附件 3

ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0222—2021

金融信息系统加密服务的技术能力评价模型

Evaluation model for technical capabilities of cryptographic service in financial information system

2021－07－22 发布　　2021－07－22 实施

中国人民银行　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。

本文件由中国银行股份有限公司提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国银行股份有限公司、中国人民银行征信中心、中国人民银行数字货币研究所、中国银联股份有限公司、网联清算有限公司、中国建设银行股份有限公司、中国人寿保险（集团）公司、中国人寿保险股份有限公司、中国信息通信研究院、中国科学院信息工程研究所、国泰君安证券股份有限公司、重庆富民银行股份有限公司、中国金融电子化公司、国家信息安全工程技术研究中心、华中科技大学、西安电子科技大学。

本文件主要起草人：刘鸿乾、李世京、袁俊德、李玉亭、高国奇、张学航、周波勇、蔡光明、徐飞燕、陈斌辉、赵新宇、汤洋、杨萌、何虎威、龙志德、汪浩鹏、王妙琼、李凤华、刘新亮、李丙洋、刘书元、李伟斌、王瑜辉、樊凯。

金融信息系统加密服务的技术能力评价模型

1 范围

本文件给出了对提供金融机构加密服务的金融信息系统（以下简称系统）的能力进行评价的方法。

本文件适用于使用专用加解密设备，并通过软件和系统提供加解密服务的金融机构。

注：专用加解密设备是指获得国家密码管理局认可的、专门用于加解密运算的商用硬件设备，广泛应用于资金支付、身份认证、密码校验等业务场景。

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。

GM/T 0019 通用密码服务接口规范

GM/T 0054 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

加解密设备 encryption and decryption device

由国家指定生产厂商研制开发的，专门应用于机构内部系统中，以规定的协议通讯，直接与主机相连接，实现对网络上传输的信息进行保护或鉴别，以保证信息的正确性，防止内部重要的数据被非法篡改或窃取的设备。

注：典型的加解密设备有金融数据密码机、服务器密码机、签名验签服务器等。

3.2

明文 plain text

未加密的信息。

[来源：GB/T 25069—2010，2.2]

3.3

密文 cipher text

利用加密技术，经变换，信息内容被隐藏起来的数据。

[来源：GB/T 25069—2010，2.2]

3.4

加密 encipherment

对数据进行密码变换以产生密文的过程。

注：加密过程一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为“密钥”。

[来源：GB/T 25069—2010，2.2]

3.5

解密 decipherment

将密文转换成明文的处理，即加密对应的逆过程。

[来源：GB/T 25069—2010，2.2]

3.6

密钥分量 key component

用于建立和维持密钥的数据。

注：是密钥的组成分量，多个密钥分量共同组成密钥。又称为“密钥组件”。

3.7

密钥校验值 check value

用于校验密钥输入时正确性的数据。

注：密钥校验值分为密钥分量的校验值和密钥合成后的总校验值。

3.8

个人识别码 personal identification number； PIN

客户持有的用于身份验证的代码或口令。

注：PIN进行一定转换后使用密钥进行加密的结果称为“PINBLOCK”，在此过程中使用的密钥称为“PIN密钥”，整个过程称为“PINBLOCK密文转换”。

[来源：GB/T 21078，3.18]

3.9

消息鉴别码 message authentication code； MAC

用于检查信息在传递过程中是否被更改的一组数据。

注：把一组数据通过算法计算得出MAC的过程称为“MAC计算”。MAC计算过程中用到的密钥称为“MAC密钥”。

3.10

数据加密密钥 data encryption key； DEK

在密钥的层次关系中，对明文进行加密的密钥。

注：典型的DEK有终端PIN密钥（TPK）、区域MAC密钥（ZAK）等。

3.11

密钥交换密钥 key encryption key； KEK

在密钥的层次关系中，对数据加密密钥进行加密的密钥。

注：典型的KEK有终端主密钥（TMK）、区域主密钥（ZMK）等。

3.12

本地主密钥 local master key； LMK

在密钥的层次关系中，用于保护其他密钥的最高层的密钥。

注：又称为“加密机主密钥”，其受硬件加解密设备保护。

3.13

对称密钥 symmetric key

加密和解密过程中使用的相同的密钥。

注：对称密钥用于对称加密算法。

3.14

非对称密钥 asymmetric key

使用其中一把密钥进行加密，则只能使用另一把密钥进行解密的一组密钥对。

注：两把密钥分别称为“公钥”和“私钥”。非对称密钥用于非对称加密算法。

3.15

签名 signature

对一个数字单元进行密码变换，以提供数据源鉴别、数据完整性和签名人抗抵赖性服务。

注：又称为“数字签名”。

3.16

摘要算法 digest algorithm

把任意长度的数据进行处理，生成固定长度数据的一种算法。

3.17

证书 certificate

确认实体与宣称身份关系的文件。

注：又称为“数字证书”。

3.18

访问控制 access control

仅允许经授权的人员或应用对信息或信息处理设施进行访问的一种管理手段。

3.19

告警 alarm

对预期外的事件进行通知的过程。

3.20

鉴别 authentication

确认实体声明身份的过程。

[来源：ISO/IEC TR 13335:2000，3.1]

3.21

审计日志 audit journal

系统运行的时序记录，该记录足够重建、复审、检查环境的系列事物和周边行为，或导出一笔交易从起始到输出最终结果路径中的每个事件。

3.22

生产环境 production environment

承担对外业务服务的软件和硬件环境。

3.23

非生产环境 non-production environment

不承担对外业务服务的软件和硬件环境。

注：典型的非生产环境有开发环境、测试环境等。生产环境加非生产环境统称为“基础环境”。

3.24

高可用集群 high-available clusters

减少由计算机硬件和软件易错性造成损失的一种架构模式。

3.25

备份 backup

业务信息的额外存储，一旦遇到信息资源丢失，可确保业务的持续性。

3.26

应急预案 contingency plan

遭遇事故后，恢复业务可用性的规程和策略。

3.27

应用程序接口 application programming interface； API

软件系统不同组成部分衔接的约定。

4 确定评价范围

对金融机构的系统进行评价前，首先明确本文件适用的评价范围。

本文件适用的评价范围如下：

a） 本文件仅针对使用硬件加解密设备的金融机构或系统。

b） 储存客户信息、账户信息、交易数据，或处理业务逻辑的软件模块在评价范围外。

c） 调用或管理加解密设备，提供数据加解密运算的服务，或者提供密钥、证书管理功能的模块在评价范围内。

一个典型的加密服务系统架构见下图，图中实线框定的应用在本文件的评价范围内。

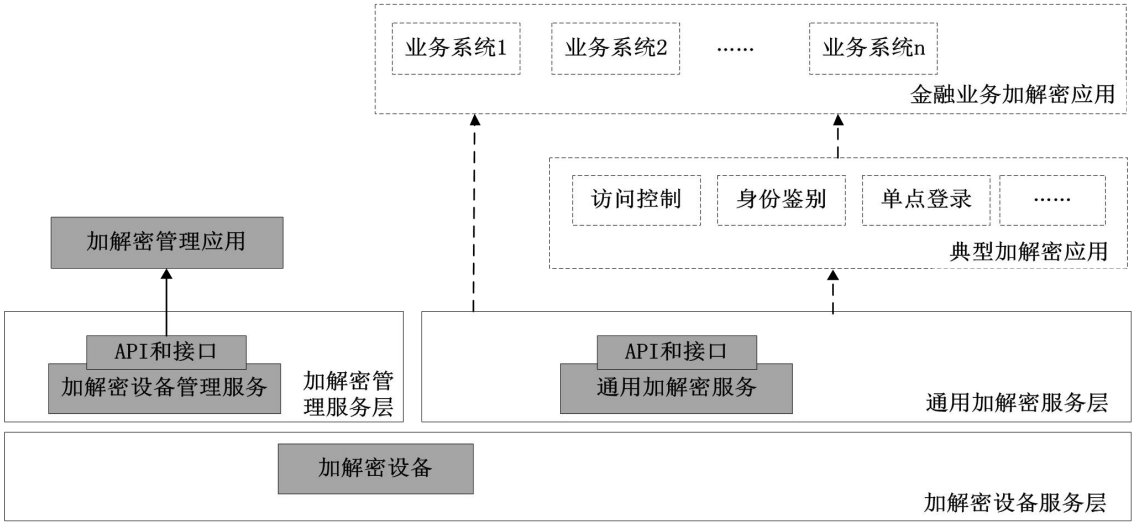

图　典型加密服务系统架构

5　能力评价模型

5.1　能力评价结果

评价标准共分为五级，表1表述了各级别所对应的整体要求。从第一级到第五级，分别对应下文6.2至6.6，成熟度能力每级递进。在每一级评价过程中，出现当前级别与其他级别指标冲突的情况，以当前评价级别指标为准。

表1　标准分级

级别	描述
第一级	满足系统完成级要求。此级别表示加密服务系统运转的最低要求。
第二级	满足系统管理级要求。满足系统可管理、有冗余、可恢复等方面要求，具备加密相关的数据保护措施。
第三级	满足系统定义级要求。满足系统可监控、可审计等要求，具备应急管理能力，具备系统架构对数据的安全保护能力。
第四级	满足系统量化管理级要求。满足系统高可用、服务连续等要求，具备应急预防能力，具备软硬件生命周期管理能力。
第五级	满足系统优化级要求。满足系统自主可控、接口规范等要求，具备对自然灾害以及国际局势变动导致的不可抗力的应对能力。

5.2　模型应用

5.2.1 概述

本模型广泛适用于使用专用加解密设备的金融信息系统。金融机构可参照模型的要求建立、保持和改进系统加密服务的能力，包括：

a） 将本模型作为指南，确定系统加密服务能力建设和改进的目标和途径。

b） 以某个能力级别为目标实施全面改进，提升系统加密服务能力。

c） 借鉴本模型的具体要求，对选定的能力域或能力项进行提升。

本模型作为评价金融信息系统加密服务能力的准则和依据，可应用以下四种模式：

a） 自我评价：系统加密服务能力的自我评价。

b） 外部评价：第三方机构对系统加密服务能力的外部评价。

c） 需方评价：服务需方对金融机构的选择评价。

d） 准入评价：金融机构评级和市场准入的辅助依据。

5.2.2 自我评价

金融信息系统加密服务能力的自我评价是指金融机构根据需要以及能力提升目标，对自身系统加密服务能力进行的内部分析和评价。自我评价旨在发现和分析系统加密服务能力的问题或不足，便于了解自身的差距，设立自身的改进目标和范围，并针对差距采取改进措施，提升系统加密服务的能力。

5.2.3 外部评价

金融信息系统加密服务能力的外部评价是指第三方机构对系统加密服务能力成熟度的评价。外部评价旨在从独立第三方角度出发，客观地评价并证实被评价系统加密服务能力已经达到的成熟度级别。其评价结果可用于金融机构了解自身的真实情况、金融服务需方选择金融机构的辅助依据，以及其他金融机构评级、市场准入的辅助依据。

5.2.4 需方评价

金融信息系统加密服务能力的需方评价是指金融服务需方选择金融机构时，为选择符合其需求的金融机构所进行的评价。需方评价旨在通过评价结果证实金融机构的系统加密服务能力所达到的成熟度级别，来确定满足要求的程度。其评价结果可以来自第三方评价机构，也可以来自于服务需方或其认可的机构。

5.2.5 准入评价

金融信息系统加密服务能力的准入评价是指相关监管机构通过评价结果证实金融机构的系统加密服务能力所达到的成熟度级别，作为金融机构是否可以进入某市场，或允许开展某类型业务的准入门槛的依据。

6 评价标准

6.1 总则

能力评价维度的总体框架见表2。

表 2 能力评价维度

能力评价维度	技术要点	评测要求
开发迭代维度	基础环境	生产隔离性
	版本管理	参数管理
		代码介质管理
持续运行维度	容量管理	容量标称
		容量感知
		容量管理
	高可用集群	集群管理
		集群冗余性
	监控告警	监控管理
		监控指标
		监控日志
	异常恢复	应急响应
		灾难与恢复
		问题管理
应用服务维度	算法支持	对称算法
		非对称算法
		摘要算法
	加解密接口	封装标准
		场景支持
	资源池管理	设备资源池
		池管理系统
		主密钥安全域
安全管控维度	制度管理	规范定义
		人员要求
		密钥操作管理
	访问控制	登录和认证
		用户管控
	审计日志	日志内容
		日志保存
密钥管理维度	加解密设备	硬件要求
		资质要求
		设备管理
	对称密钥	密钥生成
		密钥存储
		对称密钥使用
		对称密钥分发
		密钥备份
	非对称密钥	生成密钥或证书
		使用密钥或证书
		更换密钥或证书

6.2 第一级

6.2.1 持续运行维度—容量管理

第一级持续运行维度中，关于容量管理的评价标准见表3。

表 3 容量管理 - 第一级

评测要求	评测程序
6.2.1.1 容量标称	提供加解密服务的系统或加解密设备，应规定以下性能容量标称值： a) 对称算法性能容量标称值： DES/3DES 算法 64 位、128 位、192 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 AES 算法 128 位、192 位、256 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 SM4 算法每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 b) 非对称算法性能容量标称值： RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 SM2 每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够生成的密钥对数量。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够生成的密钥对数量。 SM2 算法每秒能够生成的密钥对数量。 c) 摘要算法性能容量标称值： SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3 等摘要算法每秒能够处理的交易笔数。 d) 系统或加解密设备提供服务的最大并发数。
注：DES/3DES、AES、SM4分别是对称算法的一种，RSA、ECC、SM2分别是非对称算法的一种，SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3分别是摘要算法的一种。	

6.2.2 应用服务维度—算法支持

第一级应用服务维度中，关于算法支持的评价标准见表4。

表 4 算法支持 - 第一级

评测要求	评测程序
6.2.2.1 对称算法	加解密设备应支持或部分支持以下对称算法，并达到对应的强度： a) 加解密设备支持 SM4 算法。 b) 加解密设备支持 DES/3DES 算法，并达到 64 位、128 位、192 位强度。 c) 加解密设备支持 AES 算法，并达到 128 位、192 位、256 位强度。
6.2.2.2 非对称算法	加解密设备应支持或部分支持以下非对称算法，并达到对应的强度： a) 加解密设备支持 SM2 算法。 b) 加解密设备支持 RSA 算法，并达到 1024 位、2048 位、3072 位、4096 位强度。 c) 加解密设备支持 ECC 算法，并达到 160 位、256 位、384 位、512 位强度。

表4　算法支持 - 第一级（续）

评测要求	评测程序
6.2.2.3 摘要算法	加解密设备应支持或部分支持以下摘要算法，并达到对应的强度： a)　加解密设备支持 MD5 算法。 b)　加解密设备支持 SM3 算法。 c)　加解密设备支持 SHA 系列算法，并达到 SHA-1、SHA-256、SHA-384、SHA-512 强度。

6.2.3　密钥管理维度

6.2.3.1　加解密设备

第一级密钥管理维度中，关于加解密设备的评价标准见表5。

表 5　加解密设备 - 第一级

评测要求	评测程序
6.2.3.1.1 硬件要求	在提供加解密服务的系统中应使用专用的加解密运算设备。
6.2.3.1.2 资质要求	加解密设备的资质应满足以下要求： a)　密码机具备国家密码局授予的商用型号。 b)　签名验签服务器具备国家密码局授予的商用型号。 c)　如果系统仅用于涉外业务，可以没有国家密码局授予的型号。
注：涉外业务指与国外机构之间进行的业务。	

6.2.3.2　对称密钥

第一级密钥管理维度中，关于对称密钥的评价标准见表6。

表 6　对称密钥 - 第一级

评测要求	评测程序
6.2.3.2.1 密钥生成	对称密钥的生成过程应满足以下要求： a)　使用随机数生成算法产生密钥数据。 b)　加解密设备的多组密钥分量合成密钥的算法公开并可以复制。 c)　支持以 LMK、KEK 保护的形式生成并输出密钥数据。
6.2.3.2.2 对称密钥分发	对称密钥在分发之前应对接收者的身份进行确认。

6.2.3.3　非对称密钥

第一级密钥管理维度中，关于非对称密钥的评价标准见表7。

表 7　非对称密钥 - 第一级

评测要求	评测程序
6.2.3.3.1 生成密钥或证书	非对称密钥或证书的生成过程应满足以下要求： a)　非对称密钥对的生成方式保证私钥的机密性。 b)　生成新证书时，可以指定算法、算法强度和失效日期。

6.3　第二级

6.3.1 开发迭代维度

6.3.1.1 基础环境

第二级开发迭代维度中，关于基础环境的评价标准见表8。

表 8 基础环境 - 第二级

评测要求	评测程序
6.3.1.1.1 生产隔离性	具备生产环境与非生产环境管理概念，且生产环境与非生产环境相对隔离。

6.3.1.2 版本管理

第二级开发迭代维度中，关于版本管理的评价标准见表9。

表 9 版本管理 - 第二级

评测要求	评测程序
6.3.1.2.1 参数管理	以下数据应在生产环境中配置，不应编入代码或预编译进程序： a) 生产环境的网络协议地址（IP 地址）信息。 b) 生产环境使用的密钥数据。 c) 生产环境使用的私钥数据。
6.3.1.2.2 代码介质管理	代码介质的管理应满足以下要求： a) 建立代码库，管理有关的代码以及编译后的程序。 b) 建立软件介质库，管理生产环境使用的软件产品。

6.3.2 持续运行维度

6.3.2.1 容量管理

第二级持续运行维度中，关于容量管理的评价标准见表10。

表 10 容量管理 - 第二级

评测要求	评测程序
6.3.2.1.1 容量标称	提供加解密服务的系统或加解密设备，应规定以下性能容量标称值： a) 对称算法性能容量标称值： DES/3DES 算法 64 位、128 位、192 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 AES 算法 128 位、192 位、256 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 SM4 算法每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 b) 非对称算法性能容量标称值： RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 SM2 每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够生成的密钥对数量。

表10　容量管理 - 第二级（续）

评测要求	评测程序
6.3.2.1.1 容量标称	ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够生成的密钥对数量。 SM2 算法每秒能够生成的密钥对数量。 c) 摘要算法性能容量标称值： SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3 等摘要算法每秒能够处理的交易笔数。 d) 系统或加解密设备提供服务的最大并发数。

6.3.2.2　高可用集群

第二级持续运行维度中，关于高可用集群的评价标准见表11。

表 11　高可用集群 - 第二级

评测要求	评测程序
6.3.2.2.1 集群冗余性	系统应达到以下冗余性要求： a) 每个业务系统可以调用一台以上的加解密设备，以应对单台设备出现故障的情形。 b) 拥有同样功能且处理联机加解密业务数据的软件产品部署于一个以上的节点，以应对单节点出现故障的情形。
注：业务系统指承载某项业务功能的信息系统。一个节点通常是一台服务器。	

6.3.2.3　异常恢复

第二级持续运行维度中，关于异常恢复的评价标准见表12。

表 12　异常恢复 - 第二级

评测要求	评测程序
6.3.2.3.1 应急响应	当监测到异常时，应启动应急处理流程。

6.3.3　应用服务维度

6.3.3.1　算法支持

第二级应用服务维度中，关于算法支持的评价标准见表13。

表 13　算法支持 - 第二级

评测要求	评测程序
6.3.3.1.1 对称算法	加解密设备应支持或部分支持以下对称算法，并达到对应的强度： a) 加解密设备支持 SM4 算法。 b) 加解密设备支持 DES/3DES 算法，并达到 64 位、128 位、192 位强度。 c) 加解密设备支持 AES 算法，并达到 128 位、192 位、256 位强度。
6.3.3.1.2 非对称算法	加解密设备应支持或部分支持以下非对称算法，并达到对应的强度： a) 加解密设备支持 SM2 算法。 b) 加解密设备支持 RSA 算法，并达到 1024 位、2048 位、3072 位、4096 位强度。 c) 加解密设备支持 ECC 算法，并达到 160 位、256 位、384 位、512 位强度。
6.3.3.1.3 摘要算法	加解密设备应支持或部分支持以下摘要算法，并达到对应的强度：

表13　算法支持 - 第二级（续）

评测要求	评测程序
6.3.3.1.3 摘要算法	a)　加解密设备支持 MD5 算法。 b)　加解密设备支持 SM3 算法。 c)　加解密设备支持 SHA 系列算法，并达到 SHA-1、SHA-256、SHA-384、SHA-512 强度。

6.3.3.2　加解密接口

第二级应用服务维度中，关于加解密接口的评价标准见表14。

表 14　加解密接口 - 第二级

评测要求	评测程序
6.3.3.2.1 封装标准	加解密设备或对应的软件应可提供 API 接口。

6.3.4　密钥管理维度

6.3.4.1　加解密设备

第二级密钥管理维度中，关于加解密设备的评价标准见表15。

表 15　加解密设备 - 第二级

评测要求	评测程序
6.3.4.1.1 硬件要求	加解密设备的硬件应满足以下要求： a)　在提供加解密服务的系统中使用专用的加解密运算设备。 b)　设备支持双电源，且可以在不影响设备正常运行的条件下更换电源模块。
6.3.4.1.2 资质要求	加解密设备的资质应满足以下要求： a)　密码机具备国家密码局授予的商用型号。 b)　签名验签服务器具备国家密码局授予的商用型号。 c)　如果系统仅用于涉外业务，可以没有国家密码局授予的型号。

6.3.4.2　对称密钥

第二级密钥管理维度中，关于对称密钥的评价标准见表16。

表 16　对称密钥 - 第二级

评测要求	评测程序
6.3.4.2.1 密钥生成	对称密钥的生成过程应满足以下要求： a)　使用随机数生成算法产生密钥数据。 b)　加解密设备的多组密钥分量合成密钥的算法公开并可以复制。 c)　支持以 LMK、KEK 保护的形式生成并输出密钥数据。
6.3.4.2.2 密钥存储	对称密钥数据在系统中存储应满足以下要求： a)　在加解密设备之外，不以明文或明文分量的形式存储密钥。 b)　LMK 仅储存于加解密设备中。LMK 分量可存储于由加密设备配套的 IC 卡或者 USB KEY 等电子介质中。 c)　在加解密设备外以本地数据库或文件等形式存储的密钥使用 LMK 进行保护。

表16　对称密钥 - 第二级（续）

评测要求	评测程序
6.3.4.2.3 对称密钥使用	对称密钥在使用过程中应满足以下关系： a)　LMK、KEK、DEK 不相同或混用。 b)　加解密设备不支持 LMK 明文的读取操作。 c)　系统间交互 DEK 时，使用 KEK 保护 DEK。 d)　系统间交互的需进行加密的数据，使用 DEK 进行保护。
6.3.4.2.4 对称密钥分发	对称密钥在分发之前应对接收者的身份进行确认。
6.3.4.2.5 密钥备份	对于密钥具备备份机制。
注：IC卡（Integrated Circuit Card）指集成电路卡，也称微芯片卡，是一种安全可靠的信息载体。USB KEY也称为优盾，同样是一种安全可靠的信息载体。	

6.3.4.3　非对称密钥

第二级密钥管理维度中，关于非对称密钥的评价标准见表17。

表 17　非对称密钥 - 第二级

评测要求	评测程序
6.3.4.3.1 生成密钥或证书	非对称密钥或证书的生成过程应满足以下要求： a)　非对称密钥对的生成方式保证私钥的机密性。 b)　生成新证书时可以指定算法、算法强度和失效日期。 c)　业务使用的非对称密钥对通过指定的系统或专用加解密设备生成，并定义保管私钥副本的部门或岗位。 d)　规定合规的根证书颁发机构并明确应关联根证书的场景。
6.3.4.3.2 使用密钥或证书	非对称密钥或证书的使用和保存应满足以下要求： a)　从加解密设备或配套系统中获取私钥数据时使用加密手段。 b)　业务活动不涉及私钥数据的传输。
6.3.4.3.3 更换密钥或证书	非对称密钥或证书的更换应满足以下要求： a)　定义非对称密钥或证书的更换周期以及更换流程。 b)　具备根据原证书的密钥对及其失效时间重新生成新证书的流程和能力。

6.4　第三级

6.4.1　开发迭代维度

6.4.1.1　基础环境

第三级开发迭代维度中，关于基础环境的评价标准见表18。

表 18　基础环境 - 第三级

评测要求	评测程序
6.4.1.1.1 生产隔离性	对于生产与非生产环境和数据，应满足以下隔离性要求： a)　非生产环境与生产环境保持隔离，包括但不限于物理隔离。

表18　基础环境 - 第三级（续）

评测要求	评测程序
6.4.1.1.1 生产隔离性	b)　非生产环境使用的密钥和私钥数据与生产环境不混用。 c)　维护生产环境与非生产环境的专用加密网络通道不混用。 d)　生产环境与非生产环境不混用同一台加解密设备。

6.4.1.2　版本管理

第三级开发迭代维度中，关于版本管理的评价标准见表19。

表 19　版本管理 - 第三级

评测要求	评测程序
6.4.1.2.1 参数管理	以下数据应在生产环境中配置，不应编入代码或预编译进程序： a)　生产环境的 IP 地址信息。 b)　生产环境使用的密钥数据。 c)　生产环境使用的私钥数据。
6.4.1.2.2 代码介质管理	代码介质的管理应满足以下要求： a)　建立代码库，管理有关的代码以及编译后的程序。 b)　建立软件介质库，管理生产环境使用的软件产品。 c)　开发人员只能向代码库提交或更新代码，并使用代码库中的代码进行编译。 d)　软件测试以及生产投产过程中，从代码库、介质库中取得代码、程序以及软件。 e)　生产环境使用的密钥、证书数据不纳入代码库。

6.4.2　持续运行维度

6.4.2.1　容量管理

第三级持续运行维度中，关于容量管理的评价标准见表20。

表 20　容量管理 - 第三级

评测要求	评测程序
6.4.2.1.1 容量标称	提供加解密服务的系统或加解密设备，应规定以下性能容量标称值： a)　对称算法性能容量标称值： DES/3DES 算法 64 位、128 位、192 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 AES 算法 128 位、192 位、256 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 SM4 算法每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 b)　非对称算法性能容量标称值： RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 SM2 每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。

表20　容量管理 - 第三级（续）

评测要求	评测程序
6.4.2.1.1 容量标称	RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够生成的密钥对数量。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够生成的密钥对数量。 SM2 算法每秒能够生成的密钥对数量。 c)　摘要算法性能容量标称值： SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3 等摘要算法每秒能够处理的交易笔数。 d)　系统或加解密设备提供服务的最大并发数。
6.4.2.1.2 容量感知	系统在运行过程中，应能够感知以下运行指标： a)　系统是否达到或超出规定的数据流量上限。 b)　系统是否达到或超出规定的并发数上限。 c)　系统是否达到或超出 6.4.2.1.1 中 a)、b)规定的 TPS。
6.4.2.1.3 容量管理	在容量管理方面，应具备以下能力： a)　系统支持对 6.4.2.1.1 中的性能容量标称值进行扩容。 b)　系统支持对 6.4.2.1.1 中的性能容量标称值进行回收。
注：TPS（Transaction Per Second）指每秒能够处理的交易或事务的数量。	

6.4.2.2　高可用集群

第三级持续运行维度中，关于高可用集群的评价标准见表21。

表 21　高可用集群 - 第三级

评测要求	评测程序
6.4.2.2.1 集群管理	系统应达到以下集群管理的能力： a)　提供加解密服务的系统采用集群模式进行部署。 b)　能够获取集群内全部加解密设备、节点以及软件产品的清单。 c)　能够识别集群内加解密设备、节点以及软件产品是否处于正常工作状态。

6.4.2.3　监控告警

第三级持续运行维度中，关于监控告警的评价标准见表22。

表 22　监控告警 - 第三级

评测要求	评测程序
6.4.2.3.1 监控管理	监控管理应满足以下要求： a)　根据监控信息的特性，将监控告警信息进行分级，并将其作为启用不同应对策略的依据。 b)　设置监控管理岗位，其承担对监控系统自身的稳定性以及监控信息的覆盖率、准确性进行持续改进的职责。 c)　设置监控值守岗位，其承担第一时间分析处理监控告警信息的职责。
6.4.2.3.2 监控指标	监控指标应满足以下要求： a)　对加解密设备的硬件故障、配件故障有监控手段。 b)　定义加解密设备 CPU、内存、存储的监控指标，并对异常指标进行告警。 c)　定义池管理系统 CPU、内存、存储以及关键进程的监控指标，并对异常指标进行告警。
6.4.2.3.3 监控日志	监控日志应满足以下要求：

表22　监控告警 - 第三级（续）

评测要求	评测程序
6.4.2.3.3 监控日志	a)　生产环境下加解密设备或池管理系统的监控日志中，不含有密钥的明文或完整密文数据。 b)　生产环境下加解密设备或池管理系统的监控日志中，不含有与客户身份、账户相关的数据。
注：池管理系统的定义及表述详见表54。	

6.4.2.4　异常恢复

第三级持续运行维度中，关于异常恢复的评价标准见表23。

表 23　异常恢复 - 第三级

评测要求	评测程序
6.4.2.4.1 应急响应	应急响应应满足以下要求： a)　当监测到异常时，根据既定的应急预案和程序，启动应急处理流程。 b)　应急预案中，包含对业务影响的确认与判断程序。 c)　应急预案中，包含对系统节点或相关设备进行隔离或切换的指导和说明。 d)　应急预案中，包含对系统节点、计算资源或相关设备进行扩容的指导和说明。 e)　应急预案中，包含对系统节点、应用程序或相关设备进行重启的指导和说明。 f)　应急预案中，包含停止部分或全部服务的指导与说明。
6.4.2.4.2 问题管理	应具有对生产故障的根本原因进行跟踪和改进的程序和流程。

6.4.3　应用服务维度

6.4.3.1　算法支持

第三级应用服务维度中，关于算法支持的评价标准见表24。

表 24　算法支持 - 第三级

评测要求	评测程序
6.4.3.1.1 对称算法	加解密设备应支持或部分支持以下对称算法，并达到对应的强度： a)　加解密设备支持 SM4 算法。 b)　加解密设备支持 DES/3DES 算法，并达到 64 位、128 位、192 位强度。 c)　加解密设备支持 AES 算法，并达到 128 位、192 位、256 位强度。 d)　除非对端机构要求，否则不提供 DES-128 位或以下强度密钥的支持。
6.4.3.1.2 非对称算法	加解密设备应支持或部分支持以下非对称算法，并达到对应的强度： a)　加解密设备支持 SM2 算法。 b)　加解密设备支持 RSA 算法，并达到 1024 位、2048 位、3072 位、4096 位强度。 c)　加解密设备支持 ECC 算法，并达到 160 位、256 位、384 位、512 位强度。 d)　除非对端机构要求，否则不提供 RSA-1024 位、ECC-160 位或以下强度算法的支持。
6.4.3.1.3 摘要算法	加解密设备应支持或部分支持以下摘要算法，并达到对应的强度： a)　加解密设备支持 MD5 算法。 b)　加解密设备支持 SM3 算法。 c)　加解密设备支持 SHA 系列算法，并达到 SHA-1、SHA-256、SHA-384、SHA-512 强度。

表24　算法支持 - 第三级（续）

评测要求	评测程序
6.4.3.1.3 摘要算法	d)　除非对端机构要求，否则不提供低于 SHA-1、MD5 以下强度摘要算法的支持。

6.4.3.2　加解密接口

第三级应用服务维度中，关于加解密接口的评价标准见表25。

表 25　加解密接口 - 第三级

评测要求	评测程序
6.4.3.2.1 封装标准	加解密设备或对应的软件应可提供 API 接口。
6.4.3.2.2 场景支持	加解密设备的加解密接口应支持以下业务场景： a)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 CVV。 b)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 PINBLOCK 密文。 c)　对于服务于银行卡发卡系统的加解密设备，支持在芯片验证过程中动态计算卡片的 MDK。
注：CVV即安全校验码，是印在卡片背面在网络或电话等场景进行交易时使用的一种安全代码。MDK是发卡过程中用到的与卡片信息加密相关的一种密钥。	

6.4.4　安全管控维度

6.4.4.1　制度管理

第三级安全管控维度中，关于制度管理的评价标准见表26。

表 26　制度管理 - 第三级

评测要求	评测程序
6.4.4.1.1 规范定义	在规范和制度层面，应对以下环节、岗位和方法进行明确定义： a)　明确定义密钥的生命周期，其至少涵盖密钥或证书的生成、录入、分发、保存和销毁环节。 b)　明确定义涉及与不涉及密钥数据操作的场所、设备、介质和工具。 c)　明确定义密钥生命周期各个环节的操作、审批以及记录的流程。 d)　明确定义各个岗位的职责边界和权限，规定密钥明文分量的管理责任人，规定保险柜、密钥卡、USB KEY 等涉及密钥数据的介质相关联的钥匙和密码的管理责任所属及使用流程。 e)　明确定义密钥信息泄漏的判定方法以及相应的处理流程。 f)　明确定义应使用专用加解密设备处理的加解密场景。
6.4.4.1.2 人员要求	对于岗位和人员方面，应满足以下要求： a)　对称密钥的明文分量由不同的人员持有或管理。 b)　应不同的登录者配置不同的用户，并确保其唯一性。 c)　对涉密人员进行安全保密培训，并对培训进行记录。 d)　对密钥的所有操作进行授权审批并进行记录。
6.4.4.1.3 密钥操作管理	密钥操作管理应满足以下要求： a)　密钥分发过程含有人员身份认证、数据完整性校验措施。 b)　密钥分段、分人并在隔离状态下导入安全密码设备或系统，并对以上过程进行记录。

表26　制度管理 - 第三级（续）

评测要求	评测程序
6.4.4.1.3 密钥操作管理	c) 密钥导入现场的摄像监控设备拍摄不到密钥导入设备的操作面板部位。 d) 所有密钥分量导入完成后，有检验并核对密钥校验值的过程。 e) 对密钥的操作过程有记录，内容至少涵盖工单号、时间、地点、参与人员信息、操作事由、审批情况等。

6.4.4.2　访问控制

第三级安全管控维度中，关于访问控制的评价标准见表27。

表 27　访问控制 - 第三级

评测要求	评测程序
6.4.4.2.1 登录和认证	加解密设备和系统的登录和认证应满足以下要求： a) 维护人员进入设备机房时，采取事前审批措施，并对进出机房的人员进行记录。 b) 在执行密钥有关的维护操作时（LMK 除外），使用超级管理员（如 root、administrator）以外的用户。 c) 加解密设备或相关系统具有防止短时间内频繁尝试登录的技术措施。 d) 对登录鉴别口令的复杂度有明确要求。
6.4.4.2.2 用户管控	加解密设备或关联系统的用户管控应满足以下要求： a) 为不同的岗位角色配置不同的维护用户。 b) 具备用户管理体系，其至少包含用户的创建和注销、改密、锁定和解锁、授权流程。 c) 对用户可以登录设备或系统的场所作出规定。 d) 对用户改密的策略以及实施方式做出规定。 e) 授予用户登录权限时附加时效性，并可以在超出时效后收回用户权限。 f) 对于使用静态口令的用户登录方式，在收回用户权限后采取限制或改密措施，避免维护人员在未获允许的情况下使用相同用户及口令再次登录。
注：root、administrator均为常见的超级管理员用户。静态口令指固定的无法自动修改的口令。	

6.4.4.3　审计日志

第三级安全管控维度中，关于审计日志的评价标准见表28。

表 28　审计日志 - 第三级

评测要求	评测程序
6.4.4.3.1 日志内容	提供加解密服务的系统或加解密设备，应提供以下内容的日志： a) 日志中以能够还原事件过程为基本原则，至少包含工单号、时间、登录用户或人员身份信息、操作、授权、审批的内容信息。 b) 日志中不包含业务数据。 c) 配合系统维护的授权、审批、工单流转的过程留存凭证或日志。 d) 对于不支持记录和存储日志信息的加解密设备，采取对维护动作进行记录的方式保留日志。
6.4.4.3.2 日志保存	日志的保存应满足以下要求： a) 规定日志和凭证保留的期限，其最短不能少于 12 个月。

表28　审计日志 - 第三级（续）

评测要求	评测程序
6.4.4.3.2 日志保存	b)　在系统中存储的日志数据配备防篡改的技术手段。

6.4.5　密钥管理维度

6.4.5.1　加解密设备

第三级密钥管理维度中，关于加解密设备的评价标准见表29。

表 29　加解密设备 - 第三级

评测要求	评测程序
6.4.5.1.1 硬件要求	加解密设备的硬件应满足以下要求： a)　在提供加解密服务的系统中使用专用的加解密运算设备。 b)　设备支持双电源，且可以在不影响设备正常运行的条件下更换电源模块。 c)　设备的管理端口与业务端口物理分离。 d)　设备配备有不可拆卸的、用于多因素身份认证的装置。
6.4.5.1.2 资质要求	加解密设备的资质应满足以下要求： a)　密码机具备国家密码局授予的商用型号。 b)　签名验签服务器具备国家密码局授予的商用型号。 c)　如果系统仅用于涉外业务，可以没有国家密码局授予的型号。
6.4.5.1.3 设备管理	加解密设备的管理方式应满足以下要求： a)　从设备的管理端口登录设备管理界面，业务端口无法登录。 b)　如果通过管理端口接入带外管理网络，则带外管理网络与业务端口接入的网络环境保持隔离。 c)　采用多因素认证方式登录设备管理界面。登录过程使用 6.4.5.1.1 中 d)的装置和对应的媒介。

6.4.5.2　对称密钥

第三级密钥管理维度中，关于对称密钥的评价标准见表30。

表 30　对称密钥 - 第三级

评测要求	评测程序
6.4.5.2.1 密钥生成	对称密钥的生成过程应满足以下要求： a)　使用随机数生成算法产生密钥数据。 b)　加解密设备的多组密钥分量合成密钥的算法公开并可以复制。 c)　支持以 LMK、KEK 保护的形式生成并输出密钥数据。 d)　密钥生成操作在指定的物理隔离区域进行，该区域内的进出应进行授权管理。 e)　对密钥生成操作区域部署实时监控系统，监控系统避免拍摄输入设备的键盘。 f)　KEK、DEK 的明文或密文均通过加解密设备生成。 g)　如果采取明文分量方式向加解密设备录入 LMK，则在加解密设备内部将 LMK 进行分散后的值作为实际的本地加解密密钥进行运算。
6.4.5.2.2 密钥存储	对称密钥数据在系统中存储应满足以下要求：

表30　对称密钥 - 第三级（续）

评测要求	评测程序
6.4.5.2.2 密钥存储	a) 在加解密设备之外，不以明文或明文分量的形式存储密钥。 b) LMK 仅储存于加解密设备中。LMK 分量可存储于由加密设备配套的 IC 卡或者 USB KEY 等电子介质中。 c) 在加解密设备外以本地数据库或文件等形式存储的密钥使用 LMK 进行保护。
6.4.5.2.3 对称密钥使用	对称密钥在使用过程中应满足以下关系： a) LMK、KEK、DEK 不相同或混用。 b) 加解密设备不支持 LMK 明文的读取操作。 c) 系统间交互 DEK 时，使用 KEK 保护 DEK。 d) 系统间交互的需进行加密的数据，使用 DEK 进行保护。 e) 定义 KEK、DEK 的使用生命周期以及更换的流程。 f) 不同业务系统间采用不同的 KEK、DEK。
6.4.5.2.4 对称密钥分发	对称密钥的分发过程应满足以下要求： a) 对称密钥在分发之前对接收者的身份进行确认。 b) 对称密钥的多组明文分量的分发过程中，不使用相同的快递公司、相同的经办人员、相同时间的车次或航班。 c) 人工方式进行密钥分发时，不由同一人领取或携带多段密钥分量。 d) 对称密钥分发动作完成后，有检验并核对密钥校验值的过程。 e) 密钥分发过程中使用的密钥分量记录介质，在完成密钥分发后如果不用于备份，则采取无法恢复的方法进行销毁。
6.4.5.2.5 密钥备份	对称密钥的备份应满足以下要求： a) 不同成分的密钥分量由不同的备份人员保管，封装密钥分量明文的信封存放在不同的保险箱内。 b) 同一个人不具有全部加密资料或全部加密设备钥匙的控制权。 c) 纸介质的密钥明文分量封装在防拆、防篡改信封内或者使用防拆、防篡改封条，当需要使用时只有指定人员才可以拆阅信封，并对以上过程进行记录。 d) 对于密钥导入设备，由专人进行配置和维护，并对以上过程进行记录。 e) KEK 不备份，如 KEK 丢失，则对 KEK 重新生成和录入。 f) 对于保护数据本地存放的密钥，对其密钥分量进行备份。

6.4.5.3　非对称密钥

第三级密钥管理维度中，关于非对称密钥的评价标准见表31。

表 31　非对称密钥 - 第三级

评测要求	评测程序
6.4.5.3.1 生成密钥或证书	非对称密钥或证书的生成过程应满足以下要求： a) 非对称密钥对的生成方式保证私钥的机密性。 b) 生成新证书时，可以指定算法、算法强度和失效日期。 c) 业务使用的非对称密钥对通过指定的系统或专用加解密设备生成，并定义保管私钥副本的部门或岗位。 d) 规定合规的根证书颁发机构并明确应关联根证书的场景。

表31　非对称密钥 - 第三级（续）

评测要求	评测程序
6.4.5.3.1 生成密钥或证书	e)　对存储私钥数据的系统或设备登记并备案。
6.4.5.3.2 使用密钥或证书	非对称密钥或证书的使用和保存应满足以下要求： a)　从加解密设备或配套系统中获取私钥数据时使用加密手段。 b)　业务活动不涉及私钥数据的传输。
6.4.5.3.3 更换密钥或证书	非对称密钥或证书的更换应满足以下要求： a)　定义非对称密钥或证书的更换周期以及更换流程。 b)　业务使用的证书，其非对称密钥对的生命周期不超过 5 年。 c)　定义私钥泄漏的评判标准、补救措施和更新流程。 d)　具备根据原证书的密钥对及其失效时间重新生成新证书的流程和能力。

6.5　第四级

6.5.1　开发迭代维度

6.5.1.1　基础环境

第四级开发迭代维度中，关于基础环境的评价标准见表32。

表 32　基础环境 - 第四级

评测要求	评测程序
6.5.1.1.1 生产隔离性	对于生产与非生产环境和数据，应满足以下隔离性要求： a)　非生产环境与生产环境保持隔离，包括但不限于物理隔离。 b)　非生产环境使用的密钥和私钥数据与生产环境不混用。 c)　维护生产环境与非生产环境的专用加密网络通道不混用。 d)　生产环境与非生产环境不混用同一台加解密设备。

6.5.1.2　版本管理

第四级开发迭代维度中，关于版本管理的评价标准见表33。

表 33　版本管理 - 第四级

评测要求	评测程序
6.5.1.2.1 参数管理	以下数据应在生产环境中配置，不应编入代码或预编译进程序： a)　生产环境的 IP 地址信息。 b)　生产环境使用的密钥数据。 c)　生产环境使用的私钥数据。 d)　生产环境的网络端口信息。 e)　生产环境的证书数据。
6.5.1.2.2 代码介质管理	代码介质的管理应满足以下要求： a)　建立代码库，管理有关的代码以及编译后的程序。 b)　建立软件介质库，管理生产环境使用的软件产品。 c)　开发人员只能向代码库提交或更新代码，并使用代码库中的代码进行编译。

表33 版本管理 - 第四级（续）

评测要求	评测程序
6.5.1.2.2 代码介质管理	d) 软件测试以及生产投产过程中，从代码库、介质库中取得代码、程序以及软件。 e) 生产环境使用的密钥、证书数据不纳入代码库。

6.5.2 持续运行维度

6.5.2.1 容量管理

第四级持续运行维度中，关于容量管理的评价标准见表34。

表 34 容量管理 - 第四级

评测要求	评测程序
6.5.2.1.1 容量标称	提供加解密服务的系统或加解密设备，应规定以下性能容量标称值： a) 对称算法性能容量标称值： DES/3DES 算法 64 位、128 位、192 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 AES 算法 128 位、192 位、256 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 SM4 算法每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 b) 非对称算法性能容量标称值： RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 SM2 每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够生成的密钥对数量。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够生成的密钥对数量。 SM2 算法每秒能够生成的密钥对数量。 c) 摘要算法性能容量标称值： SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3 等摘要算法每秒能够处理的交易笔数。 d) 系统或加解密设备提供服务的最大并发数。
6.5.2.1.2 容量感知	系统在运行过程中，应能够感知以下运行指标： a) 系统是否达到或超出规定的数据流量上限。 b) 系统是否达到或超出规定的并发数上限。 c) 系统是否达到或超出 6.5.2.1.1 中 a)、b)规定的 TPS。 d) 系统提供公私钥预生成和缓存机制，并可感知缓存数据量情况。
6.5.2.1.3 容量管理	在容量管理方面，应具备以下能力： a) 在不影响对外服务的情况下，对 6.5.2.1.1 中的性能容量标称值进行扩容。 b) 在不影响对外服务的情况下，对 6.5.2.1.1 中的性能容量标称值进行回收。

6.5.2.2 高可用集群

第四级持续运行维度中，关于高可用集群的评价标准见表35。

表 35　高可用集群 - 第四级

评测要求	评测程序
6.5.2.2.1 集群管理	系统应达到以下集群管理的能力： a)　提供加解密服务的系统采用集群模式进行部署。 b)　能够获取集群内全部加解密设备、节点以及软件产品的清单。 c)　能够识别集群内加解密设备、节点以及软件产品是否处于正常工作状态。 d)　在不影响业务服务的情况下，纳入或剔除加解密设备。 e)　在不影响业务服务的情况下，纳入或剔除节点。 f)　如果集群采用控制中心加执行节点的设计，在控制中心失效后，不影响业务接入。

6.5.2.3　监控告警

第四级持续运行维度中，关于监控告警的评价标准见表36。

表 36　监控告警 - 第四级

评测要求	评测程序
6.5.2.3.1 监控管理	监控管理应满足以下要求： a)　根据监控信息的特性，将监控告警信息进行分级，并将其作为启用不同应对策略的依据。 b)　设置监控管理岗位，其承担对监控系统自身的稳定性以及监控信息的覆盖率、准确性进行持续改进的职责。 c)　设置监控值守岗位，其承担第一时间分析处理监控告警信息的职责。 d)　定义影响对外服务、涉及安全泄密或其他重大影响的监控事件，并对这些监控事件的响应时效性进行要求。 e)　对于监控告警信息具备主动触发和报送通知的能力，通知形式包括但不限于邮件、短信、语音等。
6.5.2.3.2 监控指标	监控指标应满足以下要求： a)　对加解密设备，具备能够确认设备加解密功能模块工作正常的监控或巡检手段。 b)　池管理系统能够监控加解密设备响应时间，定义响应时间的监控指标，并对异常指标进行告警。 c)　设备具备非对称密钥或证书的预生成和缓存功能时，定义设备内非对称密钥或证书缓存告警指标，并对异常指标进行告警。
6.5.2.3.3 监控日志	监控日志应满足以下要求： a)　生产环境下加解密设备或池管理系统的监控日志中，不含有密钥的明文或完整密文数据。 b)　生产环境下加解密设备或池管理系统的监控日志中，不含有与客户身份、账户相关的数据。 c)　对于为解决生产问题额外收集而留在设备或系统中的数据，有过期清理的机制和要求。 d)　生产环境下池管理系统的监控日志中，可获取访问本系统的历史记录。

6.5.2.4　异常恢复

第四级持续运行维度中，关于异常恢复的评价标准见表37。

表 37　异常恢复 - 第四级

评测要求	评测程序
6.5.2.4.1 应急响应	应急响应应满足以下要求： a) 当监测到异常时，根据既定的应急预案和程序，启动应急处理流程。 b) 应急预案中，包含对业务影响的确认与判断程序。 c) 应急预案中，包含对系统节点或相关设备进行隔离或切换的指导和说明。 d) 应急预案中，包含对系统节点、计算资源或相关设备进行扩容的指导和说明。 e) 应急预案中，包含对系统节点、应用程序或相关设备进行重启的指导和说明。 f) 应急预案中，包含停止部分或全部服务的指导与说明。 g) 应急预案中，包含发生异常时收集信息、日志的指导与说明。
6.5.2.4.2 问题管理	应具有对生产故障的根本原因进行跟踪和改进的程序和流程。

6.5.3 应用服务维度

6.5.3.1 算法支持

第四级应用服务维度中，关于算法支持的评价标准见表38。

表 38 算法支持 - 第四级

评测要求	评测程序
6.5.3.1.1 对称算法	加解密设备应支持或部分支持以下对称算法，并达到对应的强度： a) 加解密设备支持 SM4 算法。 b) 加解密设备支持 DES/3DES 算法，并达到 64 位、128 位、192 位强度。 c) 加解密设备支持 AES 算法，并达到 128 位、192 位、256 位强度。 d) 除非对端机构要求，否则不提供 DES-128 位或以下强度密钥的支持。
6.5.3.1.2 非对称算法	加解密设备应支持或部分支持以下非对称算法，并达到对应的强度： a) 加解密设备支持 SM2 算法。 b) 加解密设备支持 RSA 算法，并达到 1024 位、2048 位、3072 位、4096 位强度。 c) 加解密设备支持 ECC 算法，并达到 160 位、256 位、384 位、512 位强度。 d) 除非对端机构要求，否则不提供 RSA-1024 位、ECC-160 位或以下强度算法的支持。
6.5.3.1.3 摘要算法	加解密设备应支持或部分支持以下摘要算法，并达到对应的强度： a) 加解密设备支持 MD5 算法。 b) 加解密设备支持 SM3 算法。 c) 加解密设备支持 SHA 系列算法，并达到 SHA-1、SHA-256、SHA-384、SHA-512 强度。 d) 除非对端机构要求，否则不提供低于 SHA-1、MD5 以下强度摘要算法的支持。

6.5.3.2 加解密接口

第四级应用服务维度中，关于加解密接口的评价标准见表39。

表 39 加解密接口 - 第四级

评测要求	评测程序
6.5.3.2.1 封装标准	加解密设备或对应的软件应满足以下的接口封装要求： a) 可提供加解密设备的接口指令或 API 规范文档。 b) 如果使用签名验签服务，可提供相应的接口或 API 规范文档。 c) 如果使用数字信封，可提供相应的接口或 API 规范文档。

表39　加解密接口 - 第四级（续）

评测要求	评测程序
6.5.3.2.2 场景支持	加解密设备的加解密接口应支持以下业务场景： a)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 CVV。 b)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 PINBLOCK 密文。 c)　对于服务于银行卡发卡系统的加解密设备，支持在芯片验证过程中动态计算卡片的 MDK。 d)　加解密设备或系统解析明文的接口或指令可根据需要进行限制或关闭。

6.5.4　安全管控维度

6.5.4.1　制度管理

第四级安全管控维度中，关于制度管理的评价标准见表40。

表 40　制度管理 - 第四级

评测要求	评测程序
6.5.4.1.1 规范定义	在规范和制度层面，应对以下环节、岗位和方法进行明确定义： a)　明确定义密钥的生命周期，其至少涵盖密钥或证书的生成、录入、分发、保存和销毁环节。 b)　明确定义涉及与不涉及密钥数据操作的场所、设备、介质和工具。 c)　明确定义密钥生命周期各个环节的操作、审批以及记录的流程。 d)　明确定义各个岗位的职责边界和权限，规定密钥明文分量的管理责任人，规定保险柜、密钥卡、USB KEY 等涉及密钥数据的介质相关联的钥匙和密码的管理责任所属和使用流程。 e)　明确定义密钥信息泄漏的判定方法以及相应的处理流程。 f)　明确定义应使用专用加解密设备处理的加解密场景。
6.5.4.1.2 人员要求	对于岗位和人员方面，应满足以下要求： a)　对称密钥的明文分量由不同的人员持有或管理。 b)　为不同的登录者配置不同的用户，并确保其唯一性。 c)　对涉密人员进行安全保密培训，并对培训进行记录。 d)　对密钥的所有操作进行授权审批并进行记录。
6.5.4.1.3 密钥操作管理	密钥操作管理应满足以下要求： a)　密钥分发过程含有人员身份认证、数据完整性校验措施。 b)　密钥分段、分人并在隔离状态下导入安全密码设备或系统，并对以上过程进行记录。 c)　密钥导入现场的摄像监控设备拍摄不到密钥导入设备的操作面板部位。 d)　所有密钥分量导入完成后，有检验并核对密钥校验值的过程。 e)　对密钥的操作过程有记录，内容至少涵盖工单号、时间、地点、参与人员信息、操作事由、审批情况等。

6.5.4.2　访问控制

第四级安全管控维度中，关于访问控制的评价标准见表41。

表 41　访问控制 - 第四级

评测要求	评测程序
6.5.4.2.1 登录和认证	加解密设备和系统的登录和认证应满足以下要求： a) 维护人员进入设备机房时，采取事前审批措施，并对进出机房的人员进行记录。 b) 在执行密钥有关的维护操作时（LMK 除外），使用超级管理员（如 root、administrator）以外的用户。 c) 加解密设备或相关系统具有防止短时间内频繁尝试登录的技术措施。 d) 对登录鉴别口令的复杂度有明确要求。
6.5.4.2.2 用户管控	加解密设备或关联系统的用户管控应满足以下要求： a) 为不同的岗位角色配置不同的维护用户。 b) 具备用户管理体系，其至少包含用户的创建和注销、改密、锁定和解锁、授权流程。 c) 对用户可以登录设备或系统的场所作出规定。 d) 对用户改密的策略以及实施方式做出规定。 e) 授予用户登录权限时附加时效性，并可以在超出时效后收回用户权限。 f) 对于使用静态口令的用户登录方式，在收回用户权限后采取限制或改密措施，避免维护人员在未获允许的情况下使用相同用户及口令再次登录。

6.5.4.3 审计日志

第四级安全管控维度中，关于审计日志的评价标准见表42。

表 42 审计日志 - 第四级

评测要求	评测程序
6.5.4.3.1 日志内容	提供加解密服务的系统或加解密设备，应提供以下内容的日志： a) 日志中以能够还原事件过程为基本原则，至少包含工单号、时间、登录用户或人员身份信息、操作、授权、审批的内容信息。 b) 日志中不包含业务数据。 c) 配合系统维护的授权、审批、工单流转的过程留存凭证或日志。 d) 对于不支持记录和存储日志信息的加解密设备，采取对维护动作进行记录的方式保留日志。
6.5.4.3.2 日志保存	日志的保存应满足以下要求： a) 规定日志和凭证保留的期限，其最短不能少于 12 个月。 b) 在系统中存储的日志数据配备防篡改的技术手段。

6.5.5 密钥管理维度

6.5.5.1 加解密设备

第四级密钥管理维度中，关于加解密设备的评价标准见表43。

表 43 加解密设备 - 第四级

评测要求	评测程序
6.5.5.1.1 硬件要求	加解密设备的硬件应满足以下要求： a) 在提供加解密服务的系统中使用专用的加解密运算设备。 b) 设备支持双电源，且可以在不影响设备正常运行的条件下更换电源模块。 c) 设备的管理端口与业务端口物理分离。

表43　加解密设备 - 第四级（续）

评测要求	评测程序
6.5.5.1.1 硬件要求	d)　设备配备有不可拆卸的、用于多因素身份认证的装置。 e)　设备配备有不可拆卸的、用于销毁其内部密钥数据的装置。
6.5.5.1.2 资质要求	加解密设备的资质应满足以下要求： a)　密码机具备国家密码局授予的商用型号。 b)　签名验签服务器具备国家密码局授予的商用型号。 c)　如果系统仅用于涉外业务，可以没有国家密码局授予的型号。
6.5.5.1.3 设备管理	加解密设备的管理方式应满足以下要求： a)　从设备的管理端口登录设备管理界面，业务端口无法登录。 b)　如果通过管理端口接入带外管理网络，则带外管理网络与业务端口接入的网络环境保持隔离。 c)　采用多因素认证方式登录设备管理界面。登录过程使用 6.5.5.1.1 中 d)的装置和对应的媒介。 d)　在导入密钥或输入密码时，不在操作界面上显示明文。 e)　设定销毁设备内部数据的条件和流程。销毁数据的过程使用 6.5.5.1.1 中 e)的装置。

6.5.5.2　对称密钥

第四级密钥管理维度中，关于对称密钥的评价标准见表44。

表 44　对称密钥 - 第四级

评测要求	评测程序
6.5.5.2.1 密钥生成	对称密钥的生成过程应满足以下要求： a)　使用随机数生成算法产生密钥数据。 b)　加解密设备的多组密钥分量合成密钥的算法公开并可以复制。 c)　支持以 LMK、KEK 保护的形式生成并输出密钥数据。 d)　密钥生成操作在指定的物理隔离区域进行，该区域内的进出应进行授权管理。 e)　应对密钥生成操作区域部署实时监控系统，监控系统避免拍摄输入设备的键盘。 f)　KEK、DEK 的明文或密文均通过加解密设备生成。 g)　如果采取明文分量方式向加解密设备录入 LMK，则在加解密设备内部将 LMK 进行分散后的值作为实际的本地加解密密钥进行运算。
6.5.5.2.2 密钥存储	对称密钥数据在系统中存储应满足以下要求： a)　在加解密设备之外，不以明文或明文分量的形式存储密钥。 b)　LMK 仅储存于加解密设备中。LMK 分量可存储于由加密设备配套的 IC 卡或者 USB KEY 等电子介质中。 c)　在加解密设备外以本地数据库或文件等形式存储的密钥使用 LMK 进行保护。 d)　DEK 和 KEK 不存储在加解密设备中。
6.5.5.2.3 对称密钥使用	对称密钥在使用过程中应满足以下关系： a)　LMK、KEK、DEK 不相同或混用。 b)　加解密设备不支持 LMK 明文的读取操作。 c)　系统间交互 DEK 时，使用 KEK 保护 DEK。 d)　系统间交互的需进行加密的数据，使用 DEK 进行保护。

表44　对称密钥 - 第四级（续）

评测要求	评测程序
6.5.5.2.3 对称密钥使用	e)　定义 KEK、DEK 的使用生命周期以及更换的流程。 f)　不同业务系统间采用不同的 KEK、DEK。
6.5.5.2.4 对称密钥分发	对称密钥的分发过程应满足以下要求： a)　对称密钥在分发之前对接收者的身份进行确认。 b)　对称密钥的多组明文分量的分发过程中，不使用相同的快递公司、相同的经办人员、相同时间的车次或航班。 c)　人工方式进行密钥分发时，不由同一人领取或携带多段密钥分量。 d)　对称密钥分发动作完成后，有检验并核对密钥校验值的过程。 e)　密钥分发过程中使用的密钥分量记录介质，在完成密钥分发后如果不用于备份，则采取无法恢复的方法进行销毁。
6.5.5.2.5 密钥备份	对称密钥的备份应满足以下要求： a)　不同成分的密钥分量由不同的备份人员保管，封装密钥分量明文的信封存放在不同的保险箱内。 b)　同一个人不具有全部加密资料或全部加密设备钥匙的控制权。 c)　纸介质的密钥明文分量封装在防拆、防篡改信封内或者使用防拆、防篡改封条，当需要使用时只有指定人员才可以拆阅信封，并对以上过程进行记录。 d)　对于密钥导入设备，由专人进行配置和维护，并对以上过程进行记录。 e)　KEK 不备份，如 KEK 丢失，则对 KEK 重新生成和录入。 f)　对于保护数据本地存放的密钥，对其密钥分量进行备份。

6.5.5.3　非对称密钥

第四级密钥管理维度中，关于非对称密钥的评价标准见表45。

表 45　非对称密钥 - 第四级

评测要求	评测程序
6.5.5.3.1 生成密钥或证书	非对称密钥或证书的生成过程应满足以下要求： a)　非对称密钥对的生成方式保证私钥的机密性。 b)　生成新证书时，可以指定算法、算法强度和失效日期。 c)　业务使用的非对称密钥对通过指定的系统或专用加解密设备生成，并定义保管私钥副本的部门或岗位。 d)　规定合规的根证书颁发机构并明确应关联根证书的场景。 e)　对存储私钥数据的系统或设备登记并备案。
6.5.5.3.2 使用密钥或证书	非对称密钥或证书的使用和保存应满足以下要求： a)　从加解密设备或配套系统中获取私钥数据时使用加密手段。 b)　业务活动不涉及私钥数据的传输。
6.5.5.3.3 更换密钥或证书	非对称密钥或证书的更换应满足以下要求： a)　定义非对称密钥或证书的更换周期以及更换流程。 b)　业务使用的证书，其非对称密钥对的生命周期不超过 5 年。 c)　定义私钥泄漏的评判标准、补救措施和更新流程。 d)　具备根据原证书的密钥对及其失效时间重新生成新证书的流程和能力。

6.6 第五级

6.6.1 开发迭代维度

6.6.1.1 基础环境

第五级开发迭代维度中，关于基础环境的评价标准见表46。

表 46 基础环境 - 第五级

评测要求	评测程序
6.6.1.1.1 生产隔离性	对于生产与非生产环境和数据，应满足以下隔离性要求： a) 非生产环境与生产环境保持隔离，包括但不限于物理隔离。 b) 非生产环境使用的密钥和私钥数据与生产环境不混用。 c) 维护生产环境与非生产环境的专用加密网络通道不混用。 d) 生产环境与非生产环境不混用同一台加解密设备。

6.6.1.2 版本管理

第五级开发迭代维度中，关于版本管理的评价标准见表47。

表 47 版本管理 - 第五级

评测要求	评测程序
6.6.1.2.1 参数管理	以下数据应在生产环境中配置，不应编入代码或预编译进程序： a) 生产环境的 IP 地址信息。 b) 生产环境使用的密钥数据。 c) 生产环境使用的私钥数据。 d) 生产环境的网络端口信息。 e) 生产环境的证书数据。
6.6.1.2.2 代码介质管理	代码介质的管理应满足以下要求： a) 建立代码库，管理有关的代码以及编译后的程序。 b) 建立软件介质库，管理生产环境使用的软件产品。 c) 开发人员只能向代码库提交或更新代码，并使用代码库中的代码进行编译。 d) 软件测试以及生产投产过程中，从代码库、介质库中取得代码、程序以及软件。 e) 生产环境使用的密钥、证书数据不纳入代码库。

6.6.2 持续运行维度

6.6.2.1 容量管理

第五级持续运行维度中，关于容量管理的评价标准见表48。

表 48 容量管理 - 第五级

评测要求	评测程序
6.6.2.1.1 容量标称	提供加解密服务的系统或加解密设备，应规定以下性能容量标称值： a) 对称算法性能容量标称值： DES/3DES 算法 64 位、128 位、192 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC

表48　容量管理 - 第五级（续）

评测要求	评测程序
6.6.2.1.1 容量标称	计算/数据加解密的交易笔数。 AES 算法 128 位、192 位、256 位密钥长度每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 SM4 算法每秒能够处理的 PINBLOCK 密文转换/MAC 计算/数据加解密的交易笔数。 b) 非对称算法性能容量标称值： RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 SM2 每秒能够处理的公钥加密/私钥解密/私钥签名/公钥验证签名的交易笔数。 RSA 算法 1024 位、2048 位、3072 位、4096 位密钥长度每秒能够生成的密钥对数量。 ECC 算法 160 位、256 位、384 位、512 位密钥长度每秒能够生成的密钥对数量。 SM2 算法每秒能够生成的密钥对数量。 c) 摘要算法性能容量标称值： SHA-1、SHA-256、SHA-384、SHA-512、MD5、SM3 等摘要算法每秒能够处理的交易笔数。 d) 系统或加解密设备提供服务的最大并发数。
6.6.2.1.2 容量感知	系统在运行过程中，应能够感知以下运行指标： a) 系统是否达到或超出规定的数据流量上限。 b) 系统是否达到或超出规定的并发数上限。 c) 系统是否达到或超出 6.6.2.1.1 中 a)、b)规定的 TPS。 d) 系统提供公私钥预生成和缓存机制，并可感知缓存数据量情况。
6.6.2.1.3 容量管理	在容量管理方面，应具备以下能力： a) 在不影响对外服务的情况下，对 6.6.2.1.1 中的性能容量标称值进行扩容。 b) 在不影响对外服务的情况下，对 6.6.2.1.1 中的性能容量标称值进行回收。

6.6.2.2　高可用集群

第五级持续运行维度中，关于高可用集群的评价标准见表49。

表 49　高可用集群 - 第五级

评测要求	评测程序
6.6.2.2.1 集群管理	系统应达到以下集群管理的能力： a) 提供加解密服务的系统采用集群模式进行部署。 b) 能够获取集群内全部加解密设备、节点以及软件产品的清单。 c) 能够识别集群内加解密设备、节点以及软件产品是否处于正常工作状态。 d) 在不影响业务服务的情况下，纳入或剔除加解密设备。 e) 在不影响业务服务的情况下，纳入或剔除节点。 f) 如果集群采用控制中心加执行节点的设计，在控制中心失效后，不影响业务接入。

6.6.2.3　监控告警

第五级持续运行维度中，关于监控告警的评价标准见表50。

表 50　监控告警 – 第五级

评测要求	评测程序
6.6.2.3.1 监控管理	监控管理应满足以下要求： a)　根据监控信息的特性，将监控告警信息进行分级，并将其作为启用不同应对策略的依据。 b)　设置监控管理岗位，其承担对监控系统自身的稳定性以及监控信息的覆盖率、准确性进行持续改进的职责。 c)　设置监控值守岗位，其承担第一时间分析处理监控告警信息的职责。 d)　定义影响对外服务、涉及安全泄密或其他重大影响的监控事件，并对这些监控事件的响应时效性进行要求。 e)　对于监控告警信息具备主动触发和报送通知的能力，通知形式包括但不限于邮件、短信、语音等。
6.6.2.3.2 监控指标	监控指标应满足以下要求： a)　对加解密设备，具备能够确认设备加解密功能模块工作正常的监控或巡检手段。 b)　池管理系统能够监控加解密设备响应时间，定义响应时间的监控指标，并对异常指标进行告警。 c)　设备具备非对称密钥或证书的预生成和缓存功能时，定义设备内非对称密钥或证书缓存告警指标，并对异常指标进行告警。
6.6.2.3.3 监控日志	监控日志应满足以下要求： a)　生产环境下加解密设备或池管理系统的监控日志中，不含有密钥的明文或完整密文数据。 b)　生产环境下加解密设备或池管理系统的监控日志中，不含有与客户身份、账户相关的数据。 c)　对于为解决生产问题额外收集而留在设备或系统中的数据，有过期清理的机制和要求。 d)　生产环境下池管理系统的监控日志中，可获取访问本系统的历史记录。

6.6.2.4　异常恢复

第五级持续运行维度中，关于异常恢复的评价标准见表51。

表 51　异常恢复 – 第五级

评测要求	评测程序
6.6.2.4.1 应急响应	应急响应应满足以下要求： a)　当监测到异常时，根据既定的应急预案和程序，启动应急处理流程。 b)　应急预案中，包含对业务影响的确认与判断程序。 c)　应急预案中，包含对系统节点或相关设备进行隔离或切换的指导和说明。 d)　应急预案中，包含对系统节点、计算资源或相关设备进行扩容的指导和说明。 e)　应急预案中，包含对系统节点、应用程序或相关设备进行重启的指导和说明。 f)　应急预案中，包含停止部分或全部服务的指导与说明。 g)　应急预案中，包含发生异常时收集信息、日志的指导与说明。
6.6.2.4.2 灾难与恢复	为应对如地质灾害等不可抗力的损失，灾难与恢复应满足以下要求： a)　除主要的数据中心外，在位于其他地点的数据中心有数据级备份站点、或系统级备份站点、或双活站点。 b)　如果建设了数据级或系统级备份站点，则主中心与备份中心有数据同步机制，并按计划执行数据同步。

表51　异常恢复 - 第五级（续）

评测要求	评测程序
6.6.2.4.2 灾难与恢复	c)　如果建设了数据级或系统级备份站点，则具备数据从备份站点恢复至主站点的方案。 d)　对于加密服务系统，备份的密钥数据在主数据中心和备份数据中心分别存储多个副本。
6.6.2.4.3 问题管理	应具有对生产故障的根本原因进行跟踪和改进的程序和流程。

6.6.3　应用服务维度

6.6.3.1　算法支持

第五级应用服务维度中，关于算法支持的评价标准见表52。

表 52　算法支持 - 第五级

评测要求	评测程序
6.6.3.1.1 对称算法	加解密设备应支持或部分支持以下对称算法，并达到对应的强度： a)　加解密设备支持 SM4 算法。 b)　加解密设备支持 DES/3DES 算法，并达到 64 位、128 位、192 位强度。 c)　加解密设备支持 AES 算法，并达到 128 位、192 位、256 位强度。 d)　除非对端机构要求，否则不提供 DES-128 位或以下强度密钥的支持。
6.6.3.1.2 非对称算法	加解密设备应支持或部分支持以下非对称算法，并达到对应的强度： a)　加解密设备支持 SM2 算法。 b)　加解密设备支持 RSA 算法，并达到 1024 位、2048 位、3072 位、4096 位强度。 c)　加解密设备支持 ECC 算法，并达到 160 位、256 位、384 位、512 位强度。 d)　除非对端机构要求，否则不提供 RSA-1024 位、ECC-160 位或以下强度算法的支持。
6.6.3.1.3 摘要算法	加解密设备应支持或部分支持以下摘要算法，并达到对应的强度： a)　加解密设备支持 MD5 算法。 b)　加解密设备支持 SM3 算法。 c)　加解密设备支持 SHA 系列算法，并达到 SHA-1、SHA-256、SHA-384、SHA-512 强度。 d)　除非对端机构要求，否则不提供低于 SHA-1、MD5 以下强度摘要算法的支持。

6.6.3.2　加解密接口

第五级应用服务维度中，关于加解密接口的评价标准见表53。

表 53　加解密接口 - 第五级

评测要求	评测程序
6.6.3.2.1 封装标准	加解密设备或对应的软件应满足以下的接口封装要求： a)　可提供加解密设备的接口指令或 API 规范文档。 b)　如果使用签名验签服务，可提供相应的接口或 API 规范文档。 c)　如果使用数字信封，可提供相应的接口或 API 规范文档。 d)　加解密设备或对应的软件应参考并遵循 GM/T0019。
6.6.3.2.2 场景支持	加解密设备的加解密接口应支持以下业务场景： a)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 CVV。 b)　对于服务于银行卡发卡系统的加解密设备，支持不计算明文的方式验证 PINBLOCK 密文。

表53　加解密接口 - 第五级（续）

评测要求	评测程序
6.6.3.2.2 场景支持	c)　对于服务于银行卡发卡系统的加解密设备，支持在芯片验证过程中动态计算卡片的 MDK。 d)　加解密设备或系统解析明文的接口或指令可根据需要进行限制或关闭。

6.6.3.3　资源池管理

第五级应用服务维度中，关于资源池管理的评价标准见表54。

表 54　资源池管理 - 第五级

评测要求	评测程序
6.6.3.3.1 设备资源池	维护多套使用加解密服务的业务系统时，使用多套加解密设备，形成加解密设备的资源池。资源池的设备管理应满足以下要求： a)　资源池之间不共享加解密设备。 b)　对接入资源池的接口、架构或业务类型进行定义。
6.6.3.3.2 池管理系统	对加解密设备资源池进行调用和管理的软件系统称为池管理系统。池管理系统应满足以下要求： a)　池管理系统具备白名单功能，拒绝名单外的用户或服务器等对加解密设备的访问。 b)　池管理系统提供性能容量的上限指标，并可监控这些指标。 c)　部署池管理系统的服务器采取多因素验证的方式进行身份认证。 d)　部署池管理系统的服务器具有操作审计日志，并保留一年以上。 e)　如果池管理系统采用控制中心加执行节点的设计，控制中心有备份，单个执行节点失效不影响业务接入。 f)　池管理系统应遵循 GM/T 0054。
6.6.3.3.3 主密钥安全域	在多个业务系统共享加解密设备的情况下，应对主密钥 LMK 的分布做出规划，划分为不同的主密钥安全域，并遵循以下原则： a)　不同的主密钥安全域不使用相同的本地设备主密钥 LMK。 b)　至少定义一个以上的安全域，即不让所有业务系统共享同一把主密钥。 c)　定义不同业务系统所属的主密钥安全域，通过安全域的划分减少主密钥泄漏事故带来的业务损失。

6.6.4　安全管控维度

6.6.4.1　制度管理

第五级安全管控维度中，关于制度管理的评价标准见表55。

表 55　制度管理 - 第五级

评测要求	评测程序
6.6.4.1.1 规范定义	在规范和制度层面，应对以下环节、岗位和方法进行明确定义： a)　明确定义密钥的生命周期，其至少涵盖密钥或证书的生成、录入、分发、保存和销毁环节。 b)　明确定义涉及与不涉及密钥数据操作的场所、设备、介质和工具。 c)　明确定义密钥生命周期各个环节的操作、审批以及记录的流程。

表55　制度管理 - 第五级（续）

评测要求	评测程序
6.6.4.1.1 规范定义	d)　明确定义各个岗位的职责边界和权限，规定密钥明文分量的管理责任人，规定保险柜、密钥卡、USB KEY 等涉及密钥数据的介质相关联的钥匙和密码的管理责任所属和使用流程。 e)　明确定义密钥信息泄漏的判定方法以及相应的处理流程。 f)　明确定义应使用专用加解密设备处理的加解密场景。
6.6.4.1.2 人员要求	对于岗位和人员方面，应满足以下要求： a)　对称密钥的明文分量由不同的人员持有或管理。 b)　为不同的登录者配置不同的用户，并确保其唯一性。 c)　对涉密人员进行安全保密培训，并对培训进行记录。 d)　对密钥的所有操作进行授权审批并进行记录。
6.6.4.1.3 密钥操作管理	密钥操作管理应满足以下要求： a)　密钥分发过程含有人员身份认证、数据完整性校验措施。 b)　密钥分段、分人并在隔离状态下导入安全密码设备或系统，并对以上过程进行记录。 c)　密钥导入现场的摄像监控设备拍摄不到密钥导入设备的操作面板部位。 d)　所有密钥分量导入完成后，有检验并核对密钥校验值的过程。 e)　对密钥的操作过程有记录，内容至少涵盖工单号、时间、地点、参与人员信息、操作事由、审批情况等。

6.6.4.2　访问控制

第五级安全管控维度中，关于访问控制的评价标准见表56。

表 56　访问控制 - 第五级

评测要求	评测程序
6.6.4.2.1 登录和认证	加解密设备和系统的登录和认证应满足以下要求： a)　维护人员进入设备机房时，采取事前审批措施，并对进出机房的人员进行记录。 b)　在执行密钥有关的维护操作时（LMK 除外），使用超级管理员（如 root、administrator）以外的用户。 c)　加解密设备或相关系统具有防止短时间内频繁尝试登录的技术措施。 d)　对登录鉴别口令的复杂度有明确要求。
6.6.4.2.2 用户管控	加解密设备或关联系统的用户管控应满足以下要求： a)　为不同的岗位角色配置不同的维护用户。 b)　具备用户管理体系，其至少包含用户的创建和注销、改密、锁定和解锁、授权流程。 c)　对用户可以登录设备或系统的场所作出规定。 d)　对用户改密的策略以及实施方式做出规定。 e)　授予用户登录权限时附加时效性，并可以在超出时效后收回用户权限。 f)　对于使用静态口令的用户登录方式，在收回用户权限后采取限制或改密措施，避免维护人员在未获允许的情况下使用相同用户及口令再次登录。

6.6.4.3　审计日志

第五级安全管控维度中，关于审计日志的评价标准见表57。

表 57　审计日志 – 第五级

评测要求	评测程序
6.6.4.3.1 日志内容	提供加解密服务的系统或加解密设备，应提供以下内容的日志： a)　日志中以能够还原事件过程为基本原则，至少包含工单号、时间、登录用户或人员身份信息、操作、授权、审批的内容信息。 b)　日志中不包含业务数据。 c)　配合系统维护的授权、审批、工单流转的过程留存凭证或日志。 d)　对于不支持记录和存储日志信息的加解密设备，采取对维护动作进行记录的方式保留日志。
6.6.4.3.2 日志保存	日志的保存应满足以下要求： a)　规定日志和凭证保留的期限，其最短不能少于 12 个月。 b)　在系统中存储的日志数据配备防篡改的技术手段。

6.6.5　密钥管理维度

6.6.5.1　加解密设备

第五级密钥管理维度中，关于加解密设备的评价标准见表58。

表 58　加解密设备 – 第五级

评测要求	评测程序
6.6.5.1.1 硬件要求	加解密设备的硬件应满足以下要求： a)　在提供加解密服务的系统中使用专用的加解密运算设备。 b)　设备支持双电源，且可以在不影响设备正常运行的条件下更换电源模块。 c)　设备的管理端口与业务端口物理分离。 d)　设备配备有不可拆卸的、用于多因素身份认证的装置。 e)　设备配备有不可拆卸的、用于销毁其内部密钥数据的装置。
6.6.5.1.2 资质要求	加解密设备的资质应满足以下要求： a)　密码机具备国家密码局授予的商用型号。 b)　签名验签服务器具备国家密码局授予的商用型号。 c)　如果系统仅用于涉外业务，可以没有国家密码局授予的型号。 d)　设备为国内自主研发，具备自主可控能力。
6.6.5.1.3 设备管理	加解密设备的管理方式应满足以下要求： a)　从设备的管理端口登录设备管理界面，业务端口无法登录。 b)　如果通过管理端口接入带外管理网络，则带外管理网络与业务端口接入的网络环境保持隔离。 c)　采用多因素认证方式登录设备管理界面。登录过程使用 6.6.5.1.1 中 d)的装置和对应的媒介。 d)　在导入密钥或输入密码时，不在操作界面上显示明文。 e)　设定了销毁设备内部数据的条件和流程。销毁数据的过程使用 6.6.5.1.1 中 e)的装置。

6.6.5.2　对称密钥

第五级密钥管理维度中，关于对称密钥的评价标准见表59。

表 59　对称密钥 - 第五级

评测要求	评测程序
6.6.5.2.1 密钥生成	对称密钥的生成过程应满足以下要求： a) 使用随机数生成算法产生密钥数据。 b) 加解密设备的多组密钥分量合成密钥的算法公开并可以复制。 c) 支持以 LMK、KEK 保护的形式生成并输出密钥数据。 d) 密钥生成操作在指定的物理隔离区域进行，该区域内的进出应进行授权管理。 e) 对密钥生成操作区域部署实时监控系统，监控系统避免拍摄输入设备的键盘。 f) KEK、DEK 的明文或密文均通过加解密设备生成。 g) 如果采取明文分量方式向加解密设备录入 LMK，则在加解密设备内部将 LMK 进行分散后的值作为实际的本地加解密密钥进行运算。
6.6.5.2.2 密钥存储	对称密钥数据在系统中存储应满足以下要求： a) 在加解密设备之外，不以明文或明文分量的形式存储密钥。 b) LMK 仅储存于加解密设备中。LMK 分量可存储于由加密设备配套的 IC 卡或者 USB KEY 等电子介质中。 c) 在加解密设备外以本地数据库或文件等形式存储的密钥使用 LMK 进行保护。 d) DEK 和 KEK 不存储在加解密设备中。
6.6.5.2.3 对称密钥使用	对称密钥在使用过程中应满足以下关系： a) LMK、KEK、DEK 不相同或混用。 b) 加解密设备不支持 LMK 明文的读取操作。 c) 系统间交互 DEK 时，使用 KEK 保护 DEK。 d) 系统间交互的需进行加密的数据，使用 DEK 进行保护。 e) 定义 KEK、DEK 的使用生命周期以及更换的流程。 f) 不同业务系统间采用不同的 KEK、DEK。
6.6.5.2.4 对称密钥分发	对称密钥的分发过程应满足以下要求： a) 对称密钥在分发之前对接收者的身份进行确认。 b) 对称密钥的多组明文分量的分发过程中，不使用相同的快递公司、相同的经办人员、相同时间的车次或航班。 c) 人工方式进行密钥分发时，不由同一人领取或携带多段密钥分量。 d) 对称密钥分发动作完成后，有检验并核对密钥校验值的过程。 e) 密钥分发过程中使用的密钥分量记录介质，在完成密钥分发后如果不用于备份，则采取无法恢复的方法进行销毁。
6.6.5.2.5 密钥备份	对称密钥的备份应满足以下要求： a) 不同成分的密钥分量由不同的备份人员保管，封装密钥分量明文的信封存放在不同的保险箱内。 b) 同一个人不具有全部加密资料或全部加密设备钥匙的控制权。 c) 纸介质的密钥明文分量封装在防拆、防篡改信封内或者使用防拆、防篡改封条，当需要使用时只有指定人员才可以拆阅信封，并对以上过程进行记录。 d) 对于密钥导入设备，由专人进行配置和维护，并对以上过程进行记录。 e) KEK 不备份，如 KEK 丢失，则对 KEK 重新生成和录入。

表59　对称密钥 - 第五级（续）

评测要求	评测程序
6.6.5.2.5 密钥备份	f)　对于保护数据本地存放的密钥，对其密钥分量进行备份。

6.6.5.3　非对称密钥

第五级密钥管理维度中，关于非对称密钥的评价标准见表60。

表 60　非对称密钥 - 第五级

评测要求	评测程序
6.6.5.3.1 生成密钥或证书	非对称密钥或证书的生成过程应满足以下要求： a)　非对称密钥对的生成方式保证私钥的机密性。 b)　生成新证书时，可以指定算法、算法强度和失效日期。 c)　业务使用的非对称密钥对通过指定的系统或专用加解密设备生成，并定义保管私钥副本的部门或岗位。 d)　规定合规的根证书颁发机构并明确应关联根证书的场景。 e)　对存储私钥数据的系统或设备登记并备案。
6.6.5.3.2 使用密钥或证书	非对称密钥或证书的使用和保存应满足以下要求： a)　从加解密设备或配套系统中获取私钥数据时使用加密手段。 b)　业务活动不涉及私钥数据的传输。
6.6.5.3.3 更换密钥或证书	非对称密钥或证书的更换应满足以下要求： a)　定义非对称密钥或证书的更换周期以及更换流程。 b)　业务使用的证书，其非对称密钥对的生命周期不超过 5 年。 c)　定义私钥泄漏的评判标准、补救措施和更新流程。 d)　具备根据原证书的密钥对及其失效时间重新生成新证书的流程和能力。

参 考 文 献

[1] GB/T 21078 个人识别码的管理与安全
[2] GB/T 21077—2007 银行业务 证书管理
[3] GB/T 21079—2011 银行业务 安全加密设备（零售）
[4] GB/T 21081—2007 银行业务 密钥管理相关数据元（零售）
[5] GB/T 21082—2007 银行业务 密钥管理（零售）
[6] GB/T 25069—2010 信息安全技术 术语
[7] GB/T 27910—2011 金融服务 信息安全指南
[8] GB/T 33136—2016 信息技术服务 数据中心服务能力成熟度模型
[9] GB/T 37092—2018 信息安全技术密码模块安全要求
[10] GM/T 0020—2012 证书应用综合服务接口规范
[11] GM/T 0028—2014 密码模块安全技术要求
[12] GM/T 0050—2016 密码设备管理 设备管理规范
[13] GM/T 0051—2016 密码设备管理 对称密钥管理技术规范
[14] JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引
[15] ISO/IEC TR 13335:2000 Information technology—Guidelines for the management of IT Security