四川科道芯国智能技术股份有限公司

Sichuan Keydom Smart Technology Co., Ltd

标准文件

Standard File

密钥管理标准

Key Management Standard

文件种类：管制文件 File Type: controlled document

文　件　编　号: KD-MMY-01

Doc. No.:

编　　制:安全策略部

Prepared by: Security Policy Department

审　　核:

Reviewed by:

批　　准:

Approved by:

版本 /修订状态: A9

Rev./Revision status:

受　控　状　态:

Controlled status:

2020-1-1 发布　　2020-1-1 实施

Issued on 1 / 1 /2020　　Implemented on 1 / 1 /2020

修改记录表 Document Changes

修改条款 Modified terms	修订状态 Revision Status	修改内容 Description	修改日期 Date	修改人 Changed by	审核人 Reviewed by	批准人 Approved By
/	A/0	初次发行 Initial release	2015/09/22	韩德均 Han Dejun	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
4.1	A/1	更新密钥管理组织架构图 Update the diagram of key management organization	2016/03/11	曹良攀 Cao Liangpan	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
4.1	A/2	更新密钥管理组织架构图 Update the diagram of key management organization	2016/8/29	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
19.1	A/3	1. 更新 logo Update the logo	2017/2/27	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing

		2. 审批人修改 Modified by the approver				
4.1	A/4	更新密钥管理组织架构图 Update the diagram of key management organization	2017/5/19	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
4.1	A/5	更新密钥管理组织架构图 Update the diagram of key management organization	2017/10/18	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	杜强林 Du Qianglin
6.5	A/6	条款增加 6.5. HSM 的启用及销毁 Add provision 6.5. Activation	2017/11/30	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	杜强林 Du Qianglin

		and Destruction of HSM				
/	A/7	更换 logo 及公司名称 Change of the logo and name of the company	2018/7/25	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	杜强林 Du Qianglin
4.1	A/8	更新密钥管理组织架构图 Update the diagram of key management organization	2018/12/10	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	杜强林 Du Qianglin
	A/9	文件格式更新	2019/12/28	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	陈为明

目　录

Contents

1. 目的

Purpose

此流程用于防止密钥在操作期间被非法获得及使用，所有机密信息的接收、储存、发出与传送和机密信息面临可疑时的删除与销毁过程能得到及时的控制，四川科道芯国智能技术股份有限公司智能卡及数据生产中心（以下简称为生产中心）依据 GB/T19001-2008《质量管理体系要求》、《PCI-GSMA》（2013 年 5 月 1.0 版），结合生产中心生产经营特点，形成生产中心的《密钥管理程序》。

This procedure is used for the prevention of illegal acquisition and use of key during operation and making sure the receiving, storage, deliver of all confidential information and the deletion and destruction of potentially leaked confidential information are under control. The Intelligent Card and Data Production Center (hereinafter referred to as the production center) of the Sichuan Keydom Smart Technology Co., Ltd according to GB/T19001-2008 *Requirements for Quality Management Systems*, the *Management Manual* (Version D) released by the production center on Sep. 4, 2014 and the PCI-GSMA (Version 1.0, May 2013), considering the business features of the production center, accomplished the *Key Management Program*.

2. 适用范围

Scope of Application

此流程用于密钥、机密资料操作管理流程，安全策略部密钥及机密资料的管理。

This procedure applies to the management of key and confidential information of the Security Policy Department.

3. 定义

Definition

3.1. 对称密钥

Symmetrical Key

对称密钥加密又叫专用密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES、IDEA、FEAL、BLOWFISH 等。

Symmetrical key encryption is also called dedicated key encryption, i.e. the data sender and the data receiver must use the same key to realize encryption and decryption operations to clear text. The encryption algorithm of symmetrical key mainly includes DES, 3DES, IDEA, FEAL, and BLOWFISH, etc.

3.2. 非对称密钥

Unsymmetrical key

非对称加密算法需要两个密钥：公开密钥（public key）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

The unsymmetrical encryption algorithm requires two keys, i.e. public key and private key. The public key and the private key are a pair, if public key is used to encrypt data, only the corresponding private key can decrypt the data; if private key is used to encrypt data, only the corresponding private key can decrypt the data. Encryption and decryption use two different keys, so the algorithm is called unsymmetrical encryption algorithm.

3.3. HSM

硬件密码机，又叫加密机或密码服务器。

HSM, Hardware Security Model, also interpreted as Encyption Machine or Cryptography Server

3.4. 保险箱

Safe box

保险箱用于密钥组件的暂存管理。

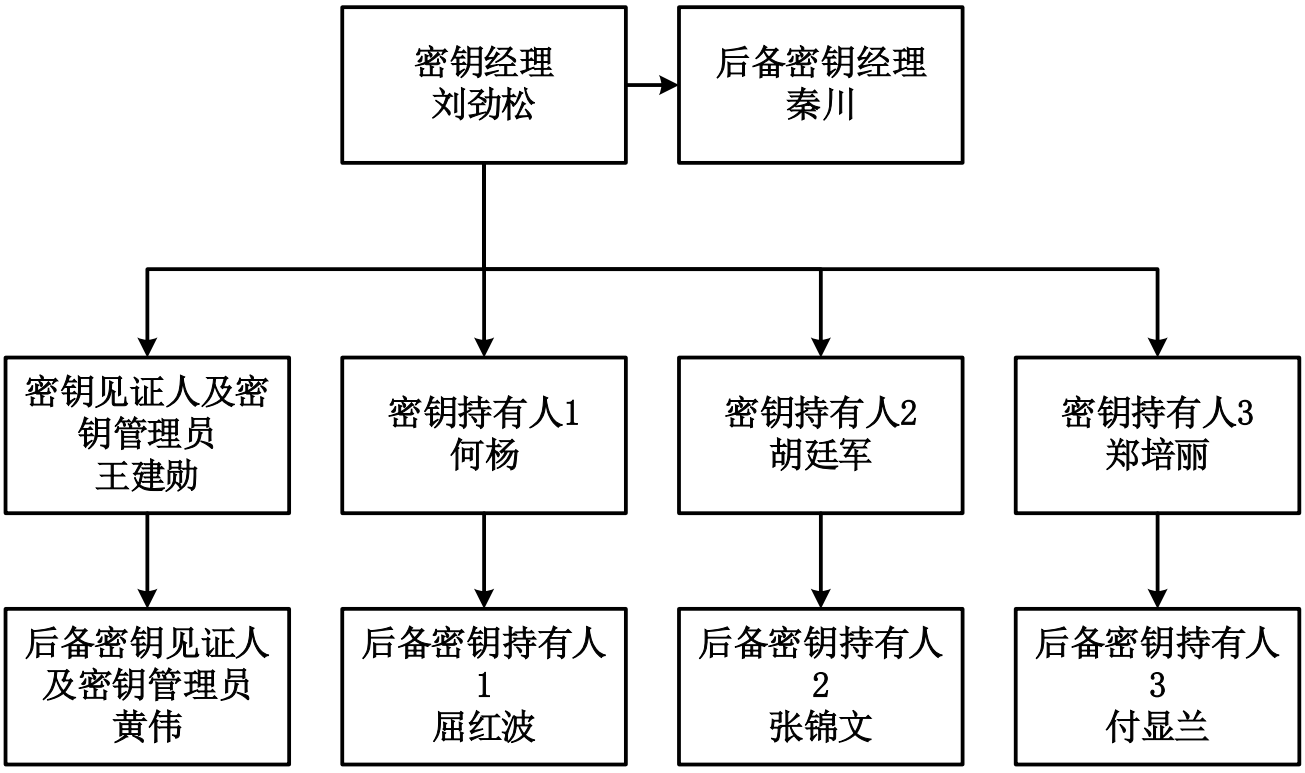
Safe box is used for temporary storage management of key components.

4. 职能职责

Duties and Responsibilities

4.1. 密钥管理组织架构

Key management organization framework



只有通过授权允许的数据的人员有权使用个人化数据、来完成相关的工作任务，不允许用于工作之外任何地方，且严格把关只能授权给必须知道的人员及必须使用的人员。

Only authorized personnel have the right to complete relevant works using personalized data, which cannot be used in other places besides workplace. The authorized personnel must be strictly identified with necessity to use it.

在密钥的密钥持有人换班期间，他（她）必须负责将安全资料与材料指派给相应的代理人；代理人必须清楚的知道自己的职责；其它相关的人员执行指派的工作任务但不能知道任何有关重要资料的内容。

When the key holders are shifting duties, security data and materials must be sent to a backup personnel who must be aware of the duties. Other relevant personnel can also be assigned with the work but are not allowed to know any content in these important files.

4.2. 密钥管理组织各岗位的职能职责

Duties and responsibilities of posts in the key management organization

密钥经理:

Key manager:

- 负责从事密钥活动中整个过程的监督、组织、审查，确保整个过程中所有操作均按照管理制度进行所有业务。

  The key manager is responsible for supervision, organization and review of the whole process of activities related to the key, making sure all operations comply with the management system.

- 负责全部的管理活动均已充分记录在案。

Make sure all activities are put on record.

- 负责通过文件证明程序实施的密钥管理活动。

  Responsible for the key management activities that carried out through the procedure of documentary proof.

- 负责与人力资源管理部协同，每年审查全部密钥管理人员以确保所有管理人员是否符合担任该岗位的要求。

  Coordinate with the Human Resource Department, and review all key management personnel to make sure they meet the requirements for the post every year.

- 密钥经理必须对密钥管理人员进行严格的安全培训，每年度至少一次。

  The key manager must provide strict safety training to key management personnel at least once a year.

密钥持有人：

Key holder:

- 负责密钥的保密性和完整性。其他人不得接触或了解密钥内容，当接触到密钥时首先检查密钥的防护袋确认没被打开和发生篡改行为。

  Ensure the confidentiality and wholeness of the key. Prevent others from engaging in the contents of the key. Check the protective packaging of the key first on acquiring the key and make sure it is not opened and tampered with.

- 密钥持有人及其后备必须由密钥经理正式指定并记录在密钥管理指派清单及密钥操作员授权表中。

  The key holder and back-up must be formally designated by the key manager and recorded in the assignment list of key management and in the key operator authorization form.

- 各个密钥持有人员禁止有密钥业务交叉，防止密钥的外泄。

  Each key holder is prohibited to involve in cross-business related to the key to prevent leakage of the key.

密钥见证人员：

Key witness：

- 负责监督整个密钥的过程是否符合标准并填写对应的记录表单。

  The key witness shall be responsible for supervising the whole process related to the key to check whether it meets the standard, and filling in the corresponding record.

密钥管理员：

Key administrator：

- 确保在使用状态中的硬件,确保硬件的正常工作。确保进行密钥仪式的环境一切正常，以及密钥的管理。

  Ensure that the hardware is in use state, to ensure the normal operation of the hardware. Ensure a normal environment for the key function, and responsible for key management.

以上人员必须持有公司的授权任命书，详情请见《逻辑安全人员管理程序》

All personnel above must hold an authorized appointment of the company, please see the *Logical Security Personnel Management Procedure* for details.

5. 密钥生命周期安全管理

Key Lifecycle Security Management

5.1. 密钥生成

Key generation

5.1.1. 所有密钥生成行为密钥管理员都必须进行日志记录，双控和分开知晓原则

必须贯穿整个过程。三个分量的方式生成必须分别独立由3个密钥持有人保管，不允许生成的密钥以明文方式存在必须是加密或者掩码。

All key generation must be recorded in the log by the key administrator, the principles of dual-control and separated informing need to be followed throughout the process. Keys generated with three components must be kept separately by three key holders, and keys that are not allowed to be generated must be proclaimed and exist as encrypted or mask.

5.1.2. 密钥生成必须在FIPS 140-2 Level 3 或者更高等级的加密机中进行。

The key must be generated in FIPS 140-2 Level 3 HSM or higher.

5.1.3. 在进行任何密钥生成动作之前，都必须对HSM及密钥管理系统进行检查，以确定对这些系统没有非授权的改动，封条完好，电脑上没有其他功能，密钥管理员填写《HSM、密钥管理系统检查表》以证明密钥生成前环境的安全性和完整性。

Before any action of key generation is made, the key management and HSM systems must be checked to determine if these systems have any unauthorized changes, if the seals are intact, and whether there is no other function. The key administrator shall then, fill in the *HSM and Key Management Checklist*, verify the security and integrity of the environment before the key is generated.

5.1.4. 每位密钥持有人负责对其个人掌握的密钥组件进行密封并存入对应保险箱密钥管理员填写《保险箱存取记录表》。密钥生成记录必须由密钥持有人、密钥见证人、密钥管理员签字，成功完成操作之后，必须由密钥经理检查确认并签字。

Each key holder is responsible for sealing and safekeeping of the key in the corresponding safe box and meanwhile the key administrator shall fill in the *Safe Box Access Record*. The key generating record must be signed by the key holder, key witness, key administrator, after which the record shall be

confirmed and signed by the key manager.

5.2. 密钥的分配

Key distribution

5.2.1. 对称密钥的分配

Distribution symmetric key

5.2.1.1. 密钥经理组织密钥持有人、密钥管理员、密钥见证人，密钥持有人分别与密钥经理、密钥管理员、密钥见证人到生产机房通过0-9、A-F的编码，密钥持有人分别编写出分量，在分别将分量加载至KMS密钥管理系统。

The key manager shall organize the key holder, key administrators and key witnesses. The key holder shall respectively, go with the key manager, key administrator and the key witness to adopt the coding of 0-9 and A-F, and the key holder shall respectively, compile the components, and load each component to the KMS key management system.

5.2.1.2. 通过加密运算最终得出校验值，密钥持有人分别将分量与校验值写入文本中，在装入防篡改信封存入保险箱，密钥管理员填写《保险箱存取记录表》、《密钥加载记录表》。

With the check value being obtained, the key holder shall respectively write the check values into a text, put it into a temper-proof envelope and then put into the safe box with the key administrator filling in the *Safe Box Access Record* and the *Key Loading Record*.

5.2.2. 非对称密钥的分配

Distribution of Asymmetric key

5.2.2.1. 密钥经理组织密钥持有人、密钥管理员、密钥见证人，密钥持有人分别与密钥经理、密钥管理员、密钥见证人到生产机房通过0-9、A-F的编码。

Key manager shall organize the key holder, key administrators and key witnesses. The key holder shall respectively, go with the key manager, key

administrator and the key witness to adopt the coding of 0-9 and A-F.

5.2.2.2. 密钥持有人分别编写出分量，在分别将分量加载至KMS密钥管理系统，通过加密运算最终得出私钥和校验值以及与私钥对应的公钥，密钥持有人分别将分量与校验值写入文本中，在装入防篡改信封存入保险箱，密钥管理员填写《保险箱存取记录表》、《密钥加载记录表》。

The key holder shall respectively, compile the components, load each component to the KMS key management system. With the private key, the corresponding public key and their check values being obtained by encryption algorithm, the key holder shall respectively have the components and the check values written in text and put in the tamper-proof envelope and into the safe box, with the key manager filling in the *Safe Box Access Record* and the *Key Loading Record*.

5.3. 密钥传输

Key transmission

5.3.1. 密钥发送程序

Key delivery procedure

5.3.1.1. 当密钥经理接收到客户服务组的密钥发送通知单时，密钥经理必须验证接收方的身份信息如（单位名称、对接人姓名、联系方式、签名笔迹样本）密钥经理并填写《密钥对接方信息表》，确认无误可直接进入传输程序。

When the key manager receives the key delivery notice from the customer service group, the key manager must verify the recipient information including company name, recipient name, contact information, handwriting sample of the signature and the key manager shall fill in the *Key Recipient Information Form* and access to the transfer procedure when the information is confirmed.

5.3.1.2. 由密钥经理组织密钥传输活动，通知密钥管理团队人员：密钥持有人，密钥见证人、密钥管理员至指定地点：生产机房安全通道。

The key manager shall organize the key transferring activity by informing the key management team members: the key holder, key witness and key administrator to the destination, that is, the secure channel of the production room.

5.3.1.3. 将密钥分量1、2、3由密钥持有人1、2、3分别与密钥见证人、密钥经理、密钥管理员进入机房从密钥保险箱取出对应的密钥检查密钥是否具有清晰标识、密钥的长度确认无误的情况下，密钥管理员并填写《密钥存取记录表》和《密钥访问日志》。

Key holder 1, 2, 3 come respectively with the key witness, key manager and key administrator to the machine room, take out keys corresponding to the component 1, 2, 3 and check if the keys are clearly identified with appropriate length. After confirmation, the key administrator shall fill in the *Key Access Record* and the *Key Access Log*.

5.3.1.4. 在分别从保险柜取出密钥的同时用防篡改信封封装各自的密钥并填写《保险箱存取记录表》，通过不同速递方式发送到接收方，并同时附有两份的清单，密钥管理员填写《密钥传输记录表》，接收方收到密钥将需返回一份清单以证明收到此密钥。

At the same time with taking out the keys from the safe box, respectively put the keys into temper-proof envelopes and fill in the *Safe Box Access Form*. Send the envelope to the recipients by different express deliveries with two lists being attached to each, after which the *Key Transmission Record* shall be filled in by the key administrator. One of the list needs to be sent back as a proof of receipt.

5.3.1.5. 在整个活动开始前首先需向安全策略部物理安全领取所需钥匙。

Before the whole process starts, the keys need to be applied for from the

Security Policy Department.

5.3.2. 密钥接收程序

Key receiving program

5.3.2.1. 当密钥经理接收到客户服务组发送的密钥接收通知时，密钥经理必须验证发送方的身份信息如（单位名称、发送人姓名、联系方式、签名笔迹样本），密钥经理并填写《密钥对接方信息表》，确认无误可直接进入接收程序。

When the key manager receives the key receiving notice from customer service group, key manager must verify the recipient information including company name, sender's name, contact information, handwriting sample of the signature and the key manager shall fill in the *Key Recipient Information Form* and access to the transfer procedure when the information is confirmed.

5.3.2.2. 密钥经理组织密钥管理人员、密钥见证人，由密钥持有人分别接收密钥，并同密钥见证人、密钥经理检查密钥包装的完整性，是否有篡改痕迹、密钥清单与实物是否吻合、确认无误并到监控室领取钥匙，将密钥分别存入生产机房保险箱中密钥管理员并填写《保险箱存取记录表》、《密钥储存记录表》、《密钥接收记录表》。

The key manager shall organize key management personnel, the key witness. The key shall be received by the key holder, who shall check the key with key witnesses, key manager. The key manager has to check the integrity of key wrapping, if there are signs of tampering, if the key is consistent with the list. After confirmation, go to the monitoring room to gain access to the safe box of the production room to have the key stored. The key administrator shall fill in the *Safe Box Access Record*, the *Key Storage Record* and *Key Receiving Record*.

5.3.2.3. 在整个活动开始前首先需向安全策略部物理安全领取所需钥匙

Before the whole process starts, the keys need to be applied for from the Security Policy Department.

5.3.3. 同城传输

Transmission within the city

密钥如在同城进行传输，由密钥持有人1、2、3分别持三件经密封的密钥信封，在不同的时间送达对方或由对方三名专人分别领取，传送或领取人员不允许乘坐同一辆交通工具。

If the key is to be transmitted within city range, the key holder 1, 2, 3 shall send the sealed key envelopes to the recipients in different time or respectively. The senders or recipients are not allowed to choose the same transportation.

5.3.4. 异地邮寄的要求

Requirements for offsite mailing

在需要采用邮寄方式传送密钥时，使用邮政部门的机要邮政系统邮寄。密钥在邮寄前按规定填写分发密钥的表格，由密钥持有人1、2、3分别到邮局邮寄，邮寄时的手续凭证作为附件妥善保管。

If mailing is needed when transmitting the key, use the confidential postal service of postal system. Mailing the key requires to complete the distribution form before mailing with the key holder 1, 2, 3, respectively, going to the post office. The receipt of procedures shall be kept as attachments.

邮寄时将每一段密钥单独作为一份邮件邮寄，不同的密钥组件在不同的日期分别寄出。

Making each component of the key a separate mail and send each of the mail in different date.

5.4. 密钥的储存及备份

Storage and backup of the key

5.4.1. 基本规定

Basic provisions

5.4.1.1. 密钥组件保存在保险箱内。

Key components are stored in safe box.

5.4.1.2. 密钥存储介质采用纸张，并用信封密封，由密钥管理员与密钥持有人签名确认，加盖密封签名章；密钥管理员与密钥持有人调离，办理交接手续时由密钥经理认可并由主管负责人审批。

The Key storage medium shall be paper and sealed in an envelope, confirmed by the signatures of both the key administrator and the key holder and stamped with sealing signature chapter. When the key administrator and the key holder leave under order, the handover process must be approved by the key manager and reviewed by the director.

5.4.1.3. 只有密钥组件的持有人才有权使用该密钥组件。

Only a key component holder has the right to use it.

5.4.1.4. 密钥组件存取、使用情况由密钥持有人作好记录，密钥见证人负责监督，该记录也应存放在保险箱内，视同密钥组件进行保管。

The access and usage of key components shall be recorded by the key holder and supervised by the key witness. The record shall be put into the corresponding safe box and safe-kept together with the key components.

5.4.2. 与密钥安全有关的机密设备及密码的保管

The safekeeping of confidential equipment and cipher related to the key

5.4.2.1. 存放密钥的保险容器

Insurance container for the key

密钥分段分人保管，每一密钥组件的持有人员都分别配备专用的保险箱，该保险箱的钥匙和密码由该持有人员负责掌管。

The key shall be kept in terms of components with each component having a special safe box, whose key and passwords are kept by its holder.

5.4.2.2. 硬件加密机钥匙的保管

Safekeeping of the HSM

硬件加密机钥匙由密钥持有人负责保管，存放在保险箱中。

The HSM is safe-kept by the key holder and kept in the safe box.

5.4.2.3. 与密钥有关的密码的保管

Safekeeping of cipher related to the key

加密机的安全密码、操作密码由密钥持有人掌管。上述密码保存在保险箱内，存入之前用信封密封、由密钥见证人确认，并加盖密封签名章。

The secure password, operating password of the HSM are running by the key holder. The ciphers mentioned above are kept in the safe box, before which they shall be sealed in envelopes, confirmed by the key witness, stamped with sealing signature chapter.

5.4.3. 密钥组件的保管

Safekeeping of key components

存储主密钥各段组件的 IC 卡或密封信封应在密钥监督员监督下，直接存入保险箱，且只有指定的密钥持有人才有权取用。

The IC card for the storage of each component of the master key or the envelope shall be directly put into the safe box under the supervision of the key supervisor with only the specific key holder having the right to open.

密钥持有人调离或离职时，需办理主密钥组件的 IC 卡和密封信封的交接手续，交接手续在密钥监督员监督下进行，且当场存入保险箱。

When the key is removed from the holder who is leaving or leaving under

order, handover the IC card and sealed envelopes, which shall be carried out under the supervision, after which the stuff must be put into the safe box at once.

5.4.4. 密钥档案资料的保管

Safekeeping of key archive

由指定的密钥持有人负责保管，存放于安全区域的保险箱内，保存期限不低于密钥的生命周期。

The key archive is safe-kept by the designated key holders and stored in a safe box in the secure area. The shelf time is not less than the life cycle of the key.

持有人员调离岗位前，需妥善办理交接手续。

When former holders leave their positions, proper handover procedures are required.

5.4.5. 密钥存储程序

Key storage procedure

5.4.5.1. 当收到密钥信息时（不能拆开任何包装），密钥持有人应立即通知密钥经理，密钥经理组织密钥持有人、密钥管理员、密钥见证人检查密钥的完整性，确认与密钥清单无误的情况下立即进入密钥储存程序，密钥持有人分别将密钥储存到保险柜中；并填写《保险箱存取记录表》、《密钥储存记录表》。这些保险柜存放在生产机房保险箱内。

Upon receipt of key information (without opening any package), the key holder shall immediately notify the key manager to organize the key holder, key administrator, key witness to conduct examination of key integrity. Confirmed by making contrast in the list, the keys shall be stored in the safe box respectively by the holders with the *Safe Box Access Record* and *Key Storage Record* being filling out. These safes are stored in the safe box in the production room.

5.4.5.2. 密钥材料经过导入/导出后,以及在进行秘密存放时,必须立即密封放入单独的防篡改袋内。必须填写《密钥访问日志》、《密钥存取记录表》，该程

序必须是在密钥经理、密钥管理员、密钥见证人、密钥持有人分别执行各自的职能所完成。

The key after being imported or exported, or being stored must be solely put into a tamper-proof bag at once. With the key manager, administrator, witness and holder respectively fulfilling their duties, the *Key Access Log* and *Key Access Record* must be filled out.

- 访问记录表需要包含以下信息：

  Access record form needs to contain the following information:

进出时间与日期

Time and date of entry and exit

密钥持有人姓名

Name of the key holder

存取原因

Access reason

信封编号（若需要）

Envelope number (if necessary)

5.4.5.3. 授权见证人员检查包装袋,确定包装袋进行了正确的封存。

Authorized key witness shall check the package to make sure a correct seal is completed.

5.4.5.4. 包装袋的识别号码必须与相应的日志中记录的号码相符合。

The identification number of the packaging bag must comply with the number recorded in the log.

5.4.5.5. 安全/密钥管理经理保留一份列表说明密钥材料的存放数量,存放位置以及各个包装袋的识别号码。

A list demonstrating the amount, location and numbers of key materials needs to be kept by the security/ key manager.

5.4.6. 密钥的备份

Key backup

5.4.6.1. 在密钥备份前，密钥管理员填写《密钥备份申请表》，由密钥经理审批同意后方可进行。

Before the key backup, the key administrator shall fill in the *Key Backup Application Form* and the backup can be started after the key manager approved.

5.4.6.2. 密钥管理员双控登录密钥管理系统，密钥管理员写下密钥值，立即封存放入单独的防篡改包装中并编号及填写《密钥访问日志》。

The key administrator logs in the key management system under duel-control, writes in the key value and immediately put it into temper-proof packaging, numbers the package and fills in *the Key Access Log*.

5.4.6.3. 授权见证人员检查包装袋，确认包装袋进行正确的封存，密钥管理员存入保险箱中同时填写《保险箱存取记录表》《密钥备份记录表》。

Authorized key witness shall check the packaging bags to confirm it is correctly sealed, and the key administrator shall put it into the safe box and at the same time, fill in the *Safe Box Access Record* and *Key Backup Record*.

5.4.6.4. 备份过程，密钥经理必须全程在场验证并签字确认。

The whole backup process requires the presence of the key manager who needs to finish the verification by affixing a signature.

5.5. 密钥的加载

Key loading

5.5.1. 基本规定

Basic provisions

5.5.1.1. 注入过程中密钥持有人、密钥见证人、密钥管理员等明确各自的工作内容和责任；

During the loading, duties and responsibilities of the key holder, witness and administrator must be specified.

5.5.1.2. 密钥分段分人并在隔离状态下注入密钥使用设备；

The key is kept separately in terms of components and holders, and shall load the equipment in separated state.

5.5.1.3. 密钥注入现场的摄像监控设备不得拍摄到密钥注入设备的操作面板部位；

The surveillance cannot cover the area where the operating panel of the key loading equipment is located.

5.5.1.4. 密钥注入完成后，按规定进行封存，并填写相关的密钥启用封存记录表格。

After the loading is completed, seal it according to corresponding rules and fill in record forms related to the activation and sealing of keys.

5.5.2. 密钥类型

Key type

根据需求,下面所示密钥管理系统的密钥,必须遵守以下标准:

According to the requirements, keys of following key management system must comply with the standards listed below:

Key Types	Key Names	Key Length (bit)	Key Lifespan
T-DES	KEK Application Key Card Key	128	29 Aug 20XX

5.5.3. 密钥加载的前提

Premise of key loading

5.5.3.1. 密钥管理系统必须处于正常的状态。

The key management system must be in a normal state.

5.5.3.2. 在进行密钥仪式前,需要先检查HSM时间、日期是否与电脑同步。 密钥管理员检查密钥管理软件、HSM是否处于正常状态，HSM时间、日期是否与整个系统同步并填写《HSM、密钥管理系统检查表》。

Before the key function start, check if the HSM time, and date are synchronized with the computer. The key administrator shall check if the key management software and HSM are in a normal state, and whether the HSM time and date are synchronized with the system and fill in the *HSM and Key Management System Checklist*.

5.5.3.3. 在使用任何系统之前,确保所有供应商默认安全设置已经改变。

Before any system is applied, make sure that default security settings of all suppliers have changed.

5.5.4. 密钥加载的构成

Constitution of key loading

5.5.4.1. 密钥管理员准备密钥加载环境及密钥系统和要使用的硬件设施。

The key administrator shall prepare for the loading environment, the key system and hardware that may be needed.

5.5.4.2. 密钥管理经理组织密钥持有人、密钥见证人、密钥管理员举行密钥加载的时间和地点（生产机房安全通道）。

The key manager shall organize the key holder, key witnesses, key administrator as well as the time and place (the secure channel of the production room).

5.5.5. 密钥加载的准备

Preparations for key loading

5.5.5.1. 在进行密钥加载之前密钥持有人立即从指定的保险柜中取出密钥材料。防护包装保持密封。取出材料后由密钥管理员填写 《保险箱存取记录表》。

Before loading, the key holder shall immediately take out materials of the

key from the specified safe box. And protective packaging shall remain sealed. After the materials is removed, the key administrator shall fill in the *Safe Box Access Record*.

5.5.5.2. 密钥持有人负责材料的保密性和完整性。其他人不得接触或了解材料内容。如果无法保证材料的保密性,必须通知适当的安全经理。

The key holder is responsible for the confidentiality and integrity of the material. Other person should not allowed to engage with the material. If confidentiality of materials cannot be guaranteed, the corresponding security manager needs to be notified.

5.5.5.3. 密钥系统管理员查看正在使用状态中的硬件,确保硬件的正常工作。

The key system administrator shall view the status of the operating hardware to ensure the normal operation of the hardware.

5.5.5.4. 确认没有任何未授权的更改迹象。

Make sure there are no signs of unauthorized changes.

5.5.5.5. 确保密钥信封密封性。

Ensure the sealing of key envelope.

5.5.5.6. 密钥见证人员确保进行密钥仪式的环境一切正常(例如,只有指定进行密钥仪式的人员在场)。

Key witness needs to ensure the environment of the function, for example, only designated personnel present for the key function).

5.5.5.7. 密钥见证人员检查装有密钥的防护袋,确定它没有被打开。防护袋上的识别号码必须与那些登记在记录表中的号码相同(从存放地领取的记录)。

The key witness shall check the protective bag of the key, making sure it is not opened yet. The identification number of the protection bag must be the same number as those registered in the record form (records where the key is sent).

5.5.5.8. 以上的所有检查通过后,则可以开始进行密钥加载活动。

All of the above checks passed, the key loading activity starts.

5.5.5.9. 在密钥加载准备活动开始之前必须先向安全策略部领取业务相关的钥匙。

Keys must be obtained before the preparation of the loading from the Security Policy Department.

5.5.6. 执行密钥生成

Implementation of key generation

5.5.6.1. 密钥组件必须在HSM内生成。

Key components must be generated within the HSM.

5.5.6.2. 在密钥生成阶段，必须完全确保双控和明确的职责分离。

During the key generating, dual-control and a clear separation of duties must be ensured.

5.5.6.3. 产生出来的明文密钥组件必须由对应的密钥持有人立刻密封在防篡改信封内。

The generated key components must be sealed in the tamper-proof envelopes by the corresponding key holder.

5.5.7. 执行密钥加载

Implementation of key loading

5.5.7.1. 相应的密钥持有人分别与密钥经理、密钥见证人、密钥管理员进入生产机房从保险箱中取出密钥组件检查完整无误的情况下，密钥管理员并填写《保险箱存取记录表》和《密钥访问日志》。（打开密钥保险箱需密钥管理员与密钥持有人一起打开）

Corresponding key holder shall respectively go with the manager, key witness and key administrator to the production room to have the key components withdrawn from the safe and check their completeness, after which the *Safe Box Access Record* and *Key Access Log* shall be filled in by the key administrator. (the safe box of the key must be opened by the key

administrator and holder together)

5.5.7.2. 密钥持有人将密钥输入到密钥管理系统,确保任何人都无法看到密钥的输入后并填写《密钥加载记录表》。

The key holder shall load the key to the key management system, to ensure that no one can see the loading before filling in the *Key Loading Record*.

5.5.7.3. 密钥输入的环境必须全程有监控,二十四小时全程摄影。

The key must be loaded under 24-hour surveillance.

5.5.7.4. 所有的密钥仪式应在三十分钟内完成。

All key functions must be accomplished within 30 minutes.

5.5.8. 密钥封存

Key Safekeeping

5.5.8.1. 密钥注入完成后，原已开封的密钥保管信封需重新封装，并加盖密钥持有人和密钥管理员签名章，通过密钥管理员与密钥持有人双控打开密钥保险箱将密钥存入，密钥管理员填写《保险箱存取记录表》、《密钥存储记录表》完成后放入保险箱保管。

After the key loading is completed, the original key storage envelopes are to be re-packaged and stamped with signature chapter by key holders and key administrators. The key administrators and key holders shall open the safe box under dual-control and have the keys stored. The key administrators shall put the key into the safe box after filling in the *Safe Box Access Record* and *Key Storage Record.*

5.5.8.2. 全程必需采双人控制,密钥见证人、密钥经理见证并签字。

The whole process must be under duel-control of the key witness and manager by supervision and signing signatures.

5.5.9. 密钥经理的准备工作

Preparations of the key manager

5.5.9.1. 重要的密钥必须存储到密钥的管理系统中并且能够清楚的确认；密钥经

理必须持有标志这些资料所在位置的详细清单。

Important keys must be stored in the key management system and can be clearly confirmed. The key manager must hold a detailed list of locations of such information.

5.5.9.2. 重要的密钥必须存储到密钥的管理系统中并且能够清楚的确认；密钥经理必须能够识别这些资料并明确的分配这些任务（如：KEY的生命周期）。

Important keys must be stored in the key management system and can be clearly confirmed. The key managers must be able to identify these materials and make a clear allocation of tasks according to such information (such as: key life cycle).

5.5.9.3. 备有证明文件的传送（是被使用过的）（登录日志或数据库）重要的资料传送只能有一位收件人能够预先详细的知道。

For the delivery of data (used) (in log or database), the important data is sent to only one recipient who knows in detail in advance.

5.5.9.4. 在传送期间，使用预先确定的加密编码及可识别的传送密钥；并填写机密信息的传送及相关密钥的传送记录表格（如：输入表格或传送表格）。

During transmission, use the pre-determined encrypted code and keys that can be identified, fill the record forms related to confidential data transmission and key transmission, for example the input form and transmission form.

5.5.9.5. 重要的资料只能单独的使用并需预先指定（如：传输密钥,密钥的生命周期）。

Important information can only be used separately and must be applied for in advance (such as: transmission keys, key life cycle).

5.6. 密钥的使用

Key usage

5.6.1. 基本规定

Basic provisions

5.6.1.1. 测试的环境不得与生产的环境一样。

The environment for testing cannot be set the same as the production environment.

5.6.1.2. 测试用的密钥不得用在生产上。

The test keys may not be used in production.

5.6.1.3. 密钥在使用于每个发卡行都应该唯一,例如(KEK,ZCMK)等。

The key shall remain unique to each card-issuing company, for example the KEK and ZCMK.

5.6.1.4. 如传送的密钥为明文时,不得以电子化的方式传送,如e-mail、软盘驱动器、光盘等。

When the key is transmitted as plain text, it cannot be transmitted in electronica manner, such as e-mail, floppy disk drive and optical disk.

5.6.1.5. 不得在非工作时间或安全环境之外操作密钥。

Do not operate the key during non-working hours or outside secure environment.

5.6.1.6. 采取适当措施,确保密钥使用如以下要求：

Take appropriate measures to ensure that key usage meets the following requirements:

- 测试，开发，验证或类似目的不能被用于生产系统。

  Test, development, verification, or process alike cannot be used in the production system.

- KEK等用于其它密钥加密和保护的密钥要确保每个发卡行或密钥区域不

一样。这类密钥只能在密钥交互的两方进行传递，不能共享给任何第三方。

KEK and other keys that used for key encryption and protection must be ensured that each issuer or key region remains distinctive. Such type of keys can only be delivered between the two parties involved and cannot be shared with any third party.

- 确保用于加密其它密钥的密钥其生命周期短于对整个密钥空间进行详尽搜索的时间。

  Ensure that the life cycle of the key used to encrypt other keys is shorter than the time for the whole key space to finish an exhaustive search.

- 仅在必要的要求和环境中使用密钥。

  Use the key only according to necessary requirements and situations.

5.6.1.7 正式密钥环境不能使用于测试密钥环境

The formal key environment cannot be used in the test key environment

5.6.2. 对称密钥的使用

Use of symmetric key

5.6.2.1. 通过有效的系统操作来确保密钥被存储在最小可能范围的密钥管理地点。

The key shall be stored in the management location with minimized possible range by effective operation in the system.

5.6.2.2. 确保对一个密钥的暴露不会导致其他密钥的泄露。

Making sure the exposure of one key does not lead to the leakage of other keys.

5.6.2.3. 一旦发现密钥泄露或者疑似泄露，立刻停止使用该密钥。

Once a key is found disclosed or potentially disclosed, stop using it immediately.

5.6.2.4. 不得在设备之外使用密钥的衍生内容，如离散，分散密钥等。

The derived functions of the key are not allowed to be used without the

devices, such as the discretion and separation of the key.

5.6.3. 非对称密钥的使用

Use of unsymmetrical key

5.6.3.1. 当密钥对失效，或者私钥泄露时，停止使用非对称密钥

When the key pair fails or the private key is disclosed, stop using the asymmetric key.

5.6.3.2. 仅仅使用私钥解密或者创建数字签名，公钥用于加密或验证签名

Use only the private key to decrypt or create a digital signature, and the public key is used to encrypt or verify signatures

5.6.3.3. 只能在HSM内部使用私钥。

The private key can only be used within the HSM.

5.6.3.4. 严格定义及限制对VISA及发行商公钥的使用，使其满足EMV和VISA的要求

Strictly define and limit the use of the public key of VISA and issuers to meet the requirements of EMV and VISA.

5.6.3.5. 不得使用VISA成员的密钥对进行其他的应用和业务开展。

The keys of VISA members are not allowed to be used in the development of other applications and business.

5.6.4. 测试环境与正式环境

Test environment and formal environment

5.6.4.1. 测试环境需与正式环境一样高安控。

The test environment must be controlled in high security as the formal environment.

5.6.4.2. 测试用的密钥不得用在生产上，正式密钥不能用于测试环境

The test keys may not be used in production. Official key cannot be used in test environment

5.6.4.3. 所有测试的密钥消毁或加载都必需要记载。

The destruction and loading of the test keys must be recorded.

5.6.4.4. 所有的测试密钥必需明文记载不得使用于生产。

The test keys that are not allowed to be used in production shall be proclaimed in written form.

5.7. 密钥的泄露及停用

Disclosure and deactivate of the key

5.7.1. 密钥泄露核查

Key leakage verification

5.7.1.1. 加强系统跟踪，在日常工作中定期核查系统状态。检查内容包括：

Strengthen the tracking system, make periodic verification of system status daily. Check the contents, including:

- 是否非法访问增多；

  Whether illegal access increased

- 是否合法访问异常操作增多；

  Whether there is more abnormal operation with legitimate access

- 异常情况是否具有一定相似性和规律性。

  Whether the abnormal situations bear similarity and regularity

5.7.1.2. 禁止发生的情形

Situations which are prohibited

对执行密钥生成、保管、启用、更新、销毁操作等过程进行检查，杜绝违规或超权限操作，禁止发生以下情形：

The implementation of key generation, storage, activation, update and destroy shall be inspected to prevent violation of rules and operations beyond authority, and prohibit the following situations:

- 未使用加密设备，密钥的明文出现在系统或程序中；

  Using without encryption equipment, with keys exposing in plain text in the

system or program.

- 加密机主密钥、成员主密钥以单个完整的密钥形式出现在硬件加密机外部，或密钥组件在权限范围外可以被合成；

  The master key of HSM and members appear as a complete key form in the HSM, or the key components can be synthesized beyond the authority limits.

- 工作密钥未按规定动态更新，长时段呈静态状况，导致被穷举攻破；

  Failure in making dynamic update of an operating key and long period of static conditions, resulting in an exhaustive break.

- 废旧设备中仍在使用的密钥未及时销毁，随意丢弃或放置；

  Keys in waste devices that are not destructed in time, discarding randomly.

- 在测试系统和生产系统使用同一密钥，或在测试系统出现生产系统密钥的明文；

  Using the same key in the test system and the production system, or the presence of key from the production system in plain text in the test system.

- 同一密钥在多个地方使用。

  The same key being used in multiple places.

5.7.1.3. 专人负责加密设备

Keeping the encryption devices by specified personnel

对硬件加密设备的使用、维护设有专人负责，每次操作都进行登记记录，且多人在场，对违规超权限的操作及时查处。

The use and maintenance of hardware encryption equipment are ensured by special-assigned personnel with every operation being recorded and supervised by more than one other personnel, handling violation of authority timely.

5.7.1.4. 系统用户权限和密码加强管理

Strengthen management of user limits and passwords

对系统管理员密码、各用户密码及用户权限应严格管理，一旦上述

密码发生泄漏、权限失控或人员离职，及时对系统各密钥进行核查跟踪，根据需要及时更新密钥。

The passwords of administrator of the system, user passwords and user limits shall be strictly managed. All keys in the system must be tracked down and update the key timely if necessary when there is a password disclosure due to limits out of control or personnel leaving position.

5.7.2. 密钥泄漏和被攻破情况的界定

Definition of key leakage and key breach

在生产中使用的各类密钥都有可能发生泄漏或被攻破，在发现下列情况时，可以考虑认定密钥已泄漏或被攻破，并及时采取措施更新密钥。

Various types of key leakage or breach could occur in the use of keys. If the following situations are found, the key can be considered as leaked or broken, and then update the key by taking effective measures.

5.7.2.1. 密钥未按本程序生成、分发、保管、注入所规定的条款执行；

The key fails to be generated, distributed, safe-kept and entered according to the provisions of this program.

5.7.2.2. 有两段或两段以上密钥明文被盗或同时丢失；

There are two or more keys stolen in plain text or missing at the same time.

5.7.2.3. 有两段或两段以上密钥明文同时存放在同一台可被人读取的设备上；

There are two or more keys simultaneously stored in plain text on the same device can be read by others.

5.7.2.4. 系统内大部分成员主密钥、工作密钥泄漏或被攻破；

Most of the master keys of personnel in the system are leaking or broken.

5.7.2.5. 其他经安全策略部门认定的情况。

Other situations identified by the Security Policy Department

5.7.3. 密钥泄漏处置程序

Disposal procedure of key leakage

5.7.3.1. 关于密钥的泄露可能来源于公司内部或外部，此时，密钥管理员必须立即通知安全策略部门经理及密钥经理。经安全策略部门共同认定，报本单位主管领导批准后，认定密钥已泄漏和被攻破。对于安全策略部门无法认定的情况，聘请有关专家和管理人员进行审核。必要时报公安部门协助追查。

The key leakage could come from inside or outside of the company, at this time, the key administrator must notify the security policy manager and key manager immediately. Jointly identified by the Security Policy Department, as well as the approval of the leader of the unit, the key can be identified as leaked or broken. For circumstances that the Security Policy Department cannot identify, relevant experts and personnel shall be invited to make further evaluation. Call the police for assistance if necessary.

5.7.3.2. 密钥经理应展开调查事故的原因，并把收集到的或记录的这些可疑或被证实的泄露情况通知到相关受影响的组织团体（密钥管理组织、发行商）。

Key managers shall conduct investigation on the cause of the accident, and notify the relevant organizations or groups (such as management organizations and issuers) with the information about the leakage or related to the leakage that collected or recorded.

5.7.3.3. 在情况出现的24小时内,必须把怀疑或者被证实泄漏的事故情况以书面形式通知VISA、万事达、银联等相关组织机构。

Within 24 hours of after the situation happens, notification of the leakage or potential leakage must be sent to VISA, MasterCard, China UnionPay and other relevant organizations in written form.

5.7.3.4. 任何被怀疑泄漏或者已经确认为被泄露的密钥信息都必须立即停止使用（密钥经理组织实施），密钥管理员填写《密钥停用申请表》。

Any key involved or potentially involved in the leakage must be deactivated (organized and implemented by the manager), and the corresponding key administrator shall fill in the *Key Deactivation Application Form*.

5.7.3.5. 被泄露的密钥管理系统的硬件、软件密钥管理员必须明显标识并禁止再做使用（密钥经理组织实施）

The key administrator shall mark and stop using the hardware and software of the key management system that suffered the leakage (organized and implemented by the manager).

5.7.3.6. 为了保留证据并继续深入调查，有问题的系统必须保持原有的状态直到安全策略部门宣布其可以重新开始被使用。

In order to preserve evidence for further investigation, the system must remain the same state until the Security Policy Department announce that it can be used again.

5.7.3.7. 密钥经理需要通过有效的记录文件，判断并确定哪些机密信息已经出现可能都泄漏的迹象：

Key managers needs to judge the signs of leakage of confidential information by valid records:

5.7.3.8. 密钥经理应考虑到那些被写进编码里面的加密的信息有可能被泄露。包括密钥资料的所有实例。

The key manager shall take into consideration the confidential information that written into codes might be involved in a leakage. This includes all instances concerning key materials.

5.7.3.9. 包括所有的存储数据的表格，如：纸质文档，安全模块（HSM，存储介质等）加密文件（如：密钥库、无附件的电子邮件）。

Including all forms of data storage, such as: paper documents, security module (HSM, storage media, etc.), encrypted files (such as: key store, e-mail without attachments).

5.7.3.10. 包括备份和涉及到机密信息的档案。

Including backup and archive related to confidential information.

5.7.3.11. 包括以证书授权的形式产生使用过的机密信息（如：公共的密钥证书）。

Including used confidential information (such as: a public key certificate) formed by certificate authorization.

5.7.3.12. 密钥经理需要通过有效的记录文件，判断并确定出被泄露的机密信息的发布情况和被应用情况。

Key manager needs to determine the degrees of the release and application of leaked confidential information through valid records.

5.7.3.13. 密钥经理应以书面形式通知所有持有被泄漏的机密信息的持有者，所有记录该机密信息的媒介（如：磁盘、密钥库文件）必须标识。

Key Manager shall notify all holders of the leaked confidential information in writing and all media that include such confidential information (such as: disk, key store files) must be marked.

5.7.3.14. 当密钥泄漏已经被证实时，将泄漏的所有资料进行销毁处理（包括备份、记录表、密钥文本文件），该程序由密钥经理组织。

When a key leakage is confirmed, all the leaked information shall be destroyed (including backup, record forms and key text files), which is organized by the key manager.

5.7.4. 密钥的停用

Deactivation of the key

5.7.4.1. 密钥管理员填写《密钥停用申请表》提交至密钥经理并说明停用原因（如：预先的密钥信息生命周期已经结束、密钥被泄漏），密钥经理检查密钥信息停用会影响到的业务。

The key administrator shall fill in the *Key Deactivation Application Form* to submit to key manager and explain the reasons (such as: key information life cycle has ended, the key is leaked), and the key manager shall check the

business that might be affected by the key deactivation.

5.7.4.2. 当一个加密密钥被停用，使用它来访问存储的密钥信息需要被屏蔽，当一个生产的密钥被停用后，应当替换那些必要的生产文件并通知供应商或相关商家；发行新的密钥将替换。

When an encrypted key is deactivated, the information accessed by the key needs to be shielded. When a production key is deactivated, flies related should be replaced if necessary with the suppliers and issuers being notified, and issue a new key to replace it.

5.7.4.3. 当密钥信息遇到可能被泄漏密钥管理员填写《密钥停用申请表》，当密钥经理接收密钥的停用申请时，必须通知客户、卡片认证组织，密钥经理通知相关组织部门，并请求认证机构设定密钥停用日期，确认后密钥管理员填写《密钥停用记录表》。

When the key information may be leaked, the key administrator shall fill in the *Key Deactivation Application Form*. When the request for deactivation is received by the key manager, the customer, the card certification organization and other relevant organizations and departments need to be notified, and the certification body would be requested to set the deactivation date, after which the key administrator shall fill in the *Key Deactivation Record*.

5.7.4.4. 密钥经理需要通过有效的记录文件，判断并确定出密钥信息有效日期：

The key manager shall determine the valid period of the key information by valid records:

5.7.4.5. 包括机密资料的所有实例（如：密钥的组成部分;，包括所有的存储数据的表格，如：纸质文档，安全模块（HSM，介质等）加密文件（如：密钥库、无附件的电子邮件）；包括备份和涉及到密钥信息的档案；包括以证书授权的形式产生使用过的密钥信息（如：公共的密钥证书）。

These valid records include all instances of confidential information (such as components of the key), forms of all data storage including paper documents,

security modules (HSM, media, etc.), encrypted files (such as key store, Email without attachment), backup and archive related to key information, used key information formed by certificate authorization (such as a public key certificate).

5.7.4.6. 如果需要在有效期到期之前，密钥信息能被归档保存；档案文件保存必须按照下面存储密钥备份的安全制度；档案文件可以保存在只能写入一次的光盘中；档案文件不能在生产系统内部不能访问；但是，档案文件可以用于今后有可能发生的需要它的事件调查，但是它存在于密钥管理系统中。

If the key information needs to be saved into the archive before expiring, the archive file must be stored in accordance with the following security system of the key backup storage. The archive files can be stored in a disposable optical disc. The archive cannot be in the internal production system and cannot be accessed. However, the archive can be used to investigate the event that is likely to occur, but it must exist in key management systems.

5.7.4.7. 密钥经理需要通过有效的记录文件，判断并确定出准备到期的密钥信息的发布情况和被使用情况。

Key managers needs to determine the issuing and using conditions of the expired key information through valid records.

5.7.4.8. 密钥经理应以书面形式通知所有密钥信息的持有者，所有记录该密钥信息的媒介（如：磁盘、密钥库文件）必须标识。

The key Manager shall notify the holder of all the key information in writing that all the key information recording media (such as disk, key store files) must be identified.

5.8. 密钥的销毁

Key Destruction

为避免泄漏风险，对失效密钥进行及时安全删除或销毁。

To avoid the risk of leakage, the invalid key must be safely deleted or destroyed in time.

5.8.1. 失效密钥的认定

Identification of invalid keys

失效密钥包括过期密钥、废除密钥、泄漏（含被攻破）密钥。

The invalid keys include expired keys, waste keys, leaked keys (including the broken ones).

5.8.1.1. 过期密钥

Expired key

对于不同密钥类型，有着一定的密钥生存期，超过这个期限，即可标志为过期密钥，对于过期密钥， 及时的进行删除和销毁。

For different types of keys, there is a certain key life cycle, over which the key can be marked as expired that requires timely deletion and destruction.

5.8.1.2. 废除密钥

Waste key

指在测试环境中不再使用的密钥、生产环境中因应用程序的修改不再使用的密钥、存放介质发生损坏的密钥、设备报废或废弃在设备中不再使用的密钥等。

The waste keys include keys that can no longer be used in tests, keys that can no longer be used in production due to modifications of program, keys whose medium is damaged and keys in a waste equipment vice versa.

5.8.1.3. 泄漏密钥

Leaked key

指密钥在其生命周期内被泄漏或怀疑可能泄漏以及密钥被攻破等情况。

It means that the key is leaked or potentially leaked, or is broken during its life cycle.

5.8.2. 基本规定

Basic provisions

5.8.2.1. 如果信息不能够完全格式化、数据有可疑之处，那么这些资料就应当被销毁。

If the information cannot be completely formatted and the data is at potential risk, then this information should be destroyed.

5.8.2.2. 储存在HSM中的信息必须完全格式化。确保其中的信息被销毁后不可恢复。

Information stored in the HSM must be fully formatted and cannot be recovered after destruction.

5.8.2.3. 若KEK已经泄密，那么必须替换用KEK加密的全部密钥。

If KEK has leaked, all keys encrypted by the KEK must be replaced.

5.8.2.4. 若MDK已经泄密，那么主密钥中衍生出来的全部密钥必须进行替换。

If MDK has leaked, all keys derived from the master key must be replaced.

5.8.3. 密钥销毁的过程

Key destruction process

对失效密钥，采用执行和检验相结合的方法删除和销毁，确保密钥被完全销毁。

For invalid keys, the deletion and destruction shall combine both implementation and examination to ensure that the keys are completely destroyed.

5.8.3.1. 密钥销毁申请

Key destruction application

在密钥进入销毁过程前，密钥管理员必须填写《密钥销毁申请表》说

明密钥销毁原因并提交至密钥经理审批，得到密钥经理的审批同意后方可进入密钥销毁程序。

Before the key is brought into the destruction process, the key administrator must fill out the *Key Destruction Application Form*, describing the reasons for the destruction and submitting it to key managers for approval. After that, the process begins.

5.8.3.2. 密钥销毁准备

Preparations of key destruction

密钥经理组织密钥持有人、密钥管理员、密钥见证人并通知密钥销毁地点（生产机房），销毁的地点由密钥持有人与密钥管理员双控销毁密钥，密钥见证人、密钥经理证明整个过程的合理性（在监控摄像下及遵守四眼原则），并且在销毁活动结束后密钥管理员填写《密钥销毁记录表》、《密钥存取记录表》。

The key manager shall organize the key holder, key administrator and key witness and inform them of the key destruction site (production room). The destruction of key is under duel-control of the holder and administrator, supervised by the manager and the witness (follow the "four eyes principle" under surveillance) with the administrator filling the *Key Destruction Record* and the *Key Access Record* after the destruction process.

5.8.3.3. 主机系统中密钥的删除

Deletion of key in the host system

找出在主机系统中存放待删除密钥的数据库表、密钥文件等，在删除操作时安排设备管理员、密钥销毁员、密钥监督员同时在场，由密钥销毁员执行，密钥监督员验证，确保密钥的真正删除。

Find the list of database in the host system that needs to be deleted and files of the key and the destruction shall be operated by the key destruction personnel with the equipment administrator, destruction personnel and

supervisor at scene. The deletion shall be supervised by the key supervisor to ensure the key is permanently deleted.

5.8.3.4. 硬件加密机中密钥的删除

Deletion of keys in the HSM

找出所有待删除密钥以及硬件加密机中相应的密钥索引值，对该密钥进行重写，冲销旧密钥。在删除操作时安排密钥持有人、密钥见证人、密经理同时在场，密钥持有人执行，密钥见证人验证，确保该密钥被覆盖且不可恢复。

Find all the keys to be deleted and the corresponding key index in the HSM, and have the key to be rewritten to write off the old key. When operating a deletion, the equipment administrator, destruction personnel and supervisor shall be at scene at the same time with the holder operating deletion and the witness supervising to make sure the deletion is irrecoverable.

5.8.3.5. 存放密钥的组件介质的销毁

Destruction of the medium for key storage

所有待销毁密钥的组件，由密钥见证人和密钥持有人同时在场执行销毁操作。有关于销毁的规定如下：

For all key components to be destroyed, the operation needs to be implemented by the witness and the holder of the key. There are provisions on the destruction as follows:

纸介质：必须通过焚烧，浆化或者交叉粉碎的方式进行销毁，保证不可恢复；

Paper medium: must be incinerated, pulverized or cross-grinded on the destruction to ensure it is unrecoverable.

IC卡：对于重复利用的介质，交密钥销毁员重新写卡，确保有写卡操作，覆盖旧密钥而不可恢复，销毁过程由密钥见证人验证。对于不再利用的介质，交密钥销毁员物理毁卡，采用芯片毁损的方式，保证不可恢复，

销毁过程由密钥见证人验证。

IC Card: for reusable, handover to the destruction personnel to re-write the card, making sure the card has a write operation and permanently covering the old key, and the destruction process shall be verified by the key witness. For the medium can no longer be utilized, the destruction personnel shall destroy the card, using the chip destruction, to ensure it cannot be restored with the key witness verifying the destruction process.

EEPROM：存储于EEPROM的密钥必须通过至少3遍的写0方式重写。存储密钥的EEPROM或者PROM当要销毁时，必须确保芯片完全破碎。

EEPROM: the keys stored in the EEPROM must be written to 0 for at least three times. When the EEPROM or PROM are to be destroyed, it must be ensured that the chip is completely broken.

电子档：密钥电子档销毁后,其实体密钥也应立即销毁。

E-file: after the destruction of electronic files of the key, the key body should also be destroyed immediately.

5.8.4. 销毁后的工作

Works after key destruction

5.8.4.1. 销毁敏感信息后,密钥见证人必需确定不可复原性。密钥销毁后,其备份数据也应立即销毁,销毁的记录需保留无限期。

After the destruction of sensitive information, it is necessary to determine the irrecoverability by the key witness. After the key is destroyed, its backup data shall be destroyed immediately as well and destruction record shall be retained permanently.

5.8.4.2. 所有密钥的销毁记录都存储至生产机房由密钥管理员管理；密钥经理应当检查那些被销毁的信息确保是正确的并且已完全销毁；如果检查的结果如实，那么密钥经理应当向安全策略部门汇报将整个销毁过程，密钥管理员填写《密钥销毁检查记录表》。

All records of key destruction shall be stored in the machine room and kept by the key administrator. The key manager shall check if the destroyed information is completely wiped. If the result is positive, the manager shall report the whole destruction process to the Security Policy Department with the administrator filling in the *Key Destruction Examination Record*.

5.8.4.3. 安全部门应当以书面形式通知相关组织（如：支付行业结构组织）被泄漏的密钥信息已经全部销毁。

Security department shall notify relevant organizations in writing (such as structural organizations in payments industry structural organization) that the leaked key information has been destroyed.

5.8.4.4. 审查记录、销毁记录必须永久被保存。

Review of records and destruction records must be saved permanently.

5.9. 异常情况处理

Disposal of abnormal situations

在密钥活动异常事故时（如密钥输入，输出，销毁，转移，产生，备份，等），必须遵守以下步骤：

For key abnormal incidents (such as failures in key input, output, destruction, transfer, production, backup, etc.), comply with the following steps:

5.9.1. 密钥管理员填写《密钥异常记录表》，影响流程的记录表单必须注明是什么异常，并汇报密钥经理 。

The key administrator shall fill out the *Record on Abnormal Situation of the Key*, the records must involve an indication of the abnormal aspect, and are reported to the key manager.

5.9.2. 密钥经理继续跟进密钥管理程序，以确保所有密钥的机密性，确保密钥不会泄漏给非授权的人，直到消除异常情况恢复其密钥管理程序的正常性。

The key manager continues to follow up the key management procedures to

ensure the confidentiality of all keys, and to ensure that key does not leak to unauthorized people until eliminating the abnormal situation to normal management of the program.

5.9.3. 密钥经理必须隔离所有异常资料相关负责人员，且不得再使用所有人负责的密钥资料。

Key managers must isolate all the responsible personnel for the abnormal data, and shall not use the information of the liable personnel.

5.9.4. 密钥管理组，连同高级经理，若需要，再连同销售部门，需展开初步调查，以决定是否要启动密钥泄漏或替代程序。

The key management group, together with senior managers, if necessary, together with the sales department, carry out a preliminary investigation to decide whether to start the key leakage or alternative procedure.

5.9.5. 若没有必要启动泄密或替代程序，受隔离的异常资料要根据机密资料销毁的程序进行销毁。需要完成的任务重新进行。

If it is not necessary to start the leakage or alternative procedure, the isolated abnormal data needs to be destroyed according to the destruction procedure of confidential data. And start over the tasks need to be finished.

6. 硬件加密机（HSM）安全及管理

Security and management of the HSM

6.1. 基本规定

Basic provisions

6.1.1. 硬件加密机用于保护密钥、产生密钥、PIN的加、解密以及报文鉴别等。这些操作在硬件加密机中完成，单个完整的密钥和PIN明文不能出现在硬件加密机之外。

The functions of HSM include the protection and production of key, the

encryption and decryption of PIN and authentication of message. These operations shall be finished in the HSM. Plain text of a complete key and PIN cannot appear outside the HSM.

6.1.2. 硬件加密机通过国家密码管理委员会办公室审核。

The HSM shall be audited by the Office of the National Cipher Management Committee.

6.1.3. 硬件加密机满足中国人民银行颁布的《银行卡联网联合技术规范》、《银行卡联网联合安全规范》以及中国银联颁布的有关规范、FIPS140-2中规定的基本功能和性能要求。

The HSM must meet the *Joint Technical Specification for Bank Card Networking* and the *Joint Security Specification for Bank Card Networking* issued by the People's Bank of China as well as the basic functional and performance requirements of the China Unionpay.

6.2. 硬件加密机（HSM）设备的功能

Functions of the HSM

6.2.1. 加密机支持64位、128位、192位三种长度的密钥。除工作密钥外，其他密钥可由两段或三段组件合成。密钥在生成和注入时产生每个分量的检验值（Check Value）和密钥合成后的总检验值。

It supports three types of keys in terms of length including 64-bit, 128-bit and 192-bit. In addition to the operating key, the other keys may be synthesized by two or three component. The check value of each component produced during the generating and loading of the key, and the check value of the key after synthesis.

6.2.2. 加密机支持单DES和三重DES的算法。作为选择项，加密机还具有支持RSA算法的功能，作为可选项具有支持CVN、PVN校验功能。

The HSM supports single DES and Triple DES algorithms. As an option, the

HSM also supports the function of the RSA algorithm as well as CVN and PVN check function.

6.2.3. 在加密机上输入密钥组件时全部显示*号

All the components are displayed as * when entered in the HSM.

6.2.4. 加密机提供密钥组件生成指令，可通过外部命令控制加密机生成密钥组件，同时写入IC卡中。

The HSM provides the production instruction of the key components which can be controlled by external command and at the same time, written in the IC card.

6.2.5. 加密机具有生产、管理两种可同时运行的状态。在进行管理操作时不影响正常的生产运行。

The HSM has two operating modes, that are, the production and management mode. The management mode would not affect normal production.

6.2.6. 加密机提供按索引删除密钥的功能，在注入新的密钥时能够自动提示是否覆盖原密钥。

The HSM can delete the key according to indexes, thus there would be auto-covering notice when a new key is entering.

6.2.7. 硬件加密设备被强行打开外壳后，自动销毁机内的所有密钥。

When the casing is forcibly dissembled, all the keys in the HSM would be auto-destroyed.

6.3. 设备存放及监控

Storage and monitoring of equipment

6.3.1. 加密机放置在有严格管理的高安全区机房内；

The HSM shall be strictly managed in the machine room of high security zone.

6.3.2. 硬件加密机存放在带锁机柜中，机柜背板固定安装；

The HSM is locked in a safe with the back-plane fixed.

6.3.3. 对于硬件加密机的操作，配备CCTV（摄像监控）进行全过程监控。

For the operation of HSM, a CCTV (camera surveillance) shall be equipped to monitor the entire process.

6.4. 设备操作

Equipment operations

6.4.1. 每次对硬件加密机的操作，必须经批准后严格按照操作手册、操作规程进行，并记录操作日志；

Each operation of HSM must be approved and carried out strictly in accordance with the operating manual, and operating procedures, and must be recorded in the operation log.

6.4.2. 在应用系统中禁止和加密机非法连接或用做其他用途；

Connection with the HSM for illegal use or other deeds are prohibited in the application system.

6.4.3. 严禁打开加密机机壳。

The casing of HSM is not allowed to be opened.

6.5. HSM 的启用及销毁

Activation and Destruction of HSM

6.5.1. HSM 的安装及调试

Installation and debugging of HSM

6.5.1.1. 在HSM启用之前，确定机壳未被拆卸；

Before the HSM starts, make sure the casing has not been detached yet.

6.5.1.2. 新购买的HSM必须修改HSM相关缺省口令；

Newly purchased HSM shall change its default passwords.

6.5.1.3. 使用IC卡保存HSM的密钥，在得到IC卡的第一时间更改卡片的缺省密码；卡片分级分人保存；

Keep the key of the HSM using the IC card and change the default passwords of the IC card as soon as it's obtained, and keep the card separately in terms of levels and personnel.

6.5.1.4. 新进入生产中心HSM，密钥管理员、密钥经理必须验证其所有配件及资料的完整性和设备的来源，对照清单确认无误由密钥管理员填写《机房进出申请表》提交至安全总监，通过密钥经理审批通过后，密钥管理员、密钥经理将HSM移至生产中心机房存放,密钥管理员填写《机房进出登记表》、《IT设备信息记录表》。

For a new HSM, integrity and source of all parts and data must be verified by the key administrator and manager according to the list. After that, the administrator shall fill in the *Machine Room Access Application Form* and send it to the Security Director. Approved by the manager, the administrator and manager shall move the HSM to the machine room of the production center with the administrator filling out *machine Room Access Record* and *IT Equipment Information Record.*

6.5.1.5. 来历不明的HSM（没有密封包装，没有适合人员监控，没有编号）不得使用。HSM可由其编号识别。

Unknown HSM (not sealed in package, not suitable for personnel monitoring, not numbered) may not be used. HSM can be identified by its number.

6.5.1.6. HSM必须至少有FIPS 140-2 Level 3认证。.安装和设置密钥管理硬件与软件的程序必须记录在《密钥管理员日志》中。

HSM must have at least FIPS 140-2 Level 3 certification. Installation and settings of hardware and software of key management program must be recorded in the *Key Administrator Log*.

6.5.2. HSM 的销毁

HSM destruction

6.5.2.1. 在硬件加密机报废时，删除存贮在该设备中的密钥。

When the HSM can no longer be used, the key stored in the device shall be deleted.

6.5.2.2. HSM销毁得到密钥经理批准,密钥管理员填写《HSM销毁申请表》，内存里的高敏感材料必须立即被销毁。销毁由密钥管理员、密钥经理采用双人控制原则进行。HSM、密钥和密钥组成部件的销毁，密钥管理员填写《HSM销毁记录表》和《密钥销毁记录表》。

If the HSM destruction is approved by the key manager, the administrator shall fill in the *HSM Destruction Application Form*. The highly sensitive information stored in it must be destroyed at once. The destruction must follow the duel-control principle involving the key administrator and the manager. After the destruction of HSM, key and its components, the administrator shall fill in the *HSM Destruction Record* and *Key Destruction Record*.

6.5.2.3. HSM的销毁需拆解,将内存取出后销毁或者是重复三次输入，不使用来生产的测试LMK将原本的信息覆盖。

HSM destruction requires disassemble, taking out the memory for destruction or repeating input for three times, using the testing LMK which is not for production to cover the original information.

6.5.3. HSM 维修与升级

HSM maintenance and upgrades

6.5.3.1. 根据需求提出书面申请，HSM设备管理员填写《故障报修申请表》。

Submit a written application in accordance with the needs, with the HSM device administrator filling out the *Maintenance Application Form*.

6.5.3.2. HSM如果要进场维修,必需重复三次输入不使用来生产的测试LMK将原本的记忆覆盖掉，密钥管理员填写《密钥销毁记录表》。

If the maintenance of HSM requires in-depth engage to the equipment, the LMK for only testing which is not used for production must be input for 3

times to cover the original memory with the key administrator filling in the *Key Destruction Record*.

6.5.3.3. HSM生产厂商、维护商专人持有效身份证明或介绍信，经证实获准后方可进行维修或升级操作，维修或升级操作必须在HSM管理员的全程陪同下进行。

HSM manufacturers, maintenance providers and the person with valid identification or a letter of introduction can be allowed to maintain and upgrade after being approved, and all operations must be completed accompanied by the HSM administrator.

6.5.3.4. 如果需要打开HSM机壳，必须通过书面申请，经安全策略部主管领导同意后方可进行。

If the HSM casing is required to be open, the operation must be approved by leaders of the Security Policy Department.

6.5.3.5. 如果HSM需要返厂维修，必须通过书面申请，经安全策略部主管领导同意后方可离开高安全区机房。

If the maintenance requires a sent-back delivery, the HSM must leave the high security machine room with the approval of Security Policy Department leader.

6.5.3.6. 详细记录工作日志，包括设备类型、故障现象、维修时间等要素。

The operation log shall be completed in detail, including the type of equipment, failure description, maintenance time and other elements.

7. 机密资料、密钥的命名

Naming of Confidential Data and Key

命名规则都遵循：公司标识-文件类型的拼音首写-编码-日期

Naming rules to be followed: company logo - Pingyin acronym of document type - code - date

如:　密钥分量:JK-MYFL-001-20150822

For example: key components: JK-MYFL- company name -001-2015082

密钥：JK-MY-001-20150822

Key: JK-MY- 001-20150822

当密钥进行演练测试时遵循：公司标识-test-001-日期

Follow the format during test of keys: company logo - test-001 - date

如：密钥 JK-test-001-20150822

For example: key JK-MY-YL- 001-20150822

8. 密钥管理流程审查

Management and Review Procedures for Key Management

- 审查记录包括但不限于以下内容：

  The investigation record includes but is not limited to the following:

  a．用户身份

  a. User identity

  b．事件类型

  b. Incident type

  c．有效时期和时间标识

  c. Valid period and time identification

  d．成功或失败指示

  d. Direction for success or failure

  e．事件起因

  e. Cause of the incident

  f．受影响的数据、系统组件或资源的特性或名称

  f. Characteristics or name of the impacted data, system components or resources

g．访问审查记录

g. Access the investigation record

- HSM、密钥管理系统等每周检查任何未授权的活动，并检查全部的访问控制和记录。

  Check HSM and the key management system for any unauthorized activity every week, and check all access and records.

- 每月检查一次全部系统是否达到记录要求。

  Check whether all systems meet recorded requirements monthly.

- 确保每日的关键系统日志记录均已备份、并保存二年。可在线访问记录三个月。

  Make sure daily key system logs have been backed up and saved for two years. People can access the record on line for three months.

- 依据《内部审查》表格，检查与填写所有记录，用作审查证据。

  Based on the *Internal Review Form*, fill and check all the records as evidence for review.

9. 记录表单

Record Form

《密钥管理员任命终止表》

Key Admin Appointment / Termination Form

《密钥人员任命/终止表》

Key Team Appointment / Termination Form

《HSM、密钥管理系统检查表》

HSM and Key Managment System Checklist

《保险箱存取记录表》

Safe Box Access Record

《密钥备份申请表》

Key Backup Application Form

《密钥停用记录表》

Key Deactivation Record

《密钥销毁记录表》

Key Destruction Record

《HSM 销毁记录表》

HSM Destruction Record

《密钥销毁申请表》

Key Destruction Application Form

《HSM 销毁申请表》

HSM Destruction Application Form

《密钥清单》

List of Keys

《密钥储存记录表》

Key Storage Record

《密钥管理员记录表》

Key Administrator Record

《密钥异常情况记录表》

Record on Abnormal Situation of the Key

《密钥停用申请表》

Key Deactivation Application Form

《密钥加载记录表》

Key Loading Record

《密钥传输记录表》

Key Transmission Record

《密钥访问日志》

Key Access Log

《密钥存取记录表》

Key Access Record

《密钥对接方信息表》

Key Recipient Information Record

《密钥生成记录表》

Key Generation Record

《密钥组任命清单》

Key Team Nominate List