ICS 35.040
CCS L80

DB15

内 蒙 古 自 治 区 地 方 标 准

DB15/T 2198—2021

大数据应用 云密码应用规范

Big data application ——Cloud cryptographic application specification

2021-05-25 发布 2021-06-25 实施

内蒙古自治区市场监督管理局 发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　云密码应用总体架构 2
4.1　概述 2
4.2　云密码建设要求 3
5　云密码资源池 4
5.1　概述 4
5.2　框架图 4
5.3　云密码管理平台 4
5.4　云密码服务 4
5.5　云密码资源 5
5.6　基础设施 5
6　云密码服务接口规范 5
6.1　概述 5
6.2　接口说明 6
附录 A（资料性）　云密码应用合规性参考表 7
附录 B（规范性）　接口规范 9
参考文献 18

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。

本文件由内蒙古自治区大数据中心提出并归口。

本文件起草单位：内蒙古自治区大数据中心、杭州安恒信息技术股份有限公司、内蒙古工业大学网络空间安全研究所、杭州弗兰科信息安全科技有限公司。

本文件主要起草人：孙卫、包瑞林、杨扬、吴卓群、王钢、林明峰、戚志军、袁国平。

大数据应用　云密码应用规范

1　范围

本文件规定了云密码应用总体技术架构，规定了云密码资源池和云密码服务接口的技术要求。

本文件适用于指导云密码建设和云平台中的用户终端、网络与接入、云平台服务、云安全管理对云密码的应用。

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 7408　数据元和交换格式 信息交换 日期和时间表示法

GB/T 31167　信息安全技术 云计算服务安全指南

GM/T 0029　签名验签服务器技术规范

GM/T 0054　信息系统密码应用基本要求

GM/T 0062　密码产品随机数检测要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

云密码 cloud cryptographic

一种将云计算技术与身份认证、授权访问、传输加密、存储加密等密码技术深度融合，实现密码服务云化的密码功能呈现模式。

3.2

云密码服务 cloud cryptographic service

按照云计算技术架构的要求整合密码产品、密码使用策略、密码服务接口和服务流程，将密码系统设计、部署、运维、管理、计费等组合成一种服务，来解决用户的密码应用需求。

3.3

云密码应用 cloud cryptographic application

通过使用云密码服务，实现密码功能的应用。

3.4

虚拟化 virtualization

一种资源管理技术，将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等），予以抽象、转换后呈现出来并可供分割、组合为一个或多个电脑配置环境。

3.5

数据退役 data retire

数据生命周期中的一个阶段，将被归档、转移、丢弃、销毁以及对存储介质的销毁处理后不再被使用。

4 云密码应用总体架构

4.1 概述

云密码服务依托核心密码防护技术，借助云计算资源，对云计算平台提供密码支撑与应用设计能力。从用户终端、网络与接入、云平台、云安全管理等角度，为云平台及云租户应用系统的安全可靠运行提供全面高效的密码应用服务，保证云平台及上云系统符合国家法律法规、政策文件、标准规范的要求，满足合规性、完整性和安全性要求。

云密码应用框架如图1所示，框架图分为上下两部分：

——上部分为云密码应用层，分为终端密码应用、网络与接入安全密码应用、云平台密码应用。其中终端密码应用包含传统 PC 端、物联网终端、移动终端、安全浏览器、智能密码钥匙等中涉及密码相关的应用；网络与接入安全密码应用包含了可信接入、访问控制、身份认证、IPSecVPN 网关、SSLVPN 网关等网络通信与接入的密码相关应用；云平台密码应用包括云管理平台与云应用平台，云应用平台涉及服务层与平台层，服务层中包含了云上托管业务密码应用与云上数据，平台层中包含了资源、系统、存储等安全。以上终端密码应用、网络与接入安全密码应用、云平台密码应用在使用密码服务时，均可通过调用密码资源池对外接口，为身份认证、访问控制、授权管理、数据安全等信息安全功能提供基础和统一的密码支撑；

——下部分为密码资源池，基于云密码资源、密码基础设施，对外开放密码服务即接口，为云平台及云租户提供统一的密码服务。

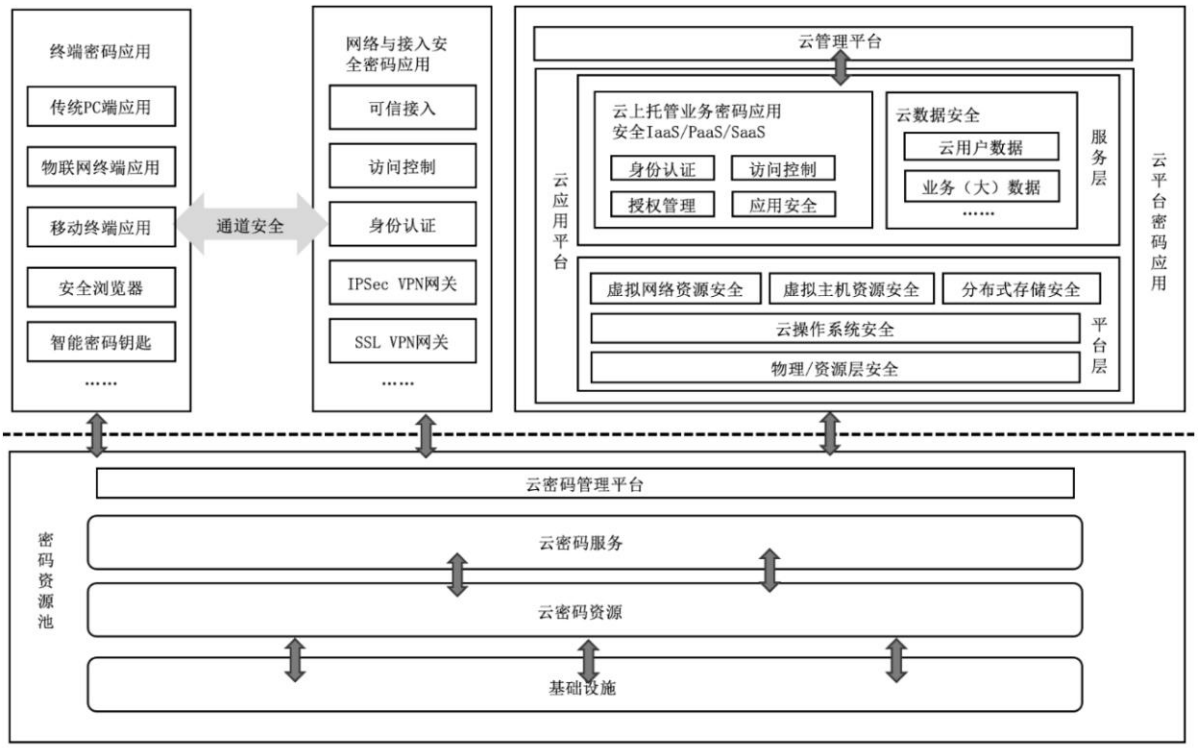

图1　云密码应用总体架构

4.2　云密码建设要求

4.2.1　环境安全

为确保云密码应用基础环境的安全，云密码服务在云端的建设应符合GB/T 31167的要求。

4.2.2　密码算法

云密码应用中凡涉及对称算法、非对称算法、杂凑算法时，需采用满足国家密码主管部门批准的算法。

4.2.3　秘钥隔离

根据不同的安全需求,云密码资源池需提供多种不同安全等级的密钥隔离机制。针对高安全等级场景，能够支持基于硬件虚拟化技术实现的密钥隔离，以保证各个虚拟业务单元独享安全密码服务。

4.2.4　访问控制

为保证云密码资源池提供的密码服务中接入应用的安全性,需结合多种认证模式,基于角色、服务、身份对云密码服务进行访问授权控制。对于不同的业务服务模式，采取最合适的访问控制机制，同时，借助访问控制机制，为云中密码服务的审计提供有效的技术支撑。

4.2.5　云密码测评

云密码应用在规划阶段、建设阶段和运行阶段,需根据《商用密码应用安全性评估管理办法(试行)》等相关要求，按照 GM/T 0054执行，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面采用密码技术措施，建立安全的密钥管理方案，采取有效的安全管理措施。云密码应用通过云密码测评是项目验收的必要条件，云密码测评合规性参考表见附录A。

5 云密码资源池

5.1 概述

构建云密码资源池，对外提供统一的密码服务是当前实现密码云化的一种有效方式。云密码资源池将虚拟化技术和云管理技术应用在密码设备集群，把密码设备集群组织成“密码设备云”，形成集成化的云密码服务资源池。

云密码资源池为云中数据提供全生命周期的安全服务，需通过硬件虚拟化技术，为多个应用系统提供高速、可靠、可扩展的密钥管理服务、随机数服务、签名与验签服务、身份认证服务和加解密服务，有效地提高密码资源的利用率。同时，云密码服务自身应能确保可伸缩、动态、高效的运行，具备抗攻击能力。

5.2 框架图

云密码资源池架构如图2所示，从上至下分为云密码管理平台、云密码服务、云计算密码资源和基础设施。其中服务层包含云密码资源池的基础设施和虚拟化出的各类密码服务，包括加解密服务、身份验证服务、签名验签服务、时间戳服务等，并通过统一的接口对外提供服务；云密码应用层是指通过云密码服务提供的密码服务接口的使用对象，包括安全浏览器、安全网关、移动云安全服务平台等。基础设施为云密码服务提供基础的物理密码运算资源。

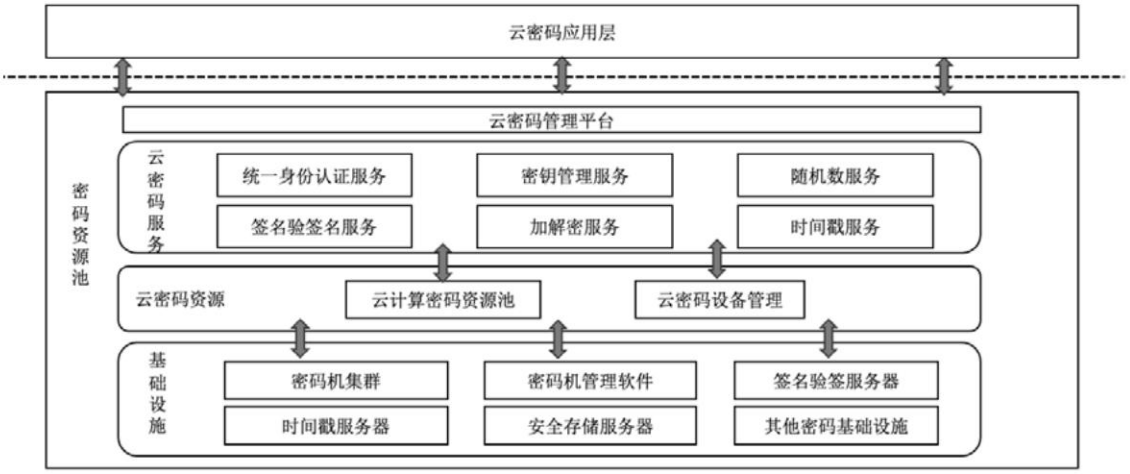

图2 密码资源池架构图

5.3 云密码管理平台

云密码管理平台是云密码服务的支撑与运维平台。其中管理层的密钥管理与认证管理为云密码服务提供密钥与证书的管理服务支撑；管理层的密码服务监管负责云密码服务的运维保障，包括监控云密码设备、云机密算密码资源、密码应用及其运行状况，同时结合云平台的运维、安全等要求，对密码服务资源池数据进行统一存储、备份和恢复。

5.4 云密码服务

5.4.1 统一身份认证服务

统一身份认证服务需基于密码资源池基础设施，对外提供统一身份认证活动。统一身份认证服务需具备身份认证模块和权限管理模块，分别用于对用户或站点身份的管理和权限管理控制，同时对外提供

用户注册、令牌获取以及身份验证的接口。首次使用身份认证服务需通过指定注册接口进行身份注册，后续使用注册的授权信息（账号密码、数字签名等）登陆服务获取访问认证令牌，携令牌访问、请求其他数据、资源时由统一身份认证服务确认认证该令牌的有效性。

5.4.2 秘钥管理服务

密钥管理服务需基于密码资源池基础设施，对外提供密钥相关的支持活动，如密钥托管服务、密钥安全隔离和存储服务、密钥安全访问服务、基于托管密钥的简单加解密服务等，并能够提供统一对外服务接口。

5.4.3 随机数服务

随机数服务需基于密码资源池基础设施，对外提供随机数服务，并能够提供统一对外服务接口。随机数的产生需采用由国家密码管理局批准使用的方式，生成随机数的密码产品应符合GM/T 0062的要求。

5.4.4 签名验签服务

签名验签服务需基于密码资源池中签名验签服务器，对外提供签名验签服务，并能够提供统一对外服务接口。密码资源池中签名验签服务器应符合GM/T 0029的要求。

5.4.5 加解密服务

加解密服务需基于密码资源池中密码机等设备，对外提供数据的加解密服务。加解算法需涵盖国家密码主管部门批准的算法以及常用国际标准算法。加解密服务应对外提供统一加解密接口。

5.4.6 时间戳服务

时间戳服务需基于密码资源池中来源于国家权威时间部门（如国家授时中心），或者使用国家权威时间部门认可的硬件和方法获得的时间提供时间戳服务，时间格式要求应符合GB/T 7408的格式要求，并能够提供统一对外时间戳服务接口。

5.5 云密码资源

云计算密码资源包括云计算密码设备池和密码设备的管理工具、基于密码基础支撑提供的密码设备，为云平台及云租户提供独立的密码资源。云计算密码设备基于硬件加密平台，采用虚拟化技术在硬件平台上同时运行多个虚拟化密码机。在提供密码设备基本功能的基础上，支持虚拟化部署。云密码设备应符合国家密码管理部门的相关标准要求及通过检测审批。

5.6 基础设施

云密码基础设施由密码物理设备建设的密码硬件资源池，包括密码机集群、密码机管理软件、签名验签服务器、时间戳服务器、安全存储服务器、安全存储服务器等其它密码基础设施。

6 云密码服务接口规范

6.1 概述

云密码服务通过接口对外提供统一身份认证服务、密钥管理服务、随机数服务、签名验签服务、加解密服务、时间戳服务。为了使云密码服务在具备通用性的同时保证提供服务的安全性，云密码服务接口需要满足下述规范要求。接口的类型及使用格式见附录B。

6.2 接口说明

6.2.1 通信协议

接口采用HTTP协议，使用HTTP POST方式进行数据请求，编码格式统一为UTF-8编码，数据传输采用HTTPS加密协议。

本规范不改变已有HTTP标准的任何定义，实现者可以充分利用开发语言的HTTP工具包进行扩充。

6.2.2 数据格式

请求参数格式和相应数据格式为JSON，编码为：UTF-8。

6.2.3 请求 URL 结构

URL按照如下结构定义：

```
https://example.com:port/testcontrol
\__/     \___________/  \_______/
   |          |             |
scheme     authority      path
```

URL参数说明见表1：

表1 URL 参数说明

字段	说明
schema	本接口规范规定 schema 采用 https
authority	提供 API 服务的主机名称（或 IP）以及端口
path	操作的目标资源的路径

附 录 A
（资料性）
云密码应用合规性参考表

云密码应用合规性参考表见表A.1。

表A.1 云密码应用合规性参考表

指标要求	密码技术应用点	采取措施
物理和环境安全	身份鉴别	在系统所在机房部署安全电子门禁系统，使用国密规定的算法（如，SM4）算法进行密钥分散，实现门禁卡的一卡一密，并对人员身份进行鉴别。
	电子门禁记录数据完整性	在系统环境监控区部署服务器密码机，使用国密规定的算法（如，HMAC-SM3）对电子门禁系统进出记录和视频监控系统记录等数据进行完整性保护。
	视频记录数据完整性	
	密码模块实现	在安全电子门禁系统和服务器密码机中实现密码算法、密码技术、云密钥管理，云密码服务。
网络和通信安全	身份鉴别	在系统网络接入区和数据灾备区分别部署IPSec VPN，对通信双方进行身份鉴别。
	访问控制信息完整性	在系统网络接入区和数据灾备区分别部署IPSec VPN，对访问控制信息进行完整性保护。
	通信数据完整性	在网络接入区和数据灾备区分别部署 IPSec VPN，对访问控制 信息进行完整性保护； 智能移动终端与本系统的通信数据机密性和完整性在“应用和数据安全”层面实现。
	通信数据机密性	通信双方调用云密码加解密与签名验签服务，建立安全的备份数据传输通道，确保数据机密性。
	集中管理通道安全	在统一管理区部署SSL VPN安全网关，建立安全的集中管理通道。
	密码模块实现	在SSL VPN安全网关中调用云密码服务加解密、签名验签、密钥管理等接口。
设备和计算安全	身份鉴别	在系统业务办公区PC 端部署安全浏览器，并向系统管理员配发USBKey，对登录堡垒机用户调用云服务接口，进行身份鉴别和远程管理身份鉴别，信息传输机密性保护。
	远程管理身份鉴别信息机密性	在远程管理时，对管理员的身份鉴别信息进行加密保护，防止鉴别信息泄漏。

表A.1　云密码应用合规性参考表（续）

指标要求	密码技术应用点	采取措施
设备和计算安全	访问控制信息完整性	仅有管理员可以访问应用服务器、数据库服务器，管理员身份鉴别通过USBKey实现，调用和用云密码服务签名验签接口,使用数字签名技术对统一身份认证系统应用用户访问权限控制列表进行完整性保护。
	敏感标记的完整性	调用云密码服务加解密接口对敏感标记的数据进行加密处理，实现敏感标记的完整性。
	日志记录完整性	调用云密码服务数据完整性验证接口,对应用日志记录进行完整性保护。
	重要程序或文件完整性	调用云密码服务数据签名接口，使用国密规定的算法（如，SM2）数字签名技术进行完整性保护，使用或读取这些程序和文件时，通过USBKey进行验签，以确认其完整性。
	密码模块实现	由密码模块、USBKey、服务器密码机实现密码算法、密码技术、云密码服务、云密钥管理。
应用和数据安全	身份鉴别	调用云密码服务的证书签发与身份认证接口实现身份的鉴别。
	访问控制信息和敏感标记完整性	调用云密码服务签名验签接口,使用数字签名技术对统一身份认证系统应用用户访问权限控制列表进行完整性保护。
	数据传输机密性	PC端安全浏览器与SSL VPN安全网关之间使用合规的SSL协议，建立安全的数据传输通道，实现数据传输机密性、完整性保护。调用云密码服务加解密接口，对数据进行加密，确保数据存储的机密性。
	数据存储机密性	
	数据传输完整性	
	数据存储完整性	
	日志记录完整性	调用云密码服务数据完整性验证接口,对应用日志记录进行完整性保护。
	重要应用程序的加载和卸载	仅有管理员可以进行重要应用程序的加载和卸载,而管理员的身份鉴别在“设备和计算安全”层面完成。
	抗抵赖	调用云密码服务电子签章服务、时间戳服务等，使用密码技术对在系统中流转的电子公文数据进行数字签名,并加盖时间戳，实现操作行为的不可否认性。
	密码模块实现	由安全浏览器、USBKey、SSL VPN 安全网关、移动端密码模块、电子签章系统、服务器密码机、时间戳服务器和证书认证系统实现密码算法、密码技术、云密码服务、云端密钥管理。

附 录 B
（规范性）
接口规范

B.1 错误响应码

当HTTP协议返回码为200时，status_code有效，接口具体返回情况见表B.1。

表B.1 接口具体返回情况表

status_code	描述
0	访问成功
1	参数错误
2	参数为空
3	其他错误
4	未知错误
102	时间戳无效
103	重复操作
104	控制失败
105	系统异常
106	身份无效
与特定业务或接口有关的返回字段在result对象中说明，具体释义参见相应端口的描述。	

B.2 接口说明

B.2.1 密钥申请接口

密钥申请接口说明见表B.2。

表B.2 密钥申请接口说明

接口功能描述	密钥申请		
接口形式化描述	applyKey {key_type}		
接口字段描述	参数	类型	描述
action	apply_key	String	密钥申请
target	key_type	String	密钥类型
	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户 token
	algorithm	String	算法

表B.2 密钥申请接口说明（续）

接口功能描述	密钥申请	

请求样例	{
	"action": "apply_key ",
	"target": {
	"key_type": "asymmetric",
	"timestamp":1581077428207,
	"token"：42dae262b8531b3df48cde9cc018c512,
	"algorithm"："SM4"
	}
	}	

响应参数	status_code	返回状态码
	status_text	返回状态信息
	result	返回结果（密文）

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result"：" aGVvc2FwMTIzZWVy"
	}	

B.2.2 密钥注销接口

密钥注销接口说明见表B.3。

表B.3 密钥注销接口说明

接口功能描述	密钥注销		
接口形式化述	revokeKey {key_tag}		
接口字段描述	参数	类型	描述
action	revoke_key	String	密钥申请
target	key_tag	String	密钥标签
	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户令牌

请求样例	{
	"action": "revoke_key ",
	"target": {
	"key_tag": "qiye_hwcwv",
	"timestamp":1581077428207,
	"token"：42dae262b8531b3df48cde9cc018c512
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	

表B.3　密钥注销接口说明（续）

接口功能描述	密钥注销

响应样例	{
	"status_code": 0,
	"status_text": "success"
	}

B.2.3　密钥更新接口

密钥更新接口说明见表B.4。

表B.4　密钥更新接口说明

接口功能描述	密钥更新		
接口形式化述	updateKey {task_tag}		
接口字段描述	参数	类型	描述
action	update_key	String	密钥申请
target	key_tag	String	密钥标签
	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户令牌
	algorithm	String	算法

请求样例	{
	"action": "update_key ",
	"target": {
	"key_tag": "qiye_hwcwv",
	"timestamp":1581077428207,
	"token"：42dae262b8531b3df48cde9cc018c512,
	"algorithm"："SM4"
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	
	result	返回结果（密文）	

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result":" aGVvc2FwMTIzZWVy"
	}		

B.2.4 加密接口

加密接口说明见表B.5。

表B.5 加密接口说明

接口功能描述	数据加密		
接口形式化述	encrypt {message}		
接口字段描述	参数	类型	描述
action	encrypt	String	加密
target	key_tag	String	密钥标签
	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户令牌
	algorithm	String	算法
请求样例	{ "action": "encrypt ", "target": { "key_tag": "qiye_hwcwv", "timestamp": 1581077428207, "token": 42dae262b8531b3df48cde9cc018c512, "algorithm": "SM4", "message": "hello" } }		
响应参数	status_code	返回状态码	
	status_text	返回状态信息	
	result	返回结果（密文）	
响应样例	{ "status_code": 0, "status_text": "success", "result":"aGVvc2FwMTIzZWVy" }		

B.2.5 解密接口

解密接口说明见表B.6。

表B.6 解密接口说明

接口功能描述	数据加密		
接口形式化述	decrypt {encrypt_message}		
接口字段描述	参数	类型	描述
action	decrypt	String	解密
target	key_tag	String	密钥标签
	timestamp	Time	时间戳,精确到毫秒

表B.6　解密接口说明（续）

接口功能描述	数据加密		
target	token	Int	用户令牌
	algorithm	String	算法

请求样例	{
	"action": "decrypt ",
	"target": {
	"key_tag": "qiye_hwcwv",
	"timestamp":1581077428207,
	"token"：42dae262b8531b3df48cde9cc018c512,
	"algorithm"："SM4",
	"message"："aGVvc2FwMTIzZWVy"
	}
	}		

B.2.6　随机数获取接口

随机数获取接口说明见表B.7。

表B.7　随机数获取接口说明

接口功能描述	获取随机数		
接口形式化描述	getRandom		
接口字段描述	参数	类型	描述
action	get_random	String	解密
target	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户令牌

请求样例	{
	"action": "get_random",
	"target": {
	"timestamp":1581077428207,
	"token"：42dae262b8531b3df48cde9cc018c512
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	
	result	返回结果（密文）	

响应样例	{
	"status_code": 0,
	"status_text": "success"
	"result" :"123"
	}		

B.2.7 时间戳获取接口

时间戳获取接口说明见表B.8。

表B.8 时间戳获取接口说明

接口功能描述	时间戳获取		
接口形式化描述	getTimestamp		
接口字段描述	参数	类型	描述
action	get_timestamp	String	时间戳获取
target	token	Int	用户 token

请求样例	{
	"action": "get_timestamp",
	"target": {
	"token"：42dae262b8531b3df48cde9cc018c512
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	
	result	返回结果（密文）	

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result"：" 1581077428207"
	}		

B.2.8 时间戳验证接口

时间戳验证接口说明见表B.9。

表B.9 时间戳验证接口说明

接口功能描述	时间戳验证		
接口形式化描述	verifyTimestamp		
接口字段描述	参数	类型	描述
action	verify_timestamp	String	时间戳验证
target	timestamp	Time	时间戳,精确到毫秒
	token	Int	用户令牌

请求样例	{
	"action": "verify_timestamp ",
	"target": {
	"token"：42dae262b8531b3df48cde9cc018c512
	}
	}		

表B.9　时间戳验证接口说明（续）

接口功能描述	时间戳验证	
响应参数	status_code	返回状态码
	status_text	返回状态信息
	result	返回结果（密文）

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result": " legal"
	}	

B.2.9　身份注册接口

身份注册接口说明见表B.10。

表B.10　身份注册接口说明

接口功能描述	身份注册		
接口形式化描述	registered		
接口字段描述	参数	类型	描述
action	registered	String	时间戳验证
target	timestamp	Time	时间戳,精确到毫秒
	id	Int	用户/企业 id
	password	String	注册口令

请求样例	{
	"action": "Registered ",
	"target": {
	"timestamp": 1581077428207,
	"id": 111,
	"password": 123abc
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	

响应样例	{
	"status_code": 0,
	"status_text": "success"
	}		

B.2.10　令牌获取接口

令牌获取接口说明见表B.11。

表B.11　令牌获取接口说明

接口功能描述	令牌获取		
接口形式化描述	getToken		
接口字段描述	参数	类型	描述
action	get_token	String	时间戳验证
target	timestamp	Time	时间戳,精确到毫秒
	id	Int	用户/企业 id
	password	String	注册口令

请求样例	{
	"action": "get_token",
	"target": {
	"timestamp"：1581077428207,
	"id"：111,
	"password"：123abc
	}
	}		

响应参数	status_code	返回状态码	
	status_text	返回状态信息	
	result	返回 token（密文）	

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result":42dae262b8531b3df48cde9cc018c512
	}		

B.2.11　身份认证接口

身份认证接口说明见表B.12。

表B.12　身份认证接口说明

接口功能描述	身份注册		
接口形式化描述	verifyId		
接口字段描述	参数	类型	描述
action	verify_id	String	时间戳验证
target	timestamp	Time	时间戳,精确到毫秒
	id	Int	用户/企业 id
	token	Int	用户令牌

请求样例	{
	"action": "verify_id",
	"target": {
	"timestamp"：1581077428207,		

表B.12　身份认证接口说明（续）

接口功能描述	身份注册	
请求样例	"id"：111, "token"：42dae262b8531b3df48cde9cc018c512 } }	
响应参数	status_code	返回状态码
	status_text	返回状态信息
	result	返回结果

响应样例	{
	"status_code": 0,
	"status_text": "success",
	"result"："legal"
	}	

参 考 文 献

[1] GB/T 35273-2017 信息安全技术 个人信息安全规范
[2] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
[3] 政务信息系统密码应用与安全性评估工作指南(2020版)
[4] 霍炜,郭启全,马原.商业密码应用与安全行评估 [M] .电子工业出版社，2020.