关于发布《廊坊银行应用

系统密钥通用安全管理规定》的通知

总行各部门、各分支行：

为规范我行密钥管理，提高信息系统安全水平，根据国家相关法律、法规，特制订《廊坊银行系统密钥通用安全管理规定》。现印发给你们，请认真贯彻执行。

附件：廊坊银行系统密钥通用安全管理规定

廊坊银行股份有限公司

2015年8月25日

内部发送：各行领导。

联系人：薛志强 联系电话：0316-2630176

廊坊银行行长办公室 2015年8月25日印发

廊坊银行

应用系统密钥通用安全管理规定

（试行）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 编制部门 | 修改日期 | 生效日期 | 修改原因和修改内容提示 |
| 1.0 | 信息技术部 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

[第一章 总则 4](#_Toc421886312)

[第二章 部门职责 5](#_Toc421886313)

[第三章 密钥生命周期 6](#_Toc421886314)

[第四章 密钥的生成 7](#_Toc421886315)

[第五章 密钥的保管 8](#_Toc421886316)

[第六章 密钥的使用和分发 8](#_Toc421886317)

[第七章 密钥的备份（恢复） 9](#_Toc421886318)

[第八章 密钥的撤销和更新 10](#_Toc421886319)

[第九章 密钥管理的监督和检查 10](#_Toc421886320)

[第十章 附则 11](#_Toc421886321)

# 总 则

1. 为保障应用系统密钥安全，提高我行密钥管理的规范化、制度化水平，制订本规定。
2. 本规定所称密钥管理是指对密钥的生成、保管、分发、使用、备份和恢复、撤销和更新等生命周期的管理，防范密钥泄漏，保障信息数据的安全。[[1]](#endnote-2)

本规定所称密钥是指密码算法的控制参数。根据密钥类型可将密钥分为：对称密钥、非对称密钥。对称密钥一般是指加密密钥和解密密钥相同，非对称密钥一般是指加密密钥和解密密钥是不同的，并且不能通过计算由加密密钥推导出解密密钥。非对称密钥中公开的密钥称为公钥，而相应的保密密钥称为私钥。

1. 应用系统密钥安全管理遵照“谁主管谁负责，谁使用谁负责”的职责划分原则,责任到人；密钥不同分量明文保存在不同的部门。

密钥生命周期各环节的主管部门，负责保障本环节密钥的安全。各环节的密钥使用人是密钥安全管理的第一责任人。

人工参与密钥管理的，必须由专人负责密钥安全，保证密钥安全责任必须落实到具体人员。

1. 为便于系统运行维护，信息技术部保管用于认证设备的服务器（设备）密钥。在密钥管理过程中，应防止密钥泄漏，避免密钥被非法更新和篡改，根据密钥的作用和用途，采用相应的管理、技术措施，对于人工参与的高风险操作环节，应由专人监督。
2. 禁止任何人私自持有我行应用系统密钥，严禁采用任何手段破解我行密钥，严禁破解加密密文获取信息数据明文。

# 部门职责

1. 信息技术部负责应用系统密钥的生成、使用、分发、备份、恢复、撤销和更新密钥的技术支持和运行维护等操作，负责开发、维护应用系统的加密软件，保管应用系统加密后的数据密文。
2. 各业务部门负责在手工生成密钥情况下生成业务应用系统密钥明文，负责保管本部门牵头管理的应用系统的密钥、密钥口令，并设立《廊坊银行应用系统密钥登记簿》管理（详见附件1），应用系统密钥的使用、分发、备份（恢复）、撤销和更新等应填写《廊坊银行应用系统密钥操作申请》（详见附件2）由监督使用人审批。

# 密钥生命周期

1. 本规定所称密钥生命周期为密钥的生成、保管、使用、分发、备份、恢复、撤销和更新等阶段。

（一）密钥的生成是指获得应用系统运行所需的密钥信息，并完成密钥信息导入。密钥的成功生成是应用系统正常运行的基础。

（二）密钥的保管是指将密钥信息（密钥明文或密钥口令）存放到相应的密钥存储介质，并对密钥存储介质妥善保管。密钥存储介质是密钥信息的载体，应确保密钥存储介质性能良好。

（三）密钥的使用是指根据密钥的用途，通过密钥完成加密、签名、散列、生成MAC和DAC（消息鉴别码和数据鉴别码）等安全操作。

（四）密钥的分发是将密钥传输给准备使用密钥的通信方的过程。

（五）密钥的备份和恢复是指对密钥信息进行复制保存，防止因丢失密钥信息而造成应用系统无法正常运行。密钥的恢复：是指用密钥备份替换现有的密钥，完成密钥的恢复操作。

（六）密钥的撤销是指由于密钥泄漏等原因，停止使用该密钥。如果涉及数字证书撤销，应按照证书颁发机构的相关流程执行证书撤销操作。

（七）密钥的更新是指在满足密钥更新条件下，用新密钥替换旧密钥的过程。

1. 应用系统可根据自身特点选择使用相应的密钥。密钥管理可采用对称密钥、非对成密钥等管理方式。

# 密钥的生成

1. 需要使用密钥的应用系统上线运行必须生成新的密钥，严禁使用测试密钥用于生产。
2. 应用系统应具有防范私自或未经授权生成密钥的功能，对于主密钥等特别重要的密钥，可采用分段保管密钥信息的方式确保密钥的安全。
3. 应用系统应支持密钥托管或密钥自生成两种方式生成非对称密钥。密钥托管是指由数字证书颁发机构产生密钥。对用于不可否认（抗抵赖）服务的非对称密钥对的生成，原则上应向第三方证明公钥的完整性以及私钥的机密性。
4. 密钥应保存在专用信封、加密的主机服务器（简称加密机）、IC卡和USB-Key等密钥存储介质中，在保证计算机安全的情况下，可采用磁盘文件的方式存储密钥。
5. 在采用磁盘文件存储生成的密钥情况下，应确保磁盘文件保存路径充分安全，并对磁盘文件的内容进行强口令加密保护；对于采用存储介质存储密钥的，应确保使用的存储介质性能良好，并对存储介质进行强口令保护和妥善保管，所有口令需定期更换，密钥登记簿上应有密钥保护口令更新日期。

# 密钥的保管

1. 在人工参与密钥管理情况下，应用系统的密钥和密钥备份原则上由业务部门保管。专用信封、密钥存储介质等应标识密级，分秘密，机密，移交相关部门保管。
2. 为保证密钥的安全，密钥必须由专人保管；同时为保证密钥的可用性，应建立有效机制，确保应用系统在应急恢复等紧急情况下能够及时获取密钥。密钥保管人员的信息应填入《廊坊银行应用系统密钥安全管理人员信息表》（详见附件3），一旦密钥保管人员变动，密钥保管部门应负责及时更新此信息。
3. 专用信封、密钥存储介质应明确标识对应系统等内容，妥善保管，避免介质丢失造成密钥泄密等安全事件。

# 密钥的使用和分发

1. 密钥应按照密钥的用途分类使用，做到专钥专用，禁止不同用途的密钥混用。禁止不同类型的密钥取值相同。
2. 密钥应设定有效期，定期或不定期更换。
3. 在密钥分发过程中，应保障密钥的安全、分发渠道的可靠性和来源的真实性。
4. 应用系统可根据自身特点选择使用合适的密钥分发方式，但必须保障对称密钥和私钥的机密性、公钥的完整性。禁止以明文传输的方式分发密钥。密钥分发的方式主要包括：专用信封、密钥存储介质分发，密钥加密后联机传输；以数字证书方式分发的，可采用加密传输、口令保护方式；参考号与授权码方式下载证书及其私钥等。
5. 密钥的接受者必须验证专用信封的完整性，及时修改密钥介质的口令，禁止接受来源可疑、分发过程中可能泄露的密钥。

# 密钥的备份和恢复

1. 为防止因意外事故导致密钥无法使用，应备份密钥。
2. 密钥备份介质和文件的保管比照密钥介质和文件进行保管。
3. 严格控制密钥恢复，严禁私自恢复密钥。满足以下条件之一时，可提出密钥恢复请求，由相关部门审批、技术部门审批后，业务部门监督技术部门恢复密钥，并由业务部门开展业务验证。
4. 密钥存储介质口令丢失而导致密钥不能使用。
5. 密钥存储介质非恶意损坏而导致密钥不能使用。
6. 其他原因导致密钥不能使用。

# 密钥的撤销和更新

1. 为保障信息数据安全，当发生以下情况之一时，必须对密钥执行撤销、更新操作，将损失降到最低。
2. 密钥丢失。
3. 密钥发生泄漏或者怀疑发生泄漏。
4. 密钥的相关信息发生变更。
5. 应用系统或者证书颁发机构本身原因。
6. 密钥到期。
7. 其他重要原因导致撤销密钥。
8. 对于撤销或过期的密钥，其存储介质必须采用不可恢复的方式进行销毁。
9. 在密钥丢失、密钥泄露或怀疑密钥泄露等情况下，应及时更新密钥，禁止继续使用存在风险的密钥。

# 密钥管理的监督和检查

1. 负责密钥管理的人员应定期对所负责工作的规范性、安全性进行自查。对自查中发现的问题应及时制定整改措施，并落实执行。
2. 密钥管理相关部门应定期对所管辖范围内密钥使用和管理情况进行监督和检查，并将检查的结果和意见写入《廊坊银行应用系统密钥安全管理检查表》（详见附件4）。对督查中发现的违规行为要严格督促其进行整改。
3. 检查内容主要包括但不限于：密钥管理人员信息备档情况；密钥的生成、保管、使用、分发、备份（恢复）、撤销、更新情况；密钥保护口令设定和定期修改情况；密钥定期或不定期更新情况；密钥交接、领用登记情况。
4. 对于违反本规定的人员，将依照相关惩罚办法处理。

# 附 则

1. 本规定由廊坊银行负责制定、解释和修改。
2. 本规定适用于廊坊银行各部门、分支行主管的应用系统密钥的安全管理。
3. 本规定相应条款适用我行证书管理。
4. 本规定自发布之日起执行。

附件：

1.廊坊银行应用系统密钥登记簿（样式）

2.廊坊银行应用系统密钥操作申请（样式）

3.廊坊银行应用系统密钥安全管理人员信息表（样式）

4.廊坊银行应用系统密钥安全管理检查表（样式）

附件1:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **密钥用途** | |  | | | | | | | **密钥类型** | |  | | | **有效期** | | □长期 □其他 | |
| **保管部门** | | **分量1** | |  | | **存储介质** | | | □磁盘文件 □加密机 □IC卡 □USB-Key □其他□口令保护 | | | | | | | | |
| **分量2** | |  | | **存储介质** | | | □磁盘文件 □加密机 □IC卡 □USB-Key □其他□口令保护 | | | | | | | | |
| **分量3** | |  | | **存储介质** | | | □磁盘文件 □加密机 □IC卡 □USB-Key □其他□口令保护 | | | | | | | | |
| **变更记录** | | | | | | | | | | | | | | | | | |
| **序号** | **类型** | | **申请部门** | | **申请人** | | **操作日期** | **监督使用人（分量1）** | | **监督使用人（分量2）** | | **监督使用人（分量3）** | **实施人** | | **复核人** | | **备注：** |
|  | 密钥  □创建密钥 □备份密钥  □恢复密钥 □撤销密钥  □更新密钥  密钥保护口令  □创建口令 □更新口令 | |  | |  | |  |  | |  | |  |  | |  | |  |
|  | 密钥  □创建密钥 □备份密钥  □恢复密钥 □撤销密钥  □更新密钥  密钥保护口令  □创建口令 □更新口令 | |  | |  | |  |  | |  | |  |  | |  | |  |
|  | 密钥  □创建密钥 □备份密钥  □恢复密钥 □撤销密钥  □更新密钥  密钥保护口令  □创建口令 □更新口令 | |  | |  | |  |  | |  | |  |  | |  | |  |
|  | 密钥  □创建密钥 □备份密钥  □恢复密钥 □撤销密钥  □更新密钥  密钥保护口令  □创建口令 □更新口令 | |  | |  | |  |  | |  | |  |  | |  | |  |

廊坊银行应用系统密钥登记簿

说明：1．A4幅面各行自行印制。2．登记簿需编制页号、装订成册、单独保管并归档。

3．密钥类型为主密钥、一般密钥、证书等。4.备注项可关联OA审批单等。

附件2：

廊坊银行应用系统密钥操作申请

|  |  |  |  |
| --- | --- | --- | --- |
| **申请部门** |  | **申请日期** |  |
| **申请人** |  | **联系电话** |  |
| **申请类型** | □密钥创建 □密钥备份□密钥恢复  □密钥撤销 □密钥更新 □其他 | | |
| **密钥分量** |  | | |
| **申请原因及内容** |  | | |
| **业务主管部门意见** | 监督使用人：  日 期： | | |
| **信息技术部意见** | 监督使用人：  日 期： | | |
| **技术实施记录** |  | | |
| **业务验证结果** |  | | |

说明：1．A4幅面各行自行印制。

2．登记簿需编制页号、装订成册、单独保管并归档。

附件3：

廊坊银行应用系统密钥安全管理人员信息表

|  |  |
| --- | --- |
| **姓名** |  |
| **所属部门** |  |
| **联系电话** |  |
| **岗位角色** | □密钥管理人员 □密钥保管员□其他 |
| **管理的系统及密钥类型** |  |
| **工作职责** |  |
| **主管领导签字** |  |
| **备注** |  |

说明：1．A4幅面各行自行印制。

2．登记簿需编制页号、装订成册、单独保管并归档。

附件4：

廊坊银行应用系统密钥安全管理检查表

|  |  |
| --- | --- |
| **应用系统密钥安全管理检查内容** | **备注** |
| **密钥管理人员信息备档情况：**  **密钥的生成、保管、使用、分发、备份（恢复）、撤销、更新情况：**  **密钥保护口令设定和定期修改情况：**  **密钥定期或不定期更新情况：**  **密钥交接、领用登记情况：**  检查人员：  日 期： |  |
| **应用系统密钥安全管理检查问题及意见** | **备注** |
| 检查人员：  日 期： |  |

说明：1．A4幅面各行自行印制。

2．登记簿需编制页号、装订成册、单独保管并归档。

1. [↑](#endnote-ref-2)