

SZSD

数 字 山 东 工 程 标 准

SZSD 0029—2024

省统建系统密码中心密码应用接入指南

Guidelines for cryptographic applications access of provincial unified construction
system cryptographic center

2024 - 04 - 15 发布

2024 - 06 - 01 实施

目 次

前 言 II

1 范围 3

2 规范性引用文件 3

3 术语和定义 3

4 缩略语 4

5 密码应用接入架构 4

6 密码应用接入流程 4

7 密码应用接口 5

附录 A 密码应用接口规范性附录..... 6

前 言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

本文件由山东省大数据局提出并归口。

本文件起草单位：山东省大数据中心、智慧齐鲁（山东）大数据科技有限公司。

本文件主要起草人：王伟、李德生、马金钊、沈政。

省统建系统密码中心密码应用接入指南

1 范围

本文件规定了省统建系统密码中心的密码应用接入架构、接入流程和密码应用接口要求。
本文件适用于省统建系统密码中心的密码服务的提供和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 39786-2021 信息安全技术 信息系统密码应用基本要求
GM/Z 0001 密码术语
GM/T 0002 SM4分组密码算法
GM/T 0003 SM2 椭圆曲线公钥密码算法
GM/T 0004 SM3 密码杂凑算法
GM/T 0015 基于SM2密码算法的数字证书格式规范
GM/T 0019 通用密码服务接口规范
GM/T 0062 密码产品随机数检测要求
GM/T 0094 公钥密码应用技术体系框架规范

3 术语和定义

界定以及下列术语和定义适用于本文件，为了便于使用，以下列出某些术语和定义。

3.1

消息鉴别码 message authentication code (MAC)

又称消息认证码，是消息鉴别算法的输出。

3.2

时间戳 time stamp (TS)

对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。

3.3

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.4

数字信封 digital envelope

一种数据结构，保护用对称密钥加密的密文和用公钥加密的该对称密钥。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Program Interface）

HMAC：带密钥的杂凑算法（Keyed-hash Message Authentication Code）

HTTPS：安全套接字层的超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）

JSON：JavaScript对象表示法（JavaScript Object Notation）

KEK：密钥加密密钥（Key Encryption Key）

TSP：时间戳协议（Time Stamp Protocol）

Restful：表现层状态转移（Representational State Transfer）

SDK：软件开发工具包（Software Development Kit）

SM2：一种椭圆曲线公钥密码算法（SM2 algorithm）

SM3：一种密码杂凑算法（SM3 algorithm）

SM4：一种分组密码算法（SM4 algorithm）

5 密码应用接入架构

用户向省统建系统密码中心申请开通账号，并申请密码服务。主管部门审核通过后，即可根据授权凭证调用所需的密码资源。密码应用接入架构如图1所示。

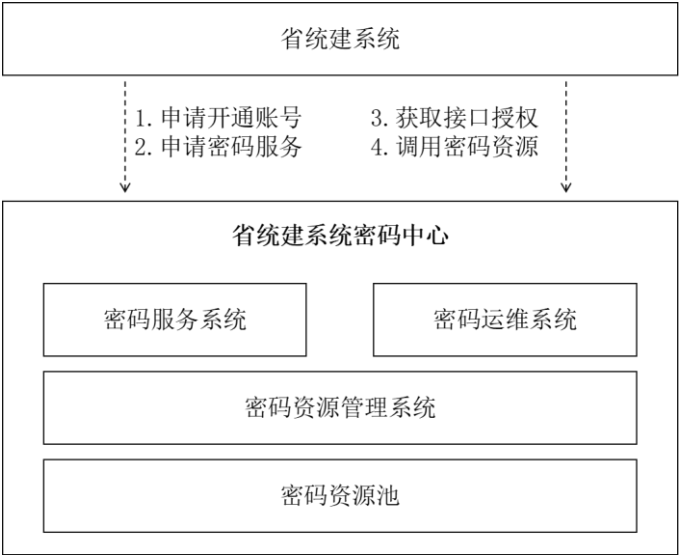


图1 密码应用接入架构图

6 密码应用接入流程

6.1 接入准备

省统建系统进行密码改造，接入密码中心前，做好以下准备工作：

- a) 明确本系统使用的技术架构和开发语言；
- b) 明确本系统的密码应用需求；
- c) 从密码中心网站下载SDK和说明文档，了解本系统改造的具体方式；
- d) 制定改造后的测试联调方案和升级方案。

6.2 接入流程

省统建系统接入密码中心，具体流程如下：

6.2.1 使用申请

根据省统建系统的运行情况，用户向密码中心申请密码服务，类别包括机密性服务、完整性服务、抗抵赖性服务、时间戳服务等。

6.2.2 申请审核

密码中心主管部门对用户的申请进行审核，并向用户反馈审核结果。满足条件的省统建系统运行实施密码应用接入，不满足条件的需说明理由。

6.2.3 开通资源

主管部门审核通过后，运维部门根据审核内容开通密码服务和密码资源。

6.2.4 测试联调

用户根据说明文档的要求对省级统建系统进行联调，并通过授权接口调用密码资源，测试系统的功能和性能是否满足业务需求。

6.2.5 系统运维

密码中心对密码资源、密码服务提供监控和运维能力，协助运维部门进行问题发现和处理，并为密码资源扩容和密码服务能力提升提供决策。

6.2.6 申请变更

用户向密码中心主管部门提出密码变更申请，审核通过后，变更密码服务和密码资源。

6.2.7 资源终止

用户向密码中心主管部门发起密码终止申请，审核通过后，经用户确认由运维部门按操作流程注销该系统密码服务，释放密码资源。

7 密码应用接口规范

密码应用接口遵循HTTPS协议，设计采用Restful风格接口，编码使用UTF-8的编码方式。HTTPS协议使用POST方法进行调用，请求和返回数据格式使用JSON数据格式。

为保证密码服务的安全性，密码中心提供的接口需符合如下要求：

- a) 密码中心对接入系统的身份进行安全验证，确保身份真实性；
- b) 密码中心基于HTTPS协议提供密码应用接口，确保数据传输安全性；
- c) 密码中心具有接口黑白名单功能，防止异常调用；
- d) 数据返回类型参考附录A具体内容。

密码应用接口名称及说明，如表1所示。

表1 密码应用接口名称及说明

序号	接口名称	接口说明
1	getToken	获取会话 Token 接口
2	bpsp.encrypt	数据加密接口
3	bpsp.decrypt	数据解密接口
4	bpsp.sm3Hash	SM3 哈希数据不可逆接口
5	bpsp.sign	数据签名接口
6	bpsp.verify	数据验签接口
7	bpsp.genMac	生成 MAC 接口
8	bpsp.verifyMac	验证 MAC 接口
9	bpsp.encryptECC	非对称外带密钥加密接口
10	bpsp.decryptECC	非对称外带密钥解密接口
11	bpsp.genBase64Sm2Key	非对称外带密钥解密接口
12	bpsp.externalSign	密钥导入并签名接口
13	bpsp.rawSignature	裸签名接口
14	bpsp.rawVerify	裸验证接口
15	bpsp.evpEncode	数字信封编码接口
16	bpsp.evpDecode	数字信封解码接口
17	bpsp.createdResponse	签发时间戳接口
18	bpsp.verifyTSValidity	验证时间戳接口
19	bpsp.generateRandom	生成随机数接口
20	bpsp.verifyCert	验证证书有效性接口
21	bpsp.attachedSignature	attached 方式签名接口
22	bpsp.attachedVerify	attached 方式验签接口
23	bpsp.detachedSignaturesdetach	方式签名接口
24	bpsp.detachedVerify	detach 方式验签接口
25	bpsp.hmacSM3	HMAC-SM3 接口

附录 A
(规范性)
密码应用接口

A. 1 数据结构定义

A. 1. 1 接口返回值数据结构定义

表A. 1 接口返回值数据结构说明

参数名称	数据类型	说明
request_id	字符串	请求序列号
code	字符串	返回码 10000 为成功，其他对应错误码
msg	字符串	返回信息，Success 表示成功，其他对应错误信息
data	字符串	返回数据实体

A. 1. 2 获取会话 Token 接口数据结构定义

表A. 2 获取会话Token接口数据结构说明

参数名称	数据类型	说明
app_id	字节数组	应用 ID
biz_content	字节数组	请求参数结构体
sk	字节数组	应用安全密钥，属于 biz_conten 内容

A. 1. 3 返回会话 Token 数据结构定义

表A. 3 返回会话Token数据结构说明

参数名称	数据类型	说明
msg	字节数组	返回信息，Success 表示成功，其他对应错误信息
code	字节数组	返回码 10000 为成功，其他对应错误码
request_id	字节数组	请求序列号
token	字节数组	会话 Token 信息

A. 1. 4 接口通用请求数据结构定义

表A. 4 接口通用请求数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号

app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
data	字节数组	请求数据，属于 biz_conten 内容
keyIndex	字节数组	应用密钥索引 ID，属于 biz_conten 内容

A. 1.5 密钥加密生成并导出数据结构定义

表A. 5 密钥加密生成并导出数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容

A. 1.6 密钥导入并签名数据结构定义

表A. 6 密钥导入并签名数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
keyCipher	字节数组	密钥密文 base64 编码，属于 biz_conten 内容
data	字节数组	请求数据，属于 biz_conten 内容

A. 1. 7 裸签名接口数据结构定义

表A. 7 裸签名接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
data	字节数组	请求数据（原文），属于 biz_conten 内容
subJect	字节数组	证书主题，属于 biz_conten 内容

A. 1. 8 裸验签接口数据结构定义

表A. 8 裸验签接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
plainText	字节数组	数据原文，属于 biz_conten 内容
data	字节数组	请求数据（签名值），属于 biz_conten 内容
cert	字节数组	证书，属于 biz_conten 内容

A. 1. 9 数字信封编码接口数据结构定义

表A. 9 数字信封编码接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字

timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (原文), 属于 biz_conten 内容
cert	字节数组	证书, 属于 biz_conten 内容

A.1.10 数字信封解码接口数据结构定义

表A. 10 数字信封解码接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (数字信封内容), 属于 biz_conten 内容
subJect	字节数组	证书主题, 属于 biz_conten 内容

A. 1. 11 签发时间戳接口数据结构定义

表A. 11 签发时间戳接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体

tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
subJect	字节数组	证书主题，属于 biz_conten 内容
data	字节数组	请求数据（原文），属于 biz_conten 内容

A. 1. 12 验证时间戳接口数据结构定义

表A. 12 验证时间戳接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
cert	字节数组	证书，属于 biz_conten 内容
data	字节数组	请求数据（时间戳数据），属于 biz_conten 内容

A. 1. 13 数据验签接口数据结构定义

表A. 13 数据验签接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
data	字节数组	请求数据（时间戳数据），属于 biz_conten 内容
keyIndex	字节数组	应用密钥索引 ID，属于 biz_conten 内容
signData	字节数组	签名数据，属于 biz_conten 内容

A. 1. 14 验证 MAC 接口数据结构定义

表A. 14 验证MAC接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (时间戳数据), 属于 biz_conten 内容
keyIndex	字节数组	应用密钥索引 ID, 属于 biz_conten 内容
macData	字节数组	MAC 数据, 属于 biz_conten 内容

A. 1. 15 生成随机数接口数据结构定义

表A. 15 生成随机数接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
randomLen	整型	随机数长度, 属于 biz_conten 内容

A. 1. 16 验证证书有效性接口数据结构定义

表A. 16 验证证书有效性接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳

version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
data	字节数组	请求数据（用户签名证书），属于 biz_conten 内容
condition	字节数组	校验条件，属于 biz_conten 内容。000 都不校验，111 都校验，100 校验证证书，010 校验有效期，001 校验 CRL，110 校验证证书与有效期，101 校验证证书与 CRL，011 校验有效期与 CRL，0102 允许过期证书通过，0103 允许未生效证书通过

A. 1. 17 attached 方式签名接口数据结构定义

表A. 17 attached方式签名接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
data	字节数组	请求数据（数字信封），属于 biz_conten 内容
subJect	字节数组	证书主题，属于 biz_conten 内容

A. 1. 18 attached 方式验签接口数据结构定义

表A. 18 attached方式验签接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token

app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (签名值), 属于 biz_conten 内容

A. 1. 19 detach 方式签名接口数据结构定义

表A. 19 detach方式签名接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (原文), 属于 biz_conten 内容
subJect	字节数组	证书主题, 属于 biz_conten 内容

A. 1. 20 detach 方式验签接口数据结构定义

表A. 20 detach方式验签接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID, 属于 biz_conten 内容
appCode	字节数组	应用编码, 属于 biz_conten 内容
data	字节数组	请求数据 (原文), 属于 biz_conten 内容
signData	字节数组	签名值, 属于 biz_conten 内容

A. 1. 21 HMAC-SM3 接口数据结构定义

表A. 21 HMAC-SM3接口数据结构说明

参数名称	数据类型	说明
method	字节数组	接口方法名字
timestamp	字节数组	请求时间戳
version	字节数组	版本号
app_auth_token	字节数组	会话 Token
app_id	字节数组	应用 ID
biz_conten	Json 结构体	请求参数结构体
tenantId	字节数组	租户 ID，属于 biz_conten 内容
appCode	字节数组	应用编码，属于 biz_conten 内容
kekIndex	整型	KEK 密钥索引默认为 1, 0 时为外带密钥，1 为内部密钥，属于 biz_conten 内容
keyData	字节数组	外带密钥，kekIndex 为 0 时不能为空，属于 biz_conten 内容
data	字节数组	请求数据（原文），属于 biz_conten 内容

A. 2 密码应用接口说明

A. 2. 1 获取会话 Token 接口

表A. 22 获取会话Token接口说明

接口功能描述	获取会话 Token 接口		
接口名称	getToken		
请求参数	参数名称	数据类型	说明
	获取会话 Token 接口数据结构 A1.2	数据结构	
请求示例	<pre>{ "app_id": "202212071050177439755403264", "biz_content": { "sk": "33BD4B55FCC6126B" } }</pre>		
返回值	返回会话 Token 数据结构 A1.3	属性数据实体为 Token，数据类型为字符串	
返回示例	<pre>{ "msg": "Success",</pre>		

	<pre>"code": "10000", "request_id": "202212071050177439755403264", "token": "d7a9b8aa7e34782c42298cba976f1120" }</pre>
--	--

A. 2. 2 数据加密接口

表A. 23 数据加密接口说明

接口功能描述	数据加密接口		
接口名称	bpsp.encrypt		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	SM4_CBC 方式
请求示例	<pre>{ "method": "bpsp.encrypt", "timestamp": "2022-12-01 14:32:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "12345678123456782", "keyIndex": "100001" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为加密后数据，数据类型为字符串	
返回示例	<pre>{ "bpsp_encrypt_response": { "request_id": "e48096eb0f744e2bacce9add22b858cd", "code": "10000", "msg": "Success", "data": "tQS4N7/C0inCnaV93p77ncxMHZ8ky5KcK+KZ0HfoCM4=" } }</pre>		

A. 2. 3 数据解密接口

表A. 24 数据解密接口说明

接口功能描述	数据解密接口		
接口名称	bbsp.decrypt		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	SM4_CBC 方式
请求示例	<pre>{ "method": "bbsp.decrypt", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "tQS4N7/C0inCnaV93p77ncxMHZ8ky5KcK+KZ0HfoCM4=", "keyIndex": "100001" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为解密后数据，数据类型为字符串	
返回示例	<pre>{ "bbsp_decrypt_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "12345678123456782" } }</pre>		

A. 2. 4 SM3 哈希数据不可逆接口

表A. 25 SM3哈希数据不可逆接口说明

接口功能描述	SM3 哈希数据不可逆接口		
接口名称	bbsp.sm3Hash		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	SM3 哈希
请求示例	<pre>{ "method": "bbsp.sm3Hash",</pre>		

	<pre>"timestamp": "2022-03-03 14:52:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "keyIndex": "100001", "data": "1234567812345678" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为哈市数据，数据类型为字符串
返回示例	<pre>{ "bbsp_sm3Hash_response": { "request_id": "11a5de2fddca4535ad1b63836ea75b69", "code": "10000", "msg": "Success", "data": "MTIzNDU2NzgzMjM0NTY3OA==" } }</pre>	

A. 2. 5 数据签名接口

表A. 26 数据签名接口说明

接口功能描述	数据签名接口		
接口名称	bbsp.sign		
请求参数	参数名称	数据类型	说明
	接口通用请求数据结构 A1.4	数据结构	使用 SM2 外带密钥
请求示例	<pre>{ "method": "bbsp.sign", "timestamp": "2022-03-03 15:09:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "1234567812345678213434", } }</pre>		

	<pre> "keyIndex": "100001" } } </pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为签名计算数据，数据类型为字符串
返回示例	<pre> { "bpsp_sign_response": { "request_id": "ee8da1cfd9e24e18bb88964f5661f879", "code": "10000", "msg": "Success", "data": "AAABj1hsehS/x1bJdr CMYyZoLUm3/2zHb4C5pLUr0Y41rwQAAIAR xn746pTct8quq0nEBoJIm/F1c5Ajs+7E+tEA7A24=" } } </pre>	

A.2.6 数据验签接口

表A. 27 数据验签接口说明

接口功能描述	数据验签接口		
接口名称	bbsp.verify		
请求参数	参数名称	数据类型	说明
	数据验签接口 数据结构 A1.13	数据结构	使用 SM2 外带密钥
请求示例	<pre> { "method": "bbsp.verify", "timestamp": "2022-03-03 15:15:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "2019032617262200001", "biz_content": { "tenantId": "100001", "appCode": "10000013", "data": "123456789", "keyIndex": "100001", "signData": "AAABj1hsehS/x1bJdrC MyYzoLum3/2zHb4C5pLUr0Y4lrwQAAIARx n746pTct8quq0nEBoJIm/F1c5Ajs+7E+tEA7A24=" } } </pre>		

	}	
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true，不通过为 false
返回示例	<pre>{ "bsp_verify_response": { "request_id": "fd3970eaae784a9897b04740d9c0711d", "code": "10000", "msg": "Success", "data": true } }</pre>	

A. 2. 7 生成 MAC 接口

表A. 28 生成MAC接口说明

接口功能描述	生成 MAC 接口		
接口名称	bpsp. genMac		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	使用 SM4_MAC
请求示例	<pre>{ "method": "bpsp.genMac", "timestamp": "2022-03-03 15:30:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "2019032617262200001", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "11111111111111333", "keyIndex": "100001" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为 MAC 计算数据，数据类型为字符串	
返回示例	<pre>{ "bpsp_genMac_response": { "request_id": "38666913a582499fb4d0dffddb9e24d5", "code": "10000", "msg": "Success", "data": "cQTPR13WPUITg8h15IMP5g==" } }</pre>		

	<pre>} }</pre>
--	--------------------

A. 2. 8 验证 MAC 接口

表A. 29 验证MAC接口说明

接口功能描述	验证 MAC 接口		
接口名称	bbsp.verifyMac		
请求参数	参数名称	数据类型	说明
	验证 MAC 接口 数据结构 A1.14	数据结构	使用 SM4_MAC
请求示例	<pre>{ "method": "bbsp.verifyMac", "timestamp": "2022-03-03 15:37:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "2019032617262200001", "biz_content": { "tenantId": "100001", "appCode": "10000013", "data": "111111111111111333", "keyIndex": "100001", "macData": "B5AA97AE845A672D86210E14F172454B", } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true，不通过为 false	
返回示例	<pre>{ "bbsp_verifyMac_response": { "request_id": "387a06852e304d6b940c5510fcaa1650", "code": "10000", "msg": "Success", "data": true } }</pre>		

A. 2. 9 非对称外带密钥加密接口

表A. 30 非对称外带密钥加密接口说明

接口功能描述	非对称外带密钥加密接口		
接口名称	bbsp.encryptECC		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	使用 SM2 外带密钥
请求示例	<pre>{ "method": "bbsp.encryptECC", "timestamp": "2022-12-01 14:32:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "12345678", "keyIndex": "100022" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为 SM2 外带密钥加密计算数据，数据类型为字符串	
返回示例	<pre>{ "bbsp_encryptECC_response": { "request_id": "e48096eb0f744e2bacce9add22b858cd", "code": "10000", "msg": "Success", "data": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADZBmvKO/bIjHVtn oZxQ0ZbGM5+vBA7jg2ZBI+CS27JCgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA5E3 nUoxXD70cc7S71ias83qAwNhEyR6CLi2wJysQMsyPX49XLg3bo5aKkpjLyhYVNT5zfWDAk37YV apmfk97NAGAAADnt23NzST1Vg==" } }</pre>		

A. 2. 10 非对称外带密钥解密接口

表A. 31 非对称外带密钥解密接口说明

接口功能描述	非对称外带密钥解密接口		
接口名称	bbsp.decryptECC		
请求参数	参数名称	数据类型	说明
	接口通用请求 数据结构 A1.4	数据结构	使用 SM2 外带密钥

请求示例	<pre>{ "method": "bpsp.decryptECC", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "AAADZBmvK0/bIjHVtnoZxQ0 ZbGM5+vBA7jg2ZBI+CS27JCgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA5E3nUoxX D70cc7S71ias83qAwNhEyR6CLi2wJysQMsyPX49XLg3bo5aKkpjLyhYVNT5zfWDAk37YVapmfk 97NAgAAADnt23NzST1Vg==", "keyIndex": "100022" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为 SM2 外带密钥解密计算数据，数据类型为字符串
返回示例	<pre>{ "bpsp_decryptECC_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "12345678" } }</pre>	

A. 2. 11 密钥加密生成并导出接口

表A. 32 密钥加密生成并导出接口说明

接口功能描述	非对称外带密钥解密接口		
接口名称	bpsp. genBase64Sm2Key		
请求参数	参数名称	数据类型	说明
	密钥加密生成并导出数据结构 A1.5	数据结构	产生一个新的 SM2 密钥，并使用指定的对称密钥加密导出
请求示例	<pre>{ "method": "bpsp.genBase64Sm2Key", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", }</pre>		

	<pre>"app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为 SM2 密钥数据，数据类型为字符串
返回示例	<pre>{ "bbsp_genBase64Sm2Key_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "AAADxjoGBU0cPjHd8v WLTbDr6InctzIQcSNELD7KmI9hv1wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC6B tYs20nS+7Skov3nWvvCarmxRIZgSVE699jQgsEUyBAAAAAQAAAAABAADoLN6fCdifCxXnmI8R 9nKd94mZEr0y3xDvre0XCz9YgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAA AAA8Y6BgVDnD4x3fL1i02w6+iJ3LcyEARDRc w+ypiPYb9cAAA8Y6BgVDnD4x3fL1i02w6+iJ3LcyEARDRc mq5sUSGYElR0vfY0ILBfGRNlXp1Zeumkuv8ZlPsNSm14L7gNbaIQHxnvqMY8b9xQAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHutvo62V2msb/DKHt1QMIWfDnCx2wLahZu71+OXGX9 LAAABw6Wk+DxeEsJ5cvWK7PSIbPZn6Phi4+ HPx142B7205TRAAAADTKJGgmjLp8pna3nquWlwF" } }</pre>	

A. 2. 12 密钥导入并签名接口

表A. 33 密钥导入并签名接口说明

接口功能描述	密钥导入并签名接口		
接口名称	bbsp. externalSign		
请求参数	参数名称	数据类型	说明
	密钥导入并签名数据 结构 A1.6	数据结构	
请求示例	<pre>{ "method": "bbsp.externalSign", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", }</pre>		

	<pre> "biz_content":{ "tenantId":"100051", "appCode":"1000064", "keyCipher":"AAADxjoGBUOcPjHd8v WL TbDr6InctzIQCsNELD7KmI9hv1wAAAC6B tYs20nS+7Skov3nWvvCarmxRIZgSVE699jQgsEUYBAAAAAQAAAAABAADoLN6fCdifCxXnnmi8R 9nKd94mZEr0y3xDvre0XCz9YgAAEAAAA AAA8Y6BgVDnD4x3fL1i02w6+iJ3LcyEArDRC w+ypiPYb9cAAA8Y6BgVDnD4x3fL1i02w6+iJ3LcyEArDRC mq5sUSGYE1ROvfY0ILBFRNLXp1Zeumkuv8ZlPsNSm14L7gNbaIQHxnvqMY8b9xQAAAAAAAAAA AAHutvo62V2msb/DKht1QMIWFDnC2wLahZu71+OXGX9 LAAABw6Wk+DxeEsJ5cvWK7PSIbPZn6Phi4+ HPx142B7205TRAAAADtkJGgmjLp8pna3nquWlWf", "data":"D//ge1x+j8JEHq/d5MUY/wHEL+4li7+rj1WVLBzuww=", } } </pre>
返回值	接口返回值数据结构 A1.1 属性数据实体为 SM2 密钥导入计算后数据，数据类型为字符串
返回示例	<pre> { "bbsp_externalSign_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "AAAKiivDSL2VMly0u lYuG8AdWuwyl170fdhV8x3CyRmkpgAAAPzf LT2bpFPzpu4ra0kjLvSOQpGA9ZRnFEft5N/YPHL8=" } } </pre>

A. 2. 13 裸签名接口

表A. 34 裸签名接口说明

接口功能描述	裸签名接口		
接口名称	bbsp.rawSignature		
请求参数	参数名称	数据类型	说明
	裸签名接口数据结构 A1.7	数据结构	
请求示例	<pre>{ "method": "bbsp.rawSignature", "timestamp": "2022-03-03 14:49:30",</pre>		

	<pre>"version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "Checktestdata1 数据", "subject": "CN=C004H101110102001TEST,OU=CCBTEST,O=CBIRC,C=CN" }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为裸签名计算后数据，数据类型为字符串
返回示例	<pre>{ "bsp_rawSignature_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "MEUCIQDKIJ009wC51mUz9JVJ194ZSbBiX2MS75lhGeuYbklg/AIgQcYUJDHOHlvPejZcS+2iArJApLb0AHO9yuCjWA01TdU=" } }</pre>	

A. 2. 14 裸验签接口

表A. 35 裸验签接口说明

接口功能描述	裸验证接口		
接口名称	bsp.rawVerify		
请求参数	参数名称	数据类型	说明
	裸验签接口数据结构 A1.8	数据结构	
请求示例	<pre>{ "method": "bsp.rawVerify", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "plainText": "Checktestdata1 数据",</pre>		

	<pre>"data": "MEUCIQcjwGWD9FY7Gp09gxkZ6rqwTFvKMRj92CR08b5cq7ENqQIGDQe7ehCf/ /Bd1mrBSLz48CeS580n9/NrxGAPtD5aIac=", "cert": "MIICKjCCAc2gAwIBAgIGAKZQ74i1MAwGCCqBHM9VAYN1BQAwNDELMakGA1UEB hMCQ04xDjAMBgNVBAoMBUNCsvJDMRUwEwYDVQDDAxDQk1SQ19TTTTjFQ0EwHhcNMjEwMzMDA 10DAxWhcNMzEwMzI5MDA10DAxWjBPMQswCQYDVQGEwJDTjEOMAwGA1UECgwFQ0JJUkMxEDA0B gNVBAwMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZMBMGBYqGSM4 9AgEGCCqBHM9VAYItA0IABEepKJwV8n9aR936zCTYBh4q0n1i1VVe/FcOIomFh75x10+e1L6/K Gs292meAOF06+VxxBNMCvkd1wDjYcVu0UWjga0wgaowHwYDVR0jBBgwFoAUHw2nL9rWhjWIJ/ FT6uCaKeqHDAwCQYDVR0TBAlwADBnBgNVHR8ERjBEMEKgQKA+pDwwOjENMAwGA1UEAwEY3JsM TEMMAoGA1UECwwDY3JsMQ4wDAYDVQQKDAVDQk1SQzELMAkGA1UEBhMCQ04wDgYDVR0PAQH/BAQ DAgbAMB0GA1UdDgQWBBTz+7x/QEDvU+DfrLLkMm145cDcxTAMBgGgqRzPVQGDdQUAA0kAMEYCI QCSJwsjDthHIYd1Kx1jYbkdTaaCSW95no/FUiBVPSE4TwIhA0yaSShSS3FURXFJ4rqEexcppN 63g1sa0BLpq92tvBH" }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true， 不通过为 false
返回示例	<pre>{ "bsp_rawVerify_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": true } }</pre>	

A. 2. 15 数字信封编码接口

表A. 36 数字信封编码接口说明

接口功能描述	数字信封编码接口		
接口名称	bsp. evpEncode		
请求参数	参数名称	数据类型	说明
	数字信封编码 接口数据结构 A1.9	数据结构	
请求示例	<pre>{ "method": "bsp. evpEncode", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", }</pre>		

	<pre>"biz_content":{ "tenantId":"100051", "appCode":"10000064", "data":"3213213123123", "cert":"MIICKjCCAc2gAwIBAgIGAKZQ74i1MAwGCCqBHM9VAYN1BQAwNDELMAkGA1UEBhM CQ04xDjAMBGNVBAoMBUNCsvJDMRUwEwYDVQQDDAxQk1SQ19TTTTJfQ0EwHhcNMjEwMzMDA1OD AxWhcNMzEwMzI5MDA1ODAxWjBPMQswCQYDVQGEwJDTjEOMAwGA1UECgwFQ0JJUkMxEDA0BgNVB AsMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZMBMGByqGSM49AgEG CCqBHM9VAYItA0IABEepKJwV8n9aR936zCTYBh4q0n1i1VVe/FcOIomFh75x10+e1L6/KGs292m eAOF06+VxxBNMCvkd1WDjYcVu0UWjga0wgaowHwYDVR0jBBgwFoAUWHw2nL9rWhjWIJ/FT6uCaK eqHDAwCQYDVR0TBAlwADBnBgNVHR8ERjBEMEKgQKA+pDwwOjENMMasGA1UEAwEY3JsMTEMMMAoGA 1UECwwDY3J3sMQ4wDAYDVQQKDAVDQk1SQzELMAkGA1UEBhMCQ04wDgYDVR0PAAQH/BAQDAgBAMB0G A1UdDgQWBBTz+7x/QEDvU+DfrLLkMm145cDcxTAMBgqgRzPVQGDdQUAA0kAMEYCIQCSJwsjDth HIYd1Kx1jYbkdTAAcSW95no/FUiBVPSE4TwIhA0yaSShSS3FURXFXJ4rqEexcppN63g1sa0BLpq 92tvBH" }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为数字信封编码结果，数据类型为字符串
返回示例	<pre>{ "bbsp_evpcEncode_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "MIIBKgYJKoZIhvcNAQcDoIIBGzCCARcCAQAxdIwgc8CAQAwPjA0MRUwE wYDVQQDDAxQk1SQ19TTTTJfQ0EwHhcNMjEwMzMDA1ODAxWjBPMQswCQYDVQGEwJDTjEOMAwGA1UECgwFQ0JJUkMxEDA0BgNVB AsMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZMBMGByqGSM49AgEG CCqBHM9VAYItAQUABHsweQIGELdV1yd2iY9SxoEhMtXeyRdu43f2a0rq0S86XfjwWioCI QCw1uZFtc+heZGXoRoOzf5f2oN/2agPgIH++v/DOD115wQgG6TqKx/PgVbY6muymuW6F7ReA3H c304F7FkjPMSdJ/gEEMRB4COyy+GNfjGJb7vWwgowPQYKKoEcz1UGAQQCATAbBgqcgRzPVQFoB BAuYzOfyZpmMg23MViJWiVdoBIEEH7sx270mAT1f9Qz2uwIysk=" } }</pre>	

A. 2. 16 数字信封解码接口

表A. 37 数字信封解码接口说明

接口功能描述	数字信封解码接口		
接口名称	bbsp.evpcDecode		
请求参数	参数名称	数据类型	说明
	数字信封解码接口数据结构	数据结构	

	A1.10	
请求示例	<pre>{ "method": "bpsp.evpDecode", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "MIIBKgYJKoZIhvcNAQcDoIIBGzCCARcCAQAxdIwgc8CAQAwPjA0MRUwEwYDV QQDDAxDAQk1SQ19TTTJfQ0ExCzAJBgNVBAYTAkNOMQ4wDAYDVQQKDAVDQk1SQwIGAKZQ74ilMA0 GCSqBHM9VAYItAQUABHsweQIhAMX0y8i90LSP1RiZAiM1jkF0xNqJbkuM9apZ2oudzNhRAiAat vM0qqfNGwc85F7LiwET7Vd1rqAydbvGf9z0nTYihQQgcoIWcky43wGHKs0QPLfGLDmJUpxwDdt ejghSJJuioHEEPyYmTGdQ+jdaHDUUt3keLkwPYKKoEcZ1UGAQQCATAbBgCqgRzPVQFoBBAuY zOfyZpmMg23MVi jWiVdoBIEEH7sx270mAT1f9Qz2uwIysk=", "subject": "CN=C004H101110102001TEST,OU=CCBTEST,O=CBIRC,C=CN" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为数字信封解码结果，数据类型为字符串
返回示例	<pre>{ "bpsp_evpDecode_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "3213213123123", } }</pre>	

A. 2. 17 签发时间戳接口

表A. 38 签发时间戳接口说明

接口功能描述	签发时间戳接口		
接口名称	bpsp.createdResponse		
请求参数	参数名称	数据类型	说明
	签发时间戳接口数据结构	数据结构	
	A1.11		
请求示例	<pre>{ "method": "bpsp.createdResponse", }</pre>		

	<pre>"timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appId": "10000064", "subject": "CN=C004H101110102001TEST,OU=CCBTEST,O=CBIRC,C=CN" }, "data": "D///gelx+j8JEHq/d5MUy/wHEL+4li7+rj1WVLBUww=" }</pre>
返回值	接口返回值数据结构 A1.1 属性数据实体为签发时间计算结果，数据类型为字符串
返回示例	<pre>{ "bpsp_createdResponse_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "MIID0gYKKoEcz1UGAQQAQCCA8IwggO+AgEBMQ8wDQYJKoEcZ1UBgxEBBQAwgeEGCyGGSIB3DQEJEAEEoIHRBIHOMIHLAGEBBgkRagSCTIE7S0gwMTANBgkqhRzPVQGDEIFAAGKJt06xrXOrwlSLvZFYZTQw8FBFMex9qtsqvF3n4ICEDE2NzuSMZI2NTAyMjg2ODUYDzIWmjMwMJA5MTYIMDUwWgiQWOvUFni1FKIuvHX9f2KkKBTPFEWTzeEMBWGA1UEAxMVQzAwNEgzMDExMTAxMDIwMDFURVNUMRAWDgyDVQQLEwdDQ0JRUVNUMQ4wDAYDVQQKEwVDQk1SQzELMAKGAA1UEBhMCQ006gggIUmiICKjcCAC2gAWIBAGIGAKZQ74ilMAwGCCQBHM9VAYN1BQAwNDLMAKAU1UEBhMCQ04xDjAMBGNVBAAoMBUNCSVJDMRUWEwyDVQQDDAxDQk1SQ19TTTJfQ0EWhhcnMjEwMzMxMjDA1ODAXWhcnMZISMDA1ODAXwjBPMSwCQYDVQQGEWJDdTJlEOMAAGA1UECGWFQ0JJUKMXEDAOBGNVBASMB0NDQLRFU1QxHjAcBgNVBAAMFUmmDRIMTAxmTEwMTAyMDAxEVEVTDBZMBMGByqGSM49AgEGCCqBHM9VAYITa0IABEpKJwV8n9AR936ZCTYbh4q0nl1lVVe/FcOIomFh75x10+e1L6/KGs292meAOF06+VxxBNMcVKd1WDjYCVu0UWjga0wgaowHWYDVR0JBbgwFoAUWHw2nL9rwhjWIJ/FT6uCaKeQHDAWCQYDVR0TBAlwADBNBgNVHR8ERjbEMEKGqKA+pDwoJENMASGA1UEAwEY3JSMTEmMAOGA1UECWwDY3JsMQ4wDAYDVQQKDAVDQk1SQzELMAKAU1UEBhMCQ04wDGYDVR0PAQH/B AQDAgbAMB0GA1UdDgQWBbtz+7x/QEDvU+dfrLLKm145CdCxTAMBgqqGRzPVQGDdQUAA0kAMEYCIQCsjwsjdThHIyd1KxljYbkDTAACSWS95no/FUIBVpSE4TwIha0yaSShSS3FURFXfJ4rqEexcpn63g1sa0BLpq92tvBHMYGRMIGOAgEBMECFzEVMBMGA1UEAxMMQ0JJUKNFU00yX0NBAGYAplDviKUwDQYJKoEcZ1UBgxEBBQAwDQYJKoEcZ1UBgi0BBQAESDBGAiEA14a08ah2LIVhjbsZ99WjI18hwMye1+7zl8Y/vAIQGKkCIQD+tIndb5K6QOOEXzaUITH4dmPCpkSmqpPDCB3Em5tjg=="</pre>

A.2.18 验证时间戳接口

表A. 39 验证时间戳接口说明

接口功能描述	验证时间戳接口
--------	---------

接口名称	bbsp.verifyTSValidity		
请求参数	参数名称	数据类型	说明
	验证时间戳接口 数据结构 A1.12	数据结构	
请求示例	<pre>{ "method": "bbsp.verifyTSValidity", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "cert": "MIICKjCCAc2gAwIBAgIGAKZQ74i1MAwGCCqBHM9VAYN1BQAwNDELMAKGA1UEBhMCQ04x DjAMBgNVBAoMBUNCsvJDMRUwEwYDVQQDDAxDAQk1SQ19TTTTJfQ0EwHhcNMjEwMzMDA1ODAx WhcNMzEwMzI5MDA1ODAxWjBPMQswCQYDVQQGEwJDTjEOMAwGA1UECgwFQ0JJUkMxEDA0BgNV BAsMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZMBMGByqGSM49A gEGCCqBHM9VAYItA0IABEepKJwV8n9aR936zCTYBh4q0n1i1VVe/FcOIomFh75x10+e1L6/KG s292meAOF06+VxxBNMCvkd1WDjYcVu0UWjga0wgaowHwYDVR0jBBgwFoAUWHw2nL9rWhjWIJ/ FT6uCaKqHDAwCQYDVR0TBAlwADBnBgNVHR8ERjBEMEKgQKA+pDwwOjENMAsgA1UEAwEY3Jjs MTEMMaOGA1UECwwDY3JSMQ4wDAYDVQQKDAVDQk1SQzELMAKGA1UEBhMCQ04wDgYDVR0PAQH/B AQDAgbAMB0GA1UdDgQWBBTz+7x/QEDvU+DfrLLkMm145cDcxTAMBgGgRzPVQGDdQUAA0kAME YCIQCSJwsjDthHIYd1Kx1jYbkdTAAcSW95no/FUiBVPSE4TwIhAOyaSShSS3FURFXJ4rqEex cppN63g1sa0BLpq92tvBH", "data": "MIID0gYKKoEcz1UGAQQCAqCCA8IwggO+AgEBMQ8wDQYJKoEcz1UBgxEBBQAwwEGCy qGSib3DQEJEAEEoIHRBIHOMIHLAgEBBgkrAgSCTIe7SQgWMTANBgkqRzPVQGDEQIFAAQgKjt O6xrx0rw1sSLvZFYJTCQw8FBFMex9qtsqGVf3n4ICEDE2NzU5MzI2NTAyMjg2ODUyDzIwMjMw MjA5MTY1MDUwWgIQW0vUFni1FKIiuvHx9f2KkKBTpFEwTzEeMBwGA1UEAxMVQzAwNEgxMDExM TAxMDIwMDFURVNUMRAwDgYDVQQLLEwdDQ0JURVNUMQ4wDAYDVQQKEwVDQk1SQzELMAKGA1UEBh MCQ06gggIuMIICKjCCAc2gAwIBAgIGAKZQ74i1MAwGCCqBHM9VAYN1BQAwNDELMAKGA1UEBhM CQ04xDjAMBgNVBAoMBUNCsvJDMRUwEwYDVQQDDAxDAQk1SQ19TTTTJfQ0EwHhcNMjEwMzMDA1 ODAxWhcNMzEwMzI5MDA1ODAxWjBPMQswCQYDVQQGEwJDTjEOMAwGA1UECgwFQ0JJUkMxEDA0B gNVBAsMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZMBMGByqGSM 49AgEGCCqBHM9VAYItA0IABEepKJwV8n9aR936zCTYBh4q0n1i1VVe/FcOIomFh75x10+e1L6 /KGs292meAOF06+VxxBNMCvkd1WDjYcVu0UWjga0wgaowHwYDVR0jBBgwFoAUWHw2nL9rWhjW IJ/FT6uCaKqHDAwCQYDVR0TBAlwADBnBgNVHR8ERjBEMEKgQKA+pDwwOjENMAsgA1UEAwEY 3JjsMTEMMaOGA1UECwwDY3JSMQ4wDAYDVQQKDAVDQk1SQzELMAKGA1UEBhMCQ04wDgYDVR0PAQ H/BAQDAgbAMB0GA1UdDgQWBBTz+7x/QEDvU+DfrLLkMm145cDcxTAMBgGgRzPVQGDdQUAA0k AMEYCIQCSJwsjDthHIYd1Kx1jYbkdTAAcSW95no/FUiBVPSE4TwIhAOyaSShSS3FURFXJ4rq EexcppN63g1sa0BLpq92tvBHMYGRMIGOAqEBMCewFzEVMBMGA1UEAxMMQ0JJUkNfU00yX0NB AgYAp1DviKUdQYJKoEcz1UBgxEBBQAwwDQYJKoEcz1UBgi0BBQAESDBGAiEA14a08ah2LIVHjb</pre>		

	<pre>SZ99WjI18hWMYe1+7z18Y/vAIQGKkCIQD+tIndb5K6Q00EXzaUITH4dmpKCpkSmqpPDCB3Em5 tjg==" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true，不通过为 false
返回示例	<pre>{ "bsp_verifyTSValidity_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": true } }</pre>	

A. 2. 19 生成随机数接口

表A. 40 生成随机数接口说明

接口功能描述	生成随机数接口		
接口名称	bbsp.generateRandom		
请求参数	参数名称	数据类型	说明
	生成随机数接口数据结构 A1.15	数据结构	
请求示例	{ "method": "bbsp.generateRandom", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "a2bad964db8b3bb9c58145e71fee573f", "app_id": "202212071050177439755403264", "biz_content": { "tenantId": "100051", "appCode": "10000064", "randomLen": 16 } }		
返回值	接口返回值数据结构 A1.1	属性数据实体为生成随机数计算结果，数据类型为字符串	
返回示例	{		

```

"bsp_generateRandom_response": {
  "request_id": "e440013245cd4feaa54e8752da972b70",
  "code": "10000",
  "msg": "Success",
  "data": "98a7f347c5a787218e14a33713d0dbbe"
}
}

```

A.2.20 验证证书有效性接口

表A. 41 验证证书有效性接口说明

接口功能描述	验证证书有效性接口		
接口名称	bbsp.verifyCert		
请求参数	参数名称	数据类型	说明
	验证证书有效性接口数据结构 A1.16	数据结构	
请求示例	<pre> { "method": "bbsp.verifyCert", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "ec7c765121890e651a4871a120b824ad", "app_id": "202302241078481875732791296", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "MIICKjCCAc2gAwIBAgIGAKZQ74iIMawGCCqBHM9VAYN1BQAwNDELMakGA1U EBhMCQ04xDjAMBgNVBAoMBUNCsVJDMRUwEwYDVQVQDDAxDQk1SQ19TTTJfQ0EwHhcNMjEwMz MxMDA1ODAxWhcNMzEwMzI5MDA1ODAxWjBPMQswCQYDVQQGEwJDTjEOMAwGA1UECgwFQ0JJU kMxEDA0BgNVBAsMB0NDQ1RFU1QxHjAcBgNVBAMMFUMwMDRIMTAxMTEwMTAyMDAxVEVTVDBZ MBMGBYqGSM49AgEGCCqBHM9VAYItA0IABEepKJwV8n9aR936zCTYBh4q0n1i1LVVe/FcOIom Fh75x10+e1L6/KGs292meAOF06+VxxBNMCvkd1WDjYcVu0UWjga0wgaowHwYDVR0jBBgwFo AUWHw2nL9rWhjWIJ/FT6uCaKqHDAwCQYDVROTBAlwADBnBgNVHR8ERjBEMEKgQKA+pDwwO jENMAsgA1UEAwEY3J3sMTEMAAoGA1UECwwDY3J3sMQ4wDAYDVQQKDAVDR0k1SQzELMAkGA1UE BhMCQ04wDgYDVROPAQH/BAQDAgBAMB0GA1UdDgQWBbBTz+7x/QEDvU+DfrLLkMml45cDcxTA MBggqgRzPVQGDdQUAA0kAMEYCIQCSJwsjDthHIYd1Kx1jYbkdTAAcSW95no/FUibVPSE4Tw IhA0YaSShSS3FURXFXJ4rqEexcppN63g1sa0BLpq92tvBH", "condition": "0103" } } </pre>		
返回值	接口返回值数据结构 A1.1		属性数据实体验证结果，通过为 true，不通 过为 false

返回示例	<pre>{ "bbsp_verifyCert_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": true } }</pre>
------	--

A. 2. 21 attached 方式签名接口

表A. 42 attached方式签名接口说明

接口功能描述	attached 方式签名接口		
接口名称	bbsp.attachedSignature		
请求参数	参数名称	数据类型	说明
	attached 方式签名 接口数据结构 A1.17	数据结构	attached 方式
请求示例	<pre>{ "method": "bbsp.attachedSignature", "timestamp": "2023-04-20 11:33:30", "version": "1.0", "app_auth_token": "f76146d6b7e8b64349d22c79b3d2e705", "app_id": "202304071093862977536262144", "biz_content": { "tenantId": "100003", "appCode": "10000001", "data": "MIIBKgYJKoZIhvcNAQcDoIIBGzCCARcCAQAxgdIwgc8CAQAwPjA0MRUwEwYDVQQDDAxDAQk1SQ19TTTJfQ0ExCzAJBgNVBAYTAkNOMQ4wDAYDVQQKDAVDQk1SQWIGAKZQ74ilMA0GCSqBHM9VAYItAQUABHsweQIhAMX0y8i90LSP1RiZAImljkF0xNqJbkuM9apZ2oudzNhRAiAatvM0qqfNGwc85F7LiWET7Vd1rqAydbvGf9z0nTYihQQgcoIWcky43wGHKs0QPLfGLDmJUpxwDtejghSJJuioHEEPyYmTGdQ+jdaHUUUt3keLkwPQYKKoEcz1UGAQQCATAbBgCqgRzPVQFoBBAuYzOfyZpmMg23MVijWiVdoBIEEH7sx270mAT1f9Qz2uwIysk=", "subject": "CN=192.168.8.55,OU=test,O=test,L=test,ST=SD,C=CN" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为 attached 方式签名结果，数据类型为字符串	
返回示例	<pre>{ "bbsp_attachedSignature_response": {</pre>		

	<pre> "request_id": "230c7552bbca4ab6953282fe4efb8860", "code": "10000", "msg": "Success", "data": "MIIFWwYJKoZIhvcNAQcCoIIFTDCCBUgCAQExDjAMBggqgRzPVQGDEQUAMIIBpwYJKoZIhvcNAQcBoIIBmASCAZRNSUICS2dZSktvWklodmNOQVFjRG9JSUJHekNDQVJjQ0FRQXhnZE13Z2M4Q0FRQXdQakEwTVJvd0V3WURWUWFEREF4RFFrbFNRMT1UVFRKZ1EwRXhDekFKQmdOVkJBWVRBa05PTVE0d0RBWURWUWFLREFWRFFrbFNRd01HQutaUTc0awxNQTbHQ1NwQkhNOVZBWU10QVFVQUJic3d1UU1oQU1YMHk4aTkWTFNQbFJpWkFpTWxqa0YweE5xSmJrdU05YXBaMm91ZHpoaFJBaUFhdHZNMHFxZk5Hd2M4NUY3TG13RVQ3VmQxcnFBwRidkdmOXowblRZaWhRUWdjB01XY2t5NDN3R0hLczBRUExmR0xEbUpVcHd4ZER0ZWpnaFNKSnpT2hFRUVQeVltVEEdkUStqZGFIRFVdDnRZUxrd1BRWUtLb0VjeJFVR0FRUUNBVEFiQmdjcWdSelBWUUZvQkJBdVl6T2Z5WnBtTWcyM01WaWpXaVZkb0JJRUVIN3N4MjcwbUFUMWY5UXoydXdJeXNrPaCCAmwggJnMIICC6ADAgECAhAgIwQYAQYXpvjyS9cSrsfMAwGCCqBHM9VAYN1BQAwdjELMAkGA1UEBhMCQ04xGTAXBgNVBAMEEABkAGUAYQBuAF8ARQBDAEMxDTALBgNVBAGEBFxxThwxZCZAJBgNVBACTAmPuMQswCQYDVQQKEWJkYTELMakGA1UECxcMCZGEXFjAUBGkqhkiG9w0BCQEWBzFAMS5jb20wHhcNMjMwNDE4MDk0NDQ0WhcNMjMwNDE4MDk0NDQ0WjBeMQswCQYDVQQGEWJDTjELMAkGA1UECAwCU0xDTALBgNVBACMBHRlc3QxDTALBgNVBAoMBHRlc3QxDTALBgNVBAsMBHRlc3QxFTATBgNVBAMMDDE5Mi4xNjguOC41NTBZMBMGBYqGSM49AgEGCCqBHM9VAYItA0IABNW9iE0nQXXOKLR82GgP5YQsCBBBoGrQbjPcmVnQs6Gu34jCjioa1UckLgsm9XTXyDPq6ALnce3bHABjDnLD3ajgZAwgY0wEQYDVR0jBAowCIAGd3F1cXd1MB0GA1UdDgQWBbTEzQ6S004V5nsz9Z6fDgqvLMPHXjAPBgNVHRMBAf8EBTADAQEAMA4GA1UdDwEB/wQEAwID6DAWBgNVHUBAf8EDDAKBggrBgEFBQcDATAgBgNVHR8BAf8EFjAUMBKqEKA0hg3d3cud2FuZy5jb20wDAYIKoEcz1UBG3UFAANIADBFAiAsPqEuWgH3uSQYwBITimIsJQY23vmBKsDpOdHpJJhxFgIhALVJdN+7a5s1ul0wpe7zcQ5Ff2+qWwETg+6/r5MwDY59MYIBFzCCARMCAQEWTjA6MQswCQYDVQQGEWJDTjELMAkGA1UEChMCZGEXCzAJBgNVBAsTAmRhMREwDwYDVQQDEWhkZWFuX0VDQWwIQICMEGAEGF6b48oEvXEq7HzAMBggqgRzPVQGDEQUAoFgwCwYDVR0PMQQDAgADMC8GCSqGSiB3DQEJBDiBCDdr7o9ghkeu7ZJfIsS1Z0KGFgu21UbHLYF58QnSx1/jAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMA0GCSqBHM9VAYItAQUBAEcwRQIgArpgS6w0xKqZF5xZ7igPUwqSUAC0D4pBix+ih0DMz20CIQCZNH6cJsiYjZYCUsbJ4idAVSgT7um84ID68gGCT+qNGA==" } } </pre>
--	---

A. 2. 22 attached 方式验签接口

表A. 43 attached方式验签接口说明

接口功能描述	attached 方式验签接口		
接口名称	bbsp.attachedVerify		
请求参数	参数名称	数据类型	说明
	attached 方式验 签接口数据结构 A1.18	数据结构	attached 方式

请求示例	<pre>{ "method": "bbsp.attachedVerify", "timestamp": "2023-04-20 11:41:30", "version": "1.0", "app_auth_token": "ab41fd62f8d5901a603d8828247eb643", "app_id": "202304071093862977536262144", "biz_content": { "tenantId": "100003", "appCode": "10000001", "data": "MIIFWwYJKoZIhvcNAQcCoIIFTDCCBUgCAQExDjAMBggqgRzPVQGDEQUAMII BpwYJKoZIhvcNAQcBoIIBmASCAZRNSU1CS2dZSkvWklodmNOQVFjRG9JSUJHekNDQVJjQ0 FRQXhnZE13Z2M4Q0FRQXdQakEwTVJvd0V3WURWUWFEREf4RFFrbFNRMt1UVFRKZ1EwRXhDe kFKQmdOVkJBWVRBa05PTVE0d0RBWURWUWFLREFWRFFrbFNrd0lHQutaUTc0awxNQTbHQ1Nx QkhNOVZBWU10QVVFVQUJjIc3dlUU1oQU1YMHk4aTkWTFNQbFJpWkFpTWxqa0YweE5xSmJrdU0 5YXBAMm91ZHpoaFJBaUFhdHZNMHFzZk5Hd2M4NUY3TG13RVQ3VmQxcnFBewRidkdmOXowb1 RZaWhRUWdjY0lXY2t5NDN3R0hLczBRUExmR0xEbUpVcHd4ZER0ZWpnaFNKSnpVt2hFRUVQe VltVEdkUStqZGFIrFVVdDNrZUxrd1BRWUtLb0VjejFVR0FRUUNBVEFiQmdjcWdSe1BWUUZv QkJBdV16T2Z5WnBtTWcyM01WaWpXaVZkb0JJRUVIN3N4MjcwbUUFUMWY5UXoydXdJeXNrPaC CAmswggJnMIICC6ADAgECAhAgIwQYQAQYXpvyjyS9cSrsfMAwGCCqBHM9VAYN1BQAwdjELMA kGA1UEBhMCQ04xGTAXBgNVBAMEEABkAGUAYQBuAF8ARQBDAAEMxDTALBgNVBAGEBFxxThwxC zAJBgNVBACTAmpuMQswCQYDVQQKEwJkYTELMakGA1UECzMCGZGExFjAUBGkqhkiG9w0BCQEW BzFAMs5jb20wHhcNMjMwNDk0NDQ0WWhcNMjMwNDk0NDQ0WjBeMQswCQYDVQQGEwJk DTjELMAkGA1UECwCU0QxDTALBgNVBACMBHRlc3QxDTALBgNVBAoMBHRlc3QxDTALBgNVBA sMBHRlc3QxFTATBgNVBAMMDDE5Mi4xNjguOC41NTBZMBMGByqGSM49AgEGCCqBHM9VAYItA 0IABNW9iE0nQXXOKLR82GgP5Y0QsCBB0GrQbjPcmVnQs6Gu34jCjioa1UckLgsm9XTXyDPq 6ALnce3bHABjDNDLD3ajgZAwgY0wEQYDVR0jBAowCIAGd3FlcXd1MB0GA1UdDgQWBbTEzQ6 S004V5nsz9Z6fDgqvLMPHXjAPBgNVHRMBAf8EBTADAQEAMA4GA1UdDwEB/wQEAwID6DAWBg NVHUBAaf8EDDAKBggrBgEFBQcDATAgBgNVHR8BAf8EFjAUMBKqEKA0hgX3d3cud2FuZy5jb 20wDAYIKoEcz1UBG3UFAANIADBFAiAsPqEuWgH3uSQYwBITimIsJQY23vmBKsDpOdHpJJhx FgIhALVJdN+7a5s1u10wpe7zcQ5Ff2+qWwETg+6/r5MwDY59MYIBFzCCARMCAQEwTjA6MQs wCQYDVQQGEwJDTjELMAkGA1UECzMCGZGExCzAJBgNVBAsTAMRhMREwDwYDVQQDEwhkZWFuX0 VDQwIQICMEGAEGF6b48oEvXEeq7HzAMBggqgRzPVQGDEQUAoFgwCwYDVR0PMQQAADM8GC SgGSIB3DQEJBDEiBCDdr7o9ghkeu7ZJfIsS1Z0KGFgu21UbHLyF58QnSx1/jAYBgqhkiG 9w0BCQMxCwYJKoZIhvcNAQcBMA0GCSqBHM9VAYItAQUABEcwRQIgArpgS6w0xKqZF5xZ7ig PUwqSUAC0D4pBix+ih0DMz20CIQCZNH6cJsYjZyCUsBj4idAVSgT7um84ID68gGCT+qNGA ==" , } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true，不通 过为 false
返回示例	<pre>{ "bbsp_attachedVerify_response": {</pre>	

```

    "request_id": "ddb2ffe274ee4df7bedb4f93579e2fbd",
    "code": "10000",
    "msg": "Success",
    "data": true ,
  }
}

```

A. 2. 23 detach 方式签名接口

表A. 44 detach方式签名接口说明

接口功能描述	detach 方式签名接口		
接口名称	bbsp.detachSignature		
请求参数	参数名称	数据类型	说明
	detach 方式签名 接口数据结构	数据结构	detach 方式
	A1.19		
请求示例	<pre>{ "method": "bbsp.attachedSignature", "timestamp": "2023-04-20 11:47:30", "version": "1.0", "app_auth_token": "6c34c6dd4d66cef2cb79d354e7ad54c2", "app_id": "202304071093862977536262144", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "123123123123123123 中", "subject": "CN=192.168.8.55,OU=test,O=test,L=test,ST=SD,C=CN" } }</pre>		
返回值	接口返回值数据结构 A1.1	属性数据实体为 detach 方式签名结果，数据类型为字符串	
返回示例	<pre>{ "bbsp_attachedSignature_response": { "request_id": "0c674a9b33b64ee0b8760e1e9cbb0044", "code": "10000", "msg": "Success", "data": "MIID1QYJKoZIhvcNAQcCoIIDxjCCA8ICAQExDjAMBggqRzPVQGDEQUAMCQGCSqGSIB3DQ EHAAaXBBUxMjMxMjMxMjMxMjMxMjMxMjPkuK2gggJrMIICZzCCAgugAwIBAgIQICMEGAEGF 6b48oEvXEq7HzAMBggqRzPVQGDdQUAMHYxCzAJBgNVBAYTAkNOMRkwFwYDVQQDHHAAZAB1 AGEAbgBfAEUAQWBDMDQ0WcwYDVQQIHGRCcU4cMQswCQYDVQQHEwJqbjlELMAKGA1UEChMCZGE xCzAJBgNVBAsTAhRlMRYwFAYJKoZIhvcNAQkBFgcxQDEuY29tMB4XDTEzMDQxODA5NDQ0NF</pre>		

	<pre>oXDTI0MDQx0DA5NDQ0NFowXjELMAkGA1UEBhMCQ04xCzAJBgNVBAGMA1NEMQ0wCwYDVQQHD AR0ZXN0MQ0wCwYDVQQKDAR0ZXN0MQ0wCwYDVQQLDAR0ZXN0MRUwEwYDVQQDDAwOTIuMTY4 LjguNTUwWTATBgqhkJOPQIBBggqRzPVQGCLQNCAATVvYhNJ0F1zii0fNhoD+WDkLAgQaB q0G4z3JlZ0L0hr+t+Iwo4qGpVHJC4LJvV018gz6ugC53Ht2xwAYwzXSw92o4GQMIGNMBEGA1 UdIwQKMAiABndxZXF3ZTAdBgNVHQ4EFgQUxM00ktDuFeZ7M/Wenw4KryzDx14wDwYDVR0TA QH/BAUwAwEBADA0BgNVHQ8BAf8EBAMCA+gwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAWewIAYD VR0fAQH/BBYwFDASoBCgDoYmD3d3LndhbmCuY29tMAwGCCqBHM9VAYN1BQADSAAwRQIgLD6 hLl0B97kkGMASE4piLCUGNt75gSrA6TnR6SSyCRYCIQC1SXTfu2ubNbdMKXu83EORX9vq1 sBE4Puv6+TMA20ftGCARYwggESAgEBME4wOjELMAkGA1UEBhMCQ04xCzAJBgNVBAoTAmRhM QswCQYDVQQLewJkYTERMA8GA1UEAxMIZGVhb19FQ0MCECAjBBgBBhem+PKBL1xKux8wDAYI KoEcz1UBGxEFAKBYMASGA1UdDzEEAwIAAzAvBgqhkiG9w0BCQQxIgQgTzL7+f15jNWHY1K P8iRILKOU32vWqbPv7ROL6wAagXAwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHAATANBgkqR zPVQGCLQEFAARGMEQCIEiHGFJVr9Mt5iSYh4aJ4YJ+yaepTVIdbL/sglT/y/pDAiAQwm+Do 9nRGSSrQ3R5hYLl0CckAQulWn4kA520Na6L4Q=="</pre> <pre>} }</pre>
--	--

A. 2. 24 detach 方式验签接口

表A. 45 detach方式验签接口说明

接口功能描述	detach 方式验签接口		
接口名称	bbsp.detachedVerify		
请求参数	参数名称	数据类型	说明
	detach 方式验签 接口数据结构 A1.20	数据结构	detach 方式
	{ "method": "bbsp.detachedVerify", "timestamp": "2022-03-03 14:49:30", "version": "1.0", "app_auth_token": "ec7c765121890e651a4871a120b824ad", "app_id": "202302241078481875732791296", "biz_content": { "tenantId": "100051", "appCode": "10000064", "data": "123123123123123123 中", "signData": "MIIDTQYJKoZIhvcNAQcCoIIDPjCCAzoCAQExDjAMBggqRzPVQGDEQU AMAsGCSqGSIb3DQEHAaCCAi4wggIqMIIBzaADAgECAGYAplDviKUwDAYIKoEcz1UBG3UFAD A0MQswCQYDVQQGEwJDTjEOMAwGA1UECgwFQ0JJUKMxFTATBgNVBAMMDENCsVJDX1NNM19DQ TAeFw0yMTAzMzEwMDU4MDFaFw0zMTAzMjkwMDU4MDFaME8xCzAJBgNVBAYTAkNOMQ4wDAYD VQQKDAVDQk1SQzEQMA4GA1UECwwHQ0NCVEVTVDEeMBwGA1UEAwVQzAwNEgxmDEXMTAxMDI wMDFURVNUMFkwEwYHKOZiZj0CAQYIKoEcz1UBgi0DQgAER6konBXyf1pH3frMJNGGHirSfW		

	<pre>KVVV78Vw4iiYWHvnhXT57Uvr8oazb3aZ4A4XTr5XHEE0wK+R3VY0Nhxw7RRa0BrTCBqjAfB gNVHSMEGDAWgBRYfDacv2taGNYgn8VPq4Jop6ocMDAJBgNVHRMEAjaAME0GA1UdHwRGMEQw QqBAoD6kPDA6MQ0wCwYDVQQDDARjcmwwMQwwCgYDVQQLDANjcmwwDjAMBgNVBAoMBUNCsVJ DMQswCQYDVQQGEwJDTJA0BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFPP7vH9AQ09T4N+ssu QyaXjlwNzFMAwGCCqBHM9VAYN1BQADSQAwwRgIhAJInCyM02Echh2UrGWNhuR1MBoJJb3mej 8VSIFU9ITHPAiEA7JpJKFJLcVRfcVcniuoR7Fymk3reDWxrQEumr3a28EcxgeUwgeICAQEw HzARMQ8wDQYDVQQDEwZEYXRlY2gCCjEyMzQ1Njc4OTAwDAYIKoEcz1UBgxEFAKBYMAsgA1U dDzEEAwIAAzAvBgqhkiG9w0BCQQxIgQg9CoTk9CFN/n2RMGOEFzDd1M2bm+68CehSTWYwV wMJakwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHAzAMBggqRzPVQGDEQUABEYwRAIghNimk 2b0ICVzcQg0Q2DbPoLuQVdfNwntNqYTQaQvJeYCIAZbNqcJlkDb89ZwY+nEo/vDzc0xLdCW 1FUZoafXI1J1" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体验证结果，通过为 true，不通 过为 false
返回示例	<pre>{ "bsp_detachedVerify_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": true } }</pre>	

A. 2. 25 HMAC-SM3 接口

表A. 46 HMAC-SM3接口说明

接口功能描述	HMAC-SM3 接口		
接口名称	bsp.hmacSM3		
请求参数	参数名称	数据类型	说明
	detach 方式验 HMAC-SM3 接口 数据结构 A1.21	数据结构	
请求示例	<pre>{ "method": "bsp.hmacSM3", "timestamp": "2023-04-01 15:22:30", "version": "1.0", "app_auth_token": "36a841e8e821d7bfbd53a8b266b407db", "app_id": "202303271089987281197989888", "biz_content": { "tenantId": "100077", "appCode": "10000061", } }</pre>		

	<pre>"kekIndex":1, "keyData":"1234567812345678", "data":"123456789 中文" } }</pre>	
返回值	接口返回值数据结构 A1.1	属性数据实体为 HMAC-SM 计算结果，数据类型为字符串
返回示例	<pre>{ "bpsp_hmacSM3_response": { "request_id": "e440013245cd4feaa54e8752da972b70", "code": "10000", "msg": "Success", "data": "236a9da99c9fb3feda410b776349715cd8499cce0b4c9ad8c5bcc ee0af3d872" } }</pre>	