天津市商用密码行业协会
Tianjin Commercial Cryptography Industry Association

# GB/T 39786-2021
# 《信息安全技术 信息系统密码应用基本要求》
# 内容解读

# 目 录

# 1 第一部分

## 标准背景及简介

# 为什么要有GB/T 39786这个标准

落实密码法及相关政策文件的需要

促进各行业领域信息系统应用密码的需要

指导商用密码应用安全性评估的需要

增强密码应用规范、正确、有效性的需要

# 为什么有了GM/T 0054-2018还需要本标准

## 《标准化法》

- 第十一条　对满足基础通用、与强制性国家标准配套、**对各有关行业起引领作用等需要的技术要求**，可以制定推荐性国家标准。
- 第十二条　对没有推荐性国家标准、需要在全国**某个行业范围内**统一的技术要求，可以制定行业标准。

## 与等保的衔接

- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

# 标准制订发布的时间线

**《中华人民共和国密码法》实行**

2019年10月26日

**《中华人民共和国密码法》通过**

2020年1月1日

里程碑

2021年3月9日

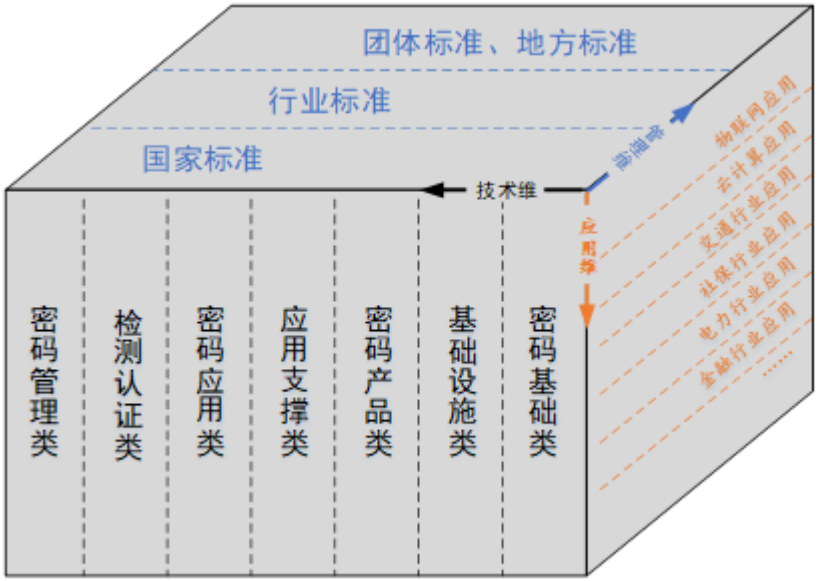

**《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）正式发布**

“信息系统密码应用基本要求”从行业标准0054上升为国家标准，是密码领域的一件大事，是《密码法》出台实施之后开展商用密码应用与安全性评估工作的重要里程碑。

**GB/T 39786-2021实行**

2021年10月1日

# 在密码标准体系中的位置




密码标准体系框架

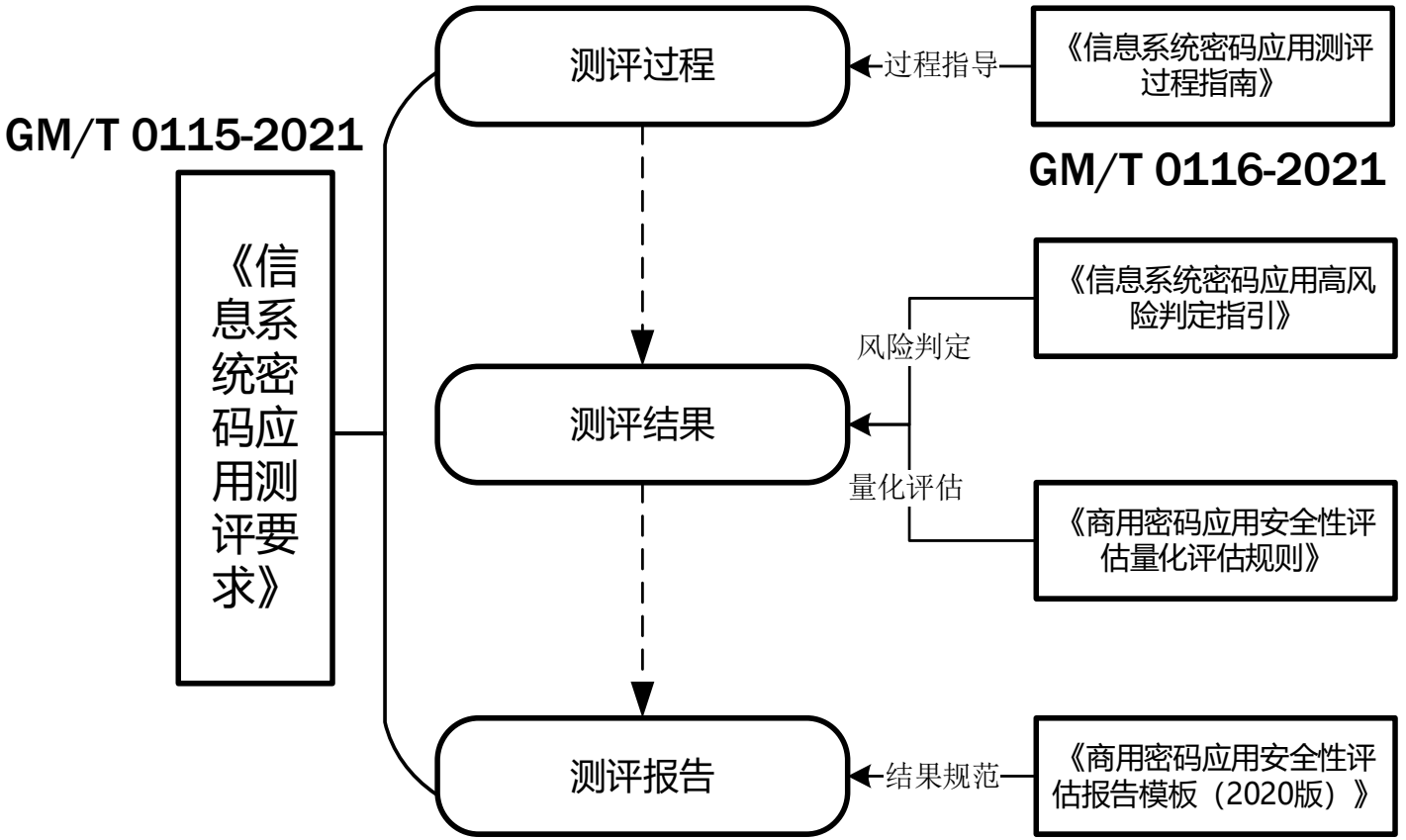
- 密码基础类
- 基础设施类
- 密码产品类
- 应用支撑类
- 密码应用类
  - 应用要求
  - 应用指南
  - 应用规范
  - 密码服务
- 检测认证类
- 密码管理类

技术维

# 39786不是唯一的密码应用标准

| | | | |
|---|---|---|---|
| 密码应用类 | 应用要求 | GM/T 0035-2014（所有部分） 射频识别系统密码应用技术要求 | GB/T 37033-2018（所有部分） 信息安全技术 射频识别系统密码应用技术要求 |
| | | GM/T 0054-2018 信息系统密码应用基本要求 | GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求 |
| | | GM/T 0070-2019电子保单密码应用技术要求 | |
| | | GM/T 0072-2019远程移动支付密码应用技术要求 | |
| | | GM/T 0073-2019手机银行信息系统密码应用技术要求 | |
| | | GM/T 0074-2019网上银行密码应用技术要求 | |
| | | GM/T 0075-2019银行信贷信息系统密码应用技术要求 | |
| | | GM/T 0076-2019银行卡信息系统密码应用技术要求 | |
| | | GM/T 0077-2019银行核心信息系统密码应用技术要求 | |
| | | GM/T 0095-2020电子招投标密码应用技术要求 | |
| | | GM/T 0100-2020人工确权型数字签名密码应用技术要求 | |
| | | GM/T 0111-2021区块链密码应用技术要求 | |
| | | GM/T 0112-2021PDF格式文档的密码应用技术要求 | |
| | 应用指南 | GM/T 0036-2014采用非接触卡的门禁系统密码应用技术指南 | |
| | | | GB/T 32922-2016 信息安全技术 IPSEC VPN安全接入基本要求与实施指南 |
| | | GM/T 0071-2019电子文件密码应用指南 | GB/T 38541-2020信息安全技术 电子文件密码应用指南 |
| | | GM/T 0096-2020射频识别防伪系统密码应用指南 | |

# 39786是密码应用标准而不是测评标准




基于39786的系列测评指导文件

# 2 第二部分

## 标准基本架构

# 标准基本架构

## 范围

规定了信息系统第一级到第四级的密码应用的基本要求，适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

## 规范性引用文件

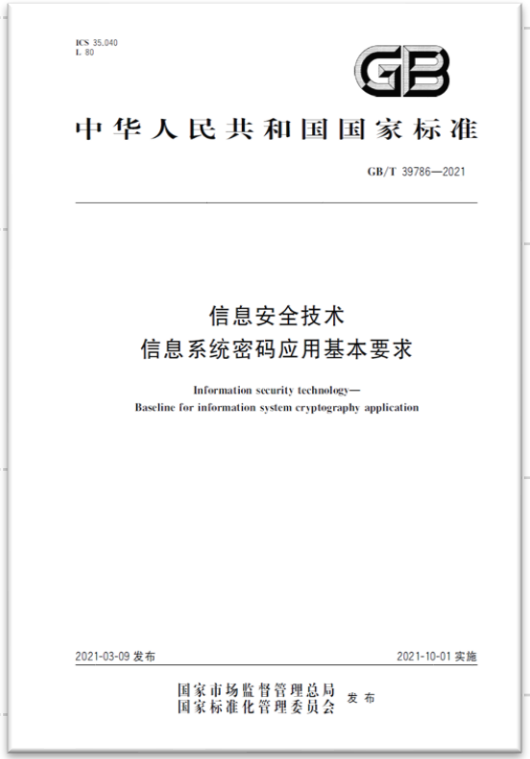
GB/T 37092 信息安全技术 密码模块安全要求。

## 术语和定义

明确了机密性、数据完整性、真实性、不可否认性、加密、密钥、密钥管理、身份鉴别、消息鉴别码、动态口令、访问控制等概念。

## 概述

规定了机密性、数据完整性、真实性、不可否认性、加密、密钥、密钥管理、身份鉴别、消息鉴别码、动态口令、访问控制等概念。




## 通用要求

规定了密码算法、密码技术、密码产品和密码服务应符合相关国家标准、行业标准的有关要求。

## 密码应用基本要求

| | | | |
|---|---|---|---|
| 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 |
| 管理制度 | 人员管理 | 建设运行 | 应急处置 |

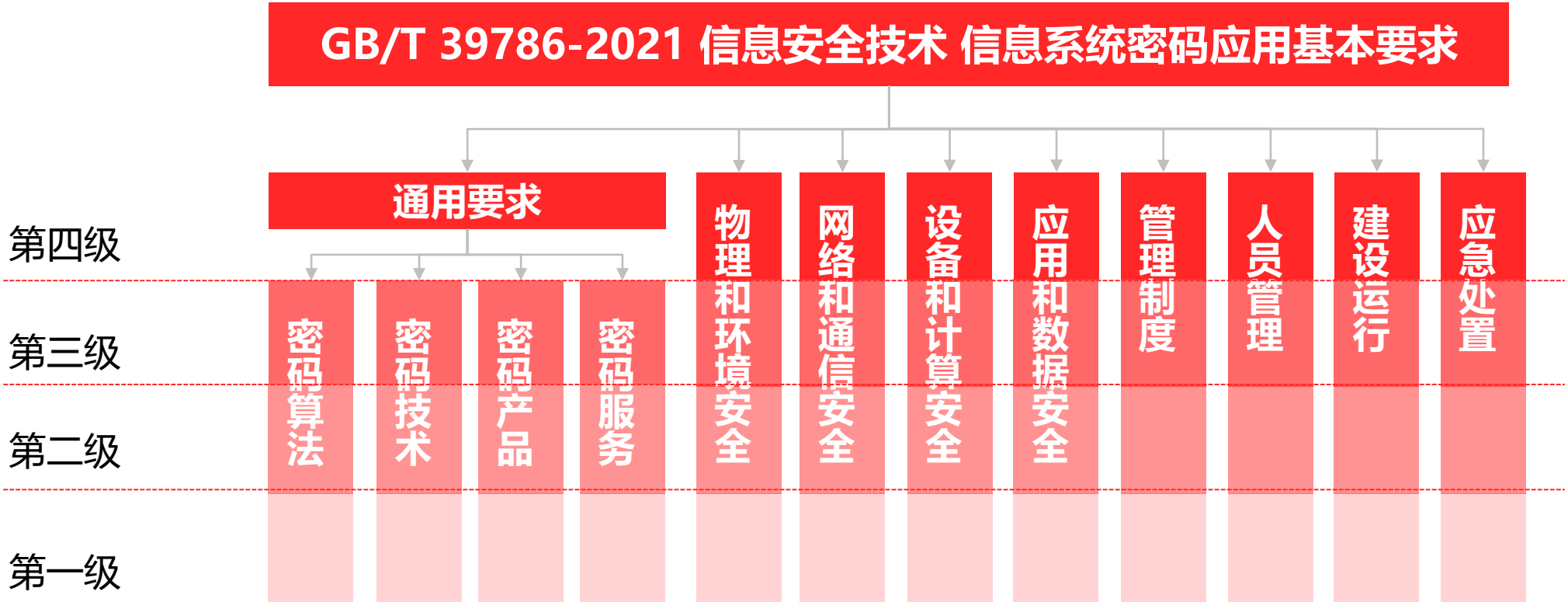
## 附录A

列出了不同级别密码应用基本要求“应”、“宜”、“可”的汇总表。

## 附录B

提出了密钥生存周期管理的建议，包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。

# 标准基本架构


GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
通用要求
密码算法
密码技术
密码产品
密码服务
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
管理制度
人员管理
建设运行
应急处置
第四级
第三级
第二级
第一级

# 应、宜、可

## GB 1.1—2020

- “应”表示应该、只准许，“宜”表示推荐、建议，“可”表示可以、允许。

## GM/T 0115—2021《信息系统密码应用测评要求》

- 若信息系统未编制密码应用方案或在方案中未对“宜”的指标要求做明确说明，则“宜”的指标要求纳入标准符合性测评范围。
- 若信息系统编制了密码应用方案，且方案通过评估，方案中明确了不适用的“宜”的指标要求项，且有对应的风险控制措施说明的情况下。密评人员在测评时，应根据信息系统的密码应用方案和方案评估报告/评审意见，核实方案中的不适用指标要求项所采用的风险控制措施的适用条件，在实际的信息系统中是否被满足，且信息系统的实施情况与方案中所描述的风险控制措施是否一致，若满足适用条件，该测评指标为“不适用”；若不满足适用条件，则应纳入标准符合性测评范围，进行测评和结果判定。

# 3 第三部分

## 标准要求条款（三级为例）

## 物理和环境安全

a 宜采用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；

b 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；

c 宜采用密码技术保证视频监控音像记录数据的存储完整性；

d 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

e 以上采用的密码产品，应达到GB/T37092二级及以上安全要求

# 物理环境的要求对象：哪些机房和区域？

## 信息设备所在的物理机房

- 机房不止一个？所有物理机房均纳入。

## 机房不属于责任单位管辖

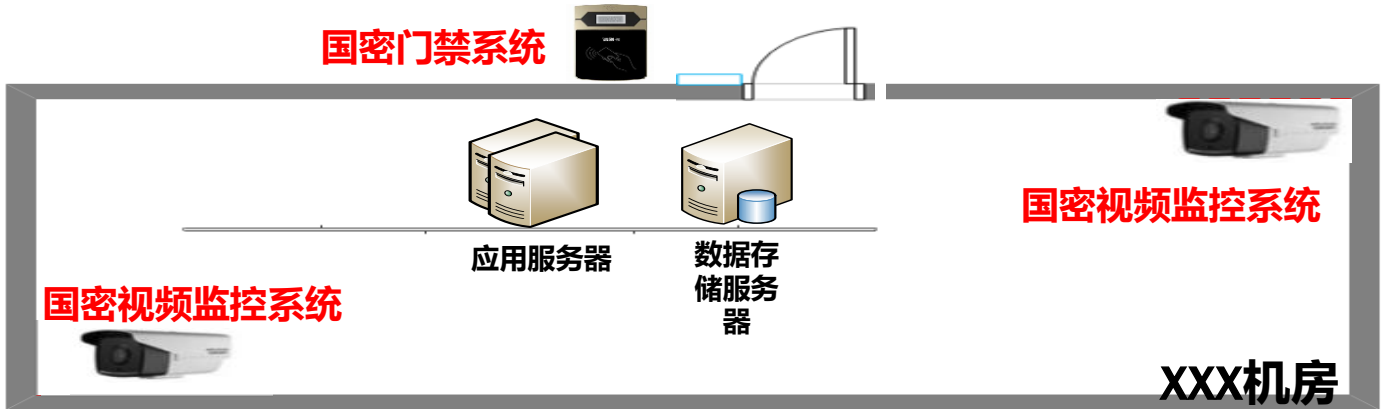
- 物理和环境安全层面仍然适用。
- 如果信息系统所在的IDC机房、运营商机房或云服务提供商机房等通过了密评，则可以复用其密评报告中“物理和环境安全”层面的结论。
- 如果未通过或未开展，密评时现场取证。条件不允许？要求运维方提供相关说明文件和证据。

# 物理和环境安全层面的常见密码应用方式

## 常见方式及注意事项

- **使用支持SM算法的门禁系统和视频监控系统**

目前市场上有支持SM算法的门禁系统；支持完整性保护的视频监控系统。如果产品本身不支持，可请产品厂商基于外挂密码设备（如密码机）来实现。



## 网络和通信安全

a) 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

b) 宜采用密码技术保证通信过程中数据的完整性；

c) 应采用密码技术保证通信过程中重要数据的机密性；

d) 宜采用密码技术保证网络边界访问控制信息的完整性；

e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；

f) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

g) 以上采用的密码产品，应达到GB/T37092二级及以上安全要求。

# 网络和通信安全层面的常见密码应用方式

## 常见方式及注意事项

- **在跨安全域通信链路部署Ipsec/SSL VPN安全通道**

  GM/T 0024 SSL VPN技术规范, GB/T 38636 TLCP协议 ……

  三级系统不要求“双向”安全通道，因此使用合规设备建立单向安全通道也是可行的。

- **注意：“专线”常常不能代替安全通道**

  通常所谓的运营商专线，会经过各种交换设备和运营商骨干网，还是需要采用密码技术保护网络和通信层面的机密性、完整性

## 设备和计算安全

a) 应采用密码技术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，应采用密码技术建立安全的信息传输通道；

c) 宜采用密码技术保证系统资源访问控制信息的完整性；

d) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；

e) 宜采用密码技术保证日志记录的完整性；

f) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；

g) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

h) 以上采用的密码产品，应达到GB/T37092二级及以上安全要求。

# 设备和计算安全层面的常见密码应用方式

## 常见方式及注意事项

- **部署支持商用密码的堡垒机，实现设备统一管理**

  管理员登录堡垒机采用基于商用密码的身份鉴别产品和技术，如使用智能密码钥匙与堡垒机之间做基于数字签名的“挑战-响应”鉴别。

  还可以基于堡垒机做日志统一管理，统一采取完整性保护措施。

- **需要注意堡垒机SSH协议的版本和算法套件**

  SSH协议的版本和算法套件决定了“远程管理通道”指标项是否合规，要注意规避高风险项，如SSH v1.0、完整性算法中出现的md5、sha1等……

## 应用和数据安全

a) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

b) 宜采用密码技术保证信息系统应用的访问控制信息的完整性；

c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

d) 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

e) 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

f) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

g) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；

i) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

j) 以上采用的密码产品，应达到GB/T37092二级及以上安全要求。

# 应用和数据安全层面的常见密码应用方式

## 常见方式及注意事项

- **对“重要数据”的界定是必须要做的**

  对系统传输、存储、处理的业务数据做分级分类，厘清“重要数据”。一般可采用风险分析的方法来界定。

  如果已经进行了等保定级和测评，那么是重要数据界定的有力依据。

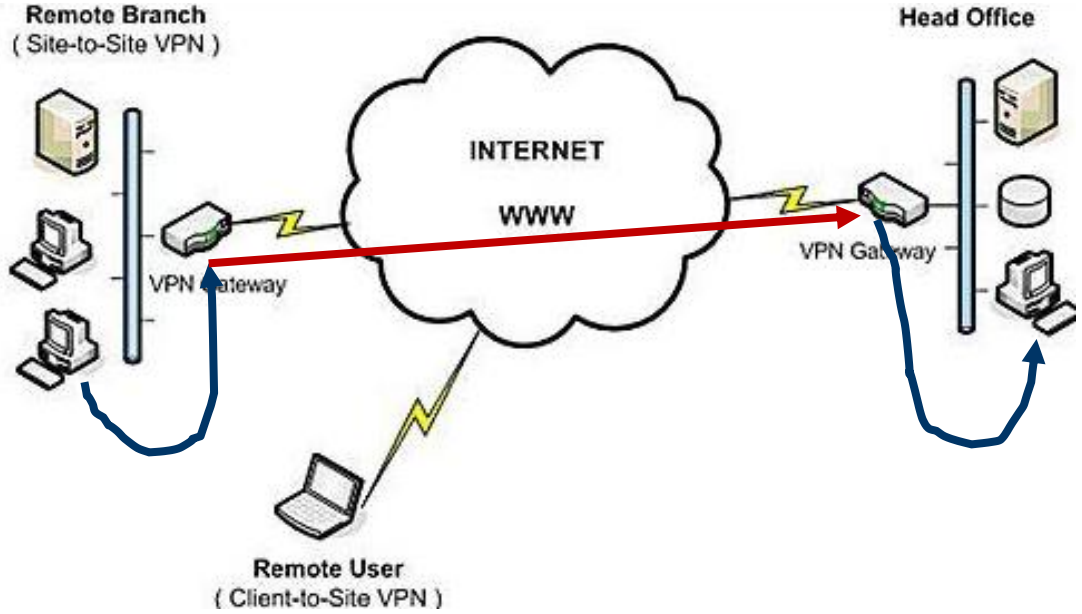
- **可以采用数字信封保障重要数据传输机密性**

  网络与通信层机密性完整性机制保障了通道安全，但不涵盖重要数据落地后的安全。对于重要数据的应用层保护，采用数字信封进行机密性保护是常见做法。

- **可以采用时间戳和数字签名保障不可否认性**

  对于不可否认性的保护，单纯使用签名是不够的，还需要结合时间戳，确保“实体不能否认在指定时刻执行了某个动作”。

# 应用数据、网络通信两层的数据传输机密性、完整性




| |
|---|
| 应用层数据 |
| 传输层**安全**通信协议，如 **TLS** |
| 网络层**安全**通信协议，如 **IPsec** |
| 链路层<br>物理层 |

## 信道加密 vs. 信源加密

**VPN**卸载后的明文数据，如果仍有多个可能的接收者，且要求只有指定的接收者才可见，那么有必要在应用层执行对传输数据的端到端密码保护（信源加密）

# 从物理到应用，四个层面上身份鉴别的对象

| 技术层面 | 身份鉴别对象 | 示例 | 作用 |
| --- | --- | --- | --- |
| 物理环境 | 进出重要区域的人 | 机房管理员，保安 | 防范非法人员进入该区域 |
| 网络通信 | 建立安全通信通道的节点设备 | SSL VPN网关设备 | 防范网络设备被替换、假冒 |
| 设备计算 | 设备的管理员 | 安装Windows操作系统的设备，Administrator用户 | 防范非法人员控制设备 |
| 应用数据 | 信息系统的用户/管理员 | 微信用户，OA用户 | 防范业务用户身份的假冒 |

# 标准内容解读

## 管理制度

a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

b) 应根据密码应用方案建立相应密钥管理规则；

c) 应对管理人员或操作人员执行的日常管理操作建立操作规程；

d) 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；

e) 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；

f) 应具有密码应用操作规程的相关执行记录并妥善保存。

## 人员管理

a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；

b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：

1) 根据密码应用的实际情况，设置密钥管理员、密码审计员、密码操作员等关键安全岗位；

2) 对关键岗位建立多人共管机制；

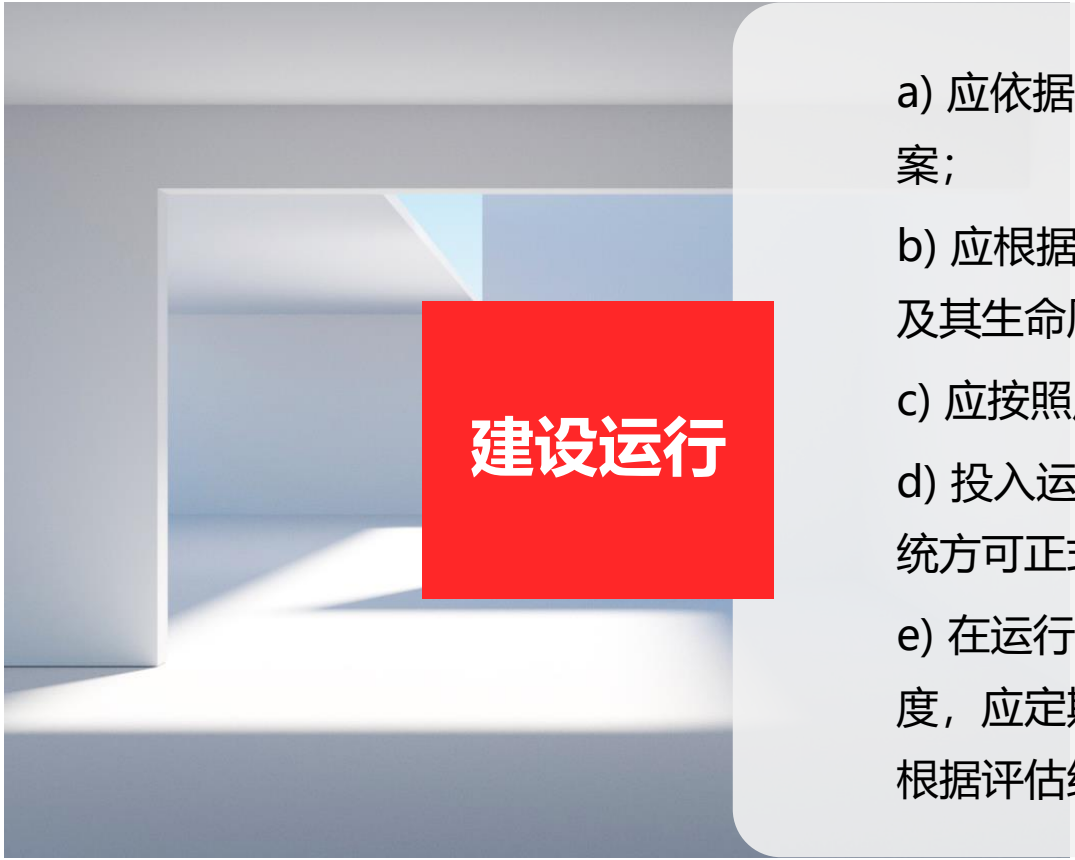
3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；

4) 相关设备与系统的管理和使用账号不得多人共用。

c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；

d) 应定期对密码应用安全岗位人员进行考核；

e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。



## 建设运行

a) 应依据密码相关标准和密码应用需求，制定密码应用方案；

b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照附录B；

c) 应按照应用方案，制定实施方案；

d) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；

e) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

## 应急处置

a) 应制定密码应用应急处置方案，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置方案，结合实际情况及时处置；

b) 事件发生后，应及时向信息系统主管部门进行报告；

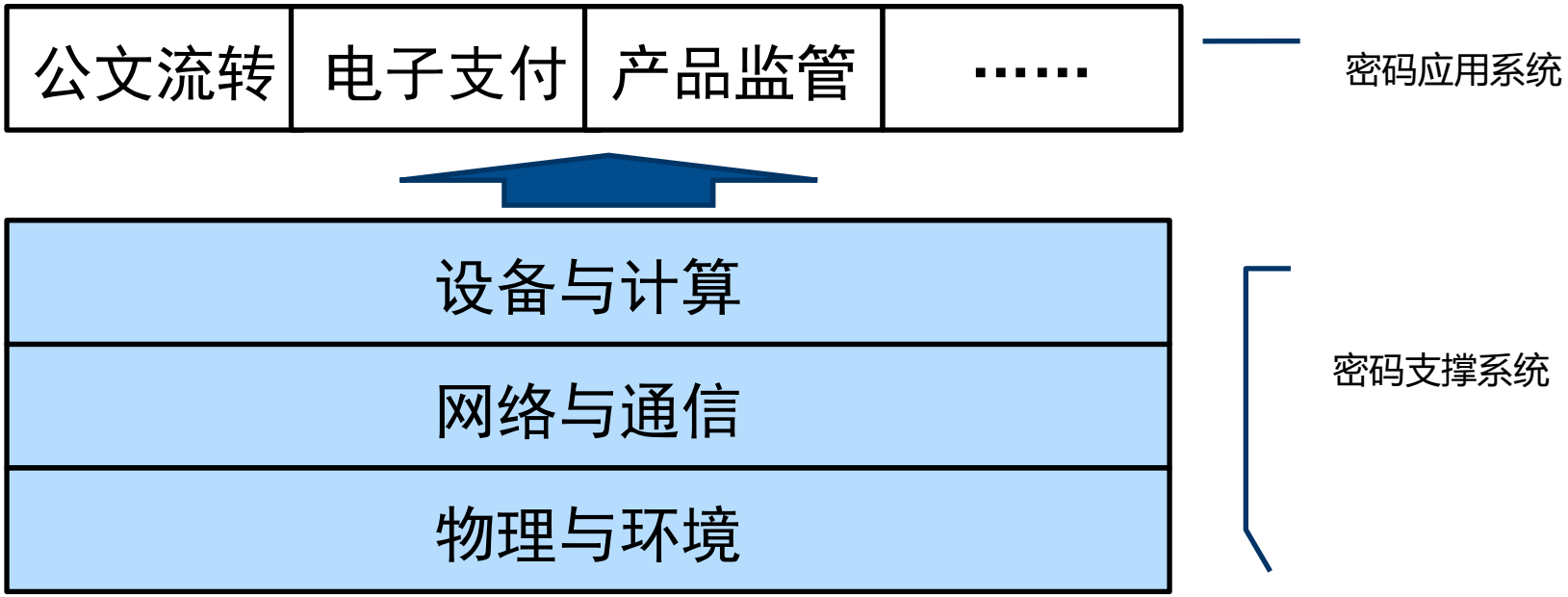
c) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

# 3 第三部分

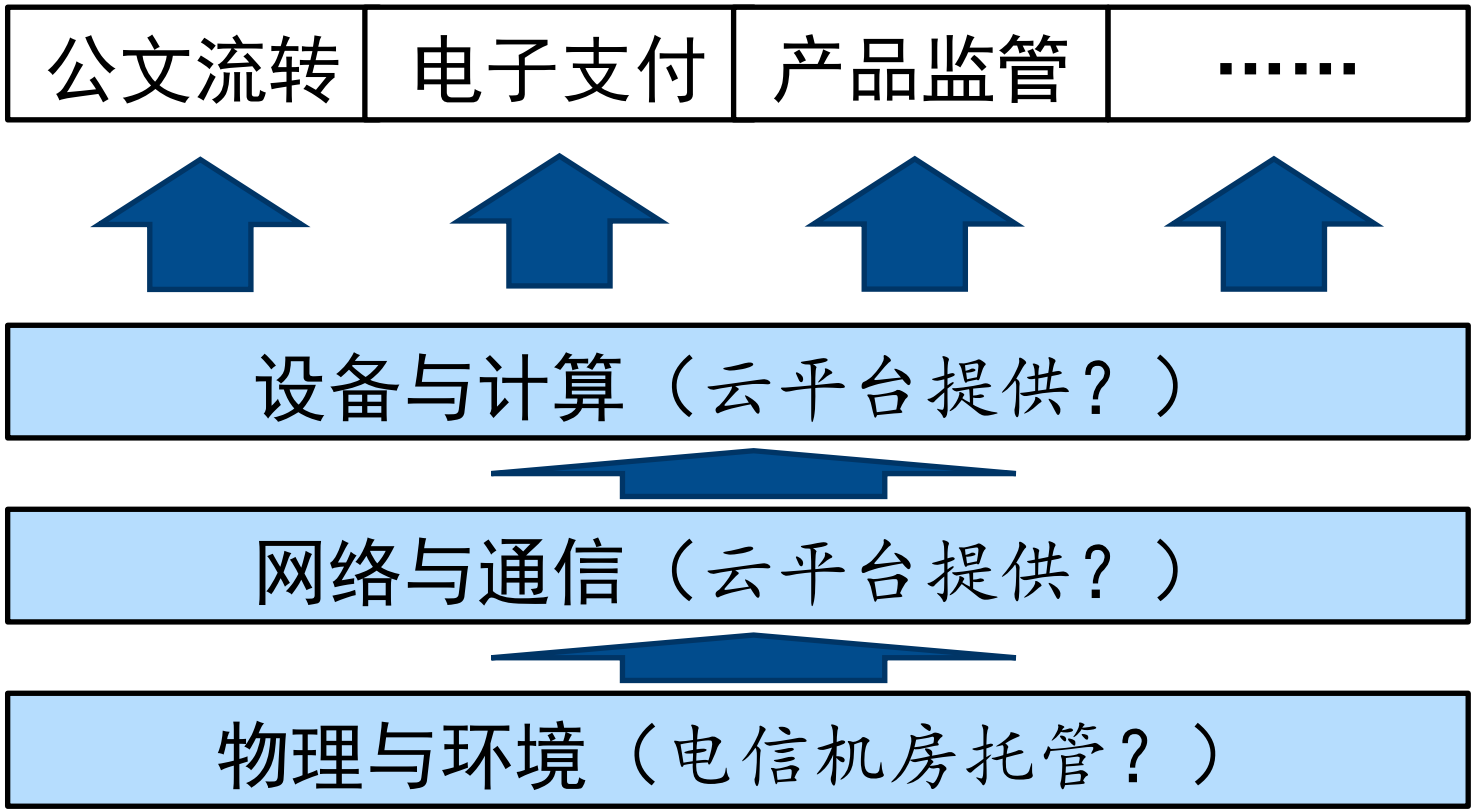
## 标准文本之外的要点

**不能指望有放之四海皆准的“标准”密码应用方案！**

不充分了解信息化业务，做不出适用的、可落地的密码应用方案



# 信息系统责任主体




不同层面可能由不同的主体运营

相同层面的不同部分可能由多个主体运营

“该部分不是自己运营”，不能作为将其排除在密码应用考虑之外的理由。

# 对信息系统所有者/建设者的建议

## 本标准是制订密码应用方案的直接依据

### 需求分析

- 业务安全需求
- 使用密码技术满足安全需求的措施

### 功能分配

- 密码功能的分层、分部拆解与相互接口
- 每层每部的责任主体

### 方案设计

- 做自己建设/运营层面、部分的方案
- 引用其他层面、部分的方案

### 合规性自评

- 各层各部是否已经通过密评
- [是]引用密评结论
- [否]各层各部责任主体对照要求自评

# 对密评机构的建议

## 本标准是密评的顶层依据

### 确定范围级别

- 等保定级范围

### 确认责任主体

- 单个密评案例，最好只针对单一责任主体
- 依赖其他责任主体信息系统时，建议先评估被依赖的信息系统
- 实在需要，则延伸评估，而非粗暴的设定为“不适用”

### 不适用分析

- 没有保护对象，或没有安全需求
- “可”项自主选择，需判断替代性措施有效性
- “宜”项复核，理由是否合理充分，替代性措施是否有效

### 量化与高风险

- 单项的分值估计
- 不同层面间的风险弥补
- 高风险的判定

# 谢谢！
# Q&A