ICS 35.040
L 80
备案号：

天 津 市 商 用 密 码 团 体 标 准

T/TCCIA 0001-2022

信息系统密码应用设计技术标准

Technical Standard for the design of information system cryptography applications

2022-9-19 发布

天津市商用密码行业协会 发布

目　　录

前 言

本文件根据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。

请注意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专利的责任。

本文件由天津市信息安全标准化技术委员会归口。

本文件起草单位：天津光电通信技术有限公司、天津灵创智恒软件技术有限公司、南开大学、天津赢达信科技有限公司、天津光电安辰信息技术股份有限公司、天津国芯科技有限公司、恒银金融科技股份有限公司、麒麟软件有限公司、飞腾信息技术有限公司、天津中网基业智能系统工程有限公司、天津市中环认证服务有限公司、天津恒御科技有限公司、安云印（天津）大数据科技有限公司、北京数字认证有限公司、江西智慧云测安全检测中心股份有限公司。

本文件主要起草人：李忠献、张俊辉、汪定、张秋璞、胡双喜、张斌、江浩然、刘博、冯彦朝、牛昱、崔悦、修凤洲、毛乃峥、高博、王泽。

天津市信息系统密码应用设计技术标准

1. 范围

本文件提出了信息系统密码应用方案设计技术的建议，包括设计概述、密码应用方案要点、通用设计指南、计算平台密码应用设计指南、信息系统应用层设计指南、密码支撑服务设计指南、密钥管理设计指南等方面。

本文件适用于信息系统建设方、密码技术应用方、密码技术服务方，为开展信息系统密码应用方案设计提供指导参考。

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 15843.2　信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3　信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15843.4　信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 15852（所有部分）　信息技术 安全技术 消息鉴别码

GB/T 17964　信息安全技术 分组密码算法的工作模式

GB/T 20984　信息安全技术 信息安全风险评估规范

GB/T 25056　信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25069　信息安全技术 术语

GB/T 32905　信息安全技术 SM3密码杂凑算法

GB/T 32907　信息安全技术 SM4分组密码算法

GB/T 32918（所有部分）　信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35114　公共安全视频监控联网信息安全技术要求

GB/T 35276　信息安全技术 SM2密码算法使用规范

GB/T 36624　信息技术 安全技术 可鉴别的加密机制

GB/T 37033　信息安全技术 射频识别系统密码应用技术要求

GB/T 37092　信息安全技术 密码模块安全要求

GB/T 38542　信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架

GB/T 38556　信息安全技术 动态口令密码应用技术规范

GB/T 38635.2　信息安全技术 SM9标识密码算法 第2部分：算法

GB/T 38636　信息安全技术 传输层密码协议（TLCP）

GB/T 39786　信息安全技术 信息系统密码应用基本要求

GM/T 0012　可信计算.可信密码模块接口规范

GM/T 0022　IPsec VPN 技术规范

GM/T 0032　基于角色的授权与访问控制技术规范

GM/T 0036　采用非接触卡的门禁系统密码应用技术指南

GM/Z 4001-2013　密码术语

3.术语和定义

GB/T 39786、GB/T 25069和GM/Z 4001-2013中界定的以及下列术语和定义适用于本文件。

密码应用方案设计 Design of Cryptography Application Scheme也称信息系统密码应用方案设计，在明确信息系统安全需求和密码应用措施的基础上，设计信息系统的密码应用解决方案。

信息系统建设方 Information System Builder：实际建设、使用、管理网络与信息系统的责任单位。

密码技术应用方 Application Parties of Cryptography：应用密码技术、产品和服务建设网络和信息系统的单位。

密码技术服务方 Cryptography Service Provider：提供密码技术、产品和服务的单位。

4.设计概述

4.1 设计原则

信息系统密码应用方案设计建议遵循如下原则：

a）总体性原则。信息系统密码应用需求和系统预期目标与本系统网络安全等级保护相结合，以此确定信息系统计算平台、应用层、密码支撑服务和密钥管理设计的密码应用需求，涵盖物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面的密码应用设计，满足信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性需求。

b）科学性原则。信息系统密码应用设计建议在满足GB/T 39786通用要求基础上，依据密码技术体系框架和密码相关标准，形成包括密码支撑体系

总体架构、密码基础设施建设部署、密钥管理体系构建、密码产品部署及管理等内容。

c）完备性原则。信息系统密码应用方案专注于满足密码相关安全需求，根据安全需求建立完备的密码支撑保障体系。针对不适用项，采用替代性风险控制措施达到有效控制。

d）可行性原则。信息系统密码应用设计建议进行可行性论证，在保证信息系统业务正常运行的同时，综合考虑信息系统的复杂性、兼容性及其他保障措施等，保证方案切合实际、合理可行。科学评估密码应用方案和实施计划，可采取整体设计、分期建设、稳步推进的策略，结合实际情况制订项目组织实施计划。

4.2 设计要点

密码应用设计以信息系统的安全需求为基础，梳理对应的密码应用需求，如信息系统不存在对应的密码应用需求或存在其他替代性风险控制措施而不采用密码技术的，需要在密码应用方案设计时进行风险评估和论证。

密码应用方案设计要点包括以下三部分：

a) 密码应用的合规性：指的是信息系统中使用的密码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，信息系统中使用的密码技术遵循密码相关国家标准、行业标准或经国家密码管理部门审查认定，密码产品和密码服务符合法律法规的相关要求。

b) 密码应用的有效性：指的是密码技术是否被正确、有效使用，以支撑信息系统的安全需求，为信息系统提供机密性、完整性、真实性、不可否认性保护。

c) 密钥管理：指的是对系统中各密钥功能进行分类，明确密钥生命周期，制定科学、合理的密钥安全管理策略。

4.3 设计过程

根据信息系统的安全需求，可结合安全风险需求（信息系统面临的安全风险分析过程可参考《信息安全技术 信息安全风险评估规范》(GB/T 20984)，设计使用密码技术来满足信息系统安全需求的业务处理机制和流程。设计过程包括三项基本流程：密码应用需求分析、密码应用设计、密码合规分析。设计过程如图1所示。

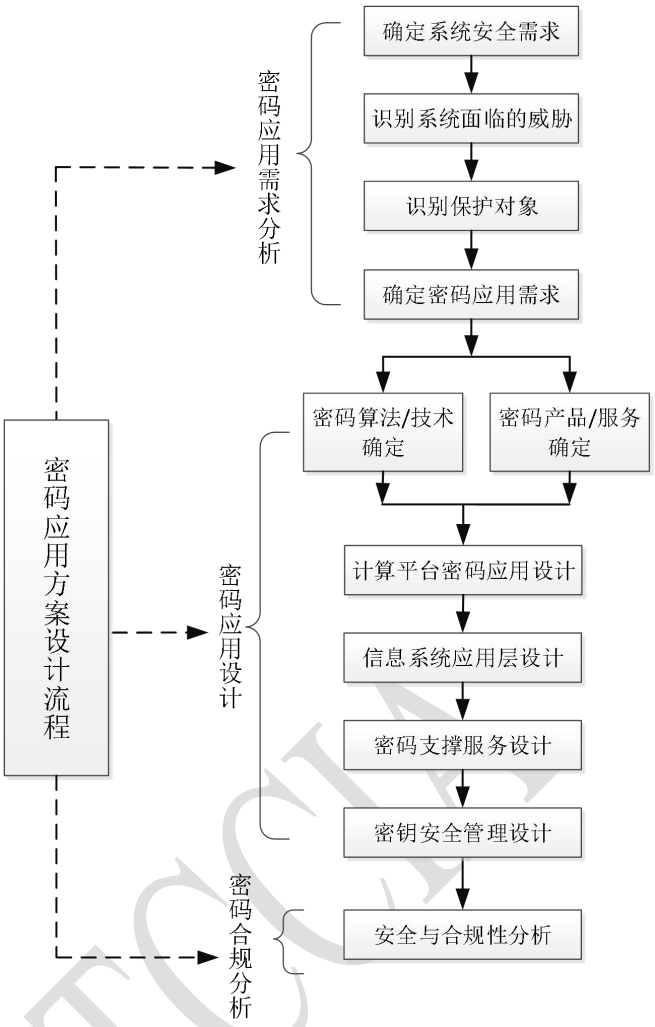

图1 设计过程流程图

4.4 设计内容

密码应用需求分析主要根据系统的安全需求，识别系统面临的威胁和需要保护的对象，确定密码应用需求。

密码应用设计依据通用设计确定密码算法、密码技术、密码产品和密码服务，并进行计算平台密码应用设计、信息系统应用层设计、密码支撑服务设计和密钥管理安全设计。密码应用设计主要包括以下内容：

a) 通用设计：包括信息系统密码应用方案设计中密码算法、密码技术、密码产品和密码服务的选取。

b) 计算平台密码应用设计：信息系统计算平台的密码应用设计，具体包含物理和环境安全、网络和通信安全、设备和计算安全三个层面，保障信息系统计算平台的物理环境、网络通信、设备管理的安全。计算平台密码应用主要由信息系统建设方、密码技术应用方、密码技术服务方设计与提供，计算平台密码应用设计可参考第7章节。

c) 信息系统应用层设计：信息系统应用层设计需要从业务应用情况入手，梳理信息系统的业务安全需求，并确定保护对象，使用密码技术保护具体业务流程和数据处理中存在的安全问题。信息系统应用层主要由信息系统建设方、密码技术应用方设计与提供，信息系统应用层设计可参考第8章节。

d) 密码支撑服务设计：根据信息系统应用层的密码应用需求，设计密码算法、密码技术的提供方式，以及密码设备的设计与部署方式，包括支撑中间件与密码设备/基础设施的设计。一是支撑中间件，设计密码功能、密码计算等密码支撑服务的提供模式，同信息系统的集成与调用方式等；二是密码设备/基础设施，设计提供密码支撑服务的密码设备、密码基础设施并确定其功能、性能需求及部署模式。密码支撑服务主要由密码技术服务方设计与提供。密码支撑服务设计及与信息系统的集成方式可参考第9章节及附录A。

e) 密钥管理安全设计：主要包括信息系统密钥功能划分、密钥体系设计和密钥生命周期管理，密钥管理安全设计可参考第10章节。

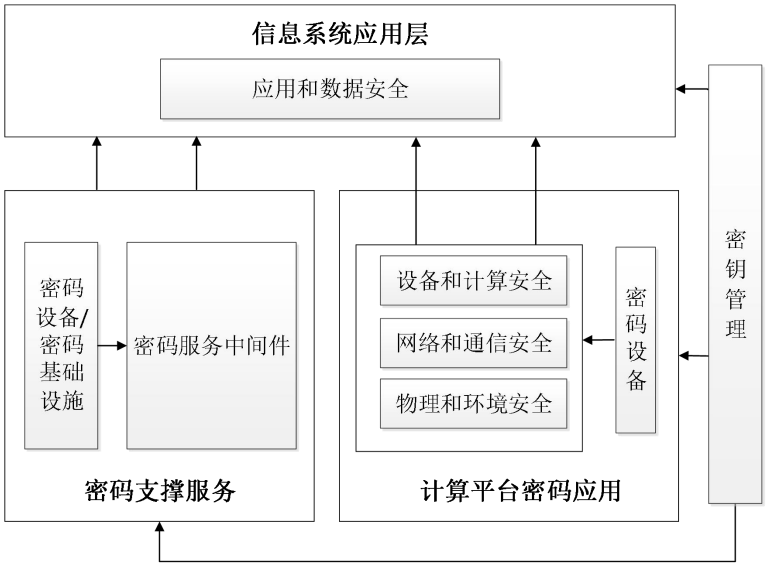

图2 信息系统密码应用设计框架

密码合规分析指安全与合规性分析，依据《密码应用合规性对照表》对每一项符合性进行自评价。附录B给出了密码应用合规性对照表。

5.密码应用方案要点

5.1 背景

包含系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述，以及该项目实施的必要性。

5.2 系统概述

包含系统基本情况、系统网络拓扑、承载的业务情况、系统软硬件构成、管理制度等。

系统基本情况包含系统名称、项目建设单位情况（名称、地址、所属密码管理部门、单位类型等）、系统上线运行时间、完成等保备案时间、网络安全保护等级、系统用户情况（使用单位、使用人员、使用场景等）等。

系统网络拓扑包含体系架构、网络所在机房情况、网络边界划分、设备组成及实现功能、所采取的安全防护措施等，并给出系统网络拓扑图。

承载的业务情况包含系统承载的业务应用、业务功能、信息种类、关键数据类型等。

系统软硬件构成包含服务器、用户终端、网络设备、存储、安全防护设备、密码设备等硬件资源和操作系统、数据库、应用中间件等软件资源。

管理制度包含系统管理机构、管理人员、管理职责、相关制度、安全策略等。

5.3 密码应用需求分析

结合系统安全风险控制需求，以及 GB/T 39786 针对信息系统网络安全保护等级提出的密码应用要求，对系统的密码应用需求进行分析。

对于密码应用要求在信息系统中不适用的部分，做出相应的原因说明，并给出替代性措施。

5.4 设计目标及原则

5.4.1 设计目标

提出总的设计目标或分阶段设计目标。

5.4.2 设计原则与依据

包含方案的设计原则、所遵循的依据等，重点是所遵循的密码相关政策法规要求和 GB/T 39786 等标准规范。

5.5 技术方案

5.5.1 密码应用技术框架

包含密码应用技术框架图及框架说明。技术框架包括密码计算平台、密码支撑服务、信息系统应用层密码应用架构、密钥管理等，能综合描述各平台、系统之间的关系，清晰展示密码应用整体技术框架。

5.5.2 计算平台密码应用

a)物理和环境安全

描述本层密码保护的对象、采用的密码措施，如密码应用工作流程、密码算法、密码协议、密码服务、密码产品及其遵循的标准、密码子系统组成和功能等。

b)网络和通信安全

说明同 a）

c)设备和计算安全

说明同 a）

5.5.3 应用层和数据安全设计

根据密码应用需求，对应用系统中的身份鉴别、数据安全存储传输、访问控制、行为不可否认性等进行密码应用设计，详细说明所采用的密码措施，包括密码应用工作流程、密码算法、密码协议、密码服务等。

5.5.4 密码支撑服务设计

包括密码功能提供模式以及密码设备部署设计。密码功能提供模式，包含提供密码功能的设备、中间件以及相关的密码应用调用方式；密码设备部署设计，包含设备选型原则、软硬件设备清单（软硬件设备均需包含已有的密码产品清单）、部署示意图及说明等。

5.5.5 密钥管理

描述计算平台、应用层、密码支撑服务中密钥全生命周期涉及的密钥管理方案，和使用的独立的密钥管理设备、设施（若有）。

5.5.6 安全与合规性分析

重点对政策法规、标准规范的符合程度进行自我评价。包含《密码应用合规性对照表》，对每一项符合性进行自评价（符合/部分符合/不符合或不适用）。对于自查中不适用的项目，逐一说明其原因（比如环境约束、业务条件约束、经济社会稳定性等），并指出所对应的风险点采用了何种替代性风险控制措施来达到有效控制。

5.6 安全管理方案

包含系统采取的密码相关管理制度、人员管理、建设运行、应急处置等方面的管理措施。

5.7 实施保障方案

5.7.1 实施内容

清晰准确地描述项目实施对象的边界及密码应用的范围、任务要求等。

实施内容包含但不限于采购、软硬件开发或改造、系统集成、综合调试、试运行等。

分析项目实施的重难点问题，提出实施过程中可能存在的风险点及应对措施。

5.7.2 实施计划

包含实施路线图、进度计划、重要节点等。

按照施工进度计划确定实施步骤，并分阶段描述任务分工、实施主体、项目建设单位、阶段交付物等。

5.7.3 保障措施

包含项目实施过程中的组织保障、人员保障、经费保障、质量保障、监督检查等措施。

5.7.4 经费概算

对密码应用项目建设和产生的相关费用进行概算。新增的密码产品和相关服务应描述产品名称和服务类型、数量等。

按照经费使用有关要求编写。

6.通用设计指南

6.1 密码算法、密码技术选取

信息系统采用的密码算法和密码技术选取指南如下：

a) 采用以国家标准或密码行业标准形式公开发布的密码算法和密码技术；

b) 在采用特定行业领域的专用密码算法和密码技术前，需要确定该密码算法和密码技术是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

c) 在采用因国际互联互通等需要而兼容的其他密码算法和密码技术前，需要确定该密码算法和密码技术是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；同时，信息系统中不涉及国际互联互通等需要的部分，采用以国家标准、行业标准形式公开发布的密码算法和密码技术。

6.2 密码产品、密码服务选取

信息系统建议采用认证合格的密码产品，以及符合法律法规的相关要求并获得主管部门许可的密码服务。

a) 等保二级信息系统选取达到GB/T 37092一级及以上安全要求的密码产品；

b) 等保三级信息系统选取达到GB/T 37092二级及以上安全要求的密码产品；

c) 等保四级信息系统选取达到GB/T 37092三级及以上安全要求的密码产品。

7.计算平台密码应用设计指南

7.1 物理和环境安全设计

物理和环境安全所需要保护的对象是信息系统所在的重要区域，重要区域得不到保障，则设备、数据、应用等都将直接暴露在威胁之下。物理和环境安全的密码应用主要实现重要区域的访问控制和相关监控信息（人员进入记录、监控记录）的完整性保护。信息系统在设计时对该信息系统所在的所有重要区域进行梳理，确定未授权人员无法访问重要场所、重要设备和监控设备并对各类物理和环境的监控信息进行完整性保护。物理和环境安全层面的密码应用主要实现物理访问身份鉴别、电子门禁系统进出记录和视频监控音像记录数据的存储完整性。

信息系统部署符合要求的电子门禁系统和视频监控设备，或使用认证合格的密码产品对电子门禁系统和视频监控设备进行安全增强，具体设计指南如下：

a) 采用安全门禁系统（建议参考 GB/T 37033、GM/T 0036 等），或参考附录 C.1 中相关要求的密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性，每个人员均配发不同的密钥；

b) 在电子门禁系统中部署 PCI-E/PCI 密码卡、服务器密码机等密码产品，并采用完整性保护技术保证电子门禁记录在存储过程中的完整性，存储的完整性保护技术可参考附录 C.2.2；

c) 采用符合《公共安全视频监控联网信息安全技术要求》（GB 35114）的系统与设备采集重要区域音像记录监控信息，或在视频监控系统中部署 PCI-E/PCI 密码卡、服务器密码机等密码产品，并采用存储完整性保护技术保证视频监控音像记录在存储过程中的完整性，存储的完整性保护技术可参考附录 C.2.2；

d) 完整性校验值（如密码杂凑算法的消息鉴别码和数字签名）可不必实时计算，但是完整性校验值的计算间隔需按照系统设计的时间进行校验，校验时间按照系统风险进行评估。

7.2 网络和通信安全设计

网络和通信安全所需要保护的对象是信息系统与外界交互的所有不可控的网络通信信道（如互联网、办公网等）。梳理信息系统与外界交互的所有网络通信信道，对各个网络通信信道的安全性进行分析，进一步明确能够使用密码技术解决的真实性、机密性、完整性需求。网络和通信安全层面的密码应用主要实现通信信道的保护和内部网络的访问控制，包含通信实体的身

份鉴别、通信过程中数据的完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性和设备的接入认证等，具体设计指南如下：

a) 采用 IPSec VPN 产品/安全网关、SSL VPN 产品/安全网关、安全认证网关等密码产品或符合《IPSec VPN 技术规范》（GM/T 0022）和《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636）相关要求的密码技术保证通信实体身份的真实性以及通信过程中数据的完整性和机密性；为特定行业、特定需求设计的专用密码技术建议满足密码技术使用要求，以及法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b) 采用密码技术保证网络边界访问控制信息的完整性，技术和机制可参考附录 C.2.2；

c) 采用 IPSec VPN 产品/安全网关、SSL VPN 产品/安全网关、安全认证网关等密码产品，或符合附录 C.1 中相关要求的密码技术，保证从外部接入到内部网络设备身份的真实性。

7.3 设备和计算安全设计

设备和计算安全所需要保护的对象是信息系统中承载业务应用的计算环境，包括通用设备（如服务器、数据库服务器、数据库管理系统等）、密码设备等。其安全设计需要梳理出信息系统中所有涉及到的设备和计算环境，对各种设备和计算环境的安全性进行分析，进一步明确能够使用密码技术解决的真实性、机密性、完整性需求。设备和计算安全层面的密码应用主要实现登录设备的用户身份鉴别、设备远程安全通信、设备安全部署等，具体设计指南如下：

a) 采用智能密码钥匙、智能 IC 卡、动态令牌（和配套动态令牌认证系统）或符合附录 C.1 中相关要求的密码技术实现对登录设备的用户进行身份鉴别，保证用户身份的真实性；

b) 远程管理设备时，建议通过堡垒机对设备进行统一运维，运维客户端与堡垒机之间、堡垒机与设备之间的通信，可采用符合《IPSec VPN 技术规范》（GM/T 0022）和《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636），或符合附录 C.2.1 和 C.3.1 要求的技术，搭建安全的信息传输通道；

c) 在设备内部部署智能密码钥匙、PCI-E/PCI 密码卡等可嵌入式密码产品，或外部部署服务器密码机等密码设备，采用密码技术保证系统资源访问控制信息的完整性、设备中的重要信息资源安全标记的完整性、日志记录的完整性，完整性保护技术可参考附录 C.2.2；

d) 完整性校验值（如密码杂凑算法的消息鉴别码和数字签名）可不必实时计算，但是完整性校验值的计算间隔需按照系统设计的时间进行校验，校验时间按照系统风险进行评估；

e) 采用代码签名、安装与部署前的鉴别码校验等机制和密码技术，保证重要可执行程序的完整性和其来源的真实性，相关机制和技术可参考附录 C.1、附录 C.2。

8. 信息系统应用层设计指南

8.1 安全需求分析

应用和数据安全层面所需要保护的对象是信息系统中的应用及其重要数据。通过对信息系统功能、系统架构、业务应用情况、密码应用情况、重要信息资源、软硬件组成和管理机制等现状的分析，了解信息系统业务逻辑，

识别系统面临的威胁，明确业务流程中重要业务数据、隐私数据存储和传输的安全需求，确定需要保护的重要信息资源和密码应用需求，进一步明确能够使用密码技术解决的真实性、机密性、完整性、不可否认性需求。应用层密码应用主要实现登录应用系统用户的身份鉴别、重要数据的安全存储与传输、重要操作行为的不可否认性等，具体设计指南如下：

a) 确定登录用户的类别和权限，确定用户权限的敏感程度和安全需求，明确对密码技术的具体需求；

b) 信息系统根据相关法律法规、政策、标准规范等，确定信息系统内数据的类别、敏感程度和安全需求，明确对密码技术的具体需求；

c) 根据相关法律法规、政策、标准规范等，确定用户操作的类型和敏感程度；确定对于可能涉及法律责任认定的用户操作，明确对密码技术的具体需求。

8.2 身份鉴别设计

信息系统可为不同权限的用户分配不同的鉴别方式，具体设计指南如下：

a) 采用密码支撑服务平台提供的密码产品、技术、服务，通过密码技术实现登录用户的身份鉴别，保证应用系统用户身份的真实性，真实性保护的密码技术设计可参考附录C.1，密码支撑服务平台技术架构设计示例可参考附录A；

b) 在每一个用户注册到系统时，采用用户唯一标识符（如用户名、用户序号）标识用户，并为每个用户生成不同的密钥；

c) 用户的身份鉴别数据（如口令、生物特征信息），通过密码技术实现其存储的安全保护和传输的安全保护，采用的密码技术可参考附录C.2、C.3。

8.3 访问控制信息完整性设计

访问控制信息包括：访问控制策略与规则、用户角色/权限信息、授权凭证等，访问控制信息需要保证完整性，以确保身份鉴别后，实体可以被正确授权以获取相应的信息系统资源，访问控制信息具体内容可参考《基于角色的授权与访问控制技术规范》（GM/T 0032）。

访问控制信息采用密码支撑服务平台提供的密码产品、技术、服务，实现数据存储的完整性保护要求，存储完整性保护技术可参考附录C.2.2。

8.4 数据传输安全设计

根据数据的类别、敏感程度和安全需求，信息系统可为不同敏感程度的数据分配不同的数据传输安全保护方法。

数据传输安全可以使用两种实现方式：信道保护和信源保护。

a) 信道保护：采用信息系统密码支撑服务提供的密码产品、技术，配合用户终端部署的安全浏览器、密码模块等密码产品，搭建安全的信息传输通道，实现信息系统应用层传输的机密性与完整性保护；

b) 信源保护：调用密码支撑服务的密码功能对信源进行安全保护后再进行传输，若涉及密钥交换，可依据第10章密钥管理设计指南，制定符合要求的密钥交换模式和机制。

8.5 数据存储安全设计

根据数据的类别、敏感程度和安全需求，信息系统可为不同敏感程度的数据分配不同的数据存储安全保护方法，具体设计指南如下：

a) 采用密码支撑服务提供的密码产品、技术或服务，或使用符合附录C.2.2、附录C.3.2中相关要求的密码技术，对数据进行安全保护后再进行存储；对于不同实体（如应用、用户）的数据，采用不同的密钥进行保护，控制单个密钥泄露造成的安全风险；

b) 日志记录的完整性校验值（如消息鉴别码或数字签名）可不必实时计算，但是完整性校验值的计算间隔需按照系统设计的时间进行校验，校验时间按照系统风险进行评估；

c) 对于不需要恢复原文的数据（如口令等），可采用密码杂凑函数对原文单向变换达成机密性保护的目的，但需要采用加盐等手段降低原文被恶意猜测的风险。

8.6 行为不可否认性设计

根据用户操作的类型和敏感程度，信息系统可为不同用户操作分配不同的行为不可否认性机制，具体设计指南如下：

a) 采用密码支撑服务平台提供的密码产品、技术、服务，或使用符合附录C.4中相关要求的密码技术，通过签名、签章等方式，满足数据原发行为和接收行为的不可否认性需求；

b) 对于时间敏感的业务应用，可采用时间戳服务器对行为的发生时间提供可信证明。

9. 密码支撑服务设计指南

9.1 密码支撑服务组成

密码支撑服务指提供密码运算、密钥管理的密码设备/基础设施，以及为应用层提供密码功能的中间件。密码设备/基础设施包括服务器密码机、签名验签服务器、时间戳服务器、安全网关等；中间件提供的密码功能包括：密码算法服务、签名验签服务、数字证书服务、安全传输服务等。信息系统可根据实际建设需求，自建或接入已有的密码支撑服务系统。密码支撑服务技术架构设计示例可参考附录A、密码设备部署相关要求可参考附录D。

9.2 真实性保护功能设计

密码支撑服务提供符合要求的密码技术，包括密码算法、密码服务，为信息系统提供用户身份真实性保护需求，真实性保护设计可参考附录C.1。

部署符合要求的签名验签服务器、服务器密码机、安全认证网关、其他密码模块等密码设备，或部署证书认证系统，在登录过程中配合使用智能密码钥匙、动态令牌等密码产品，实现登录用户的身份鉴别。

密码支撑服务需提供匹配的密钥或证书存储、使用和管理能力。

9.3 机密性与完整性保护功能设计

密码支撑服务提供符合要求的密码技术，包括密码算法、密码服务，满足信息系统对重要数据存储和传输过程的机密性与完整性保护需求，机密性和完整性设计可参考附录C.3、C.2。

a）传输过程的机密性与完整性保护

信道保护：部署符合要求的网关设备（加载经主管部门许可的机构颁发的服务器证书）或服务器端密码模块（加载经主管部门许可的机构颁发的服务器证书），与客户端部署的安全浏览器、移动密码模块、智能密码钥匙等，搭建客户端与服务器端之间的安全传输通道，实现重要数据传输的机密性和完整性。

信源保护：部署符合要求的服务器密码机或其他密码模块，采用符合要求的密码技术对数据进行安全保护后再进行传输，满足信息系统中重要数据传输的机密性与完整性需求，相关的密码技术可参考附录C.2.1、附录C.3.1。

b）存储过程的机密性与完整性保护

部署认证合格的服务器密码机、其他密码模块等存储加密产品，采用符合要求的密码技术，对重要数据、重要信息资源安全标记、系统访问控制信息进行机密性、完整性保护，满足信息系统对相关数据信息的安全存储需求，相关的密码技术可参考附录C.2.2、附录C.3.2。

9.4 不可否认性保护功能设计

部署认证合格的签名验签服务器、电子签章系统、时间戳服务器等密码产品或服务，为信息系统提供电子签章、签名验签等功能。

不可否认性保护功能需提供匹配的电子印章、证书或密钥的存储、使用和管理功能。

10.密钥管理设计指南

10.1 设计要点

明确密钥体系，针对密钥体系中的各类密钥，明确密钥从产生到销毁的全生命周期中的各个环节，确保密钥的安全性。密钥管理的设计目标是保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，保证公钥不被非授权的修改和替换。

10.2 密钥功能划分

信息系统根据密码防护需求，结合密码技术、密码产品，设计密钥功能。密钥功能主要分为：数据保护类密钥、身份鉴别类密钥以及密钥管理类密钥。

a) 数据保护类密钥：该类密钥直接保护数据的机密性、完整性、消息来源真实性和行为的不可否认性；根据不同算法和不同功能，可以进一步分为：数据加密对称密钥、数据 MAC 密钥、数据加密公/私钥、数据签名公/私钥；

b) 身份鉴别类密钥：该类密钥主要在实体鉴别协议中验证实体身份；与数据保护类密钥不同的是，该类密钥虽然也对鉴别过程数据（比如挑战值、时间戳等）进行加密/签名等操作，其目的并不是为了保护鉴别过程数据，而是为了验证对方是否持有相同/对应的密钥；根据不同的身份鉴别协议，可以进一步分为：身份鉴别对称密钥、身份鉴别公/私钥；

c) 密钥管理类密钥：该类密钥主要用于密钥管理算法，实现随机数生成、密钥派生、密钥生成等；根据不同的密钥管理功能，可以进一步分为：密钥派生密钥、密钥加密对称密钥、密钥封装公/私钥、密钥签名公/私钥、密钥协商对称密钥、密钥协商公/私钥。有些密钥的使用方法（如密钥加密对

称密钥、密钥封装公/私钥、密钥签名公/私钥）与数据保护类密钥类似，区别在于保护的内容不一致。

10.3 密钥体系设计

密钥体系设计主要是根据信息系统业务流程中业务数据、操作指令等的防护需求，构建满足业务流程、数据流转需求的密钥体系，保证受保护数据在业务流程中的安全、可控。

根据信息系统业务需求，选取或设计合适的密钥体系。密钥体系的设计或选取，需考虑以下因素：

a) 信息系统本身存在的自然层级关系（如“国家-省-市-县”结构下的密钥应用需要设计相匹配的密钥层次体系）；

b) 父密钥与子密钥的关联关系，以及子密钥生成方式，包括：密钥加密、密钥分散、密钥协商、信任传递等；

c) 密钥的生成/分发方式和使用频率（如密钥需要耗时进行手动更新时，需要建立密钥体系来降低该密钥的使用频率）；

d) 密钥的数量（如单个中心节点需要保存大量的密钥时，需要建立密钥体系，通过保护少量的密钥实现数量较多的密钥保护）。

附录E给出了典型的对称密钥体系、非对称密钥体系和混合密钥体系的构建方式。

10.4 密钥生命周期管理

信息系统根据业务应用需求，对密钥的全生命周期进行管理。

a) 密钥产生

密钥需要在密码产品内或通过密码服务产生，产生时需明确密钥用途，如数据保护类密钥、身份鉴别类密钥、密钥管理类密钥。

密钥产生的同时需要记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等，并对这些密钥关联信息进行完整性保护以确保密钥被正确使用。

b) 密钥分发

密钥分发主要用于不同密码产品/服务间的密钥共享，分发时要注意抗截取、篡改、假冒等攻击，保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。

使用密钥存储介质分发密钥的，需建立密钥存储介质的管理规范。密钥存储介质管理可参考章节 10.3.1。

c) 密钥存储

将密钥保存在密码产品/密码服务中，利用密码产品/服务自身具备的密钥防护机制保护密钥的机密性和完整性。

利用非对称加密技术、对称加密技术将密钥保存在非密码产品中，同时采用密码技术保护其完整性。

d) 密钥使用

在使用密钥前需要利用密码产品的机制进行身份鉴别获得授权，使用公钥证书前对其进行有效性验证，验证公钥的完整性和实体与公钥的关联关系。

存储在密钥存储介质的身份鉴别密钥，信息系统需建立密钥存储介质的管理规范，规范智能密码钥匙、动态令牌、智能 IC 卡等的管理，确定密钥存储介质与实体的关联关系，确保实体身份真实性。

不同类型的密钥不能混用，一个密钥不能用于不同用途（加密、签名、消息鉴别码运算等），同时提供不同的功能的算法除外，如 GB/T 36624 中规定的可鉴别的加密机制。

e) 密钥更新

信息系统需要设定密钥更换周期，并采取有效措施保证密钥更换时的安全性，在密钥超过使用期限、泄露或存在泄露风险时，根据相应的更新策略进行更新。

f) 密钥归档

如果信息系统有密钥归档需求，则根据实际安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档，需要生成审计信息，包括归档的密钥、归档的时间等。

g) 密钥撤销

密钥撤销一般针对公钥证书所对应的密钥。当证书到期后，密钥自然撤销；也可以按需进行密钥撤销，撤销后的密钥不再具备使用效力。

h) 密钥备份

密钥备份主要目的是保护密钥的可用性，作为密钥存储的补充，以防止密钥的意外损坏。备份的密钥处于不激活状态（即不能直接用于密码计算），只有完成恢复后才可以激活。需要保护备份密钥的机密性、完整性及其与拥有者身份以及其他信息的关联关系；可以将备份的密钥存储在外部存储介质中，需要有安全机制保证仅有密钥拥有者才能恢复出密钥明文。密钥备份进行记录，并生成审计信息；审计信息包括备份的主体、备份的时间等。

i) 密钥恢复

信息系统可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围，密钥恢复进行记录，并生成审计信息，包括恢复的主体、恢复的时间等。

j) 密钥销毁

密钥销毁要注意的是销毁过程的不可逆，即无法从销毁结果中恢复原密钥。密钥进行销毁时，删除所有密钥副本（但不包括归档的密钥副本）。密钥销毁主要有两种情况：

1）正常销毁：指的是密钥到达设计的使用截止时间时自动进行销毁。

2）应急销毁：指的是密钥泄露或存在泄露风险时进行的密钥销毁。对于存储在密码产品内的密钥，一般配备紧急情况下自动销毁密钥的机制；当密钥所有者发现密钥存在泄漏的风险时，需要手动提前终止密钥的生命周期，进行密钥销毁。

附录 A（资料性）

密码支撑服务技术架构设计示例

A.1 密码支撑服务集成于一体化密码服务平台

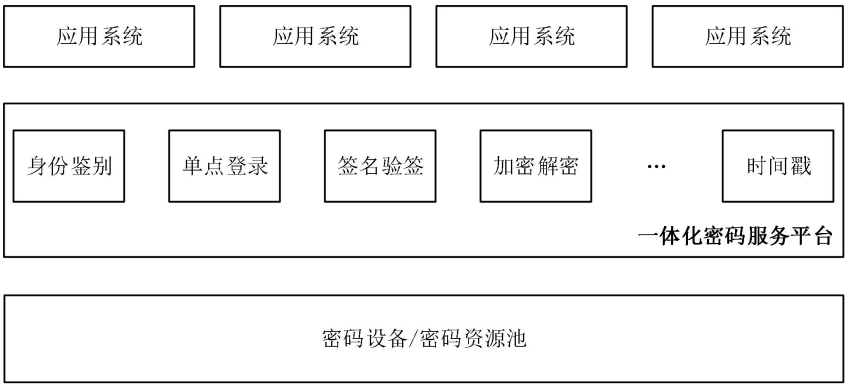

图 A.1　密码支撑服务集成于一体化密码服务平台

该方式的特点在于：典型密码功能和通用密码功能均集成在同一密码支撑服务中间件中，此类中间件可形象地称为一体化密码支撑服务平台；对应用来说，一体化密码支撑服务平台是透明的，应用仅能看到平台提供的密码功能接口；多个规模较小的应用系统可以使用该方式来获取密码支撑服务。

A.2 密码支撑服务集成于独立服务器

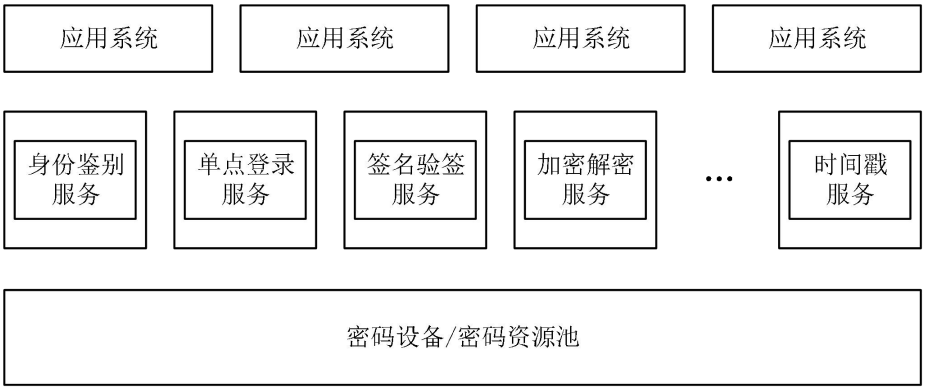

图 A.2　密码支撑中间件集成于独立服务器

该方式的特点在于：密码支撑服务设计集成在特定硬件设备中，既有签名验签服务器、加密解密服务器等提供通用密码功能的设备，又有身份鉴别服务器、单点登录服务器等提供典型密码功能的设备。一般来说，具备通用密码功能的设备，其硬件载体为密码设备；具备典型密码功能的设备，其硬件载体可为密码设备或普通服务器。

A.3 密码支撑服务集成于应用系统

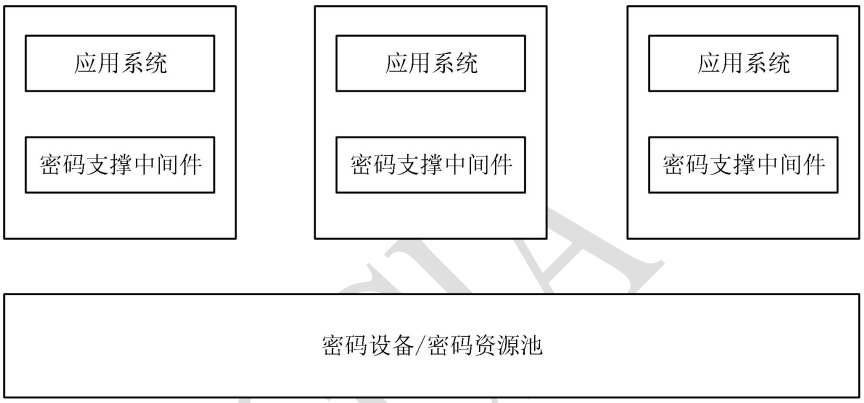

图 A.3　密码支撑中间件集成于应用系统

该方式的特点在于：密码支撑服务设计集成在应用系统并与其一同部署在应用服务器中，一般由应用系统开发商设计开发。

附录 B（资料性）

密码应用合规性对照表

信息系统密码应用方案中的《密码应用合规性对照表》见表 B.1

指标要求	密码技术应用点	采取措施	标准符合性（符合/部分符合/不符合/不适用）	说明（针对不适用项说明原因及替代性措施）
物理和环境安全	身份鉴别			
	电子门禁记录数据存储完整性			
	视频监控记录数据存储完整性			
	密码产品			
	密码服务			
网络和通信安全	身份鉴别			
	通信数据完整性			
	通信过程中重要数据的机密性			
	网络边界访问控制信息的完整性			
	安全接入认证			
	密码产品			
	密码服务			
设备和计算安全	身份鉴别			
	远程管理通道安全			
	系统资源访问控制信息完整性			
	重要信息资源安全标记完整性			
	日志记录完整性			
	重要可执行程序完整性、重要			

	可执行程序来源真实性			
	密码服务			
	密码产品			
应用和数据安全	身份鉴别			
	访问控制信息完整性			
	重要信息资源安全标记完整性			
	重要数据传输机密性			
	重要数据存储机密性			
	重要数据传输完整性			
	重要数据存储完整性			
	不可否认性			
	密码服务			
	密码产品			

表 B.1 密码应用合规性对照表

附录 C（资料性）

密码应用功能设计

C.1 真实性保护设计指南

保护实体身份真实性的主要方式是身份鉴别，基于密码技术的鉴别方式包括但不限于基于对称密码的身份鉴别、基于非对称密码的身份鉴别、基于杂凑算法的身份鉴别。此外，密码技术还可以与静态口令、生物特征等身份鉴别技术相结合，实现多因素鉴别。

a) 基于对称密码的身份鉴别，其设计时建议满足以下技术要求：

1) 身份鉴别机制遵循 GB/T 15843.2；

2) 作为实体身份凭证的对称密钥或其存储介质与实体身份标识建立可核实的绑定关系；

3) 采用认证合格的密码产品作为存储介质来存储作为实体身份凭证的对称密钥，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、智能 IC 卡、电子标签芯片、服务器密码机、PCI-E/PCI 密码卡、金融数据密码机等产品，以及安全门禁系统等。

b) 基于非对称密码的身份鉴别，其设计时建议满足以下技术要求：

1) 身份鉴别机制遵循 GB/T 15843.3；

2) 作为实体身份凭证的公钥证书能准确标识实体身份；

3) 作为实体身份凭证的公钥证书由可信任证书认证系统签发；在其使用时进行验证，验证失败则身份鉴别失败；

4) 采用认证合格的密码产品作为存储介质来存储作为实体身份凭证的非对称密钥对及公钥证书，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、安全认证网关、签名验签服务器等。

c) 基于密码杂凑算法的身份鉴别，其设计时建议满足以下技术要求：

1) 身份鉴别机制遵循 GB/T 15843.4 或使用动态口令技术进行身份鉴别，动态口令系统设计遵循 GB/T 38556；

2) 作为实体身份凭证的密钥或动态令牌与实体身份标识建立可核实的绑定关系；

3) 采用认证合格的密码产品作为存储介质来存储作为实体身份凭证的密钥数据，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、动态令牌、PCI-E/PCI 密码卡、服务器密码机，以及动态令牌认证系统等。

d) 使用密码技术结合静态口令的多因素身份鉴别，其设计时建议满足以下技术要求：

1) 可采用对称算法、杂凑算法或非对称算法保护静态口令在传输过程中的安全性，在传输时，静态口令结合如挑战码、随机数、时间戳等随机因子进行密码运算，确保其能够防截获、防假冒和防重用；

2) 作为实体身份凭证的静态口令在存储时与实体身份标识建立可核实的绑定关系，并采用密码技术实现机密性和完整性保护；

3) 采用认证合格的密码产品对静态口令进行机密性和完整性保护，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、其他密码模块等。

e) 使用密码技术结合生物特征的多因素身份鉴别，其设计时建议满足以下技术要求：

1) 鉴别过程遵循 GB/T 38542，生物特征信息若涉及传输，结合如挑战码、随机数、时间戳等随机因子进行密码运算，确保其能够防截获、防假冒和防重用；

2) 作为实体身份凭证的生物特征在存储时与实体身份标识建立可核实的绑定关系；

3) 采用认证合格的密码产品对生物特征信息进行机密性和完整性保护，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、安全芯片、PCI-E/PCI 密码卡、服务器密码机等。

C.2 完整性保护设计指南

基于密码技术的完整性保护技术包括但不限于基于消息鉴别码的完整性保护和基于数字签名的完整性保护。

C.2.1 传输的完整性保护

传输的完整性，保障数据在传输过程中的完整性，防止非授权篡改。

a) 基于消息鉴别码的传输完整性保护，其设计时建议满足以下技术要求：

1) 消息鉴别码机制遵循 GB/T 15852，其使用的密码算法遵循 GB/T 32905 或 GB/T 32907；

2) 接受方在对接收到的保护数据进行处理前，校验其传输完整性；若发现保护数据的传输完整性破坏，进行告警；

3) 采用认证合格的密码产品作为存储介质来存储密钥数据，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、VPN 产品、安全网关等。

b) 基于数字签名的传输完整性保护，其设计时建议满足以下技术要求：

1) 使用获得主管部门许可的密码服务机构颁发的签名证书，或使用自建证书认证系统颁发的签名证书，自建证书认证系统建议遵循 GB/T 25056；

2) 接收方在对收到的被保护数据进行处理前，验证发送方的签名证书；验证通过后，校验被保护数据的传输完整性；若发现被保护数据的传输完整性被破坏，进行告警；

3) 采用认证合格的密码产品作为存储介质存储数字签名私钥，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、签名验签服务器、服务器密码机产品等。

C.2.2 存储的完整性保护

存储的完整性，保护数据存储的完整性，防止非授权篡改。

a) 基于消息鉴别码的存储完整性保护，其设计时建议满足以下技术要求：

1) 消息鉴别码机制遵循 GB/T 15852 系列标准，其使用的密码算法遵循 GB/T 32905 或 GB/T 32907；

2) 基于杂凑函数的完整性保护，被保护数据与杂凑值不在同一存储介质中保存；

3) 具备主动校验被保护数据完整性的功能；可根据需求，提供定期校验被保护数据完整性的功能；

4) 若发现被保护数据的存储完整性被破坏，进行告警；

5) 采用认证合格的密码产品作为存储介质来存储密钥数据，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机等。

b) 基于数字签名的存储完整性保护，其设计时建议满足以下技术要求：

1) 使用获得主管部门许可的密码服务机构颁发的签名证书，或使用自建证书认证系统颁发的签名证书，自建证书认证系统建议遵循 GB/T 25056；

2) 具备主动校验被保护数据完整性的功能；可根据需求，提供定期校验被保护数据完整性的功能；

3) 若发现被保护数据的存储完整性被破坏，进行告警；

4) 采用认证合格的密码产品作为存储介质来存储数字签名私钥，并其使用其进行密码运算；可选用的密码产品类型包括智能密码钥匙、PCI-E/PCI 密码卡、签名验签服务器、服务器密码机产品等。

c) 基于可信计算的存储完整性保护，其设计时建议满足以下技术要求：

1) 使用的杂凑算法遵循 GB/T 32905，使用的可信密码模块遵循 GM/T 0012；

2) 系统启动前，基于杂凑算法建立从引导程序、操作系统到应用程序的信任链；

3) 若发现被保护数据的完整性被破坏，进行告警；

4) 采用认证合格的可信密码模块；可选用的密码产品类型包括可信计算密码支撑平台类产品。

C.3 机密性保护设计指南

基于密码的机密性保护技术包括但不限于基于对称密码的机密性保护和基于非对称密码的机密性保护。

C.3.1 传输的机密性保护

传输的机密性，保护数据在传输过程的机密性，防止被窃取。

a) 基于对称密码的传输机密性保护，其设计时建议满足以下技术要求：

1) 对称密码算法使用遵循 GB/T 17964、GB/T 32907、GB/T 36624；确保通信双方共享对称密钥建立的安全性，保护方式包括但不限于密钥交换协议、数字信封等；采用密钥交换协议的保护方式可遵循 GB/T 32918.3、GB/T 38635.2；采用数字信封的保护方式可遵循 GB/T 32918.4、GB/T 38635.2；

2) 采用认证合格的密码产品存储对称密钥，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、SSL VPN 产品/安全网关、服务器密码机等。

b) 基于非对称密钥的传输机密性保护，其设计时建议满足以下技术要求：

1) 非对称算法使用遵循 GB/T 32918.4；加密数据格式遵循 GB/T 35276；

2) 发送方在对被保护数据进行处理前，验证接收方的加密证书；验证通过后，再进行数据加密；

3) 采用认证合格的密码产品作为存储介质来存储加密私钥，并其使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机等。

C.3.2 存储的机密性保护

数据存储的机密性一般基于对称密码技术，其设计时建议满足以下技术要求：

a) 对称密码算法的使用遵循 GB/T 17964、GB/T 32907、GB/T 36624；

b) 采用认证合格的密码产品，作为存储介质来存储对称密钥，并使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、服务器密码机、电子文件密码应用系统、对称密钥管理产品等。

C.4 不可否认性保护设计指南

不可否认性保护一般基于数字签名技术，设计时建议满足以下技术要求：

a) 杂凑算法遵循 GB/T 32905，非对称密码算法遵循 GB/T 32918；

b) 使用获得主管部门许可的密码服务机构颁发的签名证书；

c) 可能涉及法律责任认定的应用中，对数据原发行为和数据接收行为进行验证；

d) 采用认证合格的密码产品作为存储介质来存储数字签名私钥，并其使用其进行密码运算；可选用的密码产品包括智能密码钥匙、PCI-E/PCI 密码卡、签名验签服务器、电子签章系统、服务器密码机等。

附录 D（资料性）

密码产品部署

D.1 密码产品部署

信息系统应根据密码支撑服务设计需求，进行密码产品部署，密码产品部署建议遵循相关标准与数据安全防护要求，避免因部署不当，造成明文数据在不安全网络通道、网络设备上流转。如密码支撑服务相关设备与信息系统部署在同一机房、密码支撑服务不跨机房调用、服务器密码机或其他密码模块不与核心交换机直接连接。

在密码产品部署时，建议通过密码产品标识符以及版本信息等，检查密码产品是否与密码产品的认证证书记录相一致。

如果初始化密码产品时，密码产品不包含鉴别操作员所需的鉴别数据，需建立制度并通过过程控制、使用出厂设置或默认的鉴别数据对密码产品进行初始化。如果使用默认的鉴别数据控制对密码产品的访问，默认的鉴别数据在第一次鉴别后更换；如果运行环境需要特殊配置的，需要按照安全策略的要求配置。

如果密码产品安全策略要求对操作系统等运行环境进行配置，在部署时对操作系统进行相应配置。

如果从密码产品外部获取熵源，需要确保按照安全策略正确配置熵源。

D.2 密码产品使用

信息系统需要制定密码设备管理员相关的安全管理制度，按照密码产品的安全策略，形成密码设备管理员指南，指导密码设备管理员正确使用密码产品。

对于手动建立的明文敏感安全参数，建议制定安全制度保护密钥的机密性、完整性和来源真实性。

建立安全管理制度，在密码产品执行自启动密码服务、旁路功能时进行授权和备案。

D.3 密码产品运维

对支持维护员角色（指在物理维护服务（例如，打开密码产品封盖）和/或逻辑维护服务（例如，运行某种诊断如内置的自测试）时担任的角色）的密码产品，建议制定安全管理机制对维护员角色的工作过程进行规范。

a) 建议制定定期巡查密码产品的安全管理制度，定期对以下情况进行巡查：

b) 检查密码产品是否正常运行在核准的工作模式；

c) 检查密码产品是否如预期开启或关闭自启动密码服务；

d) 检查密码产品是否如预期开启或关闭旁路服务；

e) 检查密码产品外观（如拆卸存迹的封条或防撬锁）是否被破坏；

f) 密码产品安全策略定义的其他情况。

同时制定明确的应急处理措施（如手动执行密钥销毁或者更新）。

对无法自动进行周期自测试的密码产品，建议制定密码产品自测试的安全管理制度，定期执行密码产品提供的自测试功能。

D.4 密码产品销毁

制定密码产品生命终止相关的安全管理制度，当不再使用密码产品时，按照密码产品的安全策略，对密码产品进行清理（从密码产品中去除敏感信息）或销毁。

对密钥等敏感安全参数进行清零时，如果未受保护的敏感安全参数的置零操作由密码产品管理员按照规定的程序执行而不依赖于密码产品控制（例如，硬盘格式化等），则需要制定相应的管理制度。

附录 E（资料性）

常见密钥体系构建方式

E.1　对称密钥体系

E.1.1 基于密钥加密：银行 KEK 密钥体系

如图 E.1 所示，该密钥体系中，父密钥为对称密钥，子密钥为对称密钥。该密钥体系用于保护子密钥的传输和存储。

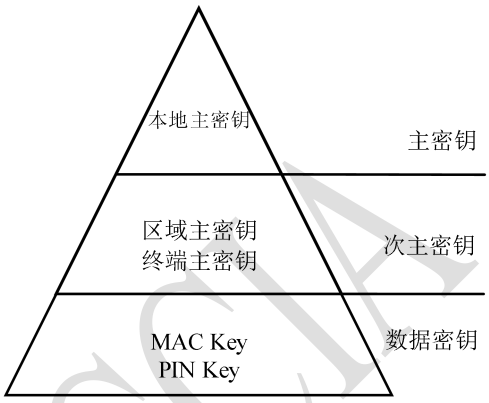

图 E.1　银行 KEK 密钥体系

该密钥体系中，所有实体持有永久的对称密钥。当实体 A 和实体 B 进行通信时，通过主密钥加密次主密钥，采用离线分发的方式实现次主密钥在实体 A 和实体 B 之间的共享，并通过共享的次主密钥实现实体 A 和实体 B 之间的数据密钥共享。

E.1.2 基于密钥分散：IC 卡分散密钥体系

如图 E.2 所示，该密钥体系中，父密钥为对称密钥，子密钥为对称密钥。该密钥体系用于子密钥的生成。

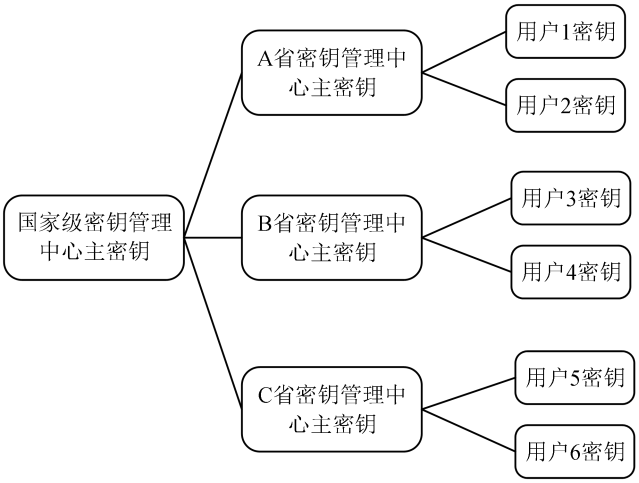

图 E.2　IC 卡分散密钥体系

该密钥体系中，所有实体持有永久的对称密钥。当对实体 A 进行身份鉴别时，父节点通过自己的主密钥和实体 A 的信息恢复出实体 A 的节点密钥，实现对 A 的身份鉴别。

E.2　非对称密钥体系

基于信任传递：PKI 密钥体系。如图 E.3 所示，该密钥体系中，父密钥为非对称密钥，子密钥为非对称密钥。该密钥体系用于构建多个实体之间的信任关系。

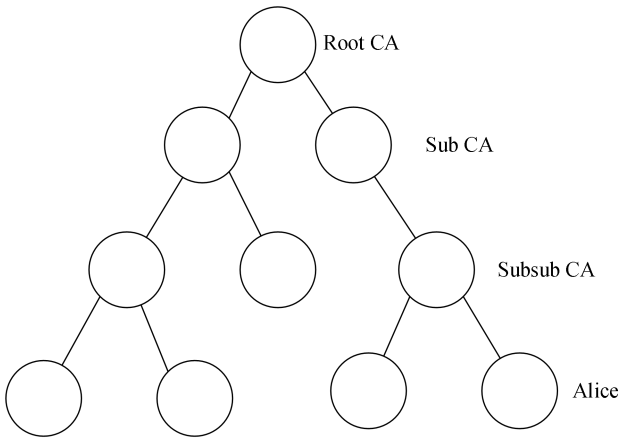

图 E.3　PKI 密钥体系

该密钥体系中，所有实体持有永久的非对称密钥。当对实体 A 进行身份鉴别时，通过证书链校验，实现对实体 A 身份的鉴别。非对称密钥体系主要应用于身份鉴别、完整性保护、不可否认性保护等场景。

E.3　混合密钥体系

E.3.1 基于密钥加密的混合密钥体系

如图 E.4 所示，该密钥体系中，父密钥为非对称密钥，子密钥为对称密钥。该密钥体系用于双方进行密钥的传输共享。

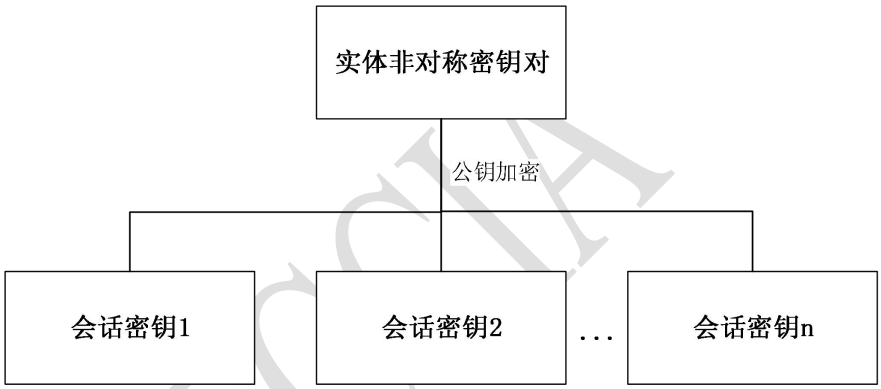

图 E.4　基于密钥加密的混合密钥体系

该密钥体系中，所有实体持有永久的非对称密钥。实体 A 和实体 B 需要进行通信时，实体 A 生成会话密钥，利用实体 B 的公钥加密后，发送给实体 B，实体 B 再利用自己的私钥解密获得会话密钥；实体 A 和实体 B 利用会话密钥进行通信。

E.3.2 基于密钥协商的混合密钥体系

如图 E.5 所示，该密钥体系中，父密钥为非对称密钥，子密钥为对称密钥。该密钥体系用于双方进行密钥的传输共享。

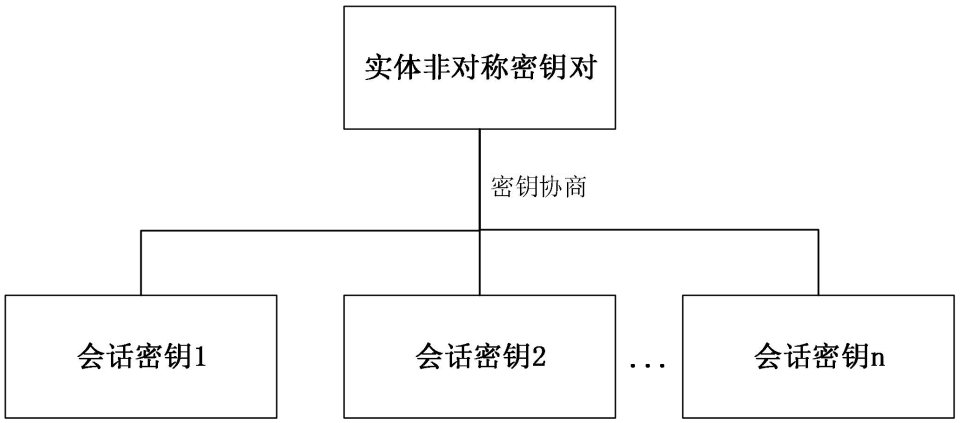

图 E.5　基于密钥协商的混合密钥体系

该密钥体系中，所有实体持有永久的非对称密钥。实体 A 和实体 B 需要进行通信时，实体 A 和实体 B 利用密钥交换协议生成会话密钥；实体 A 和实体 B 利用会话密钥进行通信。