ICS 35.240.99
L 67

ZWFW

广 东 数 字 政 府 标 准 规 范

GDZW 0012-2019

广东省业务系统接入智能网关规范

2019-08-20 发布　　2019-08-20 实施

广东省政务服务数据管理局 发布

目　　次

前　言

本标准按GB/T 1.1-2009给出的规则起草。

本标准由广东省政务服务数据管理局归口。

引　言

广东政务服务网以便利民生服务、营造高水平营商环境为目标，全面集成了广东省、市、县、镇、村五级政务服务事项，提供各类高频便民利企主题服务，支撑全省网上政务服务“一网通办”。广东政务服务网提供的各类服务，涉及到的业务系统、服务接口众多，需要管理和维护的服务数量庞大。如缺少集中的管理和访问鉴权，无法对服务的安全进行全面管控。为解决此问题，通过将各业务系统接入智能网关，为各类服务提供安全、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，同时通过API的生命周期管理，可以实现业务系统、应用模块、服务的注册、发布、授权、审核、监控。

广东省业务系统接入智能网关规范

1 范围

本标准规定了广东政务服务网的各业务系统接入智能网关的使用及开发等规范要求。

本标准适用于接入广东政务服务网的各业务系统。

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

3.1

应用标识 PaaSID

智能网关应用的全局唯一的标识。

3.2

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。

3.3

内容类型 Content-type

用于定义网络文件的类型和网页的编码，决定浏览器将以什么形式、什么编码读取这个文件。

3.4

请求头 Header

http请求头，用来设置包含日期和数值的应答头。

3.5

令牌 Token

在一些数据传输之前，要先进行暗号的核对，不同的暗号被授权不同的数据操作。

3.6

业务系统 Business system

指政务服务应用系统。如无特指，系指已集成在政务门户中的政务服务业务系统。

3.7

用户 User

指访问以及办理政务服务网相关业务的使用者。

3.8

外部应用 External Application

指调用其他应用服务时创建的调用方应用。

4 缩略语

下列缩略语适用于本文件。

API 应用程序编程接口（Application Programming Interface）
HTTP 超文本传输协议（HyperText Transfer Protocol）
HTTPS 基于安全通道的超文本传输协议(HyperText Transfer Protocol over Secure Socket Layer)
URL 统一资源定位符（Uniform Resource Locator）
JSON JavaScript 对象标记语言（JavaScript Object Notation）
XML 可扩展标记语言（Extensible Markup Language）
UNIX 程序设计语言统一扩充的信息和计算机系统(Uniplexed Information and Computer Systems)
ID标识号码（Identity document）

5 智能网关接入概述

5.1 智能网关功能概述

智能网关包括了准入网关和API网关。在保证服务安全的情况下，使得政务服务网的各业务系统之间能够安全的进行数据交换。

准入网关是针对站点和服务访问控制的安全产品，它为政务服务网各业务系统提供了安全、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服务的完整生命周期管理，包括创建、维护、发布、 运行、下线等。业务系统可以使用 API 网关封装自身业务，将数据、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、与其他业务系统的业务连接。

5.2 智能网关接入申请流程

政务服务网相关的业务系统接入智能网关需要经过申请与审核,只有审核通过之后才能够登录智能网关平台管理系统进行服务配置，申请审核流程见图1。

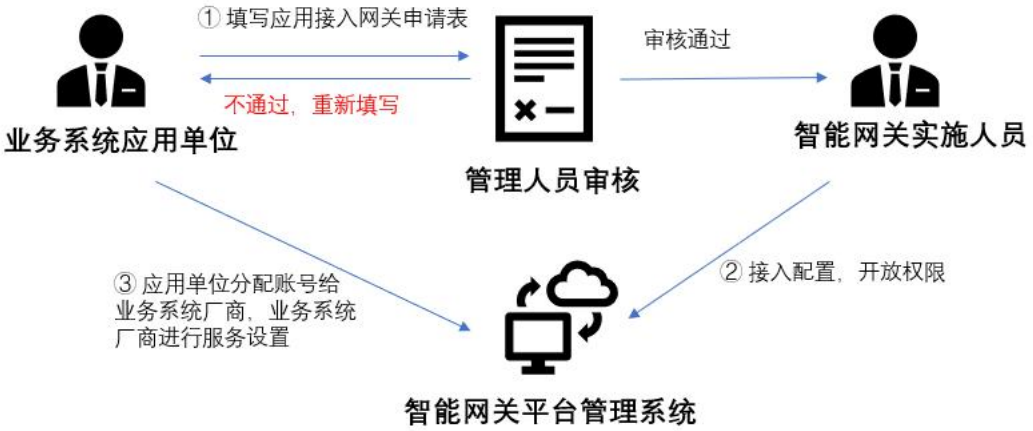

图1 智能网关接入申请流程示意图

申请流程说明如下：

a) 政务服务网相关的业务系统接入智能网关前，须填写应用接入网关申请，由政务服务网管理人员进行审核，审核不通过须按照审核意见重新填写；

b) 智能网关实施人员根据申请信息进行系统接入配置，开通智能网关平台管理系统的访问权限；

c) 业务系统应用单位分配账号给业务系统厂商，厂商登录智能网关平台管理系统进行业务服务的相关配置。

5.3 智能网关业务使用流程

政务服务网相关的业务系统接入到智能网关之后，可进行相关的业务访问与使用，智能网关业务使用过程见图2。

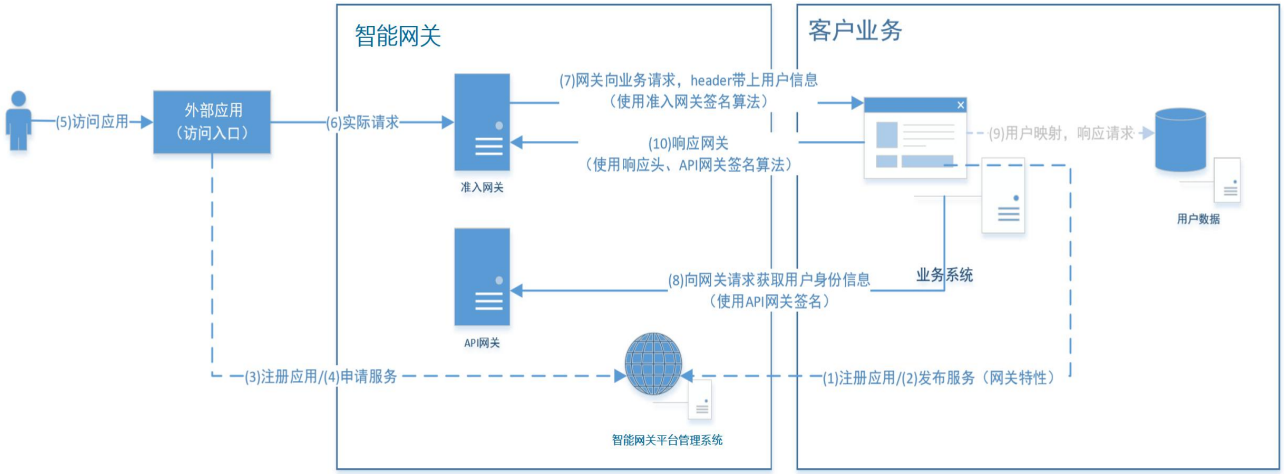

图2 智能网关业务使用过程示意图

使用过程说明如下：

a) 业务系统厂商在智能网关平台管理系统中注册一个业务系统的应用；

b) 业务系统厂商在业务系统的应用上发布一个网关特性的业务系统服务；

c) 服务调用方在智能网关平台管理系统中注册一个外部应用；

d) 外部应用要使用业务系统服务时，需要在智能网关平台管理系统上申请使用服务；
e) 用户访问业务系统服务时，通过外部应用发起请求；
f) 外部应用把实际请求转发给准入网关；
g) 准入网关使用准入网关签名算法的Header连同用户信息向业务系统服务发起请求；
h) 业务系统使用API网关的签名算法的Header向API网关获取用户完整身份信息；
i) 业务系统响应用户请求；
j) 业务系统使用响应头，连同API网关签名算法的Header向准入网关发送响应。

6 准入网关接入规范

6.1 准入网关使用

6.1.1 概述

用户访问注册到智能网关的政务服务网相关业务站点，须通过准入网关鉴权之后才能转到相应业务站点进行访问。

业务系统使用准入网关应先在智能网关管理系统创建一个应用，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：

a) 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；
b) 应用服务响应网关请求时，需要在Header带上包含这个PaaSToken所计算的签名。

6.1.2 发布网关特性服务

一个应用的服务被其它应用所调用，应先在智能网关平台管理系统上将服务发布为网关特性服务，并经过服务管理者审核。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 错误码给调用方。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。

6.1.3 申请网关特性服务

外部应用使用其它应用网关特性的服务时，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，用户需要从客户端（有用户信息）发起请求，否则网关会拒绝请求。

6.2 准入网关开发规范

6.2.1 对服务发布者的网络要求

a) 服务在互联网，应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。
b) 服务在公安网或政务外网，应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要求

a) 必须是HTTP/HTTPS协议；
b) 支持请求内容的数据包括以下格式，且应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)

c) 支持响应内容的数据包括以下格式，且应在请求头中设置相应的Content-type。

1) json (text/json)

2) xml (text/xml)

d) 请求和响应最大字节数不超过8M。

6.2.3 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鉴权要求。

6.2.4 鉴权要求

6.2.4.1 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，会向服务端的请求头上自动增加以下几个字段：

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。

6.2.4.2 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：

x-tif-signature：服务端（被请求者）生成的签名字符串
x-tif-timestamp：服务端（被请求者）时间，unix 时间戳秒
x-tif-nonce：服务端（被请求者）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 签名算法

签名算法，签名算法主要使用以下几个字段：

x-tif-timestamp：准入网关的 unix 时间戳秒
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
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）
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)

7 API 网关接入规范

7.1 API 网关使用

7.1.1 概述

当政务服务网的业务服务需要调用同样注册到智能网关的另一个业务服务时，业务服务调用者须向被调者申请访问权限，被调用者审核通过之后，调用者方可访问其服务。

a) 业务系统在使用 API 网关之前，应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，可获得一个应用标识(PaaSID)和应用密钥(PaaSToken)，这个 PaasToken 将用于；

b) 第三方应用向网关发起请求时，应在 Header 带上包含这个 PaaSToken 所计算的签名；

c) 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；

d) 后端的应用服务响应网关请求时，应在 Header 带上包含这个 PaaSToken 所计算的签名。

7.1.2 发布服务

a) 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创建“API 网关”服务。服务发布时默认 “不允许用户访问”；

b) 允许用户访问需要进行审核操作，审核通过后，访问该应用服务的请求先向网关发送请求，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，同时应用服务须响应签名，否则网关会拒绝响应并返回 403 错误码至调用方。

7.1.3 申请服务

a) 业务系统需要使用其它应用的服务，需要先在 API 网关上申请使用该服务；

b) 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；

c) 同一个应用发布的服务默认可相互调用，不需要申请。

7.2 API 网关开发规范

7.2.1 对服务发布者的网络要求

a) 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。
b) 服务在在公安网或政务外网，应与互联网服务保持相同加密级别。

7.2.2 对服务发布者的接口类协议要求

a) 必须是HTTP/HTTPS协议；
b) 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)
c) 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)
d) 请求和响应最大字节数不超过8M。
e) 响应头需要带上签名。

7.2.3 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鉴权要求。

7.2.4 鉴权要求

7.2.4.1 请求网关/请求发布在 API 网关的其它服务（请求者）

请求服务的参数设置见表1：

表 1　请求参数说明表

请求参数	参数说明
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”（7.2.2）或者“文件类协议要求” （7.2.3）。
请求	x-tif-paasid：请求者应用的 PaaSID x-tif-signature：请求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： 请求者生成的非重复的随机字符串（十分钟内不能重复）。

7.2.4.2　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：

x-tif-signature：API 网关生成的签名字符串，被请求者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

7.2.4.3　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：

x-tif-signature：被请求者生成的签名字符串
x-tif-timestamp：服务端（被请求者）时间，unix 时间戳（秒）
x-tif-nonce：服务端（被请求者）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

7.2.4.4　网关转发（网关响应，响应请求者）

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：

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
x-tif-error：网关的错误

7.2.4.5　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)

参 考 文 献

[1] 国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知（国办函〔2016〕108号）

[2] 广东省人民政府关于印发广东省加快推进一体化在线政务服务平台建设工作实施方案的通知（粤府〔2018〕103号）