



浅析密码应用及其应用安全性评估

讲师姓名：傅 罡



- 傅 罡
- 中国疾病预防控制中心网络和信息安全管理处处长
- 全国公共安全基础标准化技术委员会（SAC/TC351）应急管理标准工作组（WG3）委员；
- 中国卫生信息与卫生医疗大数据学会慢病防治与管理专业委员会副主委
- 中国卫生信息与卫生医疗大数据学会公共卫生信息专业委员会常委；
- 原卫生部网络信息安全专家组成员；
- 《中国卫生信息管理杂志》编委

- 密码与密码应用
- 密码评估的政策依据
- 密码应用安全性评估
- 讨论与展望



密码的概念与分类

- 《密码法》所称密码：采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。
- 《密码法》将密码分为**核心密码**、**普通密码**和**商用密码**，实行分类管理。
 - ◆ 核心密码用于保护国家绝密级、机密级、秘密级信息
 - ◆ 普通密码用于保护国家机密级、秘密级信息
 - ◆ **商用密码**用于保护不属于国家秘密的信息

2010年12月

国家密码管理局发布
《SM2椭圆曲线公钥密码算法》

2012年

成立“金融领域商用密码应用推进工作协调小组”

2012年

发布SM3算法标准

2015年

发布《电子签名法》

2017年4月

国家密码管理局就《密码法（草案征求意见稿）》公开征求意见

2019年

《密码法》草案提交

2010年12月

国家密码管理局发布
《SM3密码杂凑算法》

2012年3月

发布SM4算法标准

2014年

关于银行业的商用密码推广试点工作

2016年3月

国家密码管理局发布《SM9密码标识算法》等2项密码行业标准公告

2018年

《政务信息系统政府采购管理暂行办法》

密码在网络空间安全中的重要作用

- 口令 (password) 不是密码 (crypto/cryptography)
- 密码是保障网络安全的核心技术和基础支撑
 - ◆ 加密保护：将“明文”变换成“密文”，再进行传输和存储。
 - ◆ 安全认证：确认信息、身份、行为是否真实。
- 密码具有四项主要功能
 - ◆ 信息的机密性/保密性：加密
 - ◆ 信息的完整性：鉴别码
 - ◆ 消息来源 / 身份的真实性：鉴别
 - ◆ 行为的不可否认性：签名



密码在网络空间安全中的重要作用

■ “技术国界化”

- ◆ 以MD5、RSA等为代表的公钥密码存在安全风险

- ◆ 中美贸易战启示：

 - ✓ 核心技术只能“自力更生”

 - ✓ 基础信息网络、重要信息系统的核心技术及安全性保障需自己掌握。

■ 使用密码可以有效、可靠、经济的维护网络空间安全

- ◆ 密码是保障网络与信息安全的**核心技术和基础支撑**

- ◆ 密码作为保护网络与信息安全的重要手段，在身份识别、安全隔离、信息加密、完整性保护和抗抵赖性等方面发挥着**不可替代的重要作用**

- ◆ 以密码为基石构建安全网络空间

■ 密码应用不广泛

- ◆ 2018年，对1万余个等保三级及以上的信息系统进行普查，未使用密码的信息系统占比高达75.23%

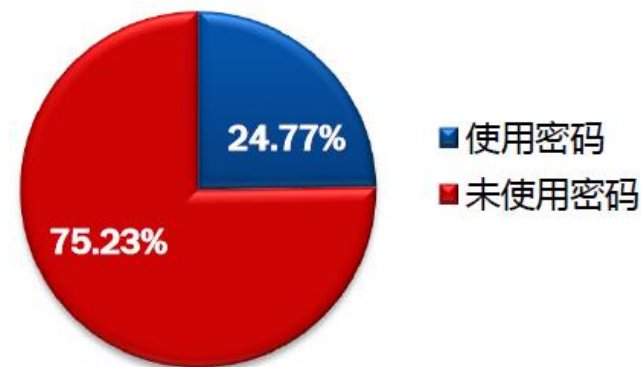
■ 密码应用不规范

- ◆ 2018年，对118个重要系统（精选的大部分都使用了密码）的密码安全性测评结果显示，85%不符合标准要求

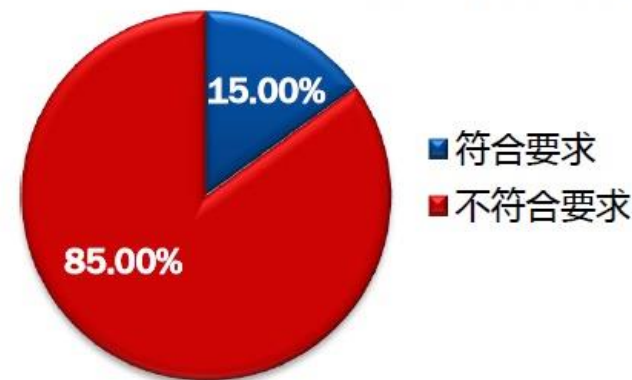
■ 密码应用不安全

- ◆ 测评结果表明：MD5、RSA1024、SHA1等有重大安全风险的算法仍在大量使用
- ◆ 密码实现生成的密钥可预测.....

等保三级及以上信息系统



重要系统（大部分使用密码）



密评的法律依据
(要用密码、要做密码
安全性评估)

- 《中华人民共和国密码法》
- 《中华人民共和国网络安全法》
- 《商用密码应用安全性评估管理办法（试行）》（2017内部印发）
- 《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）
- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960号）
- 《商用密码管理条例（征求意见稿）》
- 《网络安全等级保护条例（征求意见稿）》
- 《关键信息基础设施安全保护条例（征求意见稿）》
- 《国密局关于加强政务密评的函》（国密局函119号）
- 《政务信息系统密码应用与安全性评估工作指南》
- 《国家政务信息化项目建设管理办法（国办发〔2019〕57号）》
-

密评的行政法规

(政务信息系统落实密码应用的“三同步一评估”)

密评与等保的衔接

(所有三级以上系统和关键基础设施落实密码应用的“三同步一评估”)

“三同步一评估”——同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估

密码法及配套法规

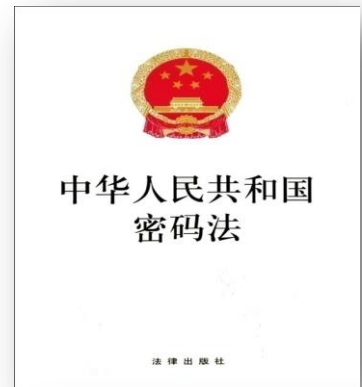
■ 《密码法》第二十七条

法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托**商用密码检测机构开展商用密码应用安全性评估**。

■ 《商用密码应用安全性评估管理办法（试行）》

第三条：涉及国家安全和公共利益的重要领域网络和信息系统的建设、使用、管理单位（以下简称责任单位）应当健全密码保障体系，**实施商用密码应用安全性评估**。

第二十条：重要领域网络和信息系统的建设、使用、管理单位（以下简称责任单位）应当健全密码保障体系，实施商用密码应用安全性评估。重要领域网络和信息系统的建设、使用、管理单位包括：基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、**网络安全等级保护第三级及以上信息系统（等保三级对应密评三级）**。



国家政务信息化项目建设管理办法

■ 《国家政务信息化项目建设管理办法（国办发〔2019〕57号）》

第九条：国家政务信息化项目，应当按规定履行审批程序并向国家发展改革委备案。备案文件应当包括项目名称、等级保护或者分级保护备案情况、**密码应用方案和密码应用安全性评估报告等内容**，其中改建、扩建项目还需提交前期项目第三方后评价报告。

第十五条：项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，**同步规划、同步建设、同步运行密码保障系统**并定进行评估。

第二十五条：国家政务信息化项目建成后半年内，项目建设单位应当按照国家有关规定申请审批部门组织验收，提交验收申请报告时应当一并附上项目建设总结、财务报告、审计报告、安全风险评估报告、**密码应用安全性评估报告等材料**。

国务院办公厅关于印发国家政务信息化 项目建设管理办法的通知

国办发〔2019〕57号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：
《国家政务信息化项目建设管理办法》已经国务院同意，现印发给你们，请认真贯彻执行。

国务院办公厅

2019年12月30日

（此件公开发布）

国家政务信息化项目建设管理办法

第一章 总 则

第一条 为规范国家政务信息化建设管理，推动政务信息系统跨部门跨层级互联互通、信息共享和业务协同，强化政务信息系统应用绩效考核，根据《国务院办公厅关于印发政务信息资源共享管理暂行办法的通知》（国发〔2016〕51号）等有关规定，制定本办法。

第二条 本办法适用的国家政务信息系统主要包括：国务院有关部门和单位负责实施的国家统一电子政务网络平台、国家重点业务信息系统、国家信息资源库、国家信息安全基础设施、国家电子政务基础设施（数据中心、机房等）、国家电子政务标准化体系以及相关支撑体系等符合《政务信息系统定义和范围》规定的系统。

公安部指导意见

■ 公网安 [2020] 1960号文

二、深入贯彻实施国家网络安全等级保护制度

(六) 落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

中华人民共和国公安部

公网安〔2020〕1960号

关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函

中央和国家机关各部委，国务院各直属机构，办事机构，事业单位，各中央企业：

为深入贯彻党中央有关文件精神 and 《网络安全法》，指导重点行业、部门全面落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，配合公安机关加强网络安全监管，严厉打击危害网络安全的违法犯罪活动，切实保障关键信息基础设施、重要网络和数据安全，公安部研究制定了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，现印送给你们，请结合本行业、本部门工作实际，认真参照执行。



不做密评或测评结果不合格的影响？

- 《密码法》第三十七条第一款规定：关键信息基础设施的运营者违反本法第二十七条第一款规定，**未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正**，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。
- 《国家政务信息化项目建设管理办法》第二十八条第三款规定：对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，**不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。**
- 《商用密码应用安全性评估管理办法（试行）》第二章第十条规定：**关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次。**

从三级等保分析密码应用的要点

等保目录编号	要求项	细则	对应产品
8.1.2.2	通信传输	<ul style="list-style-type: none">■ 应采用校验技术或密码技术保证通信过程中数据的完整性;■ 应采用密码技术保证通信过程中数据的保密性。	<ul style="list-style-type: none">■ IPSec/SSL VPN网关■ 安全认证网关
8.1.4.1	身份鉴别	<ul style="list-style-type: none">■ 应对登录的用户进行身份标识和鉴别, 身份标识具有唯一性, 身份鉴别信息具有复杂度要求并定期更换;■ 应具有登录失败处理功能, 应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;■ 当进行远程管理时, 应采取必要措施防止鉴别信息在网络传输过程中被窃听;■ 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别, 且其中一种鉴别技术至少应使用密码技术来实现。	<ul style="list-style-type: none">■ 个人数字证书+USBKey■ 安全认证网关■ IPsec/SSL VPN网关
8.1.4.7	数据完整性	<ul style="list-style-type: none">■ 应采用校验技术或密码技术保证重要数据在传输过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等;■ 应采用校验技术或密码技术保证重要数据在存储过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	<ul style="list-style-type: none">■ 安全认证网关■ IPsec/SSL VPN网关■ 签名验签服务器

从三级等保分析密码应用的要点

CHINCA

2021
CHINCA
China Hospital
Information
Network
Consensus

信息安全技术网络安全等级保护基本要求

等保目录编号	要求项	细则	对应产品
8.1.4.8	数据保密性	<ul style="list-style-type: none">■ 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；■ 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	<ul style="list-style-type: none">■ 安全认证网关■ IPsec/SSL VPN网关■ 服务器密码机
8.1.9.3	产品采购和使用	<ul style="list-style-type: none">■ 应确保网络安全产品采购和使用符合国家的有关规定；■ 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；■ 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	<ul style="list-style-type: none">■ 具备商用密码产品型号证书
8.1.9.7	测试验收	<ul style="list-style-type: none">■ 应制定测试验收方案，并依据测试验收方案测试验收，形成测试验收报告；■ 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。	<ul style="list-style-type: none">■ 密评相关内容
8.1.10.9	密码管理	<ul style="list-style-type: none">■ 应遵循密码相关国家标准和行业标准；■ 应使用国家密码管理主管部门认证核准的密码技术和产品。	<ul style="list-style-type: none">■ 具备商用密码产品型号证书

■ 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》

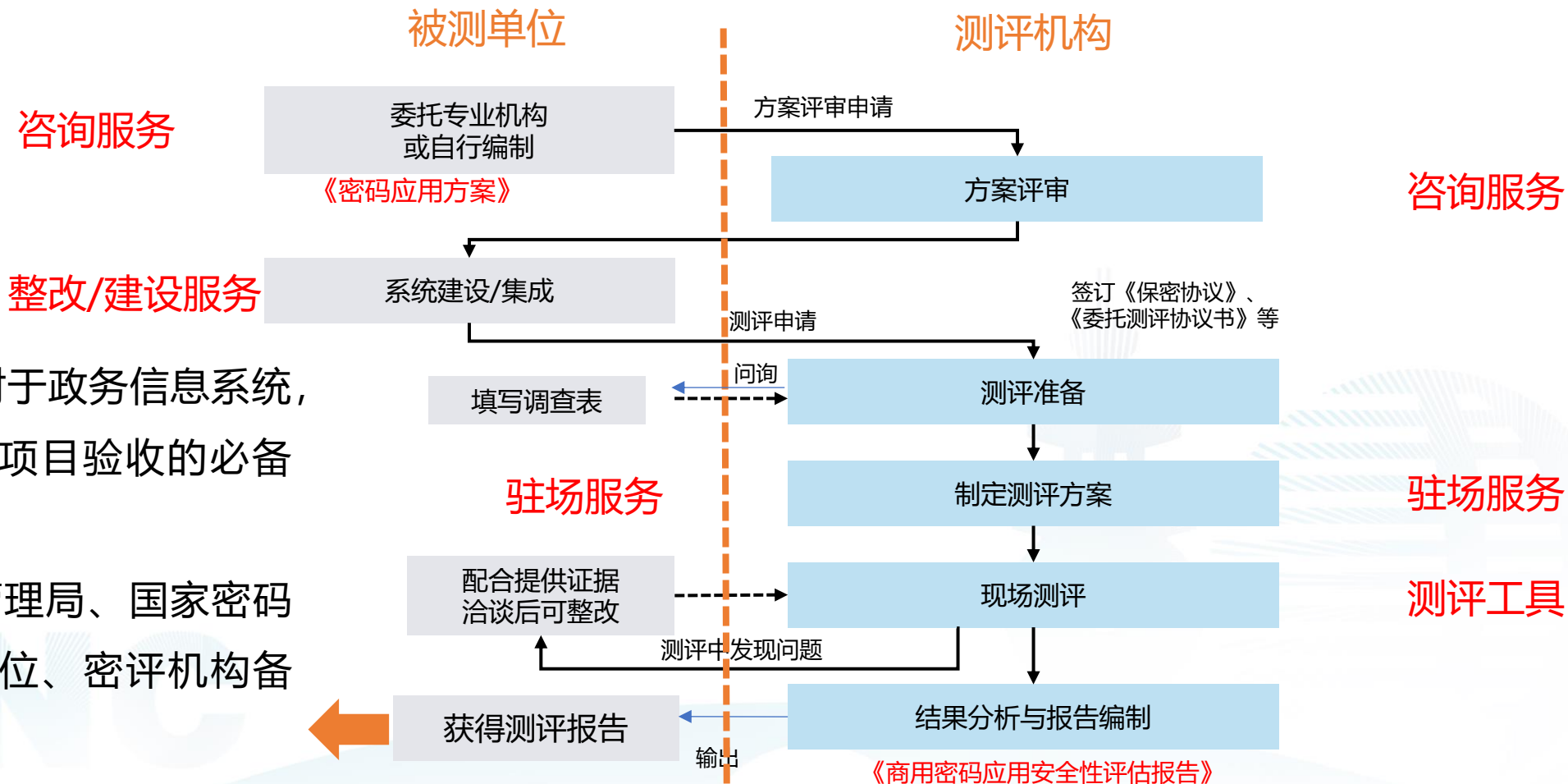
■ 现阶段实际执行测评时的5项配套指导文件：

1. 信息系统密码应用测评要求
2. 信息系统密码应用测评过程指南
3. 信息系统密码应用高风险判定指引
4. 商用密码应用安全性评估量化评估规则
5. 商用密码应用安全性评估报告模板（2020版）

- 39786是贯彻落实《密码法》、指导我国商用密码应用与安全性评估工作开展的纲领性标准。
- 具体规定4个技术层面和4个管理层面要求的标准，在原有0054密标基础上，结合前期密评试点经验进行改进修订后形成的国标。

- 国标规定的各指标的测评对象、测评实施方式和结果判定方法。
- 明确了测评过程的具体环节和各环节输入、输出
- 定义了最终报告中的高风险项判定方法及相应的缓解措施。
- 定义了最终报告中的量化评分方法。
- 2020版的测评报告的模板。

商用密码应用安全性评估(密码测评)流程



- 国办57号文件对于政务信息系统,规定密评报告是项目验收的必备材料之一。
- 提交地方密码管理局、国家密码管理局、委托单位、密评机构备案。

与等级保护测评的关联

- 密评的测评范围和定级以等级保护的定级备案为准
- 指标项设置（技术+管理）和结论（评分过线+高风险项一票否决）相似
- 密评与等保均需要定期开展（每年一次）
- 许多密评机构同时等级保护测评资质
 - ◆ 2020年7月，公布第一批密评试点机构（24）
 - ◆ 2020年9月，公布第二批密评试点机构（36+9）



密评的指标项数量不多，但**测评深度要求更高**

- 测评的关键是看密钥是否安全
- 测评时常常需要考察系统的设计和实现细节（**接近白盒测试**），而不是仅仅做黑盒测试

密评指标项解读

- 两大类（技术、管理），共分8个层面，“应”、“宜”、“可”三种
- 以三级系统为例，共41个指标项（以及一个隐含的重要指标：**密钥的管理**）
- 指标项权重

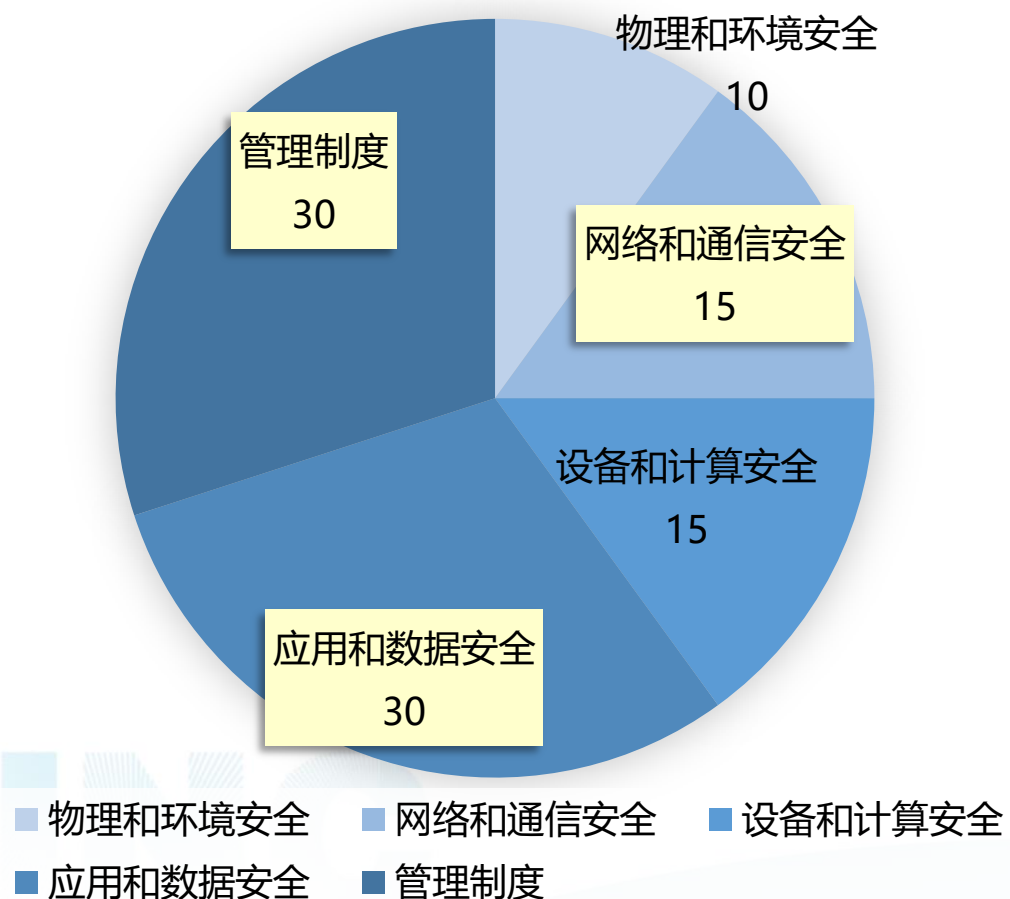
技术类指标	物理和环境安全
	网络和通信安全
	设备和计算安全
	应用和数据安全
管理类指标	管理制度
	人员管理
	建设运行
	应急处置



指标项的“不适用”判定方法

- “可”的指标，用户方可以自行论述不适用理由
- “宜”的指标，需要测评机构分析判断，并在**测评报告中阐述不适用的理由**（密码应用方案 + 专家评审意见是比较有说服力的证据）
- “应”需要遵循

密评量化分值分布



根据当前的经验，在设计密码应用方案时，可以优先考虑、重点关注：

- 网络和通信安全
- 应用和数据安全
- 管理制度

信息系统密码应用高风险项



算法

- 国密算法。
- ✓ 存在安全问题或安全强度不足的密码算法，**高风险**。如 MD5、DES、SHA-1、RSA-1024



技术

- 密码技术应遵循密码相关标准
- ✓ 存在缺陷或有安全问题警示的密码技术，**高风险**。如SSH 1.0、SSL 2.0、SSL 3.0、TLS 1.0



产品

- 合规的商用密码产品
- 0028 / 37092 密码模块安全等级
- 存在高危安全漏洞的密码产品，**高风险**。如存在 Heartbleed漏洞的OpenSSL 产品



服务

- 密码服务应通过国家密码主管部门许可
- 存在高危安全漏洞的密码产品
- ✓ 选用的密码服务提供商不具有相关资质（如电子认证服务）

- **密钥管理**：除公钥外，明文保存为**高风险项**

密评结论判定依据

- 量化评估结果
(100分制)

得分满分

得分达到阈值

得分未达到阈值

并且

并且

或者

- 逐项风险分析
(高、中、低)

没有任何风险项

没有高风险项

存在高风险项

=

=

=

- 测评结论

符合

基本符合

不符合

- 现阶段阈值 = 60分 (不排除未来阈值提高的可能性)

密评方案物理和环境安全层要求与分析

层面	指标要求	第三级
物理和环境安全 (10 分)	身份鉴别	宜
	电子门禁记录数据存储完整性	宜
	视频监控记录数据存储完整性	宜

对应产品：

- ✓ 国密算法门禁系统
- ✓ 国密算法视频监控

- 机房进出人员门禁系统，身份鉴别。
- 机房门禁业务系统的日志数据宜采用密码技术保护，则符合电子门禁记录数据存储完整性。（不能使用ID门禁卡，已经被破解IC卡（如M1卡））
- 机房采集设备的视频数据需要密码技术保护，则视频监控记录数据存储完整性。

密评方案物理和环境安全层要求与分析

层面	层面权重	指标项	影响因子	指标项要求	高风险缓解方法
物理和环境	10	身份鉴别	1	宜	生物特征、专人值守+视频监控
		门禁记录完整性	0.7	宜	
		视频记录完整性	0.7	宜	



“物理和环境”层面的身份鉴别，是指机房门禁的身份鉴别机制，是否采用了密码技术

密评方案网络和通信的要求与分析

层面	指标要求	第三级
网络和 通信安全 (15 分)	身份鉴别	应
	通信数据完整性	宜
	通信过程中重要数据机密性	应
	网络边界访问控制信息的完整性	宜
	安全接入认证	可

对应产品：

- ✓ IPSec/SSL VPN网关
- ✓ 安全认证网关

- 外部用户访问系统平台时，需要身份鉴别，保障网络和数据传输链路的安全性。
- 外部用户访问系统时，采用密码技术保证通信数据及通信过程中重要数据的机密性。
- 具备访问控制功能的设备实体采用密码技术对网络边界和系统资源访问控制信息进行保护，防止被非法篡改。
- 设备接入网络时，需要安全接入认证。

密评方案网络和通信的要求与分析

层面	层面权重	指标项	影响因子	指标项要求	高风险缓解方法
网络和通信	15	身份鉴别	1	应	无
		通信数据完整性	0.7	宜	
		通信数据机密性	1	应	应用层面传输安全
		边界访问控制完整性	0.7	宜	
		安全接入认证	0.4	可	



“网络通信”层面的身份鉴别，是指对通信设备的鉴别，三级系统只要求单向（对服务器端的鉴别）

密评方案设备和计算要求与分析

层面	指标要求	第三级
设备和 计算 (15 分)	身份鉴别	应
	远程管理通道安全	应
	系统资源访问控制信息完整性	宜
	重要信息资源安全标记完整性	宜
	日志记录完整性	宜
	重要可执行程序完整性、来源真实性	宜

对应产品：

- ✓ 安全认证网关
- ✓ 堡垒机

- 在密码设备（含签名验签服务等）、非密码设备（应用服务器、堡垒机等）要求管理员登录设备进行身份鉴别。
- 远程管理的身份鉴别信息需使用合规的密码技术进行通道安全（如SSH的安全登录）。
- 采用密码技术对操作系统层面资源访问控制信息（如设备配置信息、安全策略、资源访问控制列表等）进行保护，防止被非法篡改。
- 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。
- 系统的应用服务器、数据库服务器等设备的操作日志均使用密码技术进行完整性保护。

密评方案设备和计算要求与分析

层面	层面权重	指标项	影响因子	指标项要求	高风险缓解方法
设备和计算	15	身份鉴别	1	应	短信验证、生物特征等
		远程管理通道	1	应	隔离的管理网、网络层面安全措施
		访问控制完整性	0.7	宜	
		安全标记完整性	0.7	宜	
		日志记录完整性	0.7	宜	
		程序来源真实性	0.7	宜	



“设备计算”层面的身份鉴别，是指对登录到设备（操作系统）的人的鉴别（通常是运维人员，**堡垒机**）

密评方案应用和数据要求与分析

层面	指标要求	第三级
应用和 数据 (30 分)	身份鉴别	应
	访问控制完整性	宜
	重要信息资源安全标记完整性	宜
	重要数据传输机密性	应
	重要数据存储机密性	应
	重要数据传输完整性	宜
	重要数据存储完整性	宜
	不可否认性	宜

对应产品：

- ✓ IPsec/SSL VPN网关
- ✓ 安全认证网关
- ✓ 签名验签服务器
- ✓ 服务器密码机

- 业务系统应用人员或操作人员访问应用时的身份鉴别鉴别。
- 对应用服务器的业务管理控制台访问控制信息的命令使用密码技术进行完整性保护。
- 对业务日志等重要信息资源安全标记进行完整性保护。
- 对业务重要数据使用密码技术进行传输机密性、完整性。
- 对业务重要数据（上报关键数据清单中的）使用密码技术进行存储机密性、完整性。
- 对应用数据使用密码技术进行不可否认性，由业务系统使用签名技术保障应用数据的不可否认性。

密评方案应用和数据要求与分析

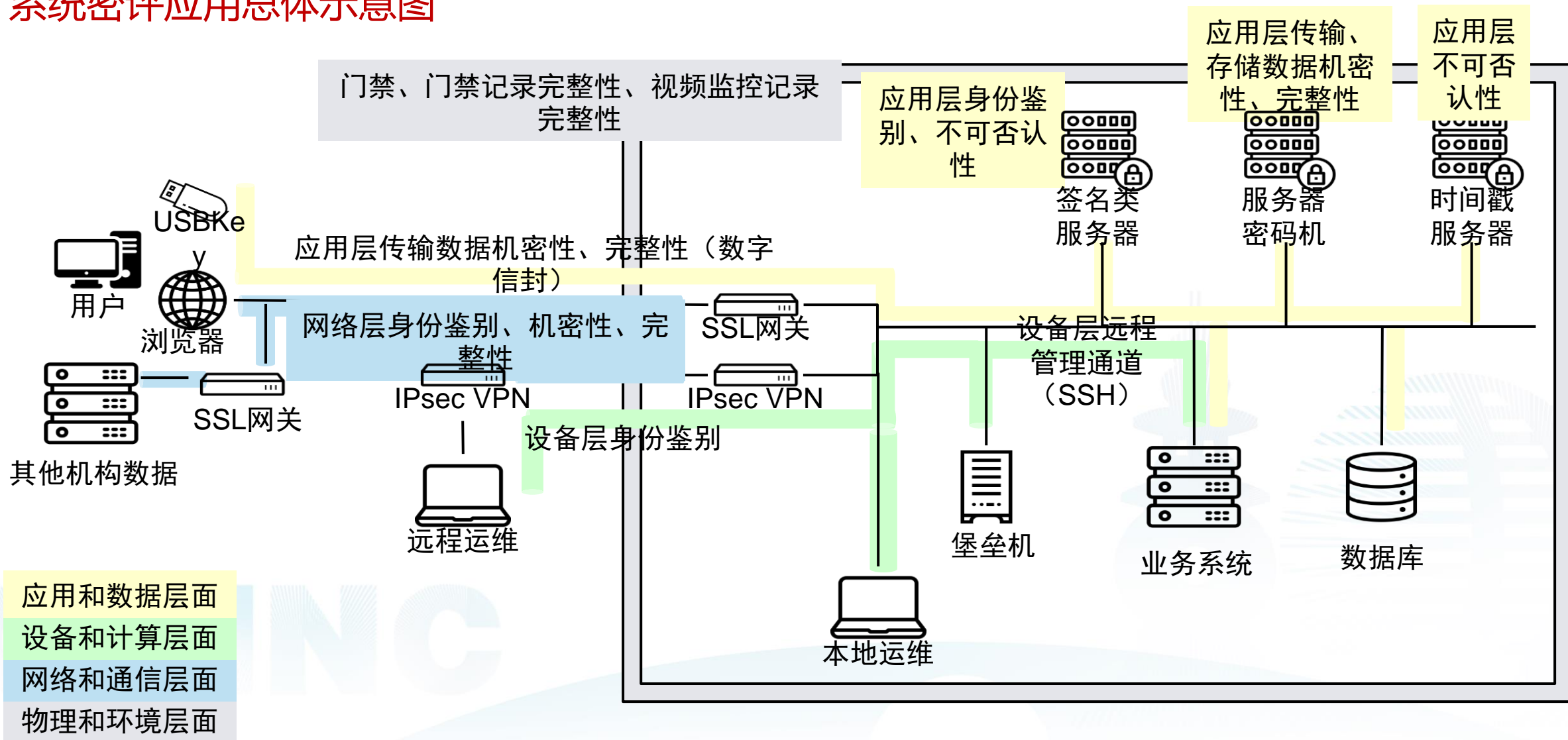
层面	层面权重	指标项	影响因子	指标项要求	高风险缓解方法
应用和数据	30	身份鉴别	1	应	短信验证、生物特征等
		访问控制完整性	0.7	宜	
		安全标记完整性	0.7	宜	
		数据传输机密性	1	应	网络层面传输安全
		数据存储机密性	1	应	无
		数据传输完整性	1	宜	
		数据存储完整性	1	宜	授权访问+定期备份
		不可否认性	1	宜	无

各层面高风险项分布情况

安全层面 高风险指标	物理环境	网络和通信	设备和计算	应用和数据	密码应用管理
通用（算法技术产品服务）	✓	✓	✓	✓	\
身份鉴别	✓	✓	✓	✓	\
重要数据传输机密性		✓		✓	\
重要数据存储机密性				✓	\
重要数据存储完整性				✓	\
远程管理通道安全	\		✓（三级）	\	\
不可否认性	\	\	\	✓（三级）	\
安全接入认证	\	✓(四级)	\	\	\
具备密码应用安全管理制度	\	\	\	\	✓
制定密码应用方案	\	\	\	\	✓

- “✓”为二级及以上高风险项，且有缓解措施，“✓”为无缓解措施的高风险项，“\”为不适用指标。
- 关于高风险的项的缓解措施，即使有缓解措施，也不影响量化打分时分值的判定，只能在打分结束后，影响最终的评估结果的判定（符合、基本符合、不符合）。

系统密评应用总体示意图



密评方案安全管理

- 从管理要求的4个管理方面（管理制度、人员管理、建设运行、应急处置），按要求设计安全管理体系。
- 在安全管理方面，需要基本的信息安全管理体系，建立相应的安全组织，设置相应的安全部门和岗位，制订安全管理制度，并在日常管理中依照制度要求执行。
- 信息系统日常运行维护，如外来人员访问管理、系统安全管理和网络安全管理等方面，拥有较完善的流程和规范。安全管理方面要求具有基本安全保障能力。

指标体系		
管理要求	管理制度	具备密码应用安全管理制度
		密钥管理规则
		建立操作规程
		定期修订安全管理制度
		明确管理制度发布流程
		制度执行过程记录留存
	人员管理	了解并遵守密码相关法律法规和密码管理制度
		建立密码应用岗位责任制度
		建立上岗人员培训制度
		定期进行安全岗位人员考核
	建设运行	建立关键岗位人员保密制度和调离制度
		制定密码应用方案
		制定密钥安全管理策略
		制定实施方案
		投入运行前进行密码应用安全性评估
		定期开展密码应用安全性评估及攻防对抗演习
	应急处置	应急预案
		事件处置
		向有关主管部门上报处置情况

密评方案实施指南相关产品







序号	产品名称	功能
1	安全认证网关	实现通信数据完整性，通信数据机密性，通信身份鉴别，远程管理身份鉴别信息机密性
2	IPSec / SSL VPN综合安全网关	具有IPSec、SSL VPN的综合安全网关。
3	签名验签服务器	数字签名验签，实现数据完整性等功能。
4	服务器密码机	利用HMAC算法实现数据完整性等功能。
5	可信单证管理系统	电子单据的可信，支持以接口形式调用系统的数据或excel文件。
6	电子签章服务器	实现在版式文件上盖章。
7	堡垒机	统一设备访问及监控管理。
8	门禁系统	支持国密IC卡进入机房的整套硬件与软件系统
9	视频监控系统	使用国密算法进行视频加密存储
10	时间戳服务器	对数据加时间戳，实现不可否认性
11	隐私保护服务器	对重要数据存储加密（需向产品部提定制）
12	国密浏览器	客户端浏览器软件，建立基于国密算法的安全通道
13	数据库加密系统	实现不改动原有系统的情况下，对数据库数据加密。
14

数据是核心

数据信息安全**管理角度**的防泄露整体策略:

识别开	管理全	防护住	监测出	追踪到
能够对数据分级分类管理	不同数据采用不同管理措施	分层部署多维度安全策略	深度监测发现异常阻断	能够追查溯源数据泄露
				

数据信息安全**技术角度**的防泄露整体策略:

进不来	找不到	拿不走	解不开	看不懂	用不了
做好边界安全防护	做好访问控制与隐藏	做好监控告警与阻断	做好数据加密存储	做好数据模糊化处理	做好数字水印
					

借助密码应用，提升卫健行业的网络安全核心技术与基础保障

- 基础设施、外包管理问题（建设与运维）
- 数据治理与共享（数据真的在我们手里吗？）
- 网络安全的对抗能力（人员能力、安全人员欠缺）
- 互联网+、云租赁
-
- ✓ 法律、法规的要求
- ✓ 合规、正确、有效地使用



谢谢观看！

讲师姓名：傅 罡