2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

商用密码应用技术体系、标准和典型方案

刘辛越
密码行业标准化技术委员会委员
全国信息安全标准化技术委员会委员
北京创原天地科技有限公司董事长

1、商用密码应用技术体系

2、商用密码技术标准

3、商用密码应用典型方案

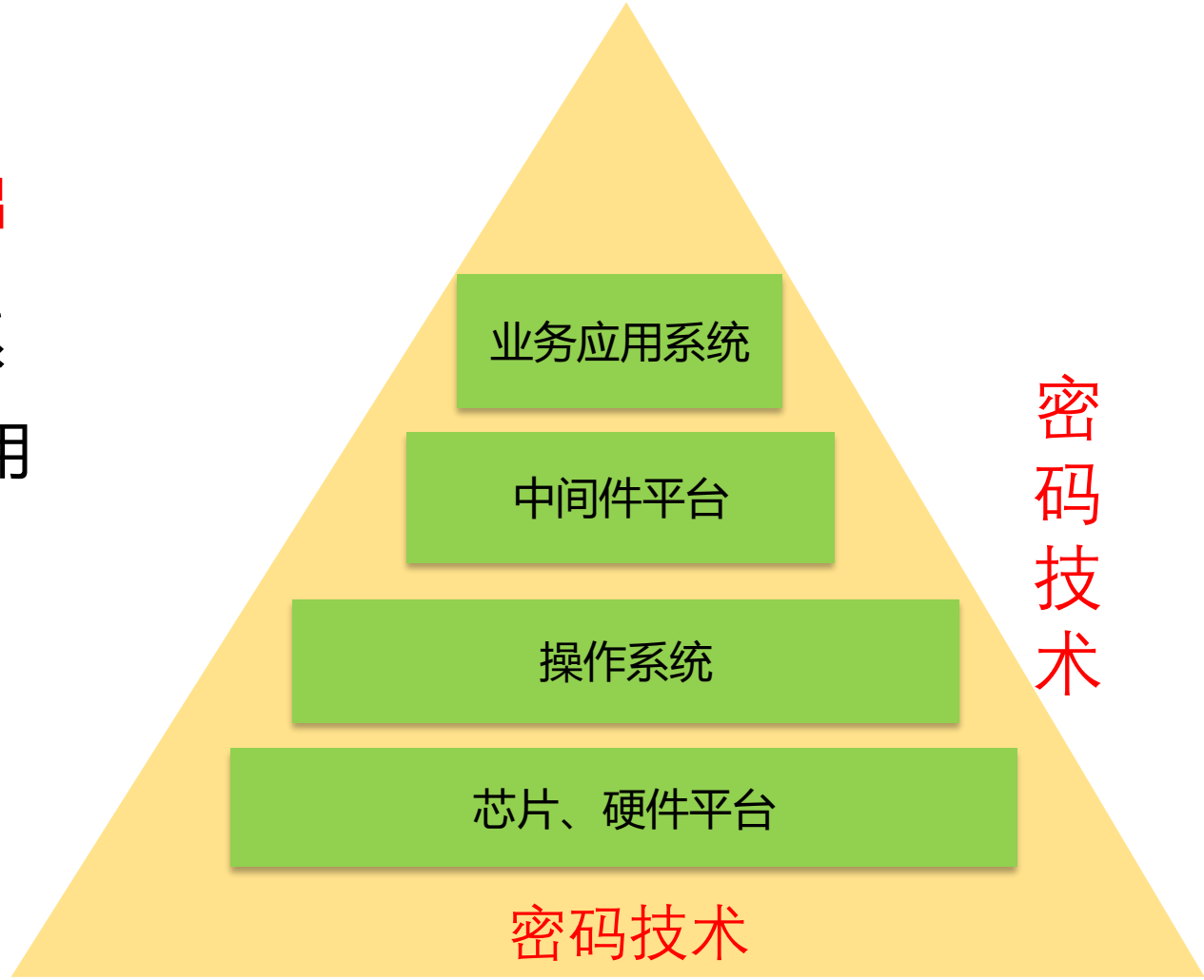
1、商用密码应用技术体系

密码技术特征：

1、密码技术是实现内生安全的核心和基础

2、整体贯穿：硬件（芯片）平台、操作系统、应用服务器（中间件平台）、业务应用系统各个层次

3、密码技术应用需从系统规划设计开始，尽量满足各个层次的密码安全设计要求



密码在业务应用系统中的作用

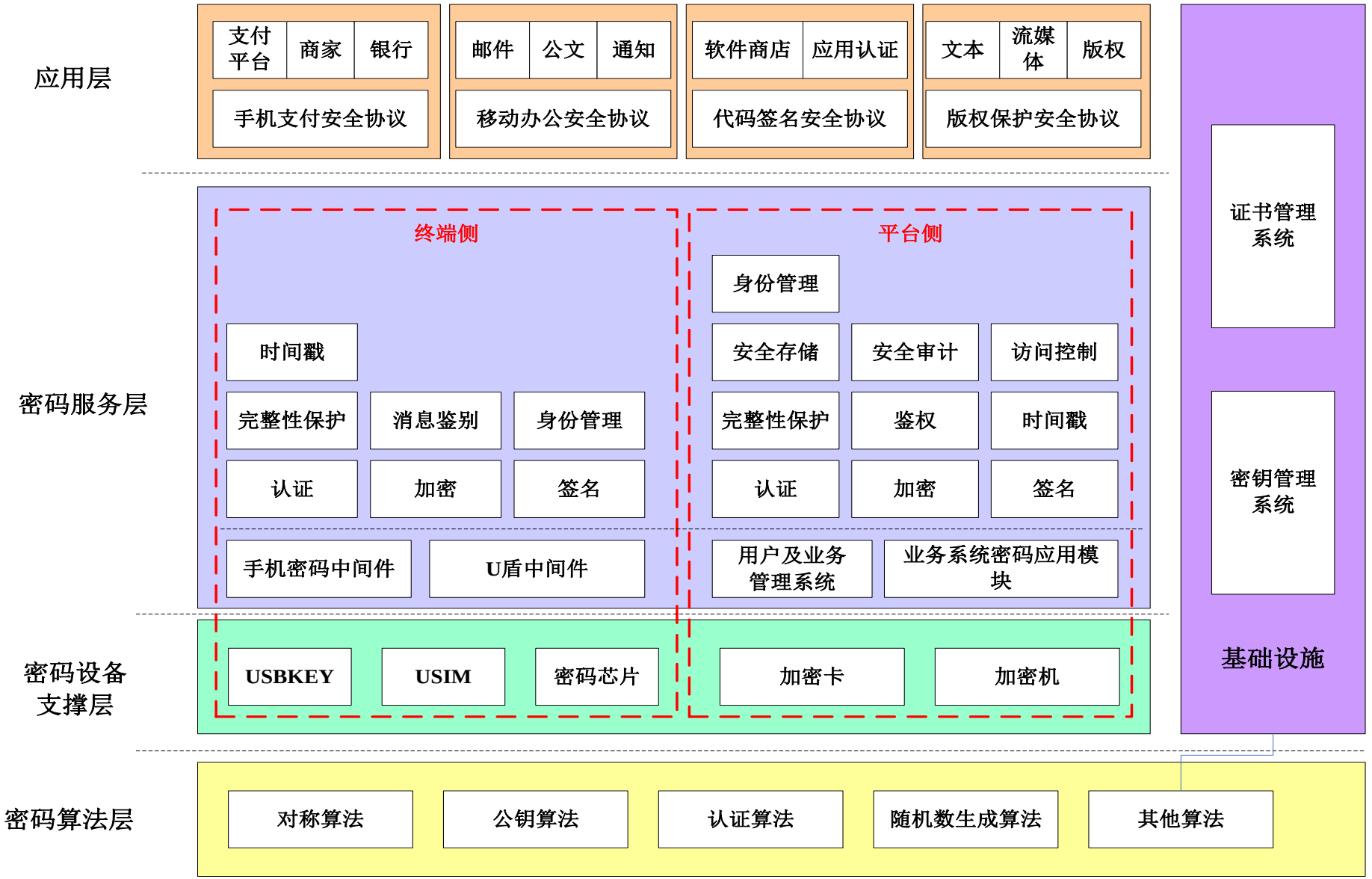
1、正确鉴别用户身份及权限。使用密码技术对网银用户进行身份标识和身份鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证用户身份的真实性；

2、保证关键数据的真实性和完整性。使用完整性保护技术，防止非法用户对关键数据进行篡改或删除，防止数据传送过程中可能的数据丢失；

3、保证关键数据的机密性：通过对敏感数据加密来保护系统数据交换安全，保障账户信息、交易数据、用户信息等关键数据的机密性；

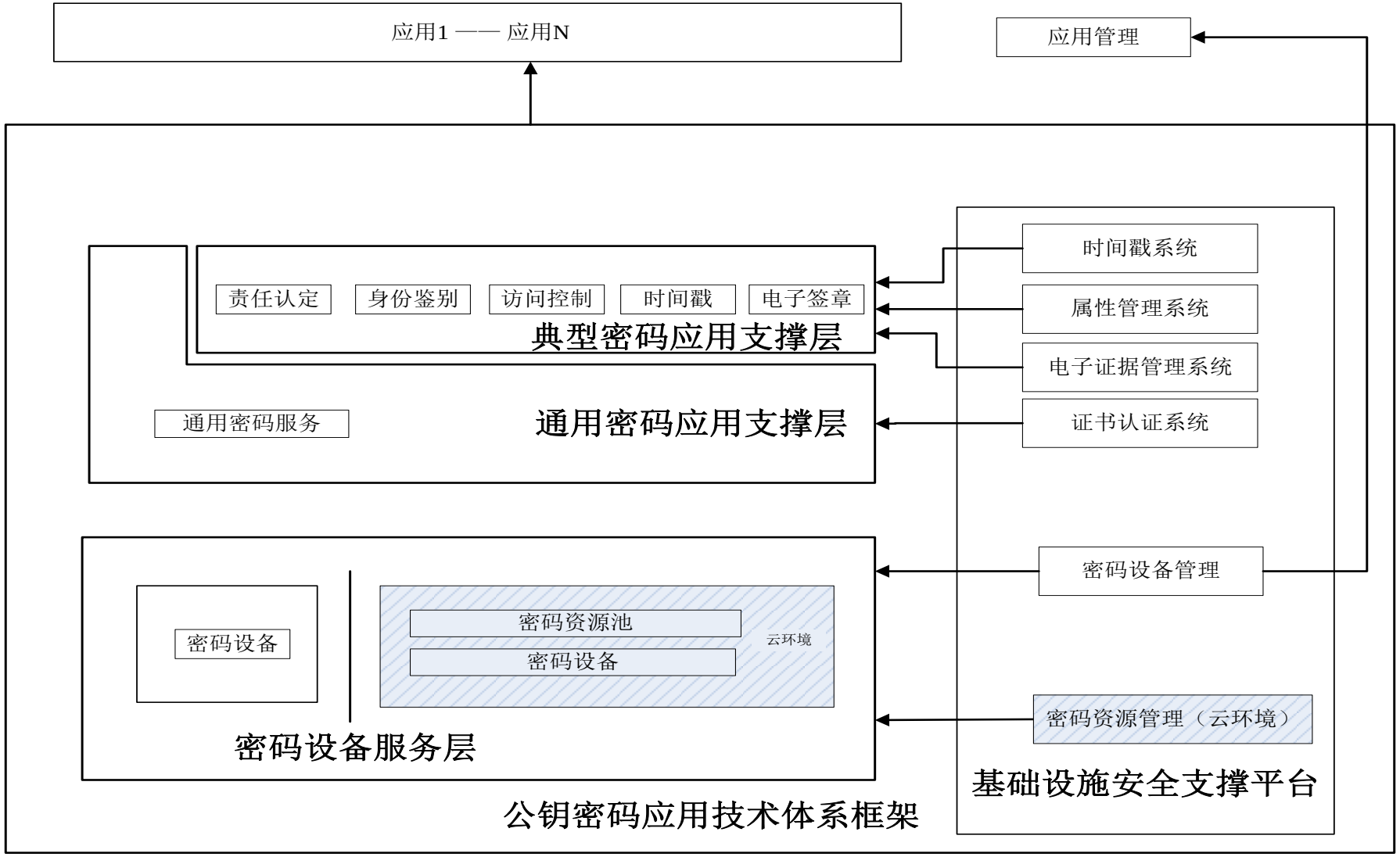
4、实现关键操作的不可否认性。对于网上交易、账务查询等重要操作，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为和数据接收行为的不可否认性。

1、商用密码应用技术体系



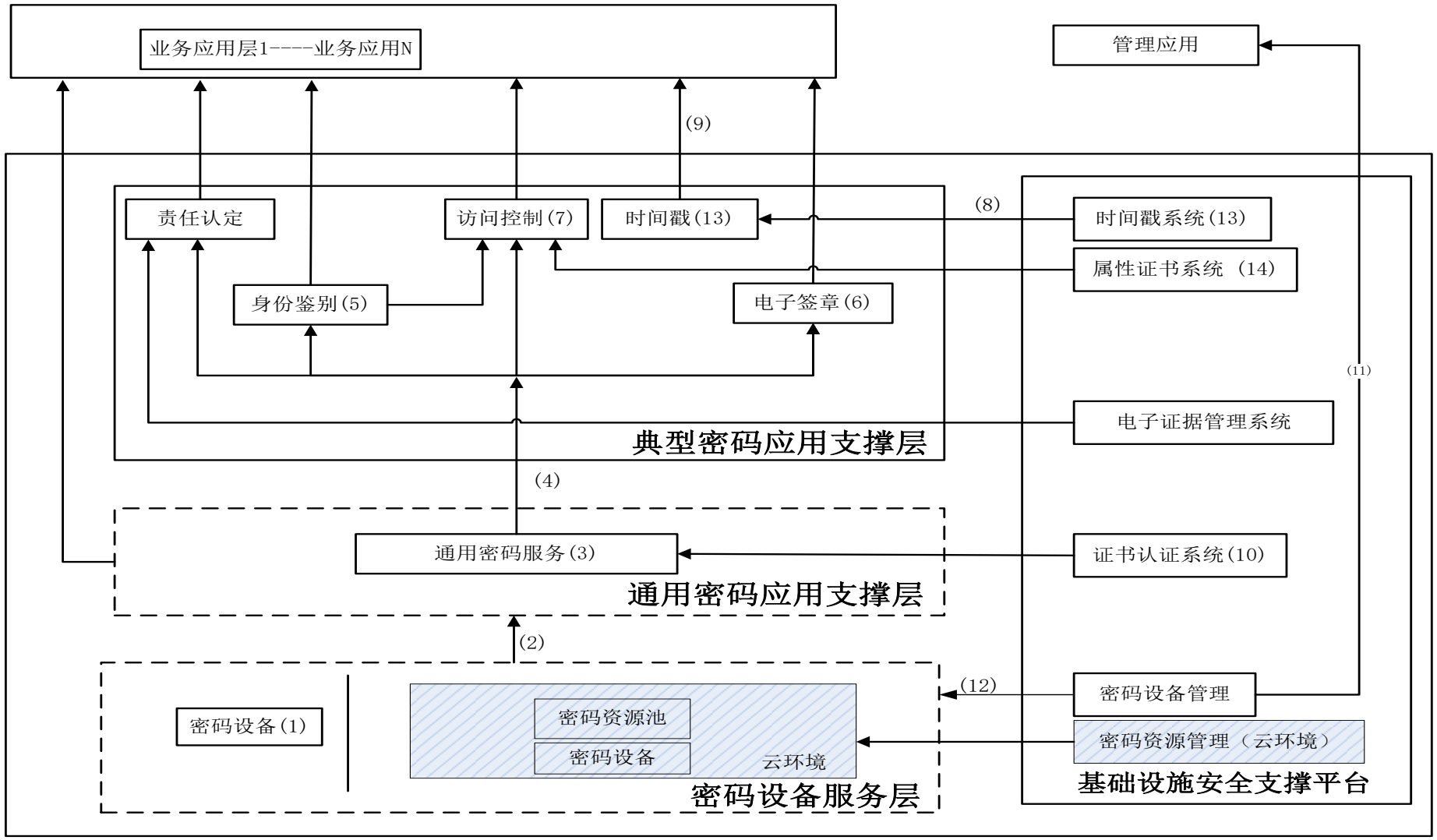
1、商用密码应用技术体系

公钥密码应用技术体系框架图



1、商用密码应用技术体系

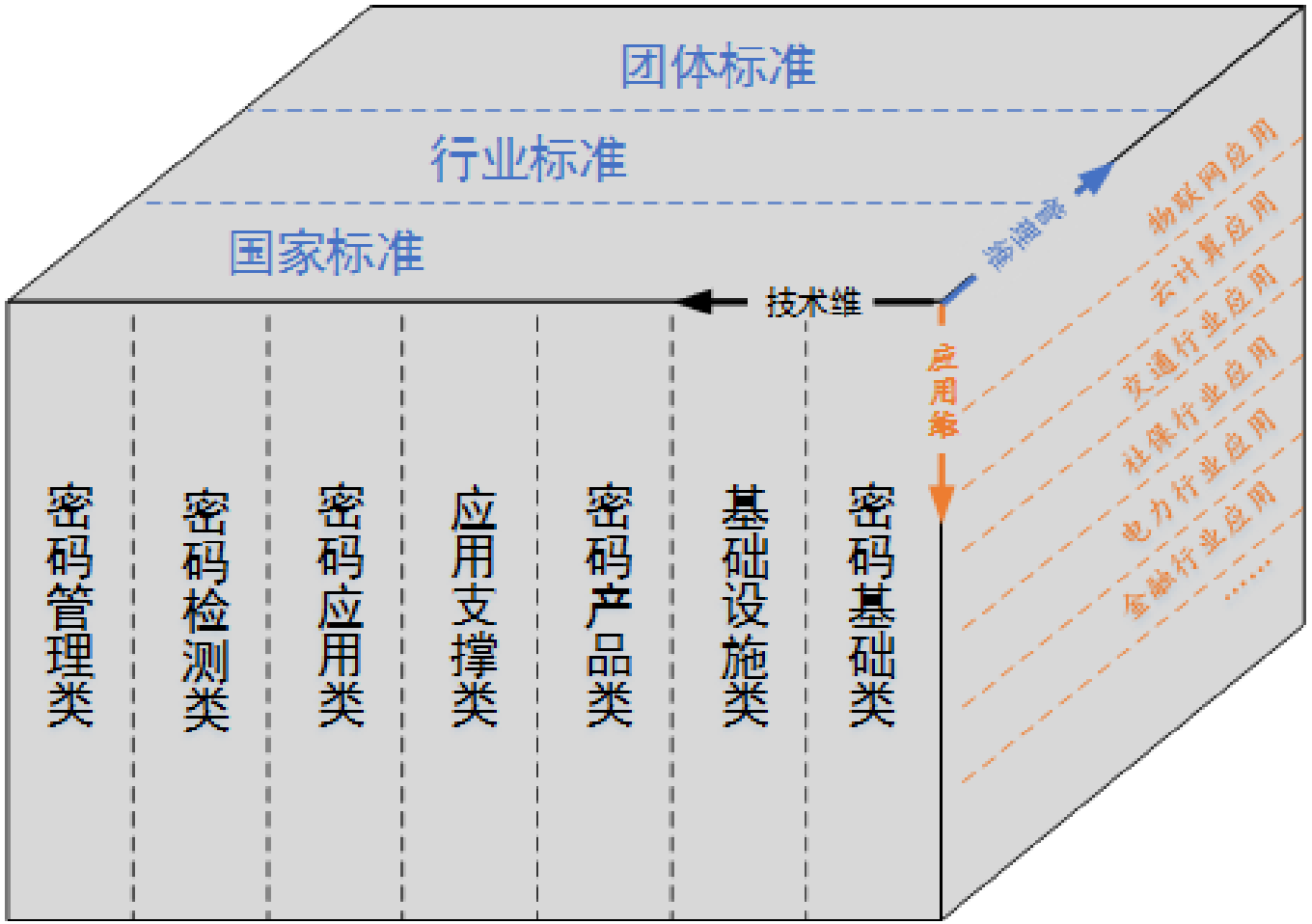
公钥密码应用技术体系框架逻辑图



2、商用密码技术标准

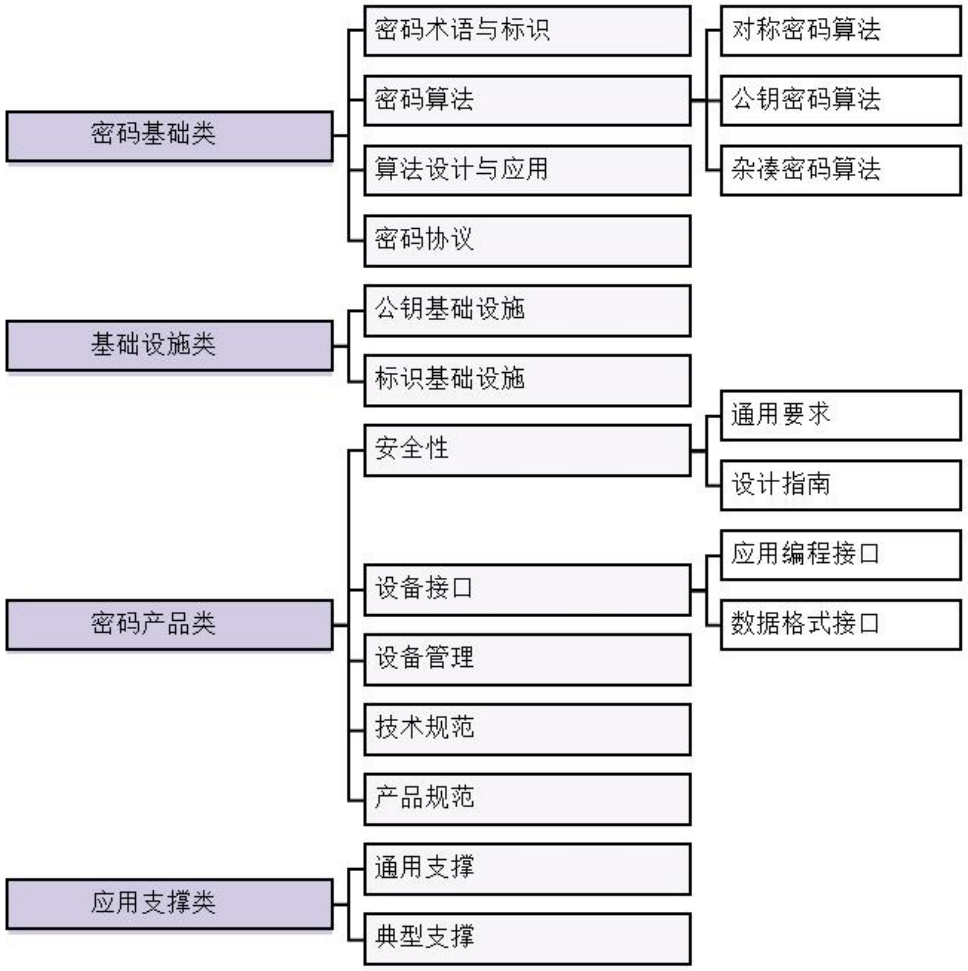
2、商用密码技术标准

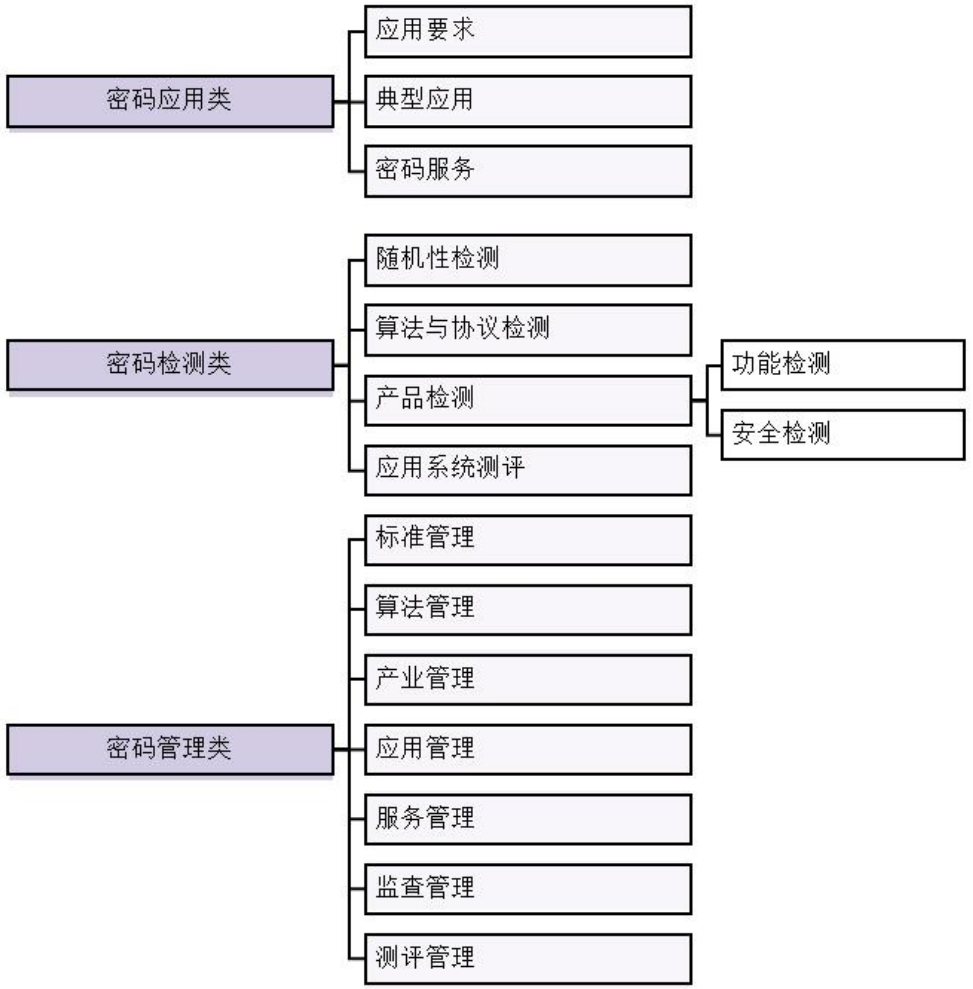
密码标准体系基本框架



2、商用密码技术标准

技术维上的进一步细分





2、商用密码技术标准

《GM/T 0054信息系统密码应用基本要求》（2018.3）

标准从信息系统的物理和环境安全、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提出了等级保护不同级别的密码技术应用要求，明确了等级保护不同级别的密钥管理和安全管理要求。

2、商用密码技术标准

密码应用总体要求

1、密码算法

信息系统中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;

2、密码技术

信息系统中使用的密码技术应遵循密码相关国家标准和行业标准;

3、密码产品

信息系统中使用的密码产品应通过国家密码管理主管部门核准;

4、密码服务

信息系统中使用的密码服务应通过国家密码管理主管部门许可。

2、商用密码技术标准

安全物理环境密码应用要点

安全物理环境主要实现对信息系统所在机房等重要区域的物理防护，密码应用要求涉及重要区域的物理访问控制，以及电子门禁系统进出记录和视频监控音像记录的存储完整性。

密码应用要点	一级	二级	三级	四级
身份鉴别	可	宜	应	应
电子门禁记录数据完整性	可	宜	应	应
视频记录数据完整性	-	-	应	应
密码模块实现	一级	一级及以上	二级及以上	三级及以上

密码安全产品：基于密码认证的电子门禁系统、视频安全系统、IC卡等

安全通信网络密码应用要点

- 安全通信网络主要实现对信息系统各实体进行网络通信时的安全防护，密码应用要求主要涉及通信过程中实体身份真实性、数据机密性和数据完整性。

密码应用要点	一级	二级	三级	四级
身份鉴别	可	宜	应	应
通信数据完整性	可	宜	应	应
通信数据机密性	可	宜	应	应
集中管理通道安全	可	宜	应	应
密码模块实现	一级	一级及以上	二级及以上	三级及以上

密码安全产品：身份认证网关、IPSec/SSL VPN、可信网络连接、终端密码模块（硬KEY、软KEY）等

安全区域边界密码应用要点

- 安全区域边界主要实现经由外部实体接入网络时的安全防护，密码应用要求主要涉及通信过程中实体身份真实性、网络边界访问控制和设备接入控制。

密码应用要求	一级	二级	三级	四级
身份鉴别	可	宜	应	应
访问控制信息完整性	可	宜	应	应
设备接入认证	可	宜	应	应
密码模块实现	一级	一级及以上	二级及以上	三级及以上

密码安全产品：身份认证网关、可信网络连接、终端密码模块（硬KEY、软KEY）等

2、商用密码技术标准

安全计算环境密码应用要点——设备与计算环境

实现对信息系统中各类设备和计算环境的安全防护，密码应用主要涉及对登录设备用户的身份鉴别、远程管理通道的建立、可信计算环境的建立、重要可执行程序来源的真实性，以及系统资源访问控制信息、设备的重要信息资源敏感安全标记、重要可执行程充完整性、日志记录的完整性。

密码应用要点	一级	二级	三级	四级
身份鉴别	可	宜	应	应
访问控制信息完整性	可	宜	应	应
敏感标记的完整性	可	宜	应	应
日志记录完整性	可	宜	应	应
远程管理身份鉴别信息机密性	可	宜	应	应
重要程序或文件完整性	可	宜	应	应
密码模块实现	一级	一级及以上	二级及以上	三级及以上

密码安全产品：身份认证系统、访问控制系统、远程安全管理系统
终端密码模块（硬KEY、软KEY）、可信计算系统等

2、商用密码技术标准

安全计算环境密码应用要点——应用与数据

主要实现对信息系统中应用及其数据的安全防护，密码应用主要涉及应用的用户身份鉴别、访问控制，以及应用相关重要数据的存储安全、传输安全和相关行为的不可否认性。

密码应用要点	一级	二级	三级	四级
身份鉴别	可	宜	应	应
访问控制	可	宜	应	应
数据传输安全	可	宜	应	应
数据存储安全	可	宜	应	应
日志记录完整性	可	宜	应	应
重要应用程序的加载和卸载	-	-	应	应
抗抵赖	-	-	-	应
密码模块实现	一级	一级及以上	二级及以上	三级及以上

密码安全产品：统一身份认证系统、访问控制系统、数据库/文件加密系统、签名验证服务器、应用程序签名系统、CA数字证书、终端密码模块（硬KEY、软KEY）等

2、商用密码技术标准

密钥管理要求

密钥管理应包括对密钥的生成、存储、使用、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程

要点	一级	二级	三级	四级
密钥生成	应	应	应	应
密钥存储	应	应	应	应
密钥使用	应	应	应	应
密钥分发	-	应	应	应
密钥导入与导出	-	应	应	应
密钥备份与恢复	-	应	应	应
密钥归档	-	-	应	应
密钥销毁	-	-	应	应

密码安全产品：CA证书认证系统、密钥管理系统、加密机、终端密码模块（硬KEY、软KEY）等

2、商用密码技术标准

安全管理要点

要点		一级	二级	三级	四级
安全管理制度	制定密码管理制度	可	宜	应	应
	定期修订密码管理制度	可	宜	应	应
	明确制度发布流程	-	宜	应	应
	制度执行过程记录留存	-	-	-	应
人员管理	了解并遵守密码相关法律法规	应	应	应	应
	正确使用密码相关产品	应	应	应	应
	建立岗位责任及人员培训制度	-	应	应	应
	建立关键岗位人员保密制度和调离制度	-	应	应	应
	设置密码管理和技术岗位并定期考核	-	-	应	应
	背景调查	-	-	-	应

2、商用密码技术标准

安全管理要点

要点		一级	二级	三级	四级
实施	规划，制定密码应用方案	可	宜	应	应
	建设，制定密码实施方案	可	宜	应	应
	运行，进行密码安全评估与整改	可	宜	应	应
应急	应急预案	-	应	应	应
	事件处置	可	应	应	应
	向有关主管部门上报处置情况	-	-	应	应

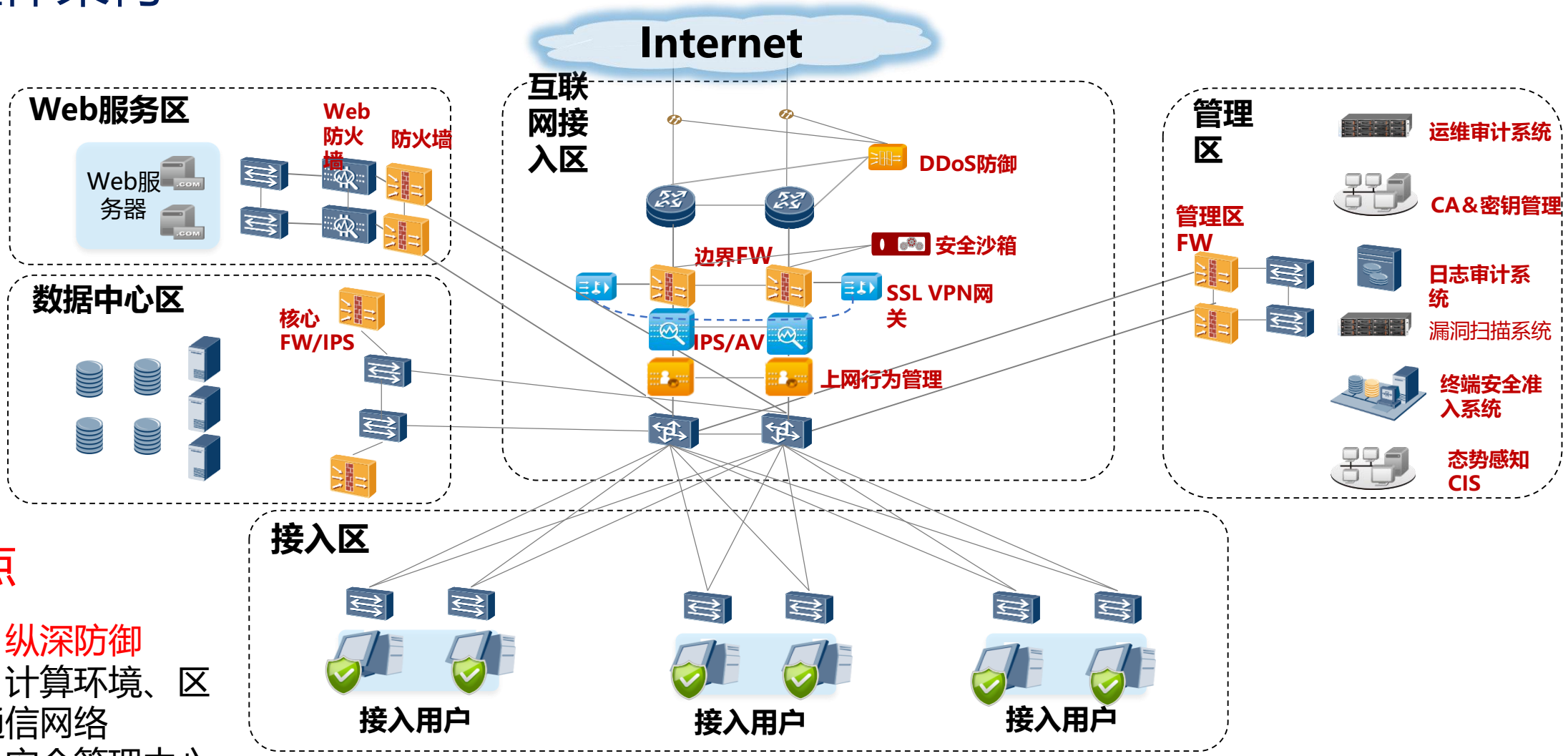
3、商用密码应用典型方案

密码应用方案设计原则

1. 三同步原则：同步规划，同步建设，同步运行（使用）
2. 总体性原则：遵循顶层设计，明确应用需求，通过总体方案和密码支撑体系总体架构设计，引导密码在系统中应用；
3. 科学性原则：总体方案要进行科学设计，应包括密码支撑体系架构、密码基础设施部署、密钥管理体系设计、密码设备部署及管理，及成体系、分层次的密码应用设计；
4. 完备性原则：按照物理环境安全、通信网络安全、网络边界安全、计算环境安全、应用数据安全及密钥管理和安全管理；
5. 可行性原则：首先保证系统业务正常运行，兼顾系统复杂性或兼容性，通过评审的密码应用方案可采取分步实施、稳步推进的策略。

3、商用密码应用典型方案

网络整体架构



设计要点

分区分域、纵深防御

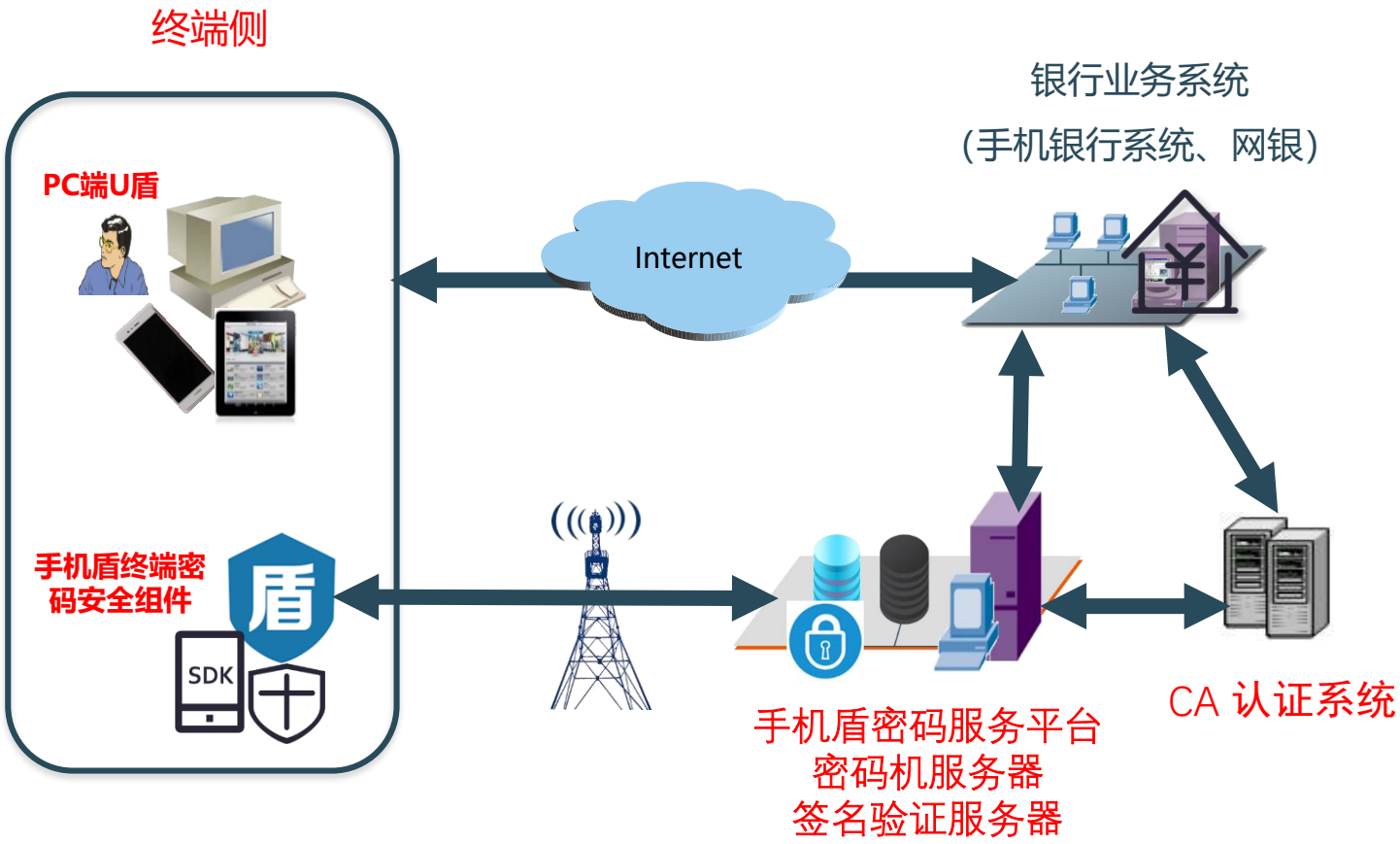
三重防护：计算环境、区域边界、通信网络

一个中心：安全管理中心

3、商用密码应用典型方案

手机银行、网上银行密码应用安全方案

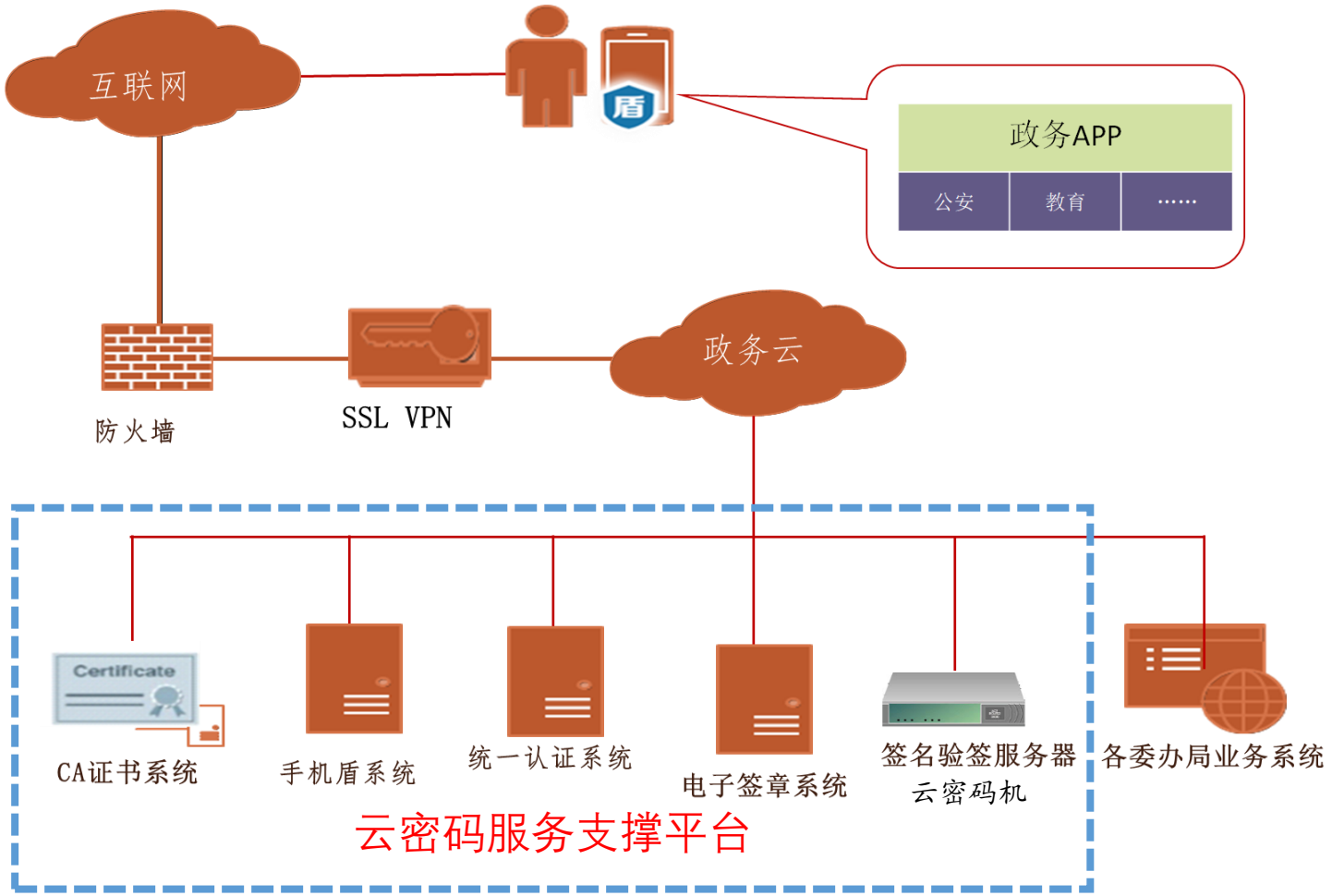
以PKI/CA、数字证书、数字签名等技术为基础，采用手机盾安全系统，建立“人-设备-应用”三位一体的安全认证体系，为交易支付、线上开户、在线签约、金融数据共享等金融创新业务提供安全支撑。



3、商用密码应用典型方案

云密码服务支撑平台

- 采用密码机、云密码机建立统一密码硬件支持平台；
- PC端采用U盾、手机端采用手机盾实现终端密码可靠支撑能力；
- 采用VPN等设备提供传输链路加密，保障数据传输安全；
- 建立统一CA数字证书系统、密钥管理系统、手机盾密码系统、电子签章、签名验签服务器、统一认证等实现云上业务应用系统的身份认证、数据加密、抗抵赖、完整性保护等。




2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音