6．活动日志（Event Journal）

密钥管理的所有活动必须记录到活动日志中，且该日志库必须保证自身管理的安全性。

5.4.4 密码设备的自身安全性

FIPS 140 标准对密码模块自身安全性做出了具体的技术规定。该标准由美国国家标准和技术委员会（NIST）发布，专门针对密码模块的安全需求（Security Requirements for Cryptographic Modules）。目前该标准的最新版本（即 FIPS 140-2）发表于 2002 年 12 月 3 日，其提供了密码模块评测、验证和最终认证的基础。NIST 正在进行该标准新版本的审核，未来将发布 FIPS PUB 140-3。FIPS 140 标准已被 ISO 标准所采用。

1．密码模块自身安全性的基本要求

① 采用并正确执行经批准的保护敏感信息的安全功能。
② 保护一个加密模块，防止未经授权的操作或使用。
③ 防止加密模块与算法被未经授权或不被发现地篡改。
④ 提供加密模块运行状态指示。
⑤ 当加密模块在一个已认可的操作模式下运行时，保证加密模块的正常运行。
⑥ 能检测到加密模块在运行中产生的错误，并防止这些错误导致对关键数据的损害。

2．安全等级划分

鉴于所要保护敏感数据的价值不同以及应用环境的多样性，密码模块在安全方面的要求也有很大差异。为了满足不同等级敏感信息和不同应用环境的安全需求，FIPS 140 将密码模块的安全级别分为 4 级，由低到高依次为 Level 1、Level 2、Level 3、Level 4。

（1）Level 1

Level 1 提供最低级别的安全性。在 Level 1 中，基本没有产品级元器件之外的安全控制功能。Level 1 允许一个密码模块的软件和固件成分，在一般用途的计算系统上运行（操作系统可能未经安全验证）。Level 1 密码设备适合一些低安全要求的应用，此时诸如物理安全、网络安全、管理程序安全限制等安全控制手段很有限或根本不存在。

（2）Level 2

Level 2 加强了 Level 1 密码模块在物理结构上的安全要求，通过提供能够识别的入侵证据，以防止明显的破坏。这些可以识别的入侵证据包括：可识别入侵的涂层或密封、在可移动的盖子或门上加锁等，并且只有破坏涂层、密封等物理防护手段，才能从物理上进入密码模块组件内部，从而获取密钥明文等关键参数。

Level 2 要求至少基于角色的验证机制。通过该验证机制，密码模块可以验证操作员的角色和权限。

（3）Level 3

Level 3 除了要求 Level 2 的物理结构外，还要求防止对密码模块内部所控制的关键安全参数过程的攻击。对企图通过物理登陆、使用或篡改密码模块的攻击活动，密码模块能够检测并及时做出反应，当可移动的门或盖子被非法打开时能够清除密码模块中的明文关键安全参数。

Level 3 要求基于身份识别的验证机制，通过此验证机制，密码模块可以验证操作员的身份、角色和权限。

Level 3 要求明文关键参数的输入和输出时，所使用的端口必须与其他端口物理上分开，或者使用其他可信的方式进行逻辑分离。关键安全参数可以以密文的方式从密码模块输入或输出。

（4）Level 4

Level 4 是最高级别的安全要求。在此级别上，物理安全机制需要一个完整的保护封装。与 Level 3 相比，Level 4 对物理入侵的要求更为严格，对贯穿封装的任意方向攻击进行高灵敏度的检测，并能立即清除所有在密码模块中的明文关键参数。

Level 4 的密码模块可以在物理上无防护的环境中操作使用。这要求密码模块既能够适应正常的操作范围环境需求（如温度、电压），又能检测具有风险的环境波动并清除关键安全参数。

3. 安全要求要点

密码模块安全要求主要包括：设计与运行，组件规格，连接端口与接口，角色、服务与验证，有限状态模式，物理安全性，操作环境，密钥管理，电磁干扰/电磁兼容性，自检与设计保证。对于不同安全级别，安全要求有所不同，具体比较参见表 5-5。

表 5-5 密码模块安全要求

	Level 1	Level 2	Level 3	Level 4
组件规格	密码模块规格、安全范围边界、认可的加密算法、认可的运行模式、密码模块说明、组件安全策略描述			
连接接口与端口	要求提供所有接口的规格与输入、输出数据的路径		对用于未保护的关键安全参数端口，应当在逻辑上与其他数据连接端口分开	
角色、服务与验证	要求逻辑上分开的可选角色与服务	基于角色的操作员验证	基于身份识别的操作员验证	
有限状态模式	有限状态模式的规格，要求的规定与可选的规定，规定转换图与规定转换条件			
物理安全性	生产合格设备	锁或入侵证据	对外壳与门的入侵检测与反应	入侵检测与反应的封装，EFP 或 EFT
操作环境	单独操作员，可执行代码，认可的集成技术	在 EAL2 中引用的外壳防护评估，自由选择访问控制机制和检测	在 EAL3 中引用的外壳防护与可信路径评估，加安全策略模式	在 EAL4 中引用的外壳防护与可信路径评估
密钥管理	人工方式建立的密钥可以明文方式输入和输出		人工方式建立的密钥应当以加密或知识分离的方式输入和输出	
EMI/EMC	47CFRFCC15，B 分册，A 类（商用）		47CFRFCC15，B 分册，B 类（家用）	
设计保证	配置管理，安全安装与设置，设计与策略一致，指导文件	配置管理，安全配置、功能规格	高级语言的实现	正式型号，详细说明，预处理和后处理

5.5 密码算法 ASN.1 描述

5.5.1 密码算法格式

密码算法格式用 ASN.1 定义如下：

```
AlgorithmIdentifier  ::=  SEQUENCE  {
    Algorithm                OBJECT IDENTIFIER,
```

```
    Parameters              ANY DEFINED BY algorithm OPTIONAL   }
```

其中，Algorithm 为算法 OID，Parameters 为算法参数。

5.5.2　密码算法 OID

常用算法的 OID 表 5-6。

表 5-6　常用算法 OID

/	算　法	OID	/	算　法	OID
1	md2	1.2.840.113549.2.2	13	md5WithRSAEncryption	1.2.840.113549.1.1.4
2	md4	1.2.840.113549.2.4	14	sha1WithRSAEncryption	1.2.840.113549.1.1.5
3	md5	1.2.840.113549.2.5	15	sha256WithRSAEncryption	1.2.840.113549.1.1.11
4	sha1	1.3.14.3.2.26	16	sha384WithRSAEncryption	1.2.840.113549.1.1.12
5	sha256	2.16.840.1.101.3.4.2.1	17	sha512WithRSAEncryption	1.2.840.113549.1.1.13
6	sha384	2.16.840.1.101.3.4.2.2	18	sm3WithSM2Encryption	1.2.156.10197.1.501
7	sha512	2.16.840.1.101.3.4.2.3	19	pbeWithMD2AndDES-CBC	1.2.840.113549.1.5.1
8	sm3		20	pbeWithMD2AndRC2-CBC	1.2.840.113549.1.5.4
9	rsaEncryption	1.2.840.113549.1.1.1	21	pbeWithMD5AndDES-CBC	1.2.840.113549.1.5.3
10	sm2	1.2.156.10197.1.301	22	pbeWithMD5AndRC2-CBC	1.2.840.113549.1.5.6
11	md2WithRSAEncryption	1.2.840.113549.1.1.2	23	pbeWithSHA1AndDES-CBC	1.2.840.113549.1.5.10
12	md4WithRSAEncryption	1.2.840.113549.1.1.3	24	pbeWithSHA1AndRC2-CBC	1.2.840.113549.1.5.11

5.6　密码消息 ASN.1 描述

PKCS #7 规范和《SM2 密码算法加密签名消息语法规范》中规定了各种密码消息的具体格式，这些消息可用于不同实体间的数据交换。

5.6.1　通用内容消息 ContentInfo

通用内容消息格式用 ASN.1 描述如下：

```
ContentInfo ::= SEQUENCE {
    contentType    ContentType,
    content        [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }
ContentType ::= OBJECT IDENTIFIER
```

其中，contentType 表示内容类型或消息类型，包括 data、signedData、envelopedData、signedAndEnvelopedData、digestData、encryptedData、keyAgreementInfo 等。content 表示内容值。

5.6.2　明文数据消息 Data

明文数据消息格式 ASN.1 描述如下：

```
Data ::= OCTET STRING
```

5.6.3 数字签名消息 SignedData

1. SignedData

数字签名消息格式用 ASN.1 描述如下：

```
SignedData ::= SEQUENCE {
    version Version,
    digestAlgorithms DigestAlgorithmIdentifiers,
    contentInfo ContentInfo,
    certificates    [0] IMPLICIT ExtendedCertificatesAndCertificates    OPTIONAL,
    crls    [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
DigestAlgorithmIdentifier ::= AlgorithmIdentifier
SignerInfos ::= SET OF SignerInfo
ExtendedCertificatesAndCertificates    ::= SET OF ExtendedCertificatesAndCertificate
ExtendedCertificatesAndCertificate    ::= CHOICE {
    certificate    Certificate, -- X.509
    extendedCertificate    [0] IMPLICIT    ExtendedCertificate    }
```

使用 SM2 算法时，SignedData 用 ASN.1 描述如下：

```
SignedData ::= SEQUENCE {
    version Version,
    digestAlgorithms DigestAlgorithmIdentifiers,
    contentInfo SM2Signature,
    certificates    [0] IMPLICIT ExtendedCertificatesAndCertificates    OPTIONAL,
    crls    [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }
```

其中，version 表示消息格式版本，缺省值为 1。digestAlgorithms 是摘要算法标识集合，可以包含零或多个摘要算法标识。contentInfo 表示待签名数据。certificates 包含签名者认证路径中的相关证书。crls 是 CRL 集合。signerInfos 是签名者信息集合，至少包含一个签名者。

2. SignerInfo

签名者信息格式用 ASN.1 描述如下：

```
SignerInfo ::= SEQUENCE {
    version Version,
    issuerAndSerialNumber IssuerAndSerialNumber,
    digestAlgorithm DigestAlgorithmIdentifier,
    authenticatedAttributes [0] IMPLICIT Attributes OPTIONAL,
    digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,
    encryptedDigest EncryptedDigest,
    unauthenticatedAttributes [1] IMPLICIT Attributes OPTIONAL }
IssuerAndSerialNumber ::= SEQUENCE {
```

```
        issuer Name,
        serialNumber CertificateSerialNumber }
    DigestEncryptionAlgorithmIdentifier ::=   AlgorithmIdentifier
    EncryptedDigest ::= OCTET STRING
```

其中，version 表示消息格式版本，缺省值为 1。issuerAndSerialNumber 用于唯一确定签名者证书，由其证书签发者 DN 和证书序列号组成。digestAlgorithm 表示摘要算法标识，应属于 SignedData 中的 digestAlgorithms 摘要算法集合。authenticatedAttributes 表示签名者用于签名的属性集合。digestEncryptionAlgorithm 表示用签名者私钥对摘要加密或签名的公钥算法进行标识。EncryptedDigest 表示用签名者私钥对摘要进行加密或签名后的值；当使用 SM2 算法时，为 SM2Signature 类型，编码格式为 r||s。unauthenticatedAttributes 表示签名者未用于签名的属性集合。

5.6.4 数字信封消息 EnvelopedData

1. EnvelopedData

数字信封消息格式用 ASN.1 描述如下：

```
EnvelopedData ::= SEQUENCE {
    version Version,
    recipientInfos RecipientInfos,
    encryptedContentInfo EncryptedContentInfo }
RecipientInfos ::= SET OF RecipientInfo
```

其中，version 表示消息格式版本，缺省值为 0。recipientInfos 是接收者信息集合，至少包含一个接收者。encryptedContentInfo 表示已加密的内容信息。

encryptedContentInfo 格式用 ASN.1 描述如下：

```
encryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
    encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }
ContentEncryptionAlgorithmIdentifier ::=   AlgorithmIdentifier
EncryptedContent ::= OCTET STRING
```

其中，contentType 表示内容类型。contentEncryptionAlgorithm 表示密码算法标识，用于加密内容；针对所有接收者，采用相同的内容加密算法。encryptedContent 表示加密后的内容。

使用 SM2 算法时，encryptedContentInfo 用 ASN.1 描述如下：

```
encryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
    encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL,
    sharedInfo [1] IMPLICIT OCTET STRING OPTIONAL,
    sharedInfo [2] IMPLICIT OCTET STRING OPTIONAL
    }
```

其中，sharedInfo 表示发送者和接收者之间协商好的共享信息。