等级测评与密码应用安全性评估

深圳市网安计算机安全检测技术有限公司
2018年11月23日

目 录

密评基本概念—名词解释

密码应用从涉及到**国家安全**的保密通信、军事指挥，到涉及**国民经济**的金融交易、防伪税控，再到涉及**公民权益**的电子支付、社会保障，密码都发挥着十分关键的基础性作用

商用密码应用安全性评估（以下简称“密评”）是指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的**合规性、正确性、有效性**进行评估

商用密码定位于“对**不涉及国家秘密内容**的信息进行加密保护或者安全认证”所使用的密码技术和密码产品

密评基本概念—名词解释

合规性

口密码算法、密码协议、密钥管理、密码产品和服务使用合规

- 即按照《商用密码管理条例》等密码法规和行业相关的密码使用要求，使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局审批的密码产品或服务
- 按照《信息系统密码应用基本要求》等标准，进行相应的密码应用建设方案设计

密评基本概念—名词解释

正确性

口密码算法、密码协议、密钥管理、密码产品和服务使用正确

- 系统中采用的标准密码算法、协议和密钥管理机制按照相应的密码国家和行业标准进行正确的设计和实现
- 自定义密码协议、密钥管理机制的设计和实现正确，符合相关标准要求
- 密码保障体系建设或改造过程中密码产品和服务的部署和应用正确

密评基本概念—名词解释

有效性

口是指密码应用安全立足系统安全、体系安全、动态安全，信息系统中采用的密码协议、密钥管理系统、密码应用子系统和密码防护机制不仅设计合理，而且在系统运行过程中**能够发挥密码效用**，保障信息的机密性、完整性、真实性、抗抵赖性

密评基本概念—密码定义

凡是有

- 机密性 → 防泄密
- 完整性 → 防篡改
- 真实性 → 防假冒
- 不可否认性 → 防抵赖

需求的，都可以用密码技术解决

密评基本概念—密码定义

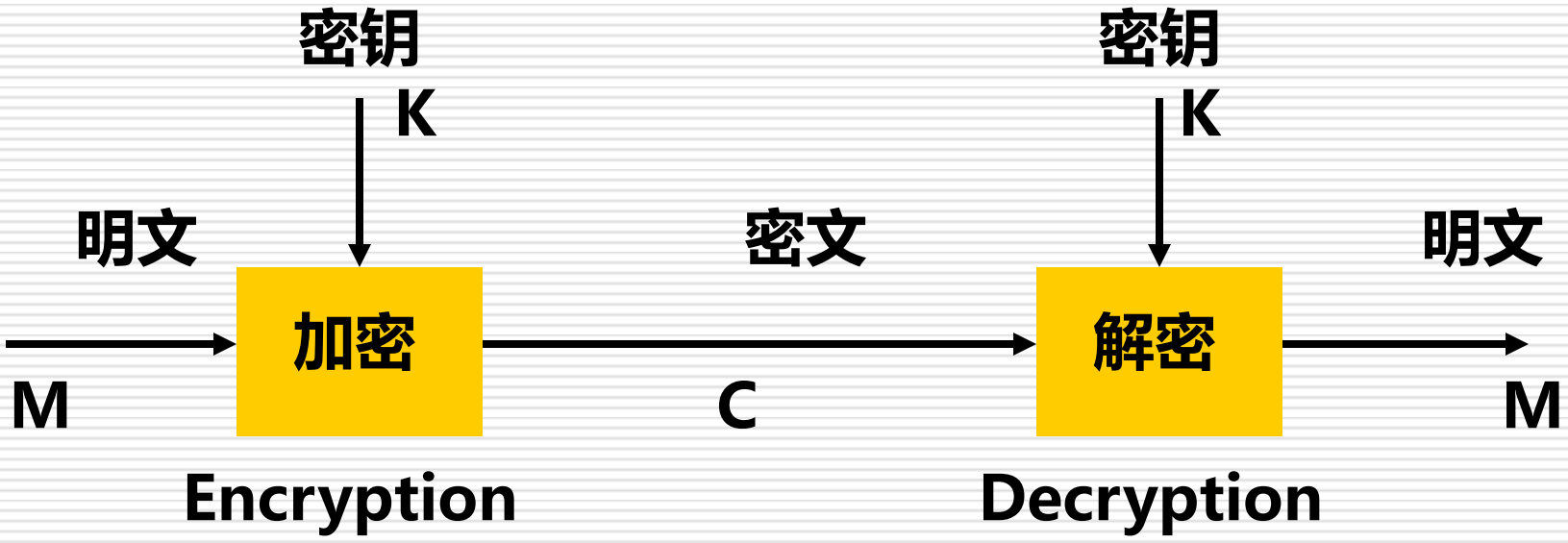
- 密码是按照约定的法则对信息实施明密变换的技术手段
- 加密就是按照约定的法则将被保护的信息-明文变换成他人不可辨识的符号-密文的过程
- 解密就是按照约定的法则将密文变换成明文的过程

常见误区：口令=密码?

密评基本概念—密码定义

- **密码**是密码算法、密钥管理和密码协议的总和
- **密码算法**是指实现明密变换的数学模型、逻辑结构、变化函数，是密码中相对固定的部分
- **密钥**是参与、控制密码算法实现明密变换的可变参数，是密码中最活跃的部分
- **密码协议**是指为完成特定任务而应用密码所必需遵循的操作步骤，是密码中最稳定的部分
  - 最基本的密码协议是**密钥交换协议**和**身份鉴别协议**

密评基本概念—加解密示意



$$E_K(M) = C$$

$$D_K(C) = M$$

密评基本概念—密码算法

口 对称密码算法

- 序列密码算法
- 分组密码算法
- ZUC、SM1、SM4、SM7

加密和解密使用相同的密钥

密钥必须保密

口 非对称密码算法

- 基于大数分解的RSA
- 基于离散对数求解的ECC
- SM2、SM9

加密和解密使用不同的密钥

有一个密钥可以公开

口 杂凑算法

- 将任意长度的数据计算为固定长度的散列值
- SM3

密评基本概念—密钥

□ Kerckhoffs原则

- 秘密必须全寓于密钥之中，即使密码分析员已经掌握了密码算法及其实现的全部详细资料，也无助于用来推导出明文或密钥

□ 算法破解的计算复杂度和存储复杂度足够大，使敌手无法实际破解

目 录

密评技术要求—相关标准

- 密码行业相关标准
- 《信息系统密码应用基本要求》(GM/T 0054-2018)
- 《信息系统密码测评要求》
- 《计算机信息安全保护等级划分准则》(GB17859-1999)

ICS 35.040
L 80
备案号:

GM

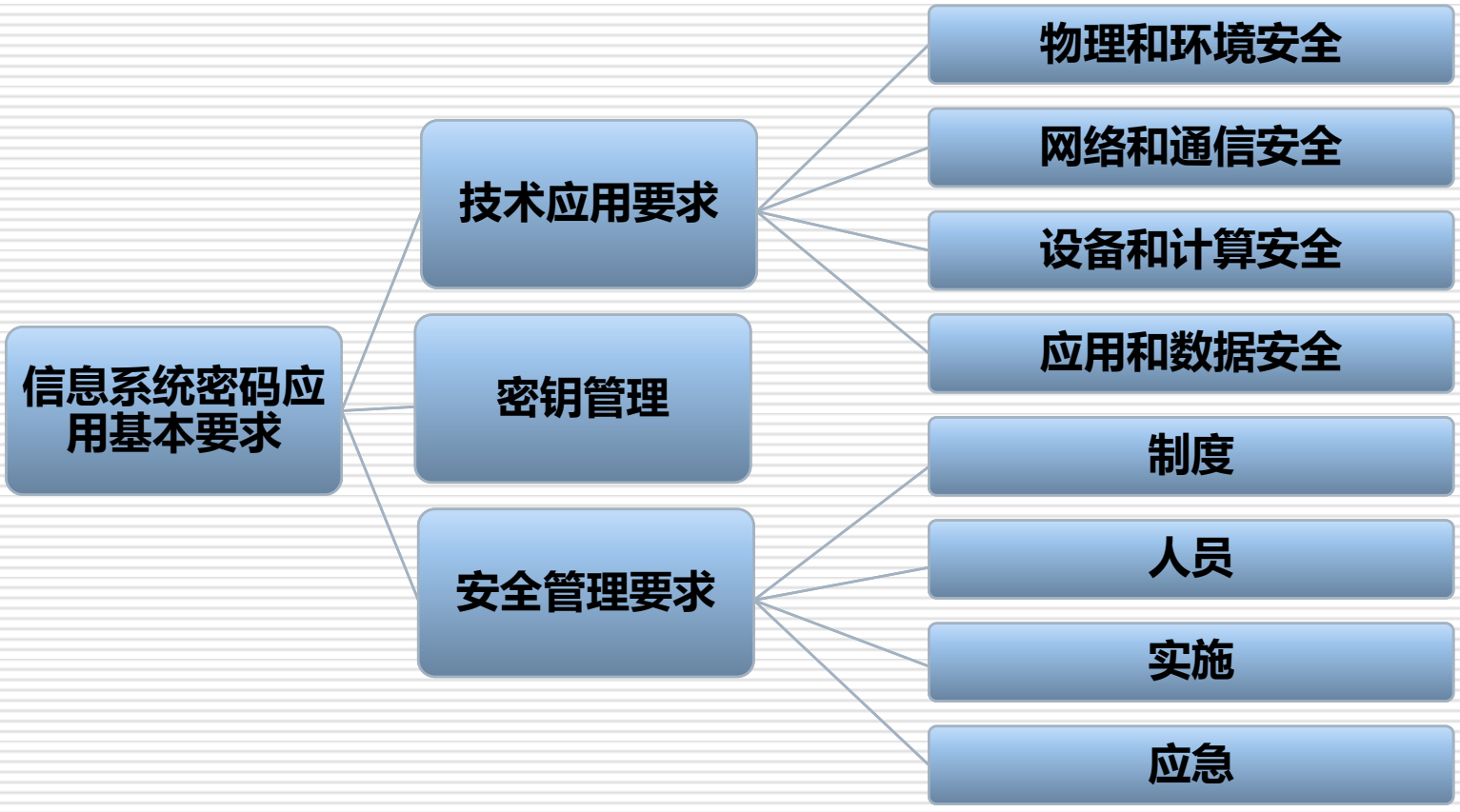
中华人民共和国密码行业标准

GM/T 0054-2018

信息系统密码应用基本要求

General requirements for information system cryptography application

密评技术要求—基本要求


信息系统密码应用基本要求
技术应用要求
密钥管理
安全管理要求
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
制度
人员
实施
应急

密评技术要求—基本要求—总体要求

密码算法	密码技术	密码产品	密码服务
□ 了解信息系统使用的算法名称、用途、位置、执行算法的设备及其实现方式 □ 核查密码算法是合规性（标准或取得密码管理部门同意使用的证明文件）	□ 核查密码协议、密钥管理等密码技术是否符合相关标准规范 □ 若密码技术由合规的密码产品实现，则重点评估技术使用是否符合标准规定	□ 核查相关部件和设备是否取得国家密码管理部门颁发的商用密码产品型号证书或被主管部门认可的测评机构出具的合格测评报告	□ 核查信息系统使用第三方提供的电子认证服务等密码服务是否获得国家密码管理局颁发的密码服务许可证

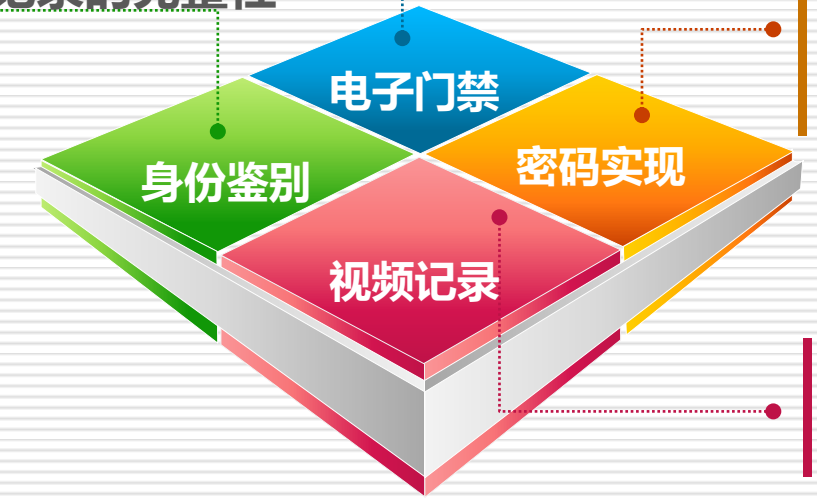
密评技术要求—基本要求—物理和环境安全

电子门禁记录

使用密码技术保证进出记录的完整性

身份鉴别

使用密码技术保护物理访问控制身份鉴别信息（真实性）



密码模块实现

应采用符合GM/T 0028或管理部门核准的硬件密码产品实现密码运算和密钥管理（三级推荐）

视频记录

使用密码技术的完整性功能来保证视频监控音像记录的完整性

密评技术要求—基本要求—网络和通信安全

01 身份鉴别

- ✓ 应在通信前基于密码技术对通信双方进行验证或认证，实现防截获、防假冒和防重用

02 设备接入认证

- ✓ 对连接到内部网络的设备进行身份鉴别

03 访问控制信息

- ✓ 保证网络边界和系统资源访问控制信息的完整性

04 通信数据完整性

- ✓ 保证通信过程中数据的完整性

05 通信数据机密性

- ✓ 保证通信过程中敏感信息数据字段或整个报文的机密性

06 集中管理通道安全

- ✓ 应使用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理

07 密码模块实现

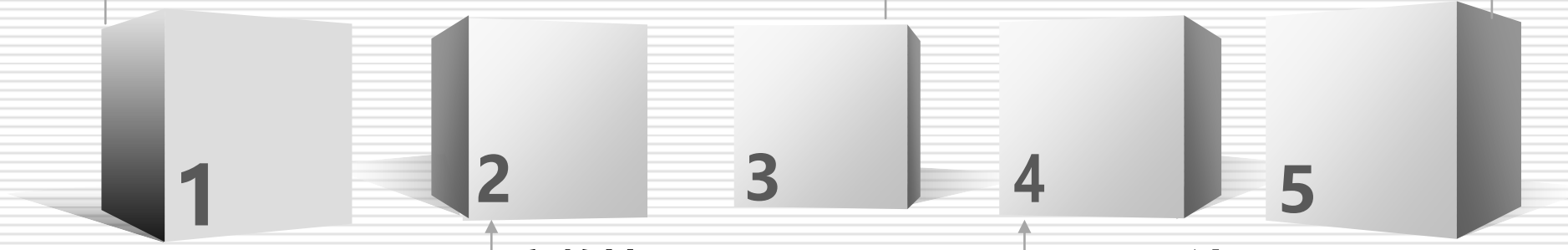
- ✓ 应采用符合GM/T 0028或管理部门核准的硬件密码产品实现密码运算和密钥管理（三级推荐）

密评技术要求—基本要求—设备和计算安全

机密性	完整性	真实性	不可否认性
□ 设备远程管理鉴别信息 远程管理时，实现鉴别信息的防窃听	□ 访问控制信息 □ 敏感标记 保证重要信息资源敏感标识的完整性 □ 日志记录 □ 设备重要文件 实现系统运行中重要程序或文件完整性保护	□ 身份鉴别 使用密码技术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	□ 身份鉴别 使用密码技术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

应采用符合GM/T 0028或管理部门核准的硬件密码产品实现密码运算和密钥管理（三级推荐）

密评技术要求—基本要求—应用和数据安全



机密性

- ✓ 数据传输
- ✓ 数据存储

应采用符合GM/T 0028或管理部门核准的硬件密码产品实现密码运算和密钥管理（三级推荐）

完整性

- ✓ 访问控制信息和敏感标记
- ✓ 数据传输
- ✓ 数据存储

真实性

- ✓ 身份鉴别

不可否认

- ✓ 身份鉴别
- ✓ 抗抵赖（仅适用于四级）

（涉及法律认定，实现数据原发行为和数据接收行为的不可否认性）

安全控制

对重要程序的加载和卸载进行安全控制

密评技术要求—基本要求—密钥管理

合规性

确认所有密钥管理的操作都是由符合规定的**密码产品或密码模块**实现

- GM/T 0005《随机性检测规范》
- GM/T 0028《密码模块安全技术要求》

理清密钥流转的关系，对信息系统内的密钥（尤其是对进出密码产品和密码模块的密钥）的安全进行检查，给出**全生命周期的密钥流转表**，即标明这些密钥是如何生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁的，并**核查是否满足要求**

密评技术要求—基本要求—安全管理

制度

- ✓ 制定密码安全管理制度及操作规范
- ✓ 定期论证和审定密码安全管理制度
- ✓ 应明确相关管理制度发布流程
- ✓ 制度执行过程应留存相关记录（四级）

实施

- ✓ 规划阶段制定密码应用方案
- ✓ 实施阶段应制定实施方案，选用被核准的密码产品或被许可的密码服务
- ✓ 投入运行前，应经测评机构进行安全性评估，评估通过后方可投入正式运行
- ✓ 每年应委托测评机构开展评估
- ✓ 有重大安全隐患时，应停止系统运行，制定整改措施，整改完成并通过评估方可投入运行

人员

- ✓ 应了解并遵守密码相关法律法规
- ✓ 应能够正确使用密码产品
- ✓ 应设置密钥管理人员、安全审计人员、密码操作人员等关键岗位
- ✓ 建立岗位责任制度，关键岗位多人共管制度
- ✓ 密码管理员、密码设备操作人员应从本机构在编的正式员工中提拔，并进行背景调查（四级）

应急

- ✓ 制定应急预案，做好应急资源准备
- ✓ 事件发生后，应及时向上级主管部门和同级的密码主管部门进行报告
- ✓ 事件处置完成后，应及时向同级的密码主管部门报告事件发生的情况及处置情况

密评技术要求—不同等级密码应用要求示意

指标要求			一级	二级	三级	四级
技术要求	物理和环境安全	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	--	宜	宜	应
	网络和通信安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	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	--	--	应	应
		密码模块实现	--	宜	宜	应
	设备和计算安全	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
.....						

注：“--”表示该项不做要求；“可”表示可以、允许；“宜”表示推荐、建议；“应”表示应该

目 录

密评实施要求—测评过程

密码应用方案评估	测评准备活动	方案编制活动	现场测评活动	分析与编制报告
◘ 委托测评机构或组织专家进行评估 ◘ 测评实施的重要依据	◘ 掌握被测信息系统的详细情况 ◘ 准备测评工具	◘ 确定与被测信息系统相适应的测评对象、测评指标及测评内容等，形成测评方案	◘ 分步骤实施所有测评项目 ◘ 了解系统的真实防护情况发掘系统存在的密码应用安全性问题	◘ 找出整个系统的安全防护现状与相应等级保护需求之间的差距，分析可能存在的风险并形成评估报告

密评实施要求—密码应用方案评估

规划阶段

密码应用建设方案由责任单位组织商用密码产业单位编写，由**《密码应用解决方案》**、**《应用实施方案》**和**《应急处置方案》**三部分组成

材料 1

《密码应用解决方案》应明确密码应用体系架构、算法使用、密钥管理等内容。

材料 2

《实施方案》应明确实施路线图、升级改造方案、责任机构和责任人、工作计划和任务分工等内容

材料 3

《应急处置方案》应分析潜在的意外事件并制定多套应急处置预案，明确应急处理人员角色和责任、应急事件通告规则、损失评估程序、预案激活条件等

方案需经专家或测评机构评审,并明确《基本要求》中“宜”的条款

密评实施要求—密码应用方案评估

口 密码应用解决方案

- 方案内容的完整性
- 密码应用合规性、正确性、有效性

口 实施方案

- 实施方案的科学合理性
- 实施方案的可行性

口 应急方案

- 文档结构的完整性
- 风险分析的完备性
- 处置措施和应急方案的合理周密性

密评实施要求—密码应用方案评估

- 对于已建信息系统，测评机构要能够从中提炼出密码应用方案
  - 明确信息系统的详细网络拓扑
  - 摸清系统中已有的密码产品
  - 梳理密钥管理层次，给出密钥全生命周期的管理过程
  - 针对重要数据或敏感信息，梳理其在信息系统中的流转过程和受保护情况

密评实施要求—测评准备活动

工作目标

- 启动测评项目（组建项目组，编制计划书等）
- 收集被测信息系统相关资料
- 准备测评所需资料
- 为编制测评方案打下良好的基础

工作流程

- 工作启动
- 信息收集和分析
- 工具和表单准备

密评实施要求—测评准备活动

- 调查表格（如果需要）
- 被测信息系统总体描述文件
- 被测信息系统密码总体描述文件
- 安全管理制度文件
- 密钥管理制度
- 各种密码安全规章制度及相关过程管理记录
- 配置管理文档
- 测评委托单位的信息化建设与发展状况以及联络方式
- 密码应用方案
- 评估结果安全保护等级定级报告
- 系统验收报告
- 安全需求分析报告
- 安全总体方案
- 自查或上次测评报告

- 测评机构收集测评所需资料
- 被测信息系统相关人员准确填写调查表格
- 测评机构根据填写完成的调查表格，分析调查结果，了解和熟悉被测系统的实际情况
- 如果调查表格填写不准确，或不完善，或存在相互矛盾的地方较多，测评机构应安排现场调查，以确认调研信息的正确性

密评实施要求—方案编制活动

工作目标

- 整理测评准备阶段中获取的信息系统相关资料
- 为现场测评活动提供指导方案

工作流程

- 测评对象确定
- 测评指标确定
- 测评内容确定
- 工具测试方法确定
- 作业指导书及测评方案编制

密评实施要求—方案编制活动

□ 测评指标确定环节

- 系统定级情况（业务信息安全保护等级）
- 从《信息系统密码应用基本要求》和《信息系统密码测评要求》中选择相应等级的基本安全要求作为基本测评指标
- 确定不适应测评指标
- 对确定的测评指标进行描述，并分析给出指标不适用的原因
- 分别针对每个定级对象加以描述：系统的定级情况、指标选择两部分

密评实施要求—方案编制活动

□ 测评内容确定环节

- 依据《信息系统密码应用基本要求》和《信息系统密码测评要求》，将前面已经得到的测评指标和测评对象结合起来
- 将测评指标映射到各测评对象上
- 结合测评对象的特点，说明各测评对象所采取的测评方法
- 构成一个个可以具体实施测评的单项测评内容
- 测评内容是测评人员开发作业指导书的基础

密评实施要求—方案编制活动

口 工具测试方法确定环节

- 可以直接获取到目标系统密码应用环境存在的风险、漏洞
- 可以分析出系统内部应用的密码算法、密码协议应用是否合规、运输结果是否正确、提供的安全服务是否有效
- 测试工具接入点应根据被测系统的密码应用领域、网络拓扑结构、访问控制策略、主机存放位置等情况后，合理选取接入点

原则：在不影响目标系统正常运行的前提下严格按照密评工作方案选定的测评范围开展工具测试

密评实施要求—现场测评活动

工作目标

- 将测评方案和测评方法等内容具体落实到现场测评活动中
- 取得报告编制所需的足够证据和资料

工作流程

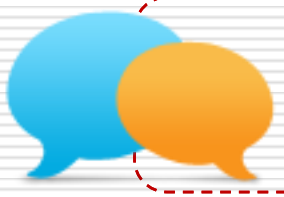
- 现场测评准备
- 现场测评和结果记录
- 结果确认和资料归还

密评实施要求—现场测评活动

口 注意事项

- 被测单位对风险确认书签字确认
- 获得现场测评授权
- 召开测评现场首次会
- 确认具备测评工作开展的条件，需要的各种资源
- 确认关键数据已备份
- 测评结束后，确认测评工作对测评对象的影响，并恢复现场

密评实施要求—分析与报告编制



- 对单元测试结果进行判断，并在此基础上，对受测信息系统进行整体测评
- 风险分析和评价

- 根据信息系统所承载的业务、部署环境以及其他系统的连接情况，分析可能面临的外在安全风险
- 通过渗透测试、逆向分析等有效手段进行验证和分析

- 测评结论形成
- 测评报告编制

信息系统自身若存在安全漏洞或面临安全风险，将直接威胁到系统密码的应用安全，严重者可造成密钥的泄露和密码保护失败

目 录

密评与等保

口 密评的推动离不开等保的大力支持

- 全社会安全意识提升
- 等保十年成绩基础是开展密评的先决条件
- 依托于测评制度开展密评
- 依赖等保测评队伍实施密评

密评与等保

□ 等保的技术体系是密评开展的前提

ICS35.040
L80

GB

中华人民共和国国家标准

GB/T 22239—2008

信息安全技术
信息系统安全等级保护基本要求

Information security technology—
Baseline for classified protection of information system

2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

ICS 35.040
L 80
备案号:

GM

中华人民共和国密码行业标准

GM/T 0054-2018

信息系统密码应用基本要求

General requirements for information system cryptography application

密评与等保

口 密评推进需要等保的成熟经验

- 密码讳莫高深
- 基线要求提高密评推进难度
- 密码技术手段与安全需求的矛盾

密评与等保

当前，密评是一个新生事物，其重要性不言而喻，但对于它的机制、标准等仍然处于不断探索和完善中，而网络安全等级保护经过十年的实践，有了扎实的根基，方法论、标准和共识上处于比较成熟和发展阶段

密评必须依托等保的基础才可能进一步发展

密评与等保

口 推动以等保为核心的安全新模式

- 2017年6月1日《中华人民共和国网络安全法》正式施行
- 网络安全领域的一部基础性法律
- 国家实行网络安全等级保护制度，关键信息基础设施在网络安全等级保护制度的基础上，实行重点保护
- 等级保护制度是国家网络安全工作的基本制度、基本策略和基本方法

《网络安全法》从国家法律层面确立了网络安全等级保护作为我国网络安全保障工作的基础地位

密评与等保

口 推动以等保为核心的安全新模式

- 网络空间的安全治理将进一步走向细分
- 关键信息基础设施保护、网络安全审查、商用密码应用安全性评估、互联网新技术新业务评估、数据出境安全评估、个人信息安全规范、大数据安全、云计算安全和工业控制系统安全和物联网安全等等相关配套性的评测、保护标准陆续推出
- 相关领域的专门性安全要求与细则被陆续制定和施行
- 对各个重点行业的信息系统提出更高的安全合规与风险管理要求

密评与等保

口 推动以等保为核心的安全新模式

- 哪些安全法规是必须满足的?
- 哪些安全标准是需要首先遵循的?
- 哪些可以后面再补上的，先后顺序?
- 一个单位拥有众多不同类型和规模的信息系统，拥有不同的安全需求，应如何组织相关的安全合规防护体系?
- 如何避免重复实施，并在预算内，完成更多的安全工作?

提出“等保为核心+相关专项安全为扩展”的安全新模式

密评与等保

- 推动以等保为核心的安全新模式
  - 扎实基础、分步实施 → 夯实安全基础
  - 标准融合，多方合规 → 满足多方合规
  - 能力叠加，重点强化 → 获得整体安全

降低安全成本

谢谢！