号需要访问的接口名,支持配置多个接口,每个接口按照"faceid:{接口名}"的格式填入,例如"faceid:SaveUserConf"。

以下为给子账户授予自助接入申请微信原生H5业务(SaveUserConf)、人工审核(ConsoleExecuteManualAudit)的授权。在 action 中填入对应的接口名:

#### 自定义策略配置示例

1. 在访问管理控制台 > 策略 中单击新建自定义策略。

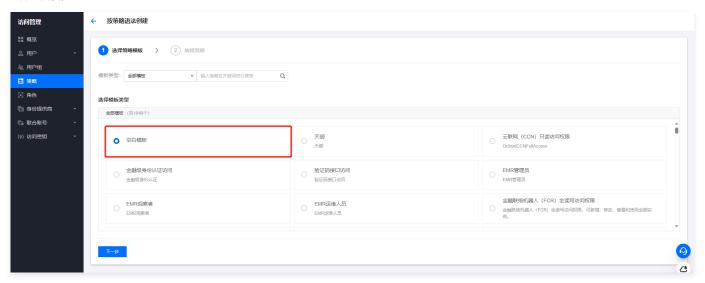




#### 2. 选择按策略语法创建。

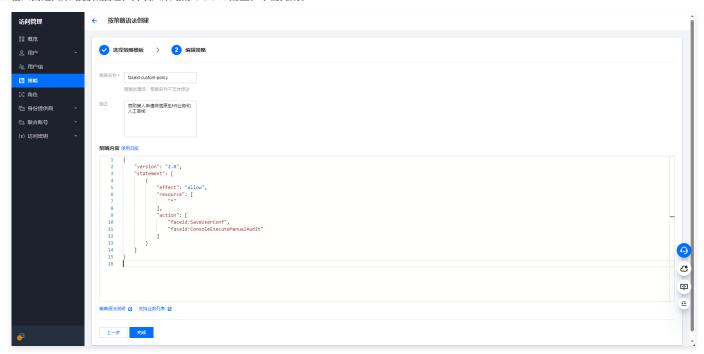


#### 3. 选择空白模板。





4. 输入自定义策略名和描述,并填入策略的 JSON 配置,单击**完成**。

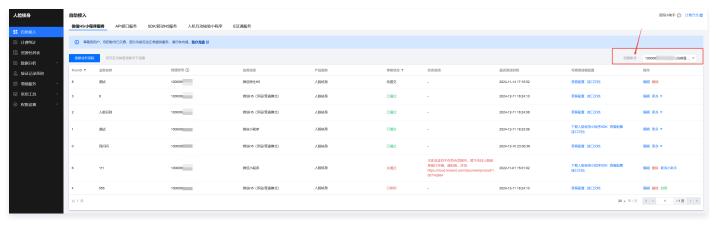


5. 完成新建后,在策略页面中可以看到新增的自定义策略,并且可以关联到需要的子账号上。



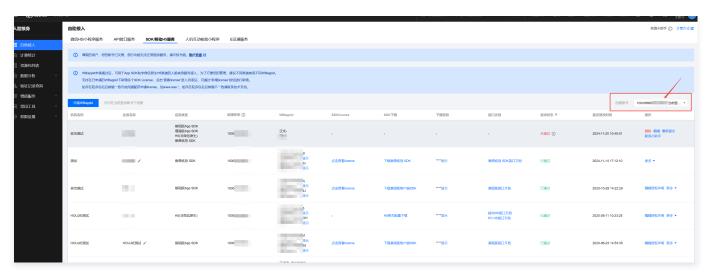
# 查询相关QA

# 主账号如何查询其下子账号与协作者账号的业务信息?



SDK/移动H5服务:

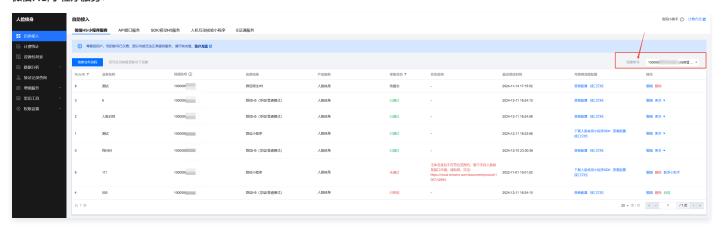




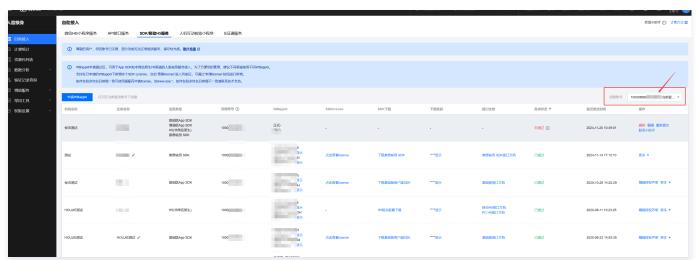
# 子账号或协作者账号如何查询主账号或其他子账号下所创建的业务信息?

- 1. 首先需要主账号给子账号或协作者账号授权全读写权限或只读权限,授权步骤请参见 预设策略配置方式 。
- 2. 授权完成后,登录子账号或协作者账号,进入需要查询的业务页面,单击右上角**创建账号**下拉选择所需查询的子账号或是协作者账号后,页面会自动展示所选 择查询账号创建的业务信息。

微信H5/小程序服务:



#### SDK/移动H5服务:





# 敏感数据加密指引

最近更新时间: 2024-08-22 15:22:12

本指引适用于使用人脸核身服务接口,需要对传输敏感数据进行加密的场景。如果您使用的开发语言是 Java、Go、Nodejs,推荐使用本篇指引的【方式一】使用官方 SDK 实现加解密;如果开发语言不在上述范围,推荐使用【方式二】实现加解密功能。

#### ① 说明:

如果您在2023年3月17日前已开通 KMS 加密服务,并且想要继续使用腾讯云密钥管理系统 KMS 安全保护的主密钥 CMK 作为加密密钥,无需看本篇指引,请参照【 KMS 加密指引文档】操作。

### 方式一: 使用官方 SDK 实现加解密(推荐)

官方 SDK 当前支持 Java、Go、Nodejs 开发语言,使用步骤如下:

#### 获取加解密 SDK

Java:

获取依赖

Demo

Golang:

获取依赖

Demo

#### 使用 SDK

#### 引入公共依赖

# 引入加解密 SDK

下载最新的 release 版本 jar 包,并在项目工程中引入。 参考下方的接口 Demo 实现敏感信息加解密功能。

# 接口敏感信息加解密 DEMO

• 实名核身鉴权: DetectAuth

• 获取实名核身结果信息增强版: GetDetectInfoEnhanced

获取E证通 Token: GetFaceIdToken 照片人脸核身: ImageRecognition

• 银行卡四要素核验: BankCard4EVerification

银行卡三要素核验: BankCardVerification

身份信息及有效期核验: CheckIdNameDate

手机号二要素核验: CheckPhoneAndName身份证识别及信息核验: IdCardOCRVerification

• 银行卡基础信息查询: CheckBankCardInformation

• 身份证二要素核验: IdCardVerification



• 手机号在网时长核验: MobileNetworkTimeVerification

• 手机号状态查询: MobileStatus

• 手机号三要素核验: Phone Verification

手机号三要素核验(移动): PhoneVerificationCMCC
手机号三要素核验(电信): PhoneVerificationCTCC
手机号三要素核验(联通): PhoneVerificationCUCC
身份证人像照片验真: CheckIdCardInformation

#### 方式二:不使用官方 SDK 实现加解密

#### 加解密流程说明

- 当前敏感信息加解密支持标准加密算法 AES-CBC 和国密算法 SM4-GCM,可以根据业务要求从中选择适合您的加密算法。
- 敏感信息加解密的本质是对接口传输的姓名、身份证号做对称加密后传输,人脸核身服务收到加密数据后先解密,然后在进行核身业务。如果人脸核身接口返回结果涉及敏感信息,则会使用相同的对称密钥加密,调用方在收到接口响应时需要对敏感信息解密。
- 对称密钥由调用方本地随机生成,为保证对称密钥的安全传输,需要调用方配合使用非对称加密算法加密对称密钥。加密的公钥可以登录人脸核身控制台 获取。

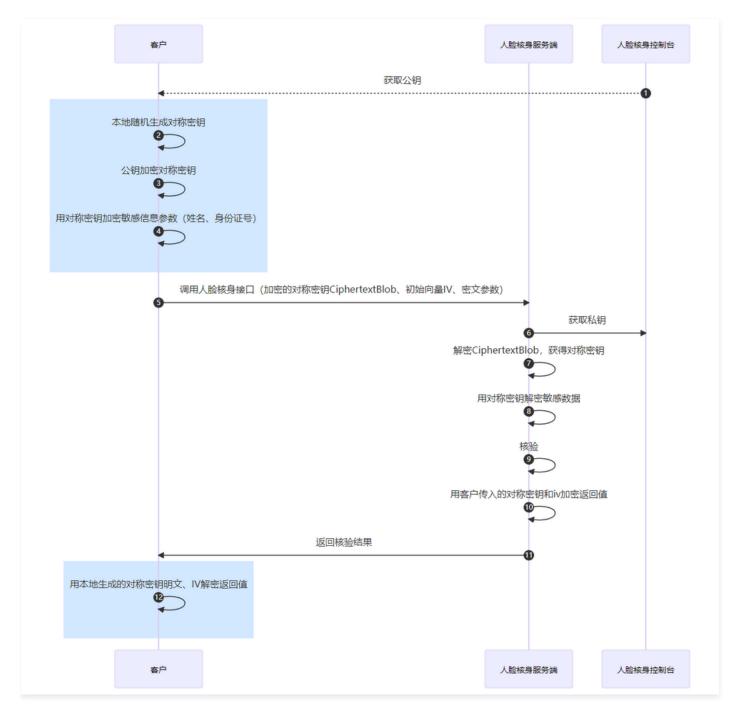
```
sequenceDiagram

participant customer as 客户
participant faceid as 人脸核身服务端
participant console as 人脸核身控制台
console-->>customer: 获取公钥

rect rgba(191, 223, 255, 0.7)
customer->>customer: 本地随机生成对称密钥
customer->>customer: 公钥加密对称密钥
customer->>customer: 用对称密钥加密敏感信息参数(姓名、身份证号)
end

customer->>faceid: 调用人脸核身接口(加密的对称密钥CiphertextBlob、初始向量IV、密文参数)
faceid->>console: 获取私钥
faceid->>faceid: 解密CiphertextBlob, 获得对称密钥
faceid->>faceid: 解密CiphertextBlob, 获得对称密钥
faceid->>faceid: 核验
faceid->>faceid: 核验
faceid->>customer: 返回核验结果
rect rgba(191, 223, 255, 0.7)
customer->>customer: 用本地生成的对称密钥明文、IV解密返回值
end
```





# 使用 AES-256-CBC 算法

#### 加载 RSA 公钥

加载 RSA 公钥:对控制台获取到的公钥字符串先做 Base64 Decode,然后按对应格式加载。

• 格式: PKCS1

• 保存格式: pem 格式 Base64编码

• 长度: 1024

```
// 加载RSA公钥

bytes, err := base64.StdEncoding.DecodeString(publicKey)

if err != nil {
  return nil, err
}

block, _ := pem.Decode(bytes)
```



x509.ParsePKCS1PublicKey(block.Bytes)

#### 生成对称密钥和向量

随机生成32字节长度的对称密钥以及16字节的初始向量,初始向量表示为 IV。

```
// 生成对称密钥
key := make([]byte, 32)
rand.Read(key)

// 生成16字节iv
iv := make([]byte, 16)
rand.Read(iv)
```

#### RSA 公钥加密对称密钥

使用 RSA 公钥加密前面生成的 对称密钥,将加密后的结果表示为 CiphertextBlob。

```
// 加密对称密钥Key
buffer := bytes.Buffer{}
bytes, _ := rsa.EncryptPKCS1v15(rand.Reader, publicKey, key)
buffer.Write(bytes)
buffer.Bytes()
```

#### 加密敏感数据

使用前面生成的 对称密钥和初始向量,采用 AES-256-CBC 算法加密敏感数据(姓名、身份证号)。

```
// AES-CBC加密明文数据
// 明文密钥key
// 初始向量iv
// 敬感数据plaintext
block, _ := aes.NewCipher(key)
blockSize := block.BlockSize()
pkcs7 := func(cipherText []byte, blockSize int) []byte {
    padding := blockSize - len(cipherText)*blockSize
    padText := bytes.Repeat([]byte{byte(padding)}, padding)
    return append(cipherText, padText...)
}
plaintext = pkcs7(plaintext, blockSize)
blockMode := cipher.NewCBCEncrypter(block, iv)
ciphertext := make([]byte, len(plaintext))
blockMode.CryptBlocks(ciphertext, plaintext)
fmt.Print(ciphertext)
```

### 调用人脸核身接口

以身份证二要素(IdCardVerification)接口为例:

原始数据为:

```
"Action": "IdCardVerification",
   "Version": "2018-03-01",
   "IdCard": "100822119610104046",
   "Name": "张三"
}
```

CiphertextBlob、IV、TAG、加密后的姓名、身份证号在传输前均需要做一次 Base64 编码:

• 生成的对称密钥为: 1abrmh7jz83awn4585vzujiyxbhi5wsd (32字节)



● 生成的初始向量(IV): t9Uf9QJ50B0uHhE26JLNxw==(16字节IV, Base64编码)

公钥加密后的对称密钥(CiphertextBlob):

eqB5H23bbNQGTxCxSHP+FaXy+LlfK2GJ8l19UxTbikdezY1mGINQxS76J9rUa61W2jrm4j6eQ39O9pus/Wk5zP6t48Gd8M6RHld17/pPTnAVzjTwYZhy0yBvuyh7N73J5/fL2TSgJTMVi79urCC17C0oYdyBsK+hP9blfzwxb3g=(Base64编码) 使用对称密钥加密IdCard和Name,加密后的结果分别为:

- IdCard: H+ZwsBfYVgbBWaHStriUV2GF0wX7MzYy0XMWNKZjZjQ=(Base64编码)
- Name: IS6wLE153MfBr639hqWmUQ==(Base64编码)

最终加密后的接口数据为:

```
{
    "Action": "IdCardVerification",
    "Version": "2018-03-01",
    "IdCard": "H+ZwsBfYVgbBWaHStriUV2GF0wX7MzYy0XMWNKZjZjQ=", // 加密后的身份证号
    "Name": "IS6wLE153MfBr639hqWmUQ==", // 加密后的姓名
    "Encryption": {
        "EncryptList": [ // 用于标记加密字段
            "IdCard",
            "Name"
        ],
        "CiphertextBlob":

"eqB5H23bbNQGTxCxSHP+FaXy+Llfk2GJ8119UxTbikdezY1mGINQxS76J9rUa61W2jrm4j6eQ39O9pus/Wk5zP6t48Gd8M6RHld17/pPT
nAVzjTwYZhy0yBvuyh7N73J5/fL2TSgJTMV179urCC17COoYdyBsK+hP9bIfzwxb3g=", // 加密后的对称密钥
        "Iv": "t9Uf9QJ5OBOuHhB26JLNxw==", // 加密初始向量
        "Algorithm": "ABS-256-CBC" // 采用的加密算法
    }
}
```

#### 使用 SM4-GCM 算法

#### 加载 SM2公钥

加载 SM2公钥:对控制台获取到的公钥字符串先做 Base64 Decode,然后按对应格式加载。

• 格式: PKCS8

• 保存格式: pem格式Base64编码

• 长度: 512

```
// 加载SM2公钥
bytes, err := base64.StdEncoding.DecodeString(publicKey)
if err != nil {
    return nil, err
}
x509.ReadPublicKeyFromPem(bytes)
```

# 生成对称密钥和向量

随机生成16字节长度的对称密钥以及12字节的初始向量,初始向量表示为 IV。

```
// 生成对称密钥
key := make([]byte, 16)
rand.Read(key)

// 生成16字节iv
iv := make([]byte, 12)
rand.Read(iv)
```

#### SM2公钥加密对称密钥

使用 SM2公钥加密前面生成的 对称密钥,将加密后的结果表示为 CiphertextBlob。



- 注意输出密文时采用 C1C3C2数据拼接方式
- 数据类型转换时,均使用 PC=04的方式,即未压缩。

```
// 加密对称密钥Key
ciphertext, err := sm2.Encrypt(publicKey, plaintext, rand.Reader, sm2.C1C3C2)
if err != nil {
    return nil, err
}
return cipherText, nil
```

#### 加密敏感数据

使用前面生成的 对称密钥和初始向量,采用 SM4-GCM 算法加密敏感数据(姓名、身份证号)。

```
// SM4-GCM加密明文数据
// 朗文密钥key
// 初始向量iv
// 敏感数据plaintext
block, err := sm4.NewCipher(key)
if err != nil {
    return nil, nil, err
}
gcm, err := cipher.NewGCM(block)
if err != nil {
    return nil, nil, err
}
ciphertext := gcm.Seal(nil, iv, plaintext, nil)
tag := ciphertext[len(ciphertext)-gcm.Overhead()]
return ciphertextWithoutTag := ciphertext[:len(ciphertext)-gcm.Overhead()]
return ciphertextWithoutTag, tag, nil
```

#### 调用人脸核身接口

以身份证二要素(IdCardVerification)接口为例:

原始数据为:

```
{
    "Action": "IdCardVerification",
    "Version": "2018-03-01",
    "IdCard": "100822119610104046",
    "Name": "张三"
}
```

CiphertextBlob、IV、TAG、加密后的姓名、身份证号在传输前均需要做一次Base64编码。

- 生成的对称密钥为: 45c3royvhyj6cavv (16字节)
- 生成的初始向量(IV): bIGEqJyU+8MIJO3u(12字节IV, Base64编码)

公钥加密后的对称密钥(CiphertextBlob):

BD1WkCZPN1Tn0jzNlZoHf1JHjBFDRRdVnj9UV9gETROOo+HhOJcQreZacgVyPqE+E4OqDvtu5cttXslhztDV7uYJZmNdpFWnTnXtSgjXFvOf2n48gNMu5l0Ung5+VrDN2SzY2D9cetiuOFktsJEzTCs=(Base64编码)

使用对称密钥加密IdCard和Name,加密后的结果分别为:

- IdCard: 8qjVE9kEqW7R3x3Nd5AM5PDb(Base64编码) Tag: wMyiG6JUzj4CliZ+V5mqwA==(Base64编码)
- Name: JiRFz1O/(Base64编码)Tag: msgrOgSfnMEK1ZzPtcaaFg==(Base64编码)

最终加密后的接口数据为:

```
{
    "Action": "IdCardVerification",
    "Version": "2018-03-01",
```



```
"IdCard": "8gjVE9kEqW7R3x3Nd5AM5PDb", // 加密后的身份证号
"Name": "diRZ1O/", // 加密后的姓名
"Encryption": {
    "EncryptList": [ // 用于标记加密字段
        "IdCard",
        "Name"
    ],
    "TagList": [ // 用于验证消息完整性
        "wMyiG6JUzj4C1iZ+V5mqwA==",
        "msgrOgSfnMEK1ZzPtcaaFg=="
    ],
    "CiphertextBlob":
"BD1WkCZPN1Tn0jzNIZoHf1JHjBFDRRdVnj9UV9gETROOo+HhOJcQreZacgVyPqE+E4OqDvtu5cttXsIhztDV7uYJZmNdpFWnTnXtSgjXF
vOf2n48gNMu5IOUng5+VrDN2SzY2D9cetiuOFktsJEzTCs=", // 加密后的对称密钥
    "Iv": "bIGEqJyU+9MIJO3u", // 加密初始向量
    "Algorithm": "SM4-GCM" // 采用的加密算法
    }
}
```



# 数据存储服务指引

最近更新时间: 2025-02-24 14:55:22

对象存储(Cloud Object Storage,COS)是腾讯云提供的一种存储海量文件的分布式存储服务,具有高扩展性、低成本、可靠安全等优点。通过控制台等方式,用户可简单、快速地接入 COS,进行多格式文件的上传、下载和管理,实现海量数据存储和管理。若您开通了人脸核身 COS 存储服务,我们会将您腾讯云账号下的人脸核身核验结果(包括身份证照片、人脸核身视频以及视频最佳帧)以及意愿核身结果(包括视频、屏幕截屏以及回答音频)自动转存到您腾讯云账号下的 COS 空间中,您可以到 COS 控制台 进行数据管理。

#### ① 说明:

- 1. 该服务仅限全读写权限账号可开通,开通后主、子账号、协作者账号共用一个 COS 存储桶。
- 2. 若您在人脸核身控制台开通了数据存储服务,调用 GetDetectInfoEnhanced 或者 GetEidResult 接口拉取结果时,会将视频、图片、音频等相关字段的 base64替换为 COS 的路径。
- 3. 该 COS 的数据存储服务为收费服务,请您了解 COS 计费概述。

目前支持以下渠道接入的人脸核身以及意愿核身核验结果存储到 COS 空间。

接入渠道	人脸核身		意愿核身(问答+点头)			
	身份证照片	人脸核身视频	视频最佳帧	意愿确认视频	屏幕截屏	回答音频(问答模式)
微信小程序	✓	✓	✓	✓	✓	✓
H5(微信浏览 器)	✓	✓	✓	1	1	<b>√</b>
E证通	✓	✓	✓	✓	1	✓

# 步骤一: 授权流程

1. 登录人脸核身控制台,选择**数据存储服务**页面。在页面第一步**服务授权**单击**前往授权**跳转到授权页面。



2. 在服务授权页面单击同意授权。



3. 勾选阅读并同意《腾讯云服务协议》和《对象存储服务等级协议》后,单击确定创建。

版权所有: 腾讯云计算(北京)有限责任公司





4. 创建成功后会展示您的 COS 存储桶,腾讯云慧眼人脸核身将可以进入您的COS桶中写入资源,您可以到您的 COS 控制台 中看到该存储桶并管理所存储的 文件。



# 步骤二: 开通流程

步骤一的授权流程只是授权腾讯云慧眼人脸核身能够访问您的COS部分资源,完成上述授权流程之后需要 联系我们 针对不同的产品进行开通。开通之后,对应产品的人脸核身核验结果(包括身份证照片、人脸核身视频以及视频最佳帧等)将自动转存到该 COS存储桶中, GetDetectInfoEnhanced 或者 GetEidResult 拉取核验结果时会将相关字段的 base64 替换为 COS 路径。

# △ 注意:

完成步骤一的授权流程只是授权腾讯云慧眼人脸核身能够访问您的COS部分资源,并不代表开通,开通需 联系我们。

# 使用指引

开通数据存储服务后,调用 GetDetectInfoEnhanced 或者 GetEidResult 拉取核验结果时会将相关字段的 base64 替换为 COS 路径,不再返回 base64格式的图片、视频等信息。 GetDetectInfoEnhanced 和 GetEidResult 接口中的 IsCustomizeStorage 字段标识当次请求是否已经开启COS 存储,当该值返回 true 时,表示该次核身结果涉及到的图片、视频、音频(如有)文件已存储到您的COS存储桶中,对应的存储路径请见图片、视频、音频的输出参数(具体的字段名称详见QA部分),您可以通过该路径在存储桶bucket中找到对应的文件。存量服务可以参考如下代码片段完成服务改造之后再开通数据存储服务。

#### ⚠ 注意:

存量服务开通数据存储服务之前确保已经对 GetDetectInfoEnhanced 或者 GetEidResult 接口的响应做了相应的适配工作,防止开通之后不再返回base64数据导致线上服务异常。

#### 数据存储服务常见问题



# 已经在控制台开通数据存储服务,但是 COS 桶中没有图片和视频?

需要提供创建账号 和 RuleID (可前往 控制台 获取),联系我们开通服务。

# 数据存储服务的收费标准?

人脸核身服务将图片和视频存储到 COS 不收费。数据存储到 COS 收费,可以参考 COS 计费概述。

#### 开通数据存储服务后,COS 路径怎么返回?

调用 GetDetectInfoEnhanced 或者 GetEidResult 接口拉取结果时,默认返回base64数据,开通数据存储服务后会将视频及图片字段的 base64替换为 COS 的路径返回。

# 图片和视频数据存储在哪里?

默认数据缓存在腾讯公有云,开通数据存储服务后存储在用户 COS 桶中。

# 开启自定义存储后哪些字段需要做特殊处理?

当启用自定义存储后,GetEidResult、GetDetectInfoEnhanced 接口中以下属性将会直接返回对应 COS路 径,而不再返回base64。

属性名	含义	备注
Response.ldCardData.OcrFront	OCR 正面照片	_
Response.ldCardData.OcrBack	OCR 反面照片	_
Response.ldCardData.ProcessedFrontImage	旋转裁边后的正面照片	_
Response.ldCardData.ProcessedBackImage	旋转裁边后的背面照片	-
Response.ldCardData.Avatar	身份证正面人像图	-
Response.BestFrame.BestFrame	活体比对最佳帧	-
Response.BestFrame.BestFrames[]	自截帧	数组中所有项目都会返回 COS 路径
Response.VideoData.LivenessVideo	活体视频	_
Response.IntentionQuestionResult.Video	意愿核身问答模式全流程视频	-
Response.IntentionQuestionResult.ScreenShot[	意愿核身问答模式屏幕截图	数组中所有项目都会返回 COS 路径
Response.IntentionQuestionResult.Audios[]	意愿核身问答模式答案录音音频	数组中所有项目都会返回 COS 路径
Response.IntentionActionResult.Details[0].Vide o	意愿核身点头模式视频(其中包含全程提示文 本和点头音频,mp4格式)	IntentionActionResult.Details 只有一个项目
Response.IntentionActionResult.Details[0].Scre enShot[]	意愿核身点头模式屏幕截图	数组中所有项目都会返回 COS 路径
Response.IntentionVerifyData.IntentionVerifyVi deo	意愿核身朗读模式录制的视频	注意:此字段不支持自定义存储,会原 样返回base64
Response.IntentionVerifyData.IntentionVerifyBe stFrame	意愿核身朗读模式录制视频的最佳帧	注意:此字段不支持自定义存储,会原 样返回base64

版权所有: 腾讯云计算(北京)有限责任公司