ICS 35.240.01
CCS L 67

团　体　标　准

T/ZSPH XXX-2024

数字家庭密码应用技术要求

Technical requirements for digital home cryptographic application

（征求意见稿）

2024-**-**发布　　2024-**-** 实施

中关村乐家智慧居住区产业技术联盟 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。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中关村乐家智慧居住区产业技术联盟提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

数字家庭是以住宅为载体，利用物联网、云计算、大数据、移动通信、人工智能等新一代信息技术，实现政务服务、社会化服务和家居产品智能化服务的互联互通互融，满足用户信息获取和使用的数字化家庭生活服务系统。数字家庭中智能家居设备互联互通日益加强，所采集的家庭数据在居家养老、家庭健康、家庭娱乐、社区治理、社区服务、电商购物等方面蕴藏巨大价值，个人信息与隐私泄露的风险随之而来，智能家居产品的安全访问控制也在经历巨大考验。

密码技术作为信息安全核心防护手段，对保护数字家庭基础平台及物联网智能设备安全性起着至关重要的作用。因此，从技术层面对数字家庭密码应用的设计、实现与使用进行要求，具有重大现实意义。

本文件根据数字家庭自身特点制定数字家庭密码应用技术要求，以促进我国数字家庭密码应用技术规范化与健康发展。

数字家庭密码应用基本要求

1 范围

本文件规定了密码在数字家庭应用中的技术要求，从密码应用的真实性、机密性、完整性、不可否认性提出了密码服务平台面向数字家庭基础平台、数字家庭APP、住宅用综合信息箱、智能设备等方面的密码支撑服务技术要求。

本文件适用于指导、规范数字家庭密码应用的规划、建设、运行及密码应用安全性评估。

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。

GB/T 39786 信息安全技术 信息系统密码应用基本要求

T/ZSPH 02 数字家庭密码建设评价标准

T/ZSPH 02 数字家庭网关软件总线技术要求

GM/T 0002 SM4分组密码算法

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

密码服务平台 cryptographic service platform

全称数字家庭行业密码服务平台，是统一密码基础设施，为数字家庭提供统一密码服务，底层资源为密码资源池。

3.2

数字家庭 digital home

以住宅为载体，利用物联网、云计算、大数据、人工智能等新一代信息技术，实现设备、系统、家居产品的互联互通，满足用户信息获取和使用的数字化家庭生活服务系统。

[来源：T/ZSPH 02—2022，3.2]

3.3

数字家庭APP digital home APP

数字家庭基础平台移动应用程序，为用户提供人机交互操作界面，承担数据上传下达功能。

3.4

数字家庭基础平台 digital home basic platform

一个为家庭用户和企业提供设备互联互通管理和服务获取功能的综合性平台，涵盖智能化服务、政务服务和社会化服务三大服务功能。

3.5

住宅用综合信息箱 residential integrated information box

由箱体以及功能模块组成，安装在居住单元套（户）内，用于实现居住单元的宽带接入、路由交换、有线电视线缆配线接入和分配， 以及数字家庭智能化设备接入、管理、 控制和家庭数据安全存储、边缘计算功能的设备箱。

[来源：T/ZSPH 03—2022，3.2]

3.6

智能设备 intelligent device

具有网络通信功能，可自描述、发布并能与其他节点进行交互操作的智能化家庭设备。

3.7

安全模块 security module

相对独立的软件或硬件模块，能够提供密码运算功能并提供调用接口。

3.8

密码算法 cryptographic algorithm

描述密码处理过程的运算规则

3.9

密码杂凑算法 cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

（3）要发现不同的输入映射到同一输出是计算上困难的。

3.10

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.11

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.12

对称密钥 symmetric secret key

信息的发送方加密数据和信息的接收方解密数据所使用的密钥相同。

3.13

公钥/私钥 public key/private key

非对称密码算法中可以公开的密钥称为公钥。非对称密码算法中只能由拥有者使用的不公开密钥称为私钥

3.14

加密/解密 encipherment/encryption / decipherment/decryption

加密是对数据进行密码变换以产生密文的过程。
解密是加密过程对应的逆过程。

3.15

数字签名 /验证 digital Signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

验证是验证者使用签名者的公开密钥对数字签名进行验证的过程。

3.16

数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.17

真实性 authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

3.18

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

3.19

完整性 data integrity

数据没有遭受以非授权方式所作的改变的性质。

3.20

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

4 缩略语

下列缩略语适用于本文件。
APP 应用程序（Application）
DEK 数据加密密钥（data encryption key）
HMAC 密钥相关的哈希运算消息认证码（Hash-based Message Authentication Code）
IOT 物联网（Internet of Things）
KEK 密钥加密密钥（key encryption key）
PC 个人电脑（Personal Computer）
PKI 公钥基础设施（Public Key Infrastructure）
RESTful API 行业密码服务平台对外服务接口
SE 安全模块（Secure Element）

5 数字家庭密码应用基本模型

5.1 数字家庭系统组成

数字家庭系统系统组成如图 1 所示。

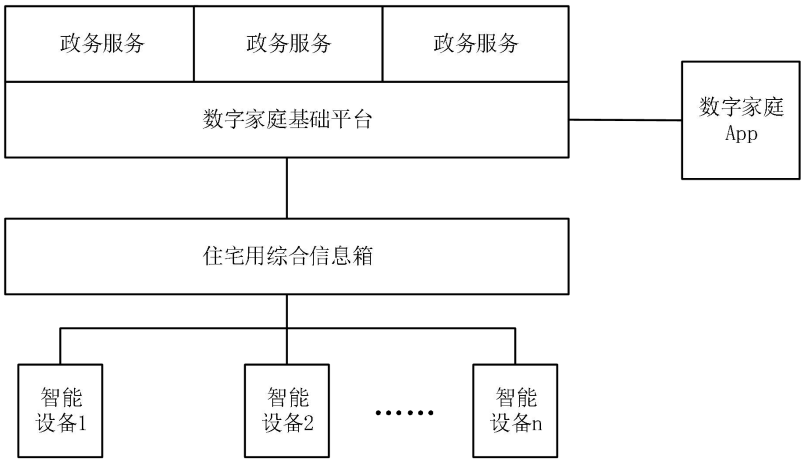

图 1 数字家庭系统组成

数字家庭系统由数字家庭 APP、数字家庭基础平台、住宅用综合信息箱和智能设备四个部分组成，各部分描述如下：

a) 数字家庭 APP 是用户统一入口，包含智控、社区、政务等板块，提供智能家电远程控制功能、跨生态智能设备控制、场景化定制等功能；
b) 数字家庭基础平台承载政务服务、社会化服务和产品智能化服务，提供统一的交互入口；
c) 住宅用综合信息箱是家庭智能控制终端，具有存储、算力等功能，可实现不同协议以及数据格式转换，并实现设备本地接入及离线控制；
d) 智能设备包括智能照明、智能安防、智能家电、智能环境、智能门窗、智能影音、消防安全监测等设备。

5.2 数字家庭密码应用架构

5.2.1 通用要求

密码服务平台是数字家庭密码应用架构的核心，负责提供身份验证、数据加密等安全服务，保护数字家庭App、数字家庭基础平台、住宅用综合信息箱和智能设备间的通信和数据安全。密码应用应符合以下通用要求：

a) 数字家庭各组成部分使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
b) 数字家庭各组成部分使用的密码技术应遵循密码相关国家标准和行业标准；
c) 数字家庭各组成部分使用的密码产品、密码服务应符合法律法规的相关要求。

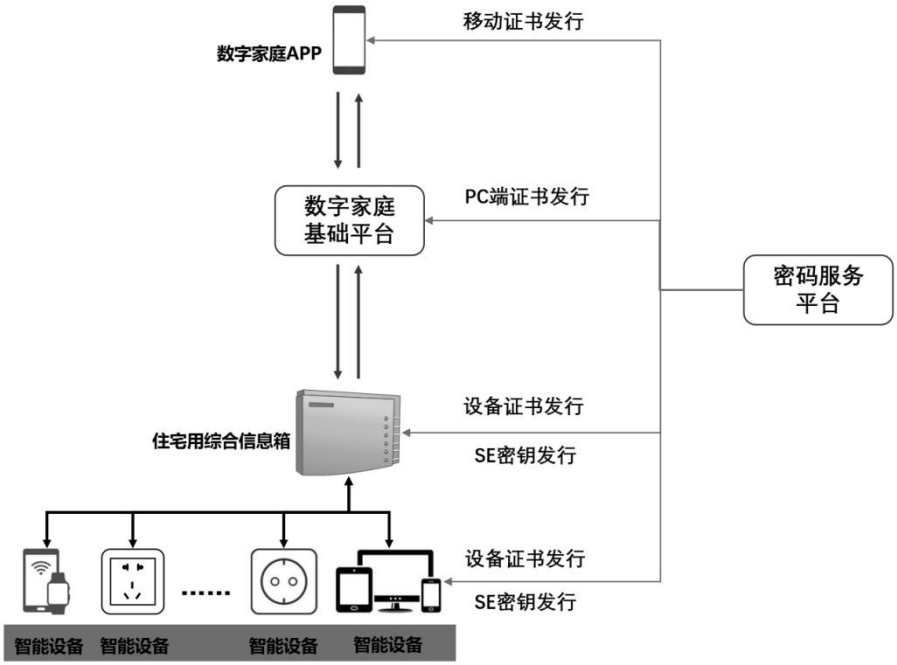

图 2 密码应用框架及证书和密钥分发

5.2.2 证书和密钥发行

数字家庭证书和密钥的发行需满足以下需求：

a) 密码服务平台向数字家庭各组成部分发行密钥，IOT 端即住宅用综合信息箱和智能设备的密钥应包含 SEID、控制密钥、EF10 安全信息文件等；密码服务平台向数

字家庭基础平台和数字家庭 APP 发行加密密钥对；

b） 密码服务平台向数字家庭各组成部分发行国密双证书，即签名证书和加密证书，签名证书用于数字签名，加密证书用于数据加密。数字证书应符合 GM/T 0015 要求；

c） 数字家庭 APP 应具有软件安全模块，软件安全模块具有密钥产生能力；

d） 住宅用综合信息箱应具有硬件安全模块，硬件安全模块具有密钥产生能力；

e） 传感类设备应具有硬件安全模块，硬件安全模块具有密钥产生能力；

f） 非传感类智能设备宜具有密钥产生能力的硬件安全模块；

g） 后续通讯数据加密应使用对称密钥结合非对称密钥；

h） 数字证书应有使用期限并定时更新；

i） 密钥应有使用期限并定期进行更新。

5.2.3 身份认证

数据家庭的身份认证流程如图 3 所示，需满足以下需求：

a） 数字家庭 APP 在接入数字家庭基础平台时，数字家庭基础平台应与数字家庭 APP 进行双向认证；

b） 传感类智能设备在接入住宅用综合信息箱时，住宅用综合信息箱应与智能设备进行双向认证；

c） 非传感类智能设备在接入住宅用综合信息箱时，住宅用综合信息箱宜与智能设备进行双向认证；

d） 住宅用综合信息箱在接入数字家庭基础平台时，数字家庭基础平台应与住宅用综合信息箱进行双向认证；

e） 密码服务平台为数字家庭基础平台提供的身份认证接口应符合 GM/T 0018 和 GM/T 0019 的规定。

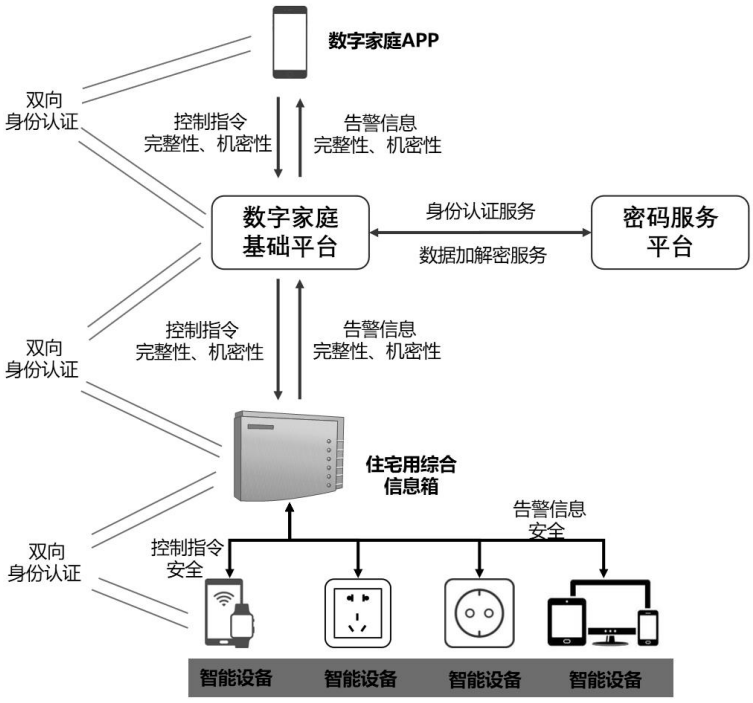

图 3 身份认证流程及数据加密

5.2.4 数据加密

数据加密需满足以下需求：

a) 数字家庭 APP 与数字家庭基础平台通信、住宅用综合信息箱与数字家庭基础平台通信，要做数据加密，保证数据传输的机密性和完整性；
b) 智能设备与住宅用综合信息箱通信，要做数据加密，保证数据传输的机密性和完整性；
c) 数字家庭 APP、数字家庭基础平台、住宅用综合信息箱、智能设备要对本地存储的重要数据做加密，保证数据存储的机密性和完整性；
d) 密码协议和密钥管理应符合 GM/T 0026 的规定；
e) 对称密码算法应采用符合 GM/T 0002 要求的 SM4 算法；
f) 非对称密码算法应采用符合 GM/T 0003 要求的 SM2 算法；
g) 密码杂凑算法应采用符合 GM/T 0004 要求的 SM3 算法并结合 HMAC；
h) 随机数发生及检测标准应符合 GM/T 0005 的要求；
f) 密码服务平台为数字家庭基础平台提供的数据加解密接口应符合 GM/T 0018 和 GM/T 0019 的规定。

6 密码应用基本要求

6.1 数字家庭 APP 密码应用要求

6.1.1 真实性要求

a) 数字家庭 APP 应配置安全模块，保障软件的物理真实性。
b) 数字家庭 APP 应具有密码管理平台发布的数字证书和密钥，用于通信时的身份鉴别，提供安全功能。
c) 数字家庭 APP 应与安全模块唯一绑定。
d) 数字家庭 APP 与数字家庭基础平台通信时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别。具体流程见附录 B 中的 B.1。

6.1.2 机密性要求

a) 数字家庭 APP 与数字家庭基础平台通信时，应采用密码技术建立安全的信息传输通道，保证通信过程中重要数据的机密性。
b) 数字家庭 APP 与数字家庭基础平台通信时，对向数字家庭基础平台发送的控制指令进行密文处理，采用对称算法加密保护，保证数据传输的机密性。具体流程见附录 E 中的 E.1。
c) 数字家庭 APP 应对本地存储的重要数据，包括日志信息、用户敏感信息、密钥数据、身份鉴别数据等进行机密性保护，采用对称算法加密保护。

6.1.3 完整性要求

a) 数字家庭 APP 与数字家庭基础平台通信时，应采用密码技术建立安全的传输通道，保证通信过程中重要数据的完整性。
b) 数字家庭 APP 对向数字家庭基础平台发送的控制指令进行完整性保护，应采用带密钥的密码杂凑算法保障指令来源的完整性。具体流程见附录 E 中的 E.1。
c) 数字家庭 APP 对本地存储的重要数据，包括日志记录、用户敏感信息、密钥数据、身份鉴别数据等进行完整性保护，应采用带密钥的密码杂凑算法保证重要数据的完整性。

6.1.4 不可否认性

a) 数字家庭 APP 对下发数字家庭基础平台的控制指令做数字签名，应采用基于公钥密码算法的数字签名机制，保障下发指令行为的不可否认性。具体流程见附录 E

中的 E.1。

b) 数字家庭 APP 对保存的日志信息做数字签名，应采用基于公钥密码算法的数字签名机制，保障日志信息的不可否认性。

6.2 数字家庭基础平台密码应用要求

6.2.1 真实性要求

a) 数字家庭基础平台应有密码服务平台下发的数字证书和密钥，用于通信时的身份鉴别，提供安全功能。

b) 数字家庭基础平台与数字家庭 APP 通信时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别，具体流程见附录 B 中的 B.1。

c) 数字家庭基础平台与住宅用综合信息箱通信时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别，具体流程见附录 B 中的 B.1。

d) 其他层面的身份鉴别，应符合 GB/T 39786 的要求。

6.2.2 机密性要求

a) 数字家庭基础平台与住宅用综合信息箱通信时，对向住宅用综合信息箱下发的控制指令应进行密文处理，采用对称算法加密保护，实现机密性，具体流程见附录 E 中的 E.2。

b) 数字家庭基础平台与数字家庭 APP 通信时，对向数字家庭 APP 回传的告警信息应进行密文处理，采用对称算法加密保护，实现机密性，具体流程见附录 E 中 E.3。

c) 数字家庭基础平台应对本地存储的重要数据，包括密钥信息、身份鉴别信息、日志记录、用户个人敏感信息、重要的业务数据等进行机密性保护，采用对称算法加密保护。

d) 其他层面的机密性实现要求，应符合 GB/T 39786 中的要求

6.2.3 完整性要求

a) 数字家庭基础平台对向住宅用综合信息箱下发的控制指令进行完整性保护，应采用带密钥的密码杂凑算法保障指令来源的完整性。具体流程见附录 E 中的 E.2。

b) 数字家庭基础平台对向数字家庭 APP 回传的告警信息进行完整性保护，应采用带密钥的密码杂凑算法保障告警信息来源的完整性。具体流程见附录 E 中的 E.3。

c) 数字家庭基础平台对本地存储的重要数据，包括密钥信息、身份鉴别信息、日志记录、用户个人敏感信息、重要的业务数据等进行完整性保护，应采用带密钥的密码杂凑算法保障重要数据的完整性。

d) 其他层面的完整性实现要求，应符合 GB/T 39786 中的要求

6.2.4 不可否认性要求

a) 数字家庭基础平台对下发住宅用综合信息箱的控制指令做数字签名，应采用基于公钥密码算法的数字签名机制，保障下发指令行为的不可否认性。具体流程见附录 E 中的 E.2。

b) 数字家庭基础平台对上报数字家庭 APP 的告警信息做数字签名，应采用基于公钥密码算法的数字签名机制，保障下发指令行为的不可否认性。具体流程见附录 E 中的 E.3。

c) 数字家庭基础平台对保存的日志信息做数字签名，应采用基于公钥密码算法的数字签名机制，保障日志信息的不可否认性。

6.3 住宅用综合信息箱密码应用要求

6.3.1 真实性要求

a) 住宅用综合信息箱应内置 SE 芯片，保障信息箱的物理真实性。
b) 住宅用综合信息箱应具有密码管理平台发布的数字证书和 SE 密钥，用于通信时的身份鉴别，提供安全功能。
c) 住宅用综合信息箱设备应与 SE 芯片唯一绑定。
d) 智能设备接入住宅用综合信息箱时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别。具体流程见附录 B 中的 B.1。
e) 住宅用综合信息箱与数字家庭基础平台通信时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别。具体流程见附录 B 中的 B.1。住宅用综合信息箱的用户登录操作系统、登录数据库时，可采用基于口令的身份鉴别与访问控制机制，用于鉴别用户身份的真实性。具体流程见附录 C 中的 C.1。
f) 住宅用综合信息箱的运维人员登录操作系统、登录数据库时，可采用基于口令的身份鉴别与访问控制机制，用于鉴别运维人员身份的真实性。具体流程见附件 C 中 C.1。
g) 住宅用综合信息箱及安全模块的固件升级时，应采用基于公钥密码算法的数字签名机制，保证升级包的真实性。具体流程见附录 D 中 D.1。

6.3.2 机密性要求

a) 住宅用综合信息箱与智能设备通信时，对向智能设备发送的指令应进行密文处理，采用对称算法加密保护，防止第三方窃取。加密流程见附录 E 中 E.1。
b) 住宅用综合信息箱与数字家庭基础平台通信时，对向数字家庭基础平台回传的告警信息，应进行密文处理，采用对称算法加密保护，实现机密性。加密流程见附录 E 中 E.2。
c) 住宅用综合信息箱应对本地存储的重要数据，包括安防数据、环境数据、设备告警数据、个人健康档案数据、下级设备信息及日志信息进行机密性保护，采用对称算法加密保存。
d) 住宅用综合信息箱及安全模块，可对固件升级包进行密文处理，在固件升级包生成时，采用对称算法加密并以密文的形式传输和升级使用。加密流程见附录 D 中 D.1。
e) 住宅用综合信息箱应保证重要数据在网络传输过程中不被第三方窃取，应采用对称算法加密处理，以密文形式传输，同时采用数字信封技术保护对称密钥。具体流程见附录 E 中 E.3。

6.3.3 完整性要求

a) 住宅用综合信息箱对向智能设备发送的控制指令进行完整性保护，应采用带密钥的密码杂凑算法保障指令来源的完整性。具体流程见附录 E 中 E.1。
b) 住宅用综合信息箱对向基础平台回传的告警信息做完整性保护，应采用带密钥的密码杂凑算法保障告警信息来源的完整性。具体流程见附录 E 中 E.2。
c) 住宅用综合信息箱对本地存储的重要数据，包括安防数据、环境数据、设备告警数据、个人健康档案数据、下级设备信息及日志信息进行完整性保护，应采用带密钥的密码杂凑算法保障重要数据的完整性。
d) 住宅用综合信息箱及安全模块，对固件升级包进行完整性保护，在固件升级包生成时，应采用带密钥的密码杂凑算法对升级包进行保护，保障升级包内容的完整性。在执行升级包时，应采用带密钥的密码杂凑算法对升级包的完整性进行校验。具体流程见附件 D 中的 D.1。

6.3.4 不可否认性要求

a) 住宅用综合信息箱对下发智能设备的控制指令做数字签名，应采用基于公钥密码

算法的数字签名机制，保障下发指令行为的不可否认性。具体流程见附录 E 中 E.1。

b) 住宅用综合信息箱对上报数字家庭基础平台的告警信息做数字签名，应采用基于公钥密码算法的数字签名机制，保障数据上报行为的不可否认性。具体流程见附录 E 中 E.2。

c) 住宅用综合信息箱对保存的日志信息做数字签名，应采用基于公钥密码算法的数字签名机制，保障日志信息的不可否认性。

6.4 智能设备密码应用要求

6.4.1 真实性要求

a) 智能设备关键设备类应内置 SE 芯片，非关键设备类宜内置 SE 芯片，保障智能设备的物理真实性。

b) 智能设备关键设备类应具有密码管理平台发布的数字证书和 SE 密钥，用于通信时的身份鉴别，提供安全功能。

c) 智能设备关键设备类应与 SE 芯片唯一绑定。

d) 智能设备关键设备类接入住宅用综合信息箱时，应采用基于数字证书的双向身份认证机制，用于通信双方的身份鉴别。具体流程见附录 B 中的 B.1。

e) 智能设备关键设备类安全模块固件升级时，应采用基于公钥密码算法的数字签名机制，保证升级包的真实性。具体流程见附录 D 中 D.1。

6.4.2 机密性要求

a) 智能设备关键设备类对向住宅用综合信息箱回传的告警信息进行加密保护，应采用对称算法，实现机密性。具体流程见附录 E 中 E.2。

b) 智能设备关键设备类对本地存储的重要数据，包括重要参数、上级设备信息、环境数据、设备告警数据、及日志信息进行机密性保护，应采用对称算法加密保存。

c) 智能设备关键设备类对安全模块固件升级包进行密文处理，在固件升级包生成时，可采用对称算法加密并以密文的形式升级使用。加密流程见附件 D 中 D.1。

6.4.3 完整性要求

a) 智能设备关键设备类对向基础平台回传的告警信息进行完整性保护，应采用带密钥的密码杂凑算法保障命令的完整。具体流程见附录 E 中 E.2。

b) 智能设备关键设备类对本地存储的重要数据，包括重要参数、上级设备信息、环境数据、设备告警数据、及日志信息进行完整性保护，应采用带密钥的密码杂凑算法保障重要数据的完整性。

c) 智能设备关键设备类的安全模块，对固件升级包进行完整性保护，在固件升级包生成时，应采用带密钥的密码杂凑算法对升级包进行保护，保障升级包内容的完整性。在执行升级包时，应采用带密钥的密码杂凑算法对升级包的完整性进行校验。具体流程见附件 D 中的 D.1。

6.4.4 不可否认性要求

a) 智能设备关键设备类对回传数字家庭基础平台的告警信息做数字签名，应使用基于公钥密码算法的数字签名机制，保障数据上报行为的不可否认性。具体流程见附录 E 中 E.2。

b) 智能设备关键设备类对保存的日志信息做数字签名，应使用基于公钥密码算法的数字签名机制，保障这一行为的不可否认性。

附录 A

（资料性）

密码服务平台密钥管理

密钥管理是密码服务平台的核心功能，负责对称密钥、非对称密钥的安全产生和安全存储，以及各类密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和密钥管理服务。密钥管理主要包括密钥模板管理、预激活密钥管理、KEK 密钥管理、DEK 密钥管理、密钥司法取证、密钥归档以及应用主密钥管理等功能。

a） 密钥模板管理：

在密钥模板中支持定义创建密钥对象的产生策略信息，用于简单快速的创建应用所需密钥对象，密钥模板管理功能包括新增密钥模板、修改密钥模板、删除密钥模板和查询密钥模板。密钥模板中支持配置模板名称、模板标识、密钥类型、密钥算法、算法参数、密钥长度、密钥用途、密钥有效期，以及支持配置密钥是否运行导出等相关策略。

b） 密钥创建：

密钥创建功能支持录入密钥名称、所属应用、指定密钥模板等信息，也可以基于密钥模板的密钥产生策略进行修改，重新指定密钥产生和策略信息创建出符合应用需求的 KEK 密钥或 DEK 密钥数据。

c） 应用主密钥管理：

每个应用系统在平台中注册后都会产生对应的应用主密钥，应用主密钥主要用于保护应用所需要的 KEK 和 DEK，以及保护此应用下的所有密钥数据。多个应用之间密钥数据以应用主密钥体系进行隔离保护，一个应用主密钥的泄露不会产生其他应用密钥数据的安全风险。应用主密钥支持查询和更新操作，在应用主密钥更新时，系统内部维护主密钥数据的版本，以确保应用内密钥数据的保护关系。

d） 备用密钥管理：

备用密钥管理可以理解为在应用使用密钥之前，批量产生各类对称密钥或非对称密钥，在应用需要使用相关类型和策略密钥的时候可以直接绑定或提取使用。备用密钥管理功能包括即时产生密钥、定时产生密钥、备用密钥统计、备用密钥销毁等功能。

e） KEK 密钥管理：

KEK 密钥是密钥加密密钥，主要用于某些应用场景下保护数据加密密钥 DEK。KEK 密钥根据实际应用业务场景选择使用。KEK 密钥管理包括密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和 KEK 密钥管理服务。

1） KEK 密钥更新，系统内会自动维护密钥版本，便于业务可以选择密钥进行加密以及自动匹配密钥解密操作；

2） KEK 密钥失信，密钥失信后不能进行加密和解密业务；

3） KEK 密钥注销（停用），密钥注销后不能进行加密业务；

4） KEK 密钥销毁，密钥销毁后不能进行加密和解密业务；

5） KEK 密钥恢复，对注销（停用）状态的密钥可以进行密钥恢复操作，密钥恢复后可以继续进行业务的加解密操作。

f） DEK 密钥管理

DEK 密钥是数据加密密钥，用于保护应用系统中的业务数据。DEK 密钥管理包括密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和 DEK 密钥管理服务。

1） DEK 密钥更新，系统内会自动维护密钥版本，便于业务可以选择密钥进行加密以及自动匹配密钥解密操作；

2） DEK 密钥失信，密钥失信后不能进行加密和解密业务；

3） DEK 密钥注销（停用），密钥注销后不能进行加密业务；

4） DEK 密钥销毁，密钥销毁后不能进行加密和解密业务；

5） DEK 密钥恢复，对注销（停用）状态的密钥可以进行密钥恢复操作，密钥恢复后可以继续进行业务的加解密操作。

g） 密钥司法取证

当在某些特定情况下，需要在密钥管理中提取某个应用的某个密钥数据时，系统支持对 KEK 和 DEK 的司法取证操作。司法取证操作时，需要多个司法取证操作员在场，根据平台配置的司法取证认证策略，验证 MofN 数量的司法取证员身份，验证通过后可以把对应的密钥数据以密文的形式安全导出。再进一步根据业务需要对提取出的密钥数据进行相关应用。

h） 密钥归档

系统支持对过期密钥或某些确定不用的密钥数据进行归档操作，以减轻密钥管理的管理负担。密钥归档支持对称密钥和非对称密钥按密钥过期状态和密钥管理状态进行归档操作。密钥归档后进入单独的密钥归档数据表中，作为历史数据备份存储，同时支持密钥归档查询功能。

附录 B

（规范性）

基于数字证书的双向身份认证

B.1 基本要求

a) 在附录 B 的描述中，字母 S 代表双向认证的发送方，字母 R 代表双向认证的接收方。
b) 该附录描述的是基于 PKI 的双向身份认证机制。

双向身份认证前提：

a) 发送方通过 SE，生成签名密钥对。
   发送方从密钥管理系统处，获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。
b) 接收方通过 SE，生成签名密钥对。
   接收方从密钥管理系统处，获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。

B.1 基于数字证书的双向身份认证

双向身份认证流程描述：

a) 发送方 S 向接收方 R 发起身份认证请求。
b) 接收方 R 向发送方 S 返回随机数 Random_R。
c) 发送方 S 用签名密钥对中的私钥对随机数 Random_R、发送方签名数字证书 ID 进行签名，生成签名值 Sigature_S。
   发送方将签名值 Sigature_S、签名数字证书 Certi_Sign_S 发送给接收方 R。
d) 接收方 R 收到数据后，用 CA 根证书验证发送方签名数字证书 Certi_Sign_S 的有效性，用发送方签名数字证书 Certi_Sign_S 验证签名值 Sigature_S 的有效性，验证发送方签名数字证书 ID 的正确性，以上验证都通过，证明发送方身份合法，继续进行下面步骤，否则发送错误提示到发送方，关闭通信。
e) 接收方 R 向发送方 S 发起身份认证请求。
f) 发送方 S 向接收方 R 返回随机数 Random_S。
g) 接收方 R 用签名私钥对中的私钥对随机数 Random_S、接收方签名数字证书 ID 进行签名，生成签名值 Sigature_R。
   接收方 R 将签名值 Sigature_R、签名数字证书 Certi_Sign_R 发送给发送方 S。
h) 发送方 S 收到数据后，用 CA 根证书验证接收方签名数字证书 Certi_Sign_R 的有效性，用接收方签名数字证书 Certi_Sign_R 验证接收方签名值 Sigature_R 的有效性，验证接收方签名数字证书 ID 的正确性，以上验证都通过，证明接收方的身份合法，双方继续后面的通信。否则发送错误提示到接收方，关闭通信。

双向身份认证流程图：

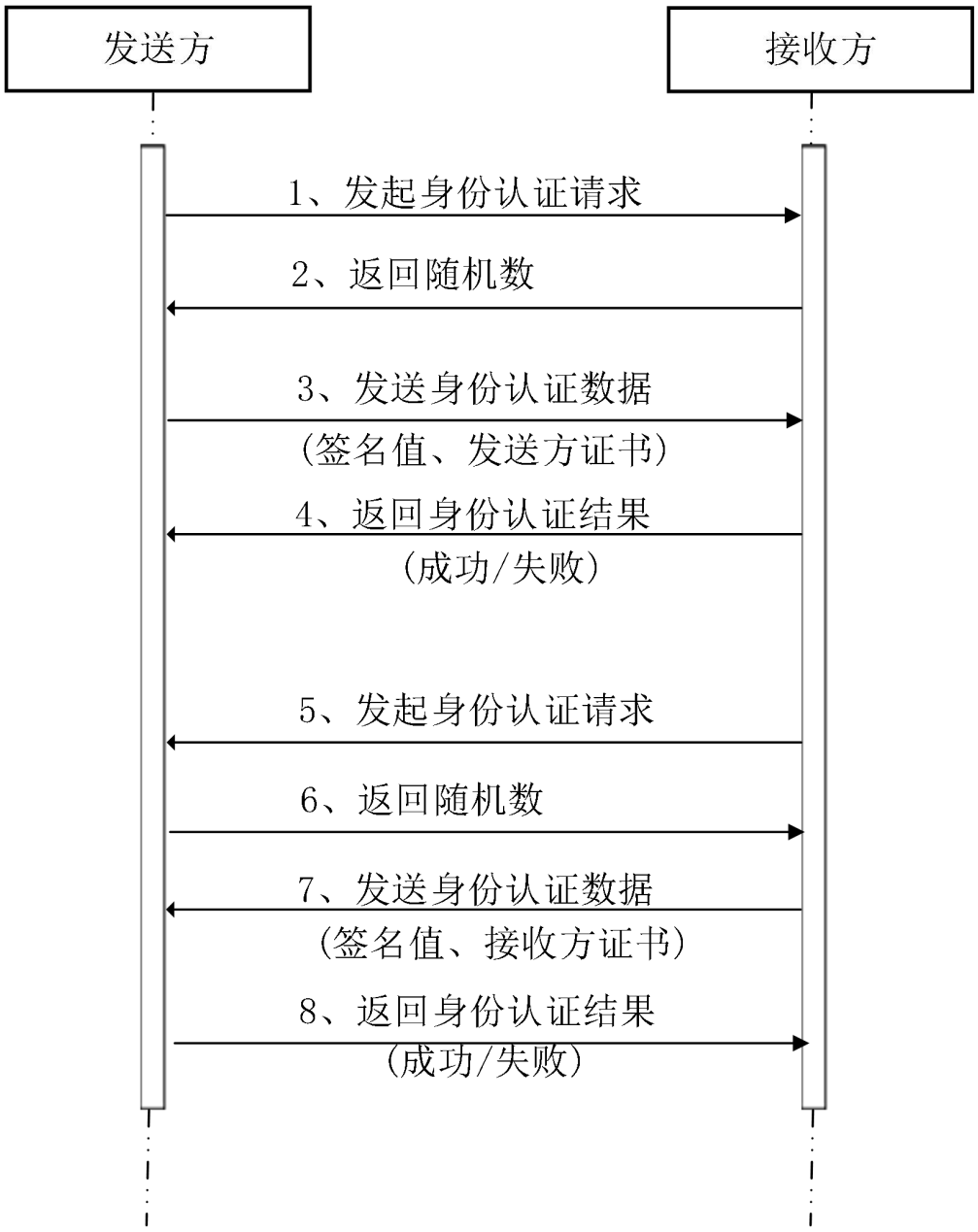

图 B.1　基于数字证书的双向身份认证

附录 C

（规范性）

基于口令的身份鉴别与访问控制机制

C.1 用户登录住宅用综合信息箱时基于口令的身份鉴别与访问控制机制

用户登录住宅用综合信息箱的操作系统、数据库时，应采用基于口令的身份鉴别与访问控制机制，鉴别流程如下：

a) 用户首次登录住宅用综合信息箱操作系统时，输入用户名和口令进行注册，选择角色为用户角色。操作系统将用户名和口令经过密码杂凑算法处理后，将 hash 值存储于内部数据库，并依据用户角色分配相应的访问权限。

b) 当用户登录时，获取信息箱的随机数，系统采用输入的用户名和口令的 hash 值作为对称密钥， 加密随机数得到密文，将密文传输给信息箱。信息箱使用第 1>步中存储的 hash 值作为对称密钥对密文进行解密，对比解密结果与随机数是否一致，如一致，用户登录成功。不一致，给出错误提示，用户登录失败。

c) 用户登录成功后，只能访问权限范围内的内容。

C.2 运维人员登录住宅用综合信息箱时基于口令的身份鉴别与访问控制机制

运维人员登录住宅用综合信息箱的操作系统、数据库时，应采用基于口令的身份鉴别与访问控制机制，鉴别流程如下：

a) 运维人员首次登录信息箱操作系统时，输入用户名和口令进行注册，选择角色为运维人员。系统将用户名和口令经过密码杂凑算法处理后，将 hash 值存储于内部数据库中，并依据运维人员角色分配相应的访问权限。

b) 当运维人员登录时，获取信息箱的随机数，系统采用输入的用户名和口令的 hash 值作为对称密钥，加密随机数得到密文，将密文传输给信息箱。信息箱使用第 1>步中存储的 hash 值作为对称密钥对密文进行解密，对比解密结果与随机数是否一致，如一致，运维人员登录成功。不一致，给出错误提示，运维人员登录失败。

c) 运维人员登录成功后，只能访问权限范围内的内容。

附录 D

（规范性）

安全模块固件升级流程

D.1 基本要求

安全模块固件升级基本要求：

a) 安全模块内部生成一对签名密钥对，该密钥对仅用于安全模块固件升级时，对固件升级包的签名和验签。安全模块出厂时，预置该密钥对到安全模块中。

b) 安全模块内部生成一支对称密钥，该密钥用于固件升级包的加密、解密。安全模块出厂时，预置该密钥到安全模块中。

D.2 制作固件升级包、执行固件升级包

安全模块固件升级包括两步，第一，制作固件升级包；第二，执行固件升级包。

制作固件升级包：

a) 安全模块使用密码杂凑算法对固件升级包进行哈希运算，得到哈希值 Hash_A。

b) 安全模块使用预置的签名密钥对中的私钥对哈希值 Hash_A 进行签名，得到签名值 Signature_A。

c) 安全模块使用预置的对称密钥，采用对称加密算法对升级包、签名值 Signature_A、签名算法，签名数字证书等进行加密，得到密文升级包 ciphertext_A。

同时，采用数字信封技术，用接收方的公钥加密对称密钥，将对称密钥密文传递给接收方，参见 E.3 数字信封的使用。（该加密步骤为可选项）。

d) 若执行了第 3>步，则安全模块厂商将密文升级包、对称密钥密文发送给接收方。

若未执行第 3>步，则安全模块厂商将升级包、签名值发送给接收方。

执行固件升级包：

a) 若接收方收到的是密文升级包 ciphertext_A、对称密钥密文，接收方用自己的私钥解密对称密钥密文得到对称密钥。用对称密钥解密密文升级包 ciphertext_A，得到升级包和签名值 Signature_A。继续执行第 2>步。

若接收方收到的是升级包和签名值，则直接执行第 2>步。

b) 接收方使用对方公钥，对签名值 Signature_A 验签。若验证通过，证明安全模块的身份合法，可以进行固件升级。若验证不通过，说明安全模块身份不合法，进行报警提示。

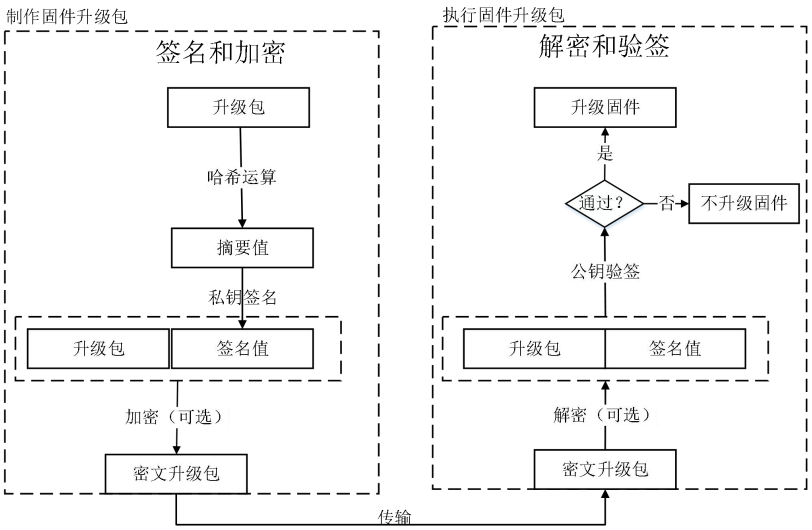

图 D.1　制作、执行固件升级包流程

附录 E

（规范性）

数字家庭 APP、数字家庭基础平台安全流程

住宅用综合信息箱执行附录 E.1 和附录 E.2 的基本要求：

a) 数字家庭 APP 通过安全模块生成签名密钥对，并预置在安全模块内。
数字家庭 APP 从密钥管理系统处，获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。
数字家庭 APP 通过安全模块生成一支对称密钥，并预置在安全模块内。

b) 数字家庭基础平台通过安全模块生成签名密钥对，并将私钥信息进行加密保存
数字家庭基础平台从密码服务平台处获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。
数字家庭基础平台所需要的密码算法和密钥支撑均由密码服务平台提供。

E.1 数字家庭 APP 下发指令流程

数字家庭 APP 下发指令流程：

a) 数字家庭 APP 向数字家庭基础平台下发控制指令。

b) 数字家庭 APP 应使用密码机制对下发控制指令进行安全处理，先对指令进行哈希运算，再使用签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给数字家庭基础平台。
同时，采用数字信封技术，使用数字家庭基础平台的公钥加密数字家庭 APP 产生的对称密钥，将对称密钥密文传递给数字家庭基础平台。

c) 数字家庭基础平台调用密码服务平台相应解密接口，对接收到的密文信息进行解密并进行完整性校验，得到明文的控制指令。

d) 数字家庭基础平台返回指令接受结果到数字家庭 APP。

e) 数字家庭基础平台返回指令执行结果到数字家庭 APP。

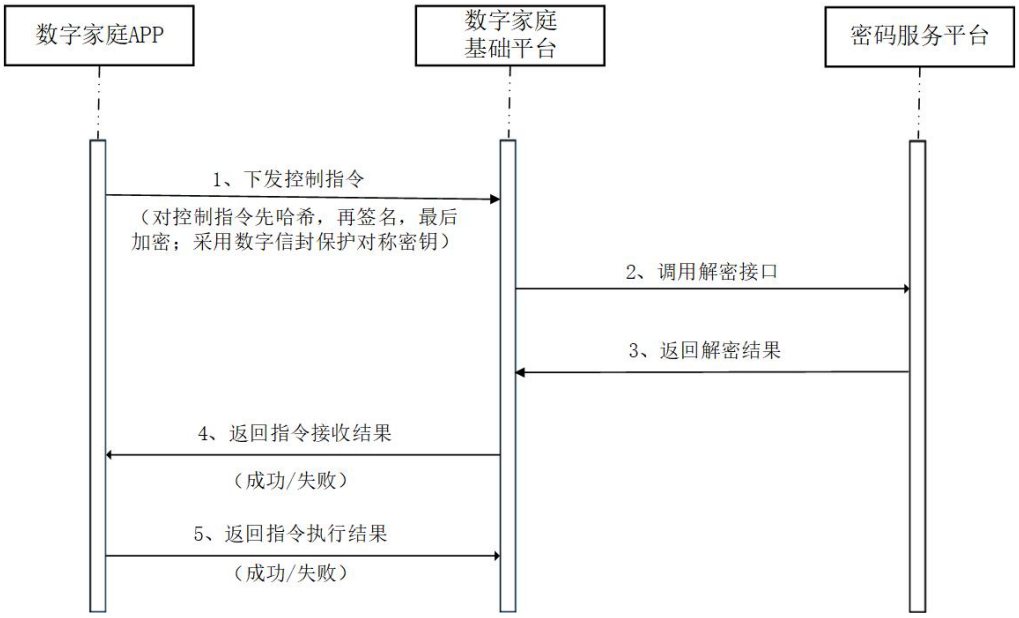

图 E.1 数字家庭 APP 下发指令流程

E.2 数字家庭基础平台下发指令流程

数字家庭基础平台下发指令流程：

a) 数字家庭基础平台向住宅用综合信息箱下发控制指令。

b) 数字家庭基础平台应调用密码服务平台 RESTful API 对下发控制指令进行安全处理。密码服务平台先对指令进行哈希运算，再使用签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给数字家庭基础平台，数字家庭基础平台再将密文传递给住宅用综合信息箱。同时，采用数字信封技术，密码服务平台使用住宅用综合信息箱加密公钥加密密码服务平台产生的对称密钥，将对称密钥密文传递给数字家庭基础平台，数字家庭基础平台再将对称密钥密文传递给住宅用综合信息箱。

c) 住宅用综合信息箱收到指令后，对接收到的密文信息进行解密并进行完整性校验，得到明文的控制指令并返回指令接收结果到数字家庭基础平台。

d) 住宅用综合信息箱返回指令执行结果到数字家庭基础平台。

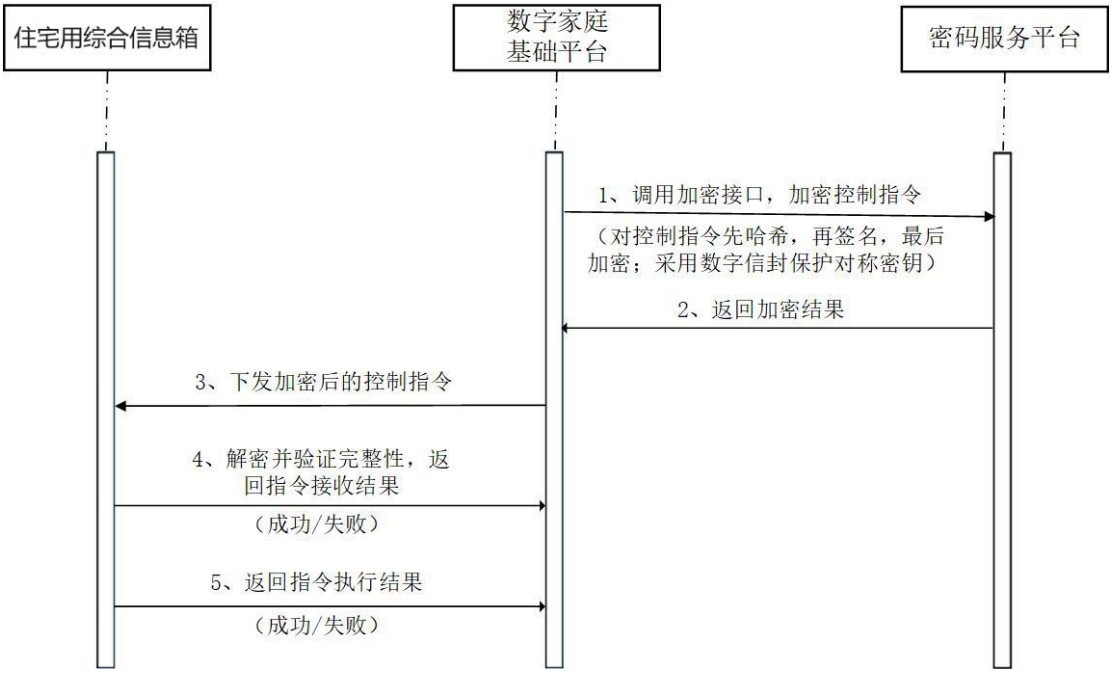

图 E.2 数字家庭基础平台下发指令流程

E.3 数字家庭基础平台回传告警信息流程

a) 数字家庭基础平台向数字家庭 APP 回传告警信息，应调用密码服务平台 RESTful API 对回传信息进行安全处理。密码服务平台先对指令进行哈希运算，再使用基础平台签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给数字家庭基础平台，数字家庭基础平台再将密文传递给数字家庭 APP。

b) 同时应采用数字信封技术，密码服务平台使用数字家庭 APP 的加密公钥对密码服务平台的对称密钥进行加密保护，将对称密钥密文传递给数字家庭基础平台，数字家庭基础平台再将对称密钥密文传递给数字家庭 APP。

c) 数字家庭 APP 对接收到的密文信息进行解密，同时验证告警信息完整性，返回告警信

息接受结果给到数字家庭基础平台。

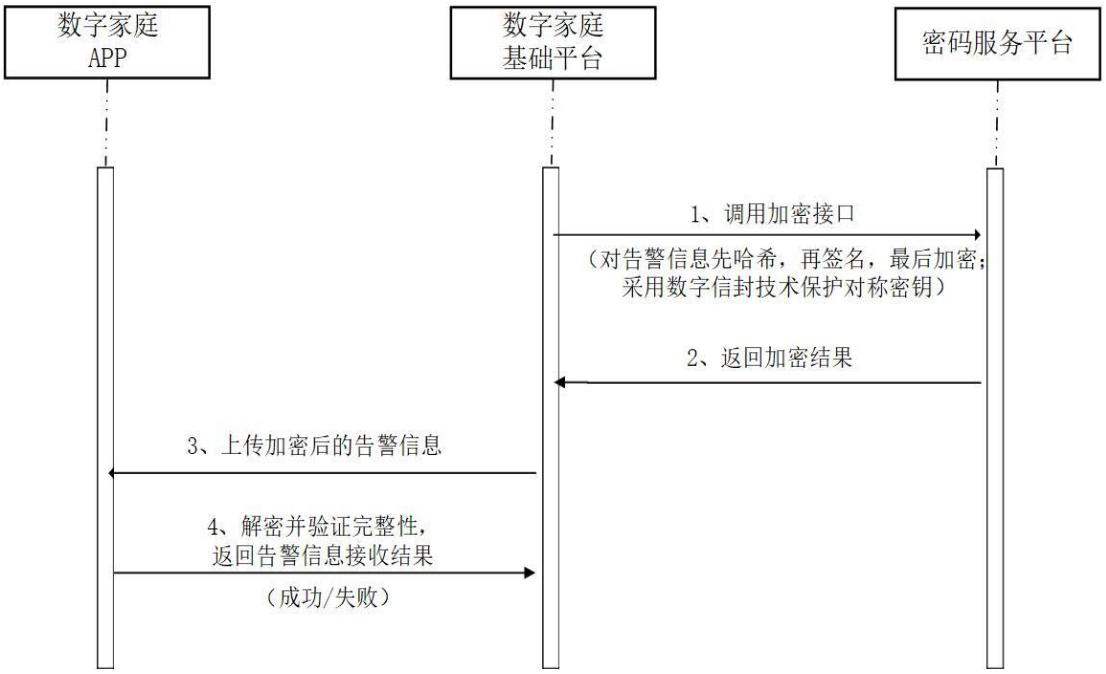

图 E.3　数字家庭基础平台回传告警信息流程

附录 F

（规范性）

住宅用综合信息箱、智能设备安全流程

住宅用综合信息箱、智能设备执行附录 E.1 和附录 E.2 的前提：

a) 住宅用综合信息箱通过 SE 生成签名密钥对，并预置在安全模块内。
住宅用综合信息箱从密钥管理系统处，获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。
住宅用综合信息箱通过调用密码服务平台接口生成一支对称密钥，并存储在安全模块内。

b) 智能设备通过 SE 生成签名密钥对，并预置在安全模块内。
智能设备从密钥管理系统处，获得 CA 根证书、签名数字证书、加密数字证书、加密密钥对。
智能设备通过调用密码服务平台接口生成一支对称密钥，并存储在安全模块内。

F.1 住宅用综合信息箱下发指令流程

住宅用综合信息箱下发指令流程：

a) 数字家庭基础平台向住宅用综合信息箱下发控制指令。

b) 住宅用综合信息箱收到指令后，向数字家庭基础平台返回指令接收结果。

c) 住宅用综合信息箱应使用密码机制对下发控制指令进行安全处理，先对指令进行哈希运算，再使用签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给智能设备。
同时，采用数字信封技术，使用智能设备的加密公钥加密住宅用综合信息箱的对称密钥，将对称密钥密文传递给智能设备。

d) 智能设备对接收到的密文信息解密并验证完整性，返回指令执行结果到住宅用综合信息箱。

e) 住宅用综合信息箱返回指令执行结果到数字家庭基础平台。

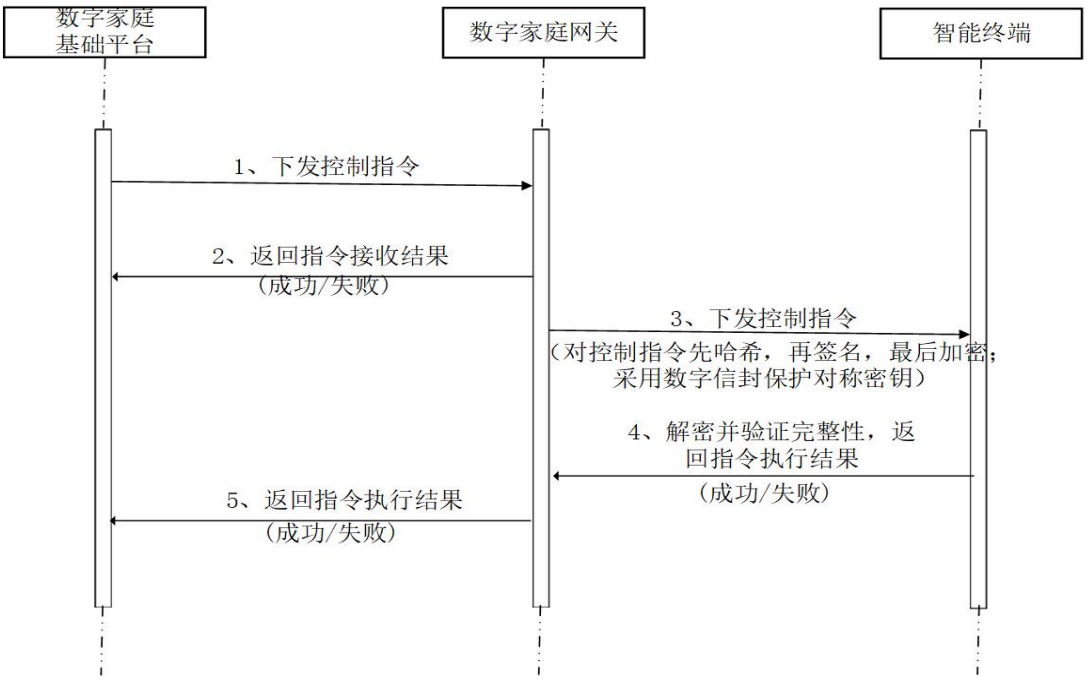

图 F.1　住宅用综合信息箱下发指令流程

F.2　住宅用综合信息箱、智能设备回传告警信息流程

住宅用综合信息箱、智能设备回传告警信息流程：

a) 智能设备向住宅用综合信息箱回传告警信息，应使用密码机制对回传信息进行安全处理，先对指令进行哈希运算，再使用签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给住宅用综合信息箱。

同时应采用数字信封技术，使用住宅用综合信息箱的公钥对智能设备的对称密钥进行加密保护，将对称密钥密文传递给住宅用综合信息箱。

b) 住宅用综合信息箱对接收到的密文信息解密并验证完整性，返回指令接收结果给智能设备。

c) 住宅用综合信息箱向数字家庭基础平台回传告警信息。应使用密码机制对回传信息进行安全处理。先对指令进行哈希运算，再使用签名密钥对中的私钥对哈希值进行签名运算，最后用对称密钥对指令、签名值、签名算法、签名证书进行加密运算，得到密文，传递给数字家庭基础平台。

同时应采用数字信封技术，使用数字家庭基础平台的公钥对住宅用综合信息箱的对称密钥进行加密保护，将对称密钥密文传递给数字家庭基础平台。

d) 数字家庭基础平台对接收到的密文信息解密并验证完整性，返回指令接收结果给住宅用综合信息箱。

住宅用综合信息箱、智能设备回传告警信息流程图：

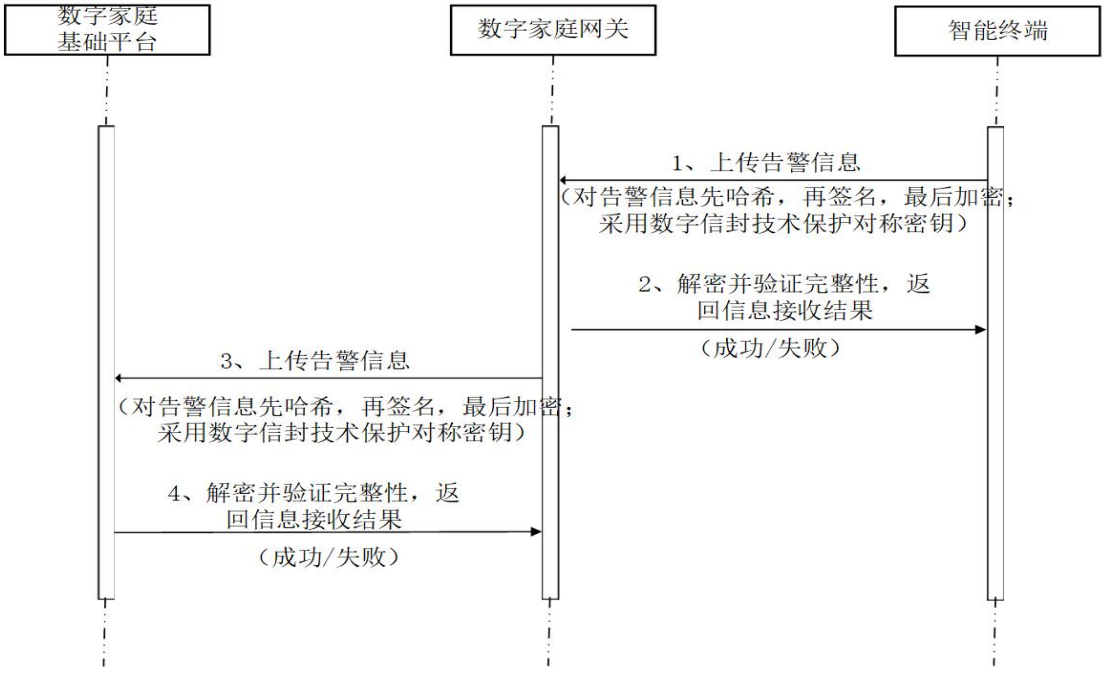

图 F.2　住宅用综合信息箱、智能设备回传告警信息流程

F.3　数字信封的使用

基于数字信封的消息加密：

使用对称密钥加密消息，生成消息密文。使用对方公钥加密对称密钥，生成密钥密文。

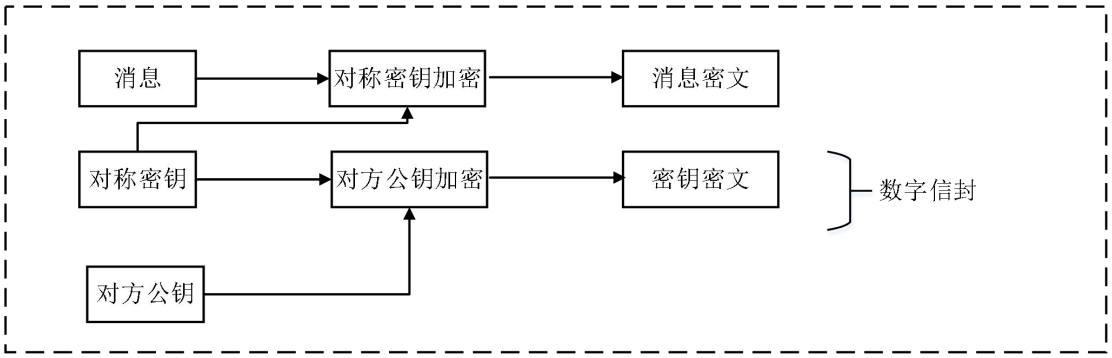

图 F.3 基于数字信封的消息加密流程

基于数字信封的消息解密：

用自己的私钥解密密钥密文，得到对称密钥。用对称密钥解密消息密文，得到消息。

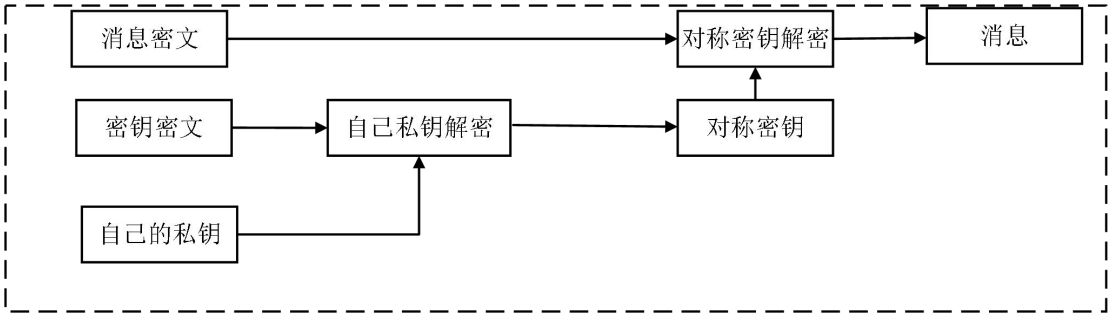

图 F.4 基于数字信封的消息解密流程