ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0088—2020

云服务器密码机管理接口规范

Cloud cryptographic server management interface specification

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京江南天安科技有限公司、阿里云计算有限公司、北京三未信安科技发展有限公司、新飞凡（上海）云计算服务有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、兴唐通信科技有限公司、中国科学院数据与通信研究教育保护中心。

本文件主要起草人：李国、胡杰、马晓艳、张钊、苏建东、杨李贝、高志权、吕鹏啸、罗俊、吴庆国、徐明翼、张超、梁乐、王伟、曹硕。

云服务器密码机管理接口规范

1 范围

本文件规定了云平台管理系统与云服务器密码机之间的设备管理接口和协议。

本文件适用于云服务器密码机的研制和检测，也适用于云平台管理系统的开发和使用。

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 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

云服务器密码机 cloud-hosted hardware security module（CHSM）；cloud cryptographic server

在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的密码设备。

3.2

虚拟密码机 virtual security module（VSM）；virtual cryptographic server

云服务器密码机上，采用虚拟化技术创建出来的提供类同实体密码机服务的密码服务实例。

3.3

CHSM 数据影像 CHSM data image

简称 CHSM 影像。

包含 CHSM 内所有 VSM 中的与用户相关的配置、密钥及敏感信息等，并使用加密和签名机制保护影像的安全性。

用于 CHSM 的漂移过程。

3.4

VSM 数据影像 VSM data image

简称 VSM 影像。

包含 VSM 内与用户相关的配置、密钥及敏感信息等，并使用加密和签名机制保护影像的安全性。

用于 VSM 的漂移过程。

3.5

VSM 漂移 VSM drift

当一台 VSM 发生故障时，云平台管理系统自动将此 VSM 的数据影像导入至另外一台空闲正常的

VSM 上，并快速切换用户网络。在用户无感知的情况下，恢复 VSM 的可用性。

3.6

云平台公钥　authentication public key

用于鉴别云平台管理系统的身份，验证管理报文的合法性。

3.7

公钥指纹　public key fingerprint

对公钥进行杂凑运算(SM3 算法)的结果，作为公钥指纹。

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)

CHSM：云服务器密码机(Cloud-hosted Hardware Security Module)

HTTP：超文本传输协议(Hyper Text Transfer Protocol)

HTTPS：安全的 HTTP 协议(Hyper Text Transfer Protocol over Secure Socket Layer)

JSON：JS 对象标记(JavaScript Object Notation)

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

URI：统一资源标识符(Uniform Resource Identifier)

URL：统一资源定位符(Uniform Resource Location)

UUID：通用唯一识别码(Universally Unique Identifier)

VSM：虚拟密码机(Virtual Security Module)

VSMID：虚拟密码机的识别码，128 位设备 UUID(VSM Identification)

5　系统结构和接口位置

云服务器密码机管理接口 API，由云平台管理系统调用，用于管理配置 CHSM 和 CHSM 内的多个 VSM。管理接口 API 在云服务应用体系结构中的位置见图 1。

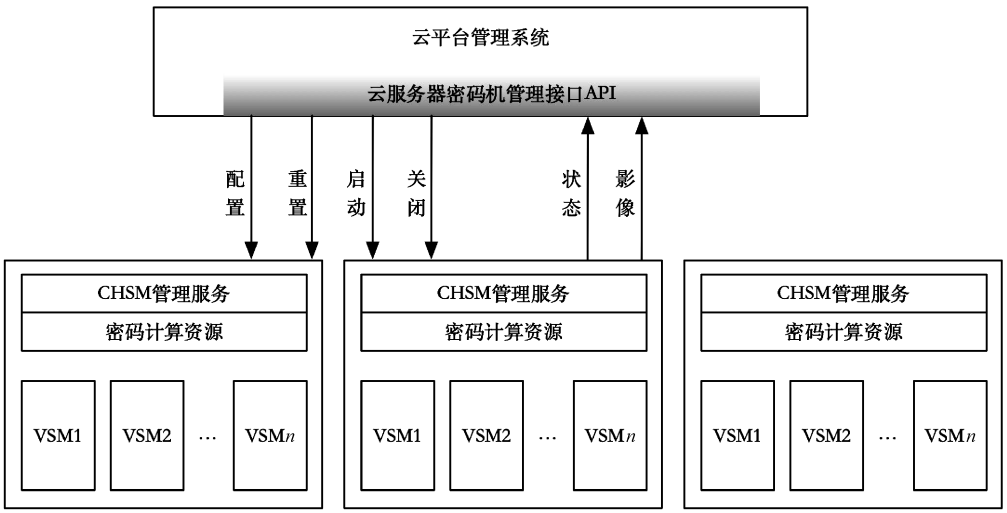

图 1　云服务器密码机管理接口在云服务应用体系结构中的位置

6 通讯协议和数据结构

6.1 通讯协议

云服务密码机管理接口应基于 HTTP 协议，以方便管理。如果采用传输层进行安全保护，宜采用 GM/T 0024 中定义的协议。

6.2 请求方法和 URL 规则

支持 HTTP GET、POST 方法。

——使用 GET 方法时，输入参数附加在请求的 URL 上，输出参数为 JSON 格式；示例如下：

http://{*chsmip:port*}/api/{*1.0*}/chsm/info?requestId={*requestId*}

——使用 POST 方法时，输入和输出参数均采用 JSON 格式；示例如下：

http://{*chsmip:port*}/api/{*1.0*}/chsm/network

{*斜体*}为可变内容域。

6.3 授权类别

当前支持的授权类别有：

——guest，无需签名即可使用；

——trusted，必须经过验证签名。

6.4 认证信息

云平台管理系统作为客户端在跟云服务密码机管理服务通讯时，应提供认证信息，用于鉴别其身份。可以通过验证签名的方式鉴别云平台管理系统身份。

请求 Header 中包含认证信息，如下：

——CHSM-AuthPK：签名使用的私钥所对应的公钥指纹；

——CHSM-SignatureAlg：“SM2WithSM3”或“RSAWithSHA256”；

——CHSM-Signature：签名值，针对整个 body 体的杂凑值计算的签名，BASE64 编码。

SM2WithSM3 算法，其签名算法符合 GB/T 32905 和 GB/T 32918 规范定义，签名值格式符合 GB/T 35276 规范定义。

RSAWithSHA256 算法，其签名值格式参考 PKCS#1 相关要求，应采用 2048 位及以上强度密钥。

6.5 状态信息

云服务密码机管理服务的 API 总会返回状态信息，状态信息包含字符形式的状态码和状态描述。状态码应按附录 A 的规定。

6.6 回调数据

因部分操作是异步操作，当异步操作完成后，云服务器密码机向回调地址发送回调数据。回调数据格式：

参数	参数类型	说明	样例值
requestId	string	请求 ID	“5c48319b”
status	int	状态码	200
timestamp	string	服务器响应时间	“2017-01-08T21:48:16.735+0800”
extMessage	string	错误信息	“”

回调数据样例：

```
{
    "requestId": "5c48319b",
    "status": 200,
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "extMessage": ""
}
```


6.7 运行状态

包括 CHSM 运行状态和 VSM 运行状态，运行状态定义如表 1 所示。

表 1 运行状态表

状态	适用 CHSM	适用 VSM	意义
normal	√	√	就绪状态
initial		√	初始状态
error	√	√	错误状态
shutdown		√	关机状态
restart		√	重启状态

7 管理接口描述

7.1 接口列表

本文件采用 http RESTful api 架构风格进行描述。

云服务器密码机应支持的管理接口见表 2。

表 2 管理接口 API 列表

	接口功能	接口 URL 对象	方法	授权	备注
CHSM 配置管理类					
1	获取 CHSM 详细信息	http://…/chsm	POST	trusted	
2	获取 CHSM 运行状态	http://…/chsm/status	GET	guest	
3	获取 CHSM 所有运行状态	http://…/chsm/allstatus	GET	guest	
4	配置 CHSM 网络信息	http://…/chsm/network	POST	trusted	
5	配置 NTP 服务器	http://…/chsm/ntp	POST	trusted	
6	配置影像上传地址	http://…/chsm/imageuploader	POST	trusted	
7	配置日志上传信息	http://…/chsm/log	POST	trusted	
8	导出 CHSM 影像	http://…/chsm/image	POST	trusted	可选
9	导入 CHSM 影像	http://…/chsm/image	POST	trusted	可选
10	升级 CHSM	http://…/chsm	POST	trusted	可选
11	重启 CHSM	http://…/chsm	POST	trusted	
12	备份 CHSM	http://…/chsm	POST	trusted	可选
13	恢复 CHSM	http://…/chsm	POST	trusted	可选

表 2　管理接口 API 列表（续）

	接口功能	接口 URL 对象	方法	授权	备注
VSM 配置管理类					
1	获取 VSM 详细信息	http://…/vsm	POST	trusted	
2	获取 VSM 运行状态	http://…/vsm/status	GET	guest	
3	配置 VSM 网络信息	http://…/vsm/network	POST	trusted	
4	配置 VSM Token	http://…/vsm/token	POST	trusted	
5	导出 VSM 影像	http://…/vsm/image	POST	trusted	
6	导入 VSM 影像	http://…/vsm/image	POST	trusted	
7	启动 VSM	http://…/vsm	POST	trusted	
8	停止 VSM	http://…/vsm	POST	trusted	
9	重置 VSM	http://…/vsm	POST	trusted	
10	重启 VSM	http://…/vsm	POST	trusted	
11	创建 VSM	http://…/vsm	POST	trusted	可选
12	删除 VSM	http://…/vsm	POST	trusted	可选
13	升级 VSM	http://…/vsm	POST	trusted	可选
接口授权配置类					
1	配置 CHSM 的云平台公钥	http://…/chsm/authpk	POST	trusted /guest	初次配置时，guest 权限即可
2	获取 CHSM 的云平台公钥信息	http://…/chsm/authpk	GET	guest	

7.2　CHSM 配置管理类接口

7.2.1　获取 CHSM 详细信息

URL：　http://{*chsmip:port*}/*api*/{*1.0*}/chsm

调用方法：　POST

功能描述：　获取 CHSM 内详细信息，包括配置和运行信息。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："getinfo"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间（毫秒）
	result	object	返回数据对象
result 对象：	id	string	chsm uuid
	version	string	chsm 版本
	ip	string	chsm ip 地址
	ntpAddr	string	ntp 地址

ntpSyncPeriod	int	ntp 同步周期(分钟)
imageUploaderUrl	string	数据影像上传地址
sysLogUrl	string	日志收集地址
vsmIds	array	chsm 所有 vsm 的识别码
netAddrs	array	CHSM 的各网口配置信息,内含每个网口的属性 object,每 object 包含下述 4 个键值
name	string	网口标识,属于 netAddrs 中 object 的子域
ip	string	IP 地址,属于 netAddrs 中 object 的子域
mask	string	子网掩码,属于 netAddrs 中 object 的子域
gateway	string	网关地址,属于 netAddrs 中 object 的子域
dnsList	array	chsm 实例 DNS 列表
extensions	object	扩展信息

返回内容示例:

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
    "result": {
        "id": "1",
        "version": "1.0",
        "ip": "192.168.1.1",
        "ntpAddr": "192.168.1.2",
        "ntpSyncPeriod": 1,
        "imageUploaderUrl": "http://192.0.0.1/image/upload",
        "vsmIds": [
            "00000000-0000-0000-0000-0CC47AB492BE",
            "F8BF1A34-E3A2-415D-AC91-A54363BBC859"
        ],
        "netAddrs": [
            {"name": "eth0", "ip": "192.168.0.1",
             "mask": "255.255.255.0", "gateway": "192.168.0.254"},
            {"name": "eth1", "ip": "192.168.2.1",
             "mask": "255.255.255.0", "gateway": ""}
        ],
        "dnsList": [
            "100.1.0.0",
            "10.1.0.0"
        ]
    }
}
```

7.2.2 获取 CHSM 运行状态

URL: http://{*chsmip:port*}/api/{*1.0*}/chsm/status

调用方法：　GET

功能描述：　获取 CHSM 的运行状态是否正常。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)
	result	object	返回数据对象
result 对象：	status	string	hsm 状态(参见表 1)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
    "result": {
        "status": "normal"
    }
}
```

7.2.3 获取 CHSM 所有状态信息

URL：　http://{*chsmip:port*}/api/{*1.0*}/chsm/allstatus

调用方法：　GET

功能描述：　获取 CHSM 和内部所有 VSM 的运行状态是否正常。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)
	result	object	返回数据对象
result 对象：	chsmStatus	string	hsm 状态(ok 或者 fail)
	vsmStatusMap	object	所有 vsm 状态(ok 或者 fail)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
```

```
    "result": {
        "chsmStatus": "ok",
        "vsmStatusMap": {
            "F8BF1A34-E3A2-415D-AC91-A54363BBC859": "ok",
            "546E1503-0902-426B-86A8-641D52F8047B": "ok"
        }
    }
}
```


7.2.4 配置 CHSM 网络信息

URL：　http://{*chsmip*:*port*}/api/{*1.0*}/chsm/network

调用方法：　POST

功能描述：　修改 CHSM 的网络属性配置，支持配置一个或多个网口的网络地址。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	netAddrs	array	CHSM 的各网口配置信息，内含每个网口的属性 object，每 object 包含下述 4 个键值
	name	string	网口标识，属于 netAddrs 中 object 的子域
	ip	string	IP 地址，属于 netAddrs 中 object 的子域
	mask	string	子网掩码，属于 netAddrs 中 object 的子域
	gateway	string	网关地址，属于 netAddrs 中 object 的子域
	dnsList	array	dns 列表
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：


```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```


7.2.5 配置 CHSM 的 NTP 服务

URL：　http://{*chsmip*:*port*}/api/{*1.0*}/chsm/ntp

调用方法：　POST

功能描述：　向 CHSM 设置 NTP 服务器地址，用于同步 CHSM 内系统时间。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	addr	string	NTP 服务器地址，如"10.1.1.1"
	syncPeriod	int	同步周期，分钟

输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.6 配置 CHSM 的影像上传地址

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm/imageuploader

调用方法： POST

功能描述： 配置 CHSM 内部备份或影像(包括 VSM 影像)的上传地址。

当调用导出 CHSM 影像、备份 CHSM 或导出 VSM 影像接口时，CHSM 将向此处配置的 URL 上传影像或备份。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	url	string	影像上传地址，如"http://192.168.0.1/image/upload"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.7 配置 CHSM 的日志上传地址

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm/loguploader

调用方法： POST

功能描述： 配置 CHSM 内部日志(包括 VSM)的上传地址。CHSM 日志包含运行日志和监控日志。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	logServerType	string	日志服务器类型，取值："syslog"或"logserver"
	logServerAddress	string	对 syslog 类型，该域为 syslog 服务器地址，如"192.168.1.2"； 对 logserver 类型，该域可指定一个 URL，如"http://192.168.1.2/log"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.8 导出 CHSM 影像

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm/image

调用方法： POST

功能描述： 导出 CHSM 内所有 VSM 的数据影像。采用加密和签名机制对数据影像进行保护，其保护算法符合 GB/T 32918 和 GB/T 32907 规范定义。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："export"
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.9 导入 CHSM 影像

URL：http://{*chsmip*:*port*}/api/{*1.0*}/chsm/image

调用方法：POST

功能描述：导入 CHSM 所有 VSM 的数据影像。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："import"
	imageUrl	string	影像地址，如"http://192.168.0.1/image.zip"
	alg	string	签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	数字签名值，BASE64 编码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.10 升级 CHSM

URL：http://{*chsmip*:*port*}/api/{*1.0*}/chsm

调用方法：POST

功能描述：升级 CHSM 的服务。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："upgrade"
	packVersion	string	升级包版本，如"v1.0"
	packUrl	string	升级包地址，如"http://192.168.0.1/update.zip"
	alg	string	签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	数字签名值，BASE64 编码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"

输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.11 重启 CHSM

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm

调用方法： POST

功能描述： 重启 CHSM 系统。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型,取值:"restart"
	callbackUrl	string	回调地址,如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.12 备份 CHSM

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm

调用方法： POST

功能描述： 备份导出 CHSM 内的各类敏感数据。

采用加密和签名机制对数据备份进行保护,其保护算法符合 GB/T 32918 和 GB/T 32907 规范定义。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："backup"
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.2.13 恢复 CHSM

URL： http://{*chsmip:port*}/api/{*1.0*}/chsm

调用方法： POST

功能描述： 恢复导入 CHSM 的备份数据。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："restore"
	backupUrl	string	备份数据包地址，如"http://192.168.0.1/backup.bak"
	alg	string	签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	数字签名值，BASE64 编码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
```

}

7.3 VSM 配置管理类接口

7.3.1 获取 VSM 详细信息

URL：　http://{*chsmip*:*port*}/api/{*1.0*}/vsm
调用方法：　POST
功能描述：　获取指定 VSM 的详细信息。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："getinfo"
	vsmId	string	VSM 识别码
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)
	result	object	返回数据对象
result 对象：	id	string	vsm 识别码
	version	string	vsm 版本
	token	string	vsm 的 token
	ip	string	vsm ip 地址
	mask	string	vsm 实例掩码地址
	gateway	string	vsm 实例网关
	digest	string	影像摘要，算法不做统一要求
	communication	int	通信方式，取值范围： 1——密文；2——明文；
	extensions	object	扩展信息，可选域，厂商自定义

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
    "result": {
        "id": "00000000-0000-0000-0000-0CC47AB492BE",
        "version": "1.0",
        "ip": "192.168.1.1",
        "token": "0",
        "mask": "255.255.255.0",
        "gateway": "192.168.1.100",
        "digest":"digest",
        "communication": 1
    }
}
```

7.3.2 获取 VSM 运行状态

URL：http://{*chsmip:port*}/api/{*1.0*}/vsm/status

调用方法：GET

功能描述：获取指定 VSM 的运行状态。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	vsmId	string	VSM 识别码
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)
	result	object	返回数据对象
result 对象：	status	string	vsm 状态(参见表 1)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
    "result": {
        "status": "normal"
    }
}
```

7.3.3 配置 VSM 网络信息

URL：http://{*chsmip:port*}/api/{*1.0*}/vsm/network

调用方法：POST

功能描述：修改 VSM 的网络属性配置。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	vsmId	string	VSM 识别码
	ip	string	ip 地址
	mask	string	掩码
	gateway	string	网关
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
```

```
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```


7.3.4 配置 VSM Token 信息

URL：http://{*chsmip:port*}/api/{*1.0*}/vsm/token

调用方法：POST

功能描述：配置 VSM 的 Token 信息。

Token 指使用该 VSM 的用户标识名，用于表明该 VSM 已租用给某个用户使用。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	vsmId	string	VSM 识别码
	token	string	token，用户标识
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：


```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```


7.3.5 导出 VSM 影像

URL：http://{*chsmip:port*}/api/{*1.0*}/vsm/image

调用方法：POST

功能描述：获取指定 VSM 的数据影像。

采用加密和签名机制对数据影像进行保护，其保护算法符合 GB/T 32918 和 GB/T 32907 规范定义。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："export"
	vsmId	string	VSM 识别码
	callbackUrl	string	回调地址，如 "http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```


7.3.6 导入 VSM 影像

URL：　http://{*chsmip:port*}/api/{*1.0*}/vsm/image

调用方法：　POST

功能描述：　向指定的 VSM 导入数据影像。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："import"
	vsmId	string	VSM 识别码
	imageUrl	string	影像地址，如"http://192.168.0.1/image.zip"
	alg	string	签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	数字签名值，BASE64 编码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：


```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```


7.3.7 启动 VSM

URL：　http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法：　POST

功能描述：　启动一个 VSM。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："start"
	vsmId	string	VSM 识别码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"

输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.8 停止 VSM

URL： http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法： POST

功能描述： 关闭一个 VSM。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型,取值:"stop"
	vsmId	string	VSM 识别码
	callbackUrl	string	回调地址,如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.9 重启 VSM

URL： http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法： POST

功能描述： 重启一个 VSM。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型,取值:"restart"
	vsmId	string	VSM 识别码

	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.10 重置 VSM

URL： http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法： POST

功能描述： 重置 VSM。清除 VSM 的用户数据，使 VSM 恢复为出厂空闲状态。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："reset"
	vsmId	string	VSM 识别码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.11 升级 VSM

URL： http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法： POST

功能描述： 升级一个 VSM。

	参数	类型	说明
输入参数：	requestId	string	请求流水号

	oprType	string	操作类型，取值："upgrade"
	vsmId	string	VSM 识别码
	packVersion	string	升级包版本，如"v1.0"
	packUrl	string	升级包地址，如"http://192.168.0.1/update.zip"
	alg	string	签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	数字签名值，BASE64 编码
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.12 创建 VSM

URL： http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法： POST

功能描述： 创建一个 VSM。

支持从内部默认 VSM 镜像创建实例和从外部下载指定 VSM 镜像创建实例。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型，取值："create"
	imageUrl	string	可选域，若该域存在则后述两个域应存在；镜像包地址，如"http://192.168.0.1/img/vsmxx.img"
	alg	string	可选域，若 imageUrl 存在则应存在；签名算法，取值范围："SM2WithSM3"或"RSAWithSHA256"
	sign	string	可选域，若 imageUrl 存在则应存在；数字签名值，BASE64 编码
	flavor	int	VSM 占用资源规格，如 1、2、3
	callbackUrl	string	回调地址，如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID

	costMillis	long	服务器处理时间(毫秒)
	vsmId	string	新创建的 VSM 实例 ID

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "vsmId": "00000000-0000-0000-0000-0CC47AB492BE",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.3.13 删除 VSM

URL：http://{*chsmip:port*}/api/{*1.0*}/vsm

调用方法：POST

功能描述：删除一个 VSM。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	oprType	string	操作类型,取值:"destroy"
	vsmId	string	待删除的 VSM 实例 ID
	callbackUrl	string	回调地址,如"http://192.168.0.1/callback"
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

7.4 授权配置类接口

7.4.1 获取 CHSM 云平台公钥的指纹

URL：http://{*chsmip:port*}/api/{*1.0*}/chsm/authpk

调用方法：GET

功能描述：获取 CHSM 内云平台公钥的指纹,输出的指纹为 BASE64 编码格式。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
输出参数：	status	int	状态码
	message	string	状态描述

	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)
	result	object	返回数据对象
result 对象：	algorithm	string	指纹的杂凑算法标识，取值："sm3"
	fingerprints	array	指纹列表，经过杂凑之后的指纹，使用 BASE64 编码格式

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500,
    "result": {
        "algorithm": "sm3",
        "fingerprints": [
            "fingerprints1",
            "fingerprints2"
        ]
    }
}
```

7.4.2 配置 CHSM 的云平台公钥

URL： http://{*chsmip*:*port*}/api/{*1.0*}/chsm/authpk

调用方法： POST

功能描述： 设置允许访问 CHSM 管理接口的多个云平台公钥。

	参数	类型	说明
输入参数：	requestId	string	请求流水号
	algorithm	string	算法标识，取值："sm2"
	pks	array	公钥列表，取值样例：["pk1","pk2"]
输出参数：	status	int	状态码
	message	string	状态描述
	timestamp	string	服务器响应时间
	requestId	string	请求 ID
	costMillis	long	服务器处理时间(毫秒)

返回内容示例：

```
{
    "status": 200,
    "message": "success",
    "timestamp": "2017-01-08T21:48:16.735+0800",
    "requestId": "5c48319b",
    "costMillis": 500
}
```

附 录 A
（规范性）
接口返回状态码定义和说明

接口返回状态码的定义和说明见表 A.1。

表 A.1 状态码的定义和说明

状态码	说明
200	操作成功
400	请求数据错误
401	授权错误
403	操作被禁止
404	URI 不存在
405	操作方法不准许
409	冲突错误
500	内部错误

参 考 文 献

[1] GM/T 0024—2014 SSL VPN 技术规范

[2] PKCS#1 v2.1:RSA Cryptography Standard

[3] RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2). IETF. May 2015 [14 May 2015]

[4] RFC 4627 The application/json Media Type for JavaScript Object Notation (JSON)

中华人民共和国密码
行业标准
云服务器密码机管理接口规范
GM/T 0088—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 54 千字
2021年6月第一版 2021年6月第一次印刷
*
书号:155066·2-35899 定价 32.00 元

GM/T 0088-2020

码上扫一扫 正版服务到