附件

重庆《云密码服务分类》

序号	服务分类	服务项目	应用场景	对应高风险项	服务/产品简介	服务类型
1	基础加解密类服务	数据加解密/校验服务	用于重要数据存储机密性/完整性保护	应用和数据安全： 1) 采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。 2) 采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	通过为业务应用提供数据加解密、文件加解密服务，实现应用系统重要存储方面的数据机密、完整性保护；支持 SM2/3/4 等算法。	SDK/API
2		密钥管理服务	用于整体密码体系集中式管理。	配合密码产品或密码服务，进行密钥管理。	密钥管理服务创建和管理密钥，保护密钥的保密性、完整性和可用性，满足用户多应用多业务的密钥管理需求。基于硬件 HSM 实现密钥安全生成、存储，符合合规要求。提供自助控制台，支持图形化的密钥管理服务。	SDK/API
3		签名验签服务	用于应用身份鉴别/不可否认性/签名验签。	设备和计算安全： 1）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。 应用和数据安全： 1) 采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。 2) 在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收 证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	通过为业务应用提供签名验签服务，支持数据签名验签、文件签名验签，实现应用系统身份真实性、数据保密性、数据完整性以及不可否认性等保护。	SDK/API

4		数据库加密服务	用于应用数据库透明加密。	应用和数据安全： 1) 采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。 2) 采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	为业务应用提供透明化的结构化数据加密和完整性校验服务，从而实现数据库中敏感字段的机密性和完整性保障。通过具备国家商用密码产品认证的数据库加密模块完成密码运算，满足合规要求。	SDK/API
5		文件加密服务	用于应用文件透明加密。	/	为业务应用提供透明化的非结构化数据加解密和完整性校验服务，从而实现敏感文件在磁盘中存储的机密性和完整性保障。通过具备国家商用密码产品认证的文件加密模块完成密码运算，满足合规要求。	SDK/API
6	通道加密类服务	SSL/IP Sec 通道加密服务	用于通信数据机密性/完整性。	网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 2）采用密码技术保证通信过程中重要数据的机密性。	通过 SSL/IP Sec 安全网关构建安全访问通道，实现远程安全接入、访问权限控制、审计，为应用与用户之间建立加密通道。支持商密 SSLVPN、IP Sec VPN 协议，在用户端与云平台之间建立远程安全传输通道，支持 SSL 解析与卸载服务，保障云上应用用户接入的身份可信以及数据传输过程中的机密性与完整性。	/
7		商密安全运维管理服务	用于 PC 端商密堡垒机实现安全运维，身份鉴别/远程管理通道	设备和技算安全： 1)采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性. 2)远程管理通道安全。	通过具备国家商用密码产品认证的堡垒机提供服务，包括运维管理人员身份鉴别、远程安全运维管理通道、账号密码安全托管、单点登录等服务。	/

8		移动安全密码服务	用于移动终端、定制终端身份鉴别以及数据传输中的机密性/完整性/不可否认性。	针对移动端、定制终端环境： 1.网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 2）采用密码技术保证通信过程中重要数据的机密性。 2.应用和数据安全： 在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	为云平台自身以及云上业务应用的使用者提供手机端的电子身份识别签发、为云上租户在手机端涉及电子公文应用中的公文盖章人身份的确认性、电子公文的信息完整性、公文盖章人的不可抵赖性；通过 SSL 安全网关，实现远程安全接入、访问权限控制、审计，为云上业务应用与用户手机端之间建立加密通道；为云上平台及云上业务提供的基于密码技术的服务，用于标识身份信息及业务操作过程中进行可靠电子签名、加密等。	SDK
9		远程安全接入服务	用于用户从外部连接到内部网络的设备进行身份鉴别以及数据传输的机密性。	网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 2）安全接入认证： 采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性	支持商密 SSL VPN、IP Sec VPN 协议，对于从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性，保障应用用户接入的身份可信以及数据传输过程中的机密性与完整性。	/
10	身份认证类服务	动态口令认证服务	用于通信实体进行身份鉴别，保证通信实体身份的真实性。	设备和计算安全： 1）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。 应用和数据安全： 1）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	该服务和数字证书认证服务二选一，支持产生基于商用密码算法的认证口令，可支持硬件令牌、移动 APP、SDK 集成等方式。	SDK API
11		协同签名服务	用于移动端身份鉴别。	针对移动端、定制终端环境： 1.网络和通信安全： 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 2.应用和数据安全： 采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	协同签名服务提供密钥分片、协同签名服务，基于该服务可实现安全导出用户密钥分片到本地，在本地提供高安全性的密钥存储和运算环境。软件密码模块具备国家商用密码产品认证，支持 android 和 iOS 版本，满足合规要求。	SDK

12		数字证书认证服务	用于应用用户的身份鉴别。	网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 设备和计算安全： 1）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。 应用和数据安全： 1）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	该服务和动态口令认证服务二选一，基于数字证书安全登录与身份认证，保证每个应用用户在登录时具有证明其身份的唯一标志，系统通过惟一标志验证用户身份真实身份。	/
13		身份认证系统	提供业务应用系统用户的身份鉴别。	应用和数据安全： 1）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	利用密码技术为业务系统提供口令和证书结合的双因素身份认证手段，基于 SM2 或 SM9 国密算法，实现用户的身份真实性验证，提升系统终端访问的安全性。	SDK/API
14	应用类密码服务	时间戳服务	防止重要数据被篡改，不可否认性。	针对特定环境的应用和数据安全： 1）在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	时间戳服务是一种能够提供电子文件的日期和时间信息的安全保护的技术，人们可以依赖它来确定电子文档在何时创建和签署的。 时间戳是使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。	SDK API
15		电子签章服务	用于业务需要电子签章。	针对特定环境的应用和数据安全： 1）在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	电子签章服务是一种能够提供安全，便捷的电子合同签约及证据保全服务的产品。 电子签章服务是基于文档的签名，无需上传文档，直接在 PDF 文档就可完成签名。	SDK/API

16		邮件透明加密服务	用于邮件系统机密性。	/	为电子邮件系统提供透明化的邮件数据加解密服务，从而实现电子邮件在邮件系统中存储的机密性。通过具备国家商用密码产品认证的邮件加密模块完成密码运算，满足合规要求。	SDK/API
17		物联网标识密钥服务	用于物联网终端与平台之间的设备认证以及数据机密性/完整性。	/	为物联网安全场景提供设备标识管理、设备认证密钥管理服务，配套提供终端 SDK，SDK 支持常见类型物联网终端集成对接。基于该服务可实现物联网场景中终端与平台之间的设备认证以及数据机密性保护、完整性保护。	SDK/API
18		物联网标识密钥增值服务	用于物联网终端安全认证。	/	物联网终端 SDK 依托运营商 NB 超级 SIM 卡实现物联网终端安全认证，终端标识密钥及算法运算由 SIM 卡安全芯片提供安全保障。	SDK/API
19		视频加密服务	用于视频终端接入认证、视频数据传输机密性与完整性保护服务。	/	提供视频采集终端接入认证、视频数据传输机密性与完整性保护服务。	SDK/API
20	终端选配类	商密安全浏览器	用于 PC 端使用，配合安全认证网关，用于数据传输机密性和完整性保护。	网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 2）采用密码技术保证通信过程中重要数据的机密性。 应用和数据安全： 1) 采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。	保护客户端与 WEB 服务器之间通信数据的机密性和完整性，并实现基于数字证书的认证、签名等密码服务。支持商密算法 SM2/3/4	软件

21		USB Key	用于 PC 终端实体用户的身份鉴别。	网络和通信安全： 1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。 设备和计算安全： 1）采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。 应用和数据安全： 1）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	为业务应用系统用户和管理员发放 USB Key，主要提供签名验签、杂凑等密码运算服务，实现信息的真实性、完整性保护，同时提供一定的存储空间，用于存放数字证书或电子签章等用户数据。	硬件购置

备注：

1.适用范围：根据《密码法》《商用密码管理条例》《商用密码应用安全性评估管理办法》等法律法规要求，在云平台上运行的关键信息基础设施、网络安全等级保护第三级及以上信息系统、政务信息系统、重要工业控制系统等均适用。本密码服分类基于商用密码应用场景进行分类。

2.按照《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》和密码应用安全性评估测评项要求，若信息系统存在任意 1 条高风险项或评分低于 60 分，则密评不通过。为通过密评，最低配置方案建议如下：

（1）“数据加解密/校验服务”，若未选择则导致“应用和数据安全”指标中的重要数据存储机密性和完整性无法得到保障且属于高风险项。

（2）“密钥管理服务”，若未选择则导致安全管理中的密钥管理服务无法保障且属于高风险项目。

（3）“SSL/IP Sec 通道加密服务”，若未选择则导致“网络和通信安全”指标中的通信实体的身份鉴别和重要数据传输的机密性和完整性无法得到保障且属于高风险项。

（4）“商密安全运维管理服务”，若未选择则导致“设备和计算安全”指标中的身份鉴别以及远程管理通道安全无法得到保障且属于高风险项。

（5）“动态口令认证服务”和“数字证书认证服务+USB key+签名验签服务”二选一，主要是实现技术指标层面通信实体的身份鉴别且属于高风险项，若未选择，则密评不通过。

3.实际密码应用方案需根据信息系统实际加选其他密码服务。在物理层面、管理层面符合相关要求以及必选密码服务均被有效调用的前提下，以信息系统最小原型为评估对象，预估密评得分可达 70 分以上且无高风险。

4.云平台密码服务分类根据国家密码应用相关标准变化适时增减。

5.提供服务的所有硬件设备、安全模块等均需取得商用密码产品认证证书。

6.SDK 是指软件开发工具包，主要用于移动端环境，可以帮助开发者集成密码服务。

7.API 是指接口程序，可以帮助开发者通过 API 接口方式直接调用所需密码服务