ICS
X xx
备案号：

GDZW

广 东 政 务 服 务 平 台 标 准

GDZW xxxx—2019

智能网关业务接入规范

（征求意见稿）

2019-XX-XX 发布　　201x-xx-xx 实施

XXX 发布

目　　次

前　　言

本标准按GB/T 1.1-2009给出的规则起草。

智能网关业务接入规范

1 范围

本标准规定了智能网关的使用过程、开发规范等基本要求。

本标准适用于智能网关v1.0版本。使用该规范前需要部署智能网关v1.0。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25068.3-2010 信息技术 安全技术 IT网络安全 第3部分:使用安全网关的网间通信安全保护

GB/T 29265.204-2017 信息技术 信息设备资源共享协同服务 第204部分:网关

3 术语和定义

下列术语和定义适用于本标准

3.1

应用程序编程接口 (API)

软件系统不同组成部分衔接的函数，应用将自身的服务能力封装成 API，并通过 API 网关开放给用户调用。

3.2

超文本传输协议 (HTTP)

一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。

3.3

超文本传输安全协议 (HTTPS)

由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议。

3.4

应用标识 (PaaSID)

智能网关应用的全局唯一的标识，由英文组成，最长20个字符。

3.5

应用密钥 (PaaSToken)

一种分配给调用方之后，调用方每次发起请求都应该将根据 token 计算出来的签名（signature）和当前时间戳放入请求头中提供给网关进行来源合法性验证的标识符。

3.6

统一资源定位符 (URL)

以字符串的抽象形式来描述一个资源在万维网上的地址。一个URL唯一标识一个Web资源，通过与之对应的URL即可获得该资源。

4 概述

智能网关是一款主要包括了准入网关和API网关一体化的产品平台。在保证服务安全的情况下，使得政府、大型企业内部服务和互联网服务之间能够安全的进行数据交换。智能网关业务使用过程见图1。

准入网关是一款针对站点和服务访问控制的安全产品，它为互联网、政务外网、公安网等民生服务应用提供了安全、可控、高效的身份接入、设备鉴权和按应用授权的资源准入服务。

API网关提供API的完整生命周期管理，包括创建、维护、发布、运行、下线等。可以使用 API Gateway 封装自身业务，将用户的数据、业务逻辑或功能安全可靠的开放出来，用以实现自身系统集成、以及与合作伙伴的业务连接的产口。

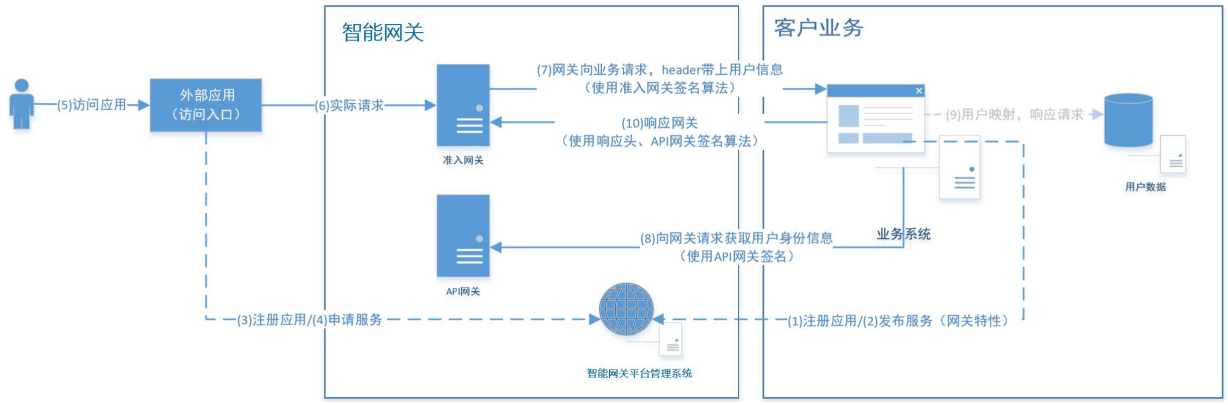

图1 智能网关业务使用过程示意图

交互过程说明如下：

——在智能网关平台管理系统中注册一个的客户业务系统的应用；

——在智能网关平台管理系统的应用上发布一个网关特性的业务系统服务；

——在智能网关平台管理系统中注册一个外部应用；

——外部应用要使用的网关特性的业务系统服务，需要在智能网关平台管理系统上“申请使用服务”；

——用户通过向外部应用发起请求；

——外部应用把实际请求转发给准入网关；

——网关使用带上准入网关签名算法的Header头向业务系统发起请求；

——业务系统使用API网关的签名算法的Header头向API网关获取用户身份信息；

——业务系统响应用户请求；

——业务系统使用响应头、带上API网关签名算法的Header头向准入网关发送响应。

5 准入网关接入规范

5.1 准入网关使用

5.1.1 概述

使用准入网关应先在智能网关管理系统创建一个应用，开通智能网关的服务并配置客户端信息。创建应用后可获得一个应用标识（PaaSID）和应用密钥（PaaSToken），这个PaaSToken 将用于：

——当网关收到用户的请求，网关向后端的服务转发请求时，会在Header带上包含这个PaaSToken所计算的签名；

——应用服务响应网关请求时，需要带在Header带上包含这个PaaSToken所计算的签名；

5.1.2 发布网关特性服务

5.1.2.1 通则

一个应用的服务若被其它应用的用户所使用，应先在智能网关平台管理系统上“发布服务”选择访问特性为“网关特性”，并通过智能网关平台管理系统上报给服务管理者审核。审核通过后，用户访问该应用的请求会先请求网关。再从网关转发到应用的服务地址上，并按照应用的 PaaSToken 计算签名放进请求 Header，同时应用服务需要响应签名，否则网关会拒绝响应并返回 403 给调用方。如果当前请求是从后端（无用户信息）发起，则网关会直接拒绝该请求，并不会转发到该服务的地址。

5.1.2.2 路径生成

路径生成规则：https:// {部署API网关时的域名}/{发布服务的应用PaaSID}/

示例：

例如公积金原始服务地址为 https://xxxx.com/getcity，公积金在智能网关平台创建的应用PaaSID为hpfund，则发布服务成功后，则对外的服务地址如下：

https:// {部署API网关时的域名}/hpfund/getcity

注：同一个应用的服务默认可以不用发布为网关特性服务，可以直接调用后端地址，网关也会按照应用的 PaaSToken 计算签名放进请求 Header，同时应用的服务需要响应签名，否则网关会拒绝响应并返回 403 给调用方。

5.1.3 申请网关特性服务

使用其它应用的网关特性的服务时，应先在智能网关平台管理系统上“申请使用服务”。审核通过后，网关会生成服务请求地址，用户可通过请求该地址使用该服务，用户应从客户端发起请求，否则网关会拒绝请求。

5.2 准入网关开发规范

5.2.1 对服务发布者的网络要求如下：

——服务在互联网，应满足以下任意一种条件：

a) 提供 HTTPS 协议的接口

b) 提供内容加密的 HTTP 协议接口

——服务在公安网或政务外网：宜使用与互联网服务保持相同加密级别；

5.2.2 对服务发布者的接口类协议应符合以下请求和响应的签名要求：

——必须是HTTP/HTTPS协议；

——支持的请求内容的数据格式包括以下格式，且应在请求头中设置相应的Content-type：

a) Urlencoded (text/x-www-form-urlencoded)

b) json (text/json)

c) xml (text/xml)

——支持的响应内容的数据格式包括以下格式，且应在请求头中设置相应的Content-type：

a) json (text/json)

b) xml (text/xml)

——请求和响应最大字节数不超过8M。

5.2.3 对服务发布者的文件类协议要求

文件类接口请求应符合请求和响应的签名要求。

5.2.4 鉴权要求

5.2.4.1 网关转发（网关请求，被请求者）

所有从客户端发起的请求，准入网关都会自动进入身份认证过程。网关鉴权后，会在向服务端的请求头上自动增加以下几个字段：

请求头：

x-tif-signature：准入网关生成的签名字符串，您需要验证该字符串是否合法
x-tif-timestamp：准入网关的 unix 时间戳秒
x-tif-nonce：准入网关生成的非重复的随机字符串，用于结合时间戳防止重放
x-tif-uid：用户的 id
x-tif-uinfo：用户的身份证信息
x-tif-ext：用户信息扩展字段，json 对象

被请求者需要根据签名算法计算签名并验证请求来源。

5.2.4.2 响应网关（被请求者）

为了保证鉴权链路的完整性，业务服务也需要按照同样的签名算法将签名放入 Header 中，网关会根据签名算法进行调用验证。如果没有进行签名计算，网关默认不转发该响应内容并返回 403 错误给请求方。

网关要校验服务端返回数据的合法性，服务端需要在响应头中增加如下字段：

响应头：

x-tif-signature：被调用者生成的签名字符串
x-tif-timestamp：服务端（被调用者）时间，unix 时间戳秒
x-tif-nonce：服务端（被调用者）生成的非重复的随机字符串（十分钟内不能重复），用于结合时间戳防止重放 。

——网关转发（网关响应，响应请求者），HTTP响应状态码，常见的异常响应码见表1：

a) 大于等于 200 小于 300 表示成功;
b) 大于等于 400 小于 500 为客户端错误;
c) 大于 500 为服务端错误。

表 1 常见的异常响应码说明

错误码	描述	错误原因
400	错误的请求	1） 请求内容与请求头中的 Content-Type 不符 2） 请求内容格式遭到破坏（不完整的 json 或 xml 格式） 3） API 服务商认为该请求提交的数据不合法
403	禁止访问	1） 调用者签名算法计算有误或用于计算的 PaaSToken 不正 确； 2） 调用者服务器上生成的时间戳与标准时间误差超过 180 秒； 3） 响应头中未带上签名
404	API 服务不存在	可能是调用的 API 地址不正确
421	并发调用数超过限制	来源 IP 的并发调用数超过限制
502	服务不可用	API 网关出现异常
503	频率超过限制	API 调用频率超过申请的频率限制

——全局错误码，错误码分配见表2，网关响应错误码见表3。

表 2　错误码分配说明

厂商	错误码区间
smartgate	0-9999
openapi	10000-99999999
小马达	100, 00000-100, 99999
天健	101, 00000-101, 99999
华滋	102, 00000-102, 99999
优路加	103, 00000-103, 99999
注：各区间错误码中 00001 是未定义错误（errmsg 中附带错误信息）如小马达系统中出现未定义错误，返回的错误码为 10000001	

表 3　网关响应错误码说明

错误码	错误说明	排查方法或处理
1001	系统错误	
1002	未登录或登录失效	
1003	需要刷脸二次认证	
1004	需要实名二次认证	
1005	需要指纹二次认证	
1006	需要实人绑定	
1007	刷脸二次认证与实名绑定的身份证信息不一致	
2001	系统错误	
2002	系统数据错误	
2003	签名错误	
2004	非法请求	
2005	无效的 uid	
2006	无效的 paasid	
2007	无效的 appid	
2008	用户未实名	
2009	无效的证件 ID	
2010	无效的证件码	
2011	openapi 错误	
2012	证件不存在	
2013	总线上发布的 API 调用失败	

请求头：

x-tif-error：网关的错误

——签名算法，签名算法主要使用以下几个字段：

a)　x-tif-timestamp：准入网关的 unix 时间戳秒

b) x-tif-uid：用户的 id
c) x-tif-uinfo：用户的身份证信息
d) x-tif-ext：用户信息扩展字段，json 对象
e) x-tif-nonce：由调用者/被调用者/网关生成的非重复的随机字符串（十分钟内不能重复）
f) PaaSToken：创建应用时分配的加密密钥；

——签名算法公式：

```
x-tif-signature = sha256(x-tif-timestamp + PaaSToken + x-tif-nonce +","+ xtif-uid +","+ x-tif-uinfo+"," +
x-tif-ext + x-tif-timestamp)
```

——签名字符串签名算法说明如下：

```
func calcSign(x-tif-timestamp, x-tif-nonce, x-tif-uid, x-tif-uinfo, x-tif-ext string) {
    // 拼接从请求头中读取的 x-tif-timestamp x-tif-nonce x-tif-uid x-tif-uinfo x-tif-ext 字段
    // 注意逗号分隔符，x-tif-nonce x-tif-uid x-tif-uinfo x-tif-ext 之间有逗号分隔
    sign_data := fmt.Sprintf("%s%s%s,%s,%s,%s%s", x-tif-timestamp, PaaSToken, x-tif-nonce,
x-tif-uid,x-tif-uinfo, x-tif-ext, x-tif-timestamp)
    // 对拼接后的字符串计算 sha256，将计算后的结果转成 Hex 字符串并转成大写
    Return strings.ToUpper(fmt.Sprintf("%x", sha256.Sum256([]byte(signData))))
}
```

5.3 准入网关小程序 SDK

5.3.1 概述

准入网关小程序 SDK 是准入网关面向微信小程序开发者提供的微信小程序开发工具包。通过使用准入网关小程序 SDK，微信小程序开发者可借助准入网关高效的使用登录、实名认证、人脸识别、微信支付验证等统一身份鉴权的能力，同时通过准入网关使用第三方发布的服务。

5.3.2 网络请求

发起网络请求，对微信小程序 wx.request 接口的封装，会自动检测小程序的登录态，并自动登录，会自动处理鉴权和身份相关的错误。返回参数应与 wx.request 完全一致。

示例：

https://developers.weixin.qq.com/miniprogram/dev/api/networkrequest.html

方法名：

tif.request ({}); 参数与 wx.request 的保持一致。

5.3.3 实名认证

5.3.3.1 唤起实名实人验证（已经绑卡的情况）

对当前用户进行实名实人验证，如果用户未实名认证，则自动跳转到授权页面完成首次认证过程。当使用 tif.request 访问 API 网关的服务时，业务方无需调用，此授权过程自动完成。

示例：

```
tif.selfFaceVerify({
success: function(res) {
console.log(res.useridkey)
```

```
},
fail: function(err) {
console.log(err)
},
cancel: function() {
}
})
```

5.3.3.2 唤起人脸识别（没有绑卡的情况）

对当前用户进行人脸识别验证，如果用户未实名认证，则自动跳转到授权页面完成首次认证过程。当使用 tif.request 访问 API 网关的服务时，业务方无需调用，此授权过程自动完成。

示例：

```
tif.faceVerifyWithIdCard ({
name: "张三",
idCardNumber: "123456789987654321",
success: function(res) {
    console.log(res.data)
},
fail: function(err) {
     console.log(err)
}
})
```

表 唤起人脸识别 success 返回参数说明

参数	类型	说明
name	string	身份证姓名
idCardNumber	string	身份证号码
useridkey	string	身份信息临时票据

5.3.3.3 唤起微信支付验证

唤起微信支付验证，输入支付密码可以完成二次验证，如果用户未实名认证，则自动跳转到授权页面完成首次认证过程。当使用 tif.request 访问 API 网关的服务时，业务方无需调用，此授权过程自动完成。

示例：

```
tif.authRealName ({
success: function(res) {
  console.log(res.data)
},
fail: function(err) {
console.log(err)
},
cancel: function() {
}
})
```

表 唤起微信支付验证 success 返回参数说明

参数	类型	说明
useridkey	string	身份信息临时票据

5.3.3.4 身份信息

获取当前用户的登录态相关信息，返回脱敏身份数据。

示例：

```
tif.getSession({
success: function(res) {
        console.log(res.data)
},
    fail: function(err) {
        console.log(err)
}
})
```

表 身份信息 success 返回参数说明

参数	类型	说明
faceExpire	string	人脸过期时间（Unix 时间戳秒）
realnameExpire	string	实名过期时间（Unix 时间戳秒）
cid	string	身份证号（脱敏-带*）
name	string	身份证姓名（脱敏-带*）

6 API 网关接入规范

6.1 API 网关使用过程说明

在开始使用 API 网关之前，需要先在智能网关平台创建一个系统，然后在系统下创建应用。创建应用后，可以获得一个应用标识(PaaSID)和应用密钥(PaaSToken)，这个 PaasToken 将用于：

a) 第三方应用向网关发起请求时，需要在 Header 带上包含这个 PaaSToken 所计算的签名；
b) 网关向后端的应用服务转发请求时，会在 Header 带上包含这个 PaaSToken 所计算的签名；
c) 后端的应用服务响应网关请求时，需要带在 Header 带上包含这个 PaaSToken 所计算的签名；

6.1.1 发布服务

如果有一个应用服务需要被其它应用所使用，需要先在智能网关管理系统中—选择系统—选择应用，并在该应用上创建“API 网关”服务。服务发布时默认勾选“不允许用户访问”。待审核通过后，访问该应用服务的请求会先请求网关，再从网关转发到该应用服务上，并按照 PaaSToken 计算签名放进请求 Header，同时应用服务需要响应签名，否则网关会拒绝响应并返回 403 给调用方。

路径生成规则：https:// {部署 API 网关时的域名}/{应用标识 PaaSID}/

示例：

生活服务的应用有一个获取城市列表的服务，该服务的原始服务地址为 https://xxxx.com/getcity，生活服务在智能网平台创建的应用 PaaSID 为 life，则发布服务成功后，则对外的服务地址默认如下：

https://{部署 API 网关时的域名}/life/getcity

也可以在发布的时候输入其他的访问地址或者单独的域名。

6.1.2 申请第三方服务

如果需要使用其它应用的服务，需要先在 API 网关上“申请使用服务”，当服务所属的管理者审核通过之后，会生成服务请求地址，可以通过请求该地址使用该服务，但是需要按照 PaaSToken 计算签名放进请求 Header，否则网关会拒绝请求。

注：同一个应用发布的服务默认可相互调用，不需要申请。

6.2 API 网关开发规范

6.2.1 对服务发布者的网络要求：

——服务在互联网，必须满足以下任意一种条件：

1) 提供 HTTPS 协议的接口
2) 提供内容加密的 HTTP 协议接口

——服务在特殊网络：建议使用与互联网服务保持相同加密级别；

6.2.2 对服务发布者的接口类协议应符合如下请求和响应的签名要求：

——必须是HTTP/HTTPS协议；

——支持的请求内容的数据格式包括： 以下格式须在请求头中设置相应的Content-type。

1) Urlencoded (text/x-www-form-urlencoded)
2) json (text/json)
3) xml (text/xml)

——支持的响应内容的数据格式包括： 以下格式须在请求头中设置相应的Content-type。

1) json (text/json)
2) xml (text/xml)

——请求和响应最大字节数不超过8M。

——响应头需要带上签名。

6.2.3 对服务发布者的文件类协议要求

文件类接口无请求内容格式要求，但是需要符合请求和响应的签名要求。

6.2.4 鉴权要求

6.2.4.1 通则

请求头/响应头的字段可能会根据部署时的设置有所改变，实际返回字段名称以部署时设置为准。

6.2.4.2 请求网关/请求发布在 API 网关的其他服务（请求者）

请求地址：所有接入 API 网关的服务都会生成一个唯一的 URL，如果您需要使用在网关上的服务，需要在网关上先申请使用服务。

请求方法：POST

请求体：参考“接口类协议要求”或者“文件类协议要求”

请求头：

x-tif-paasid：您的（调用者）应用的 PaaSID

x-tif-signature：您（调用者）生成的签名字符串，详细算法见“签名算法”部分

x-tif-timestamp：当前 unix 时间戳（秒）

x-tif-nonce： 您（调用者）生成的非重复的随机字符串（十分钟内不能重复），用于结合时间戳防止重放

6.2.4.3 网关转发（网关请求，被请求者）

所有请求经过网关后，网关鉴权后，会在请求头上自动增加以下几个字段：

请求头：

x-tif-signature：API 网关生成的签名字符串，您需要验证该字符串是否合法；

x-tif-timestamp：API 网关的 unix 时间戳（秒）

x-tif-nonce：API 网关生成的非重复的随机字符串，用于结合时间戳防止重放

6.2.4.4 响应网关（被请求者）

为了保证鉴权链路的完整性，业务服务也需要按照同样的签名算法将签名放入 Header 中，API 网关会根据签名算法进行调用验证。如果没有进行签名计算，网关默认不转发该响应内容并返回 403 错误给请求方。

网关要校验服务端返回数据的合法性，服务端需要在响应头中增加以下字段：

响应头:

x-tif-signature：被调用者生成的签名字符串

x-tif-timestamp：服务端（被调用者）时间，unix 时间戳（秒）

x-tif-nonce：服务端（被调用者）生成的非重复的随机字符串（十分钟内不能重复），用于结合时间戳防止重放

6.2.4.5 网关转发（网关响应，响应请求者）

响应头：

x-tif-signature：API 网关生成的签名字符串，您需要验证该字符串是否合法；

x-tif-timestamp：API 网关的 unix 时间戳（秒）

x-tif-nonce：API 网关生成的非重复的随机字符串，用于结合时间戳防止重放

x-tif-error：网关的错误

6.2.4.6 签名算法

签名算法主要使用以下几个字段：

x-tif-timestamp：当前时间 unix 时间戳，精确到秒

x-tif-nonce：由调用者/被调用者/网关生成的非重复的随机字符串（十分钟内不能重复）

Token：创建应用时分配的加密密钥；

签名算法公式：

x-tif-signature = sha256(x-tif-timestamp + Token + x-tif-nonce + x-tif-timestamp)