




# GB/T 39786-2021 标准解读

 主讲人：张桂金

天津市商用密码行业协会



# 目录

# CONTENTS

01 什么是“密评”

02 密评依据

03 GB/T39786测评指标解析

04 密评流程

# 什么是“密评”

---

PART. 01

# 什么是商用密码



商用密码是指**对不涉及国家秘密内容的信息进行加密保护或安全认证**所使用的**密码技术和密码产品**。商用密码技术是商用密码的核心，是信息化时代社会团体、组织、企事业单位和个人用于保护自身权益的重要工具。国家将商用密码技术列入国家秘密，任何单位和个人都有责任和义务保护商用密码技术的秘密。

# 什么是密评

商用密码应用安全性评估（简称“密评”），是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。



## 合规性

密码算法、密码协议、密钥管理密码产品和服务使用合规，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核准的密码产品，许可的密码服务。



## 正确性

密码算法、密码协议、密钥管理、密码产品和服务使用正确，即采用的密码算法、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；密码保障系统建设或改造过程中密码产品和服务的部署和应用正确。



## 有效性

采用的密码协议、密钥管理系统、密码应用子系统和密码安全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。

# 相关法律法规

## 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。

第三十七条 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。

## 关键信息基础设施安全保护条例（征求意见稿）

第五十三条**关键信息基础设施**中的密码使用和管理，还应当遵守密码法律、行政法规的规定。



## 网络安全法

第十条 建设、运营网络或者通过网络提供服务，应当维护网络数据的**完整性、保密性和可用性**。

第二十一条 采取数据分类、**重要数据**备份和**加密**等措施，保障网络免受干扰、破坏或者未经授权的访问，**防止网络数据泄露或者被窃取、篡改**。

## 网络安全等级保护条例（征求意见稿）

第四条 网络运营者在网络建设过程中应当同步规划、同步建设、同步运行网络安全保护、保密和**密码保护措施**。

第四十七条 非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。**第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务**。

# 谁要做密评

## 责任单位

涉及国家和社会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。

## 覆盖单位

重要领域网络和信息系统的覆盖范围包括：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。

## 其他单位

第三条规定范围之外的其他网络和信息系统的责任单位可以参考本办法自愿开展商用密码应用安全性评估。



# 谁要做密评



基

## 基础信息网络：

电信网、广播电视网、互联网。

政

## 面向社会服务的政务信息系统：

党政机关和使用财政性资金的事业单位和团体组织使用的面向社会服务的信息系统。

重

## 重要信息系统：

能源、教育、公安、测绘地理信息、社保、交通、卫生计生、金融等涉及国计民生和基础信息资源的重要信息系统。

控

## 重要工业控制系统：

核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要工业控制系统。



# 密评缘起今生

**1999**

国务院颁布施行《商用密码管理条例》

**2007**

国家密码管理局印发《信息安全等级保护商用密码管理办法》

**2016**

国家密码管理局研究起草《商用密码应用安全性评估管理办法（试行）》

**2017**

国家密码管理局组织开展密码应用安全性评估试点工作

《商用密码应用安全性评估管理办法（试行）》等密评制度体系实施

**2018**

发布第一批密评试点单位  
国家密码管理局组织金融和重要领域密码应用专项检查  
GM/T 0054-2018《信息系统密码应用基本要求》实施

**2019**

第一批试点工作评审总结  
密评联委会成立

《密码法》正式发布

**2020**

《国家政务信息化项目建设管理办法》印发

《密码法》正式实施



# 密码应用现状

## 密码应用不广泛

目前，我国网络的整体安全防护能力十分脆弱，大量数据没有使用密码技术保护，处于“裸奔”状态，有些数据即使用了密码技术保护措施也是使用了不合规的密码技术，存在巨大的安全隐患。有关部门对所辖信息系统进行检查，结果表明商用密码应用比重较低，系统安全防护能力十分薄弱。



## 密码应用不规范

现有大量系统依旧在使用MD5、SHA-1、RSA-512、RSA-1024、DES等已被警示有风险的密码算法，以及基于这些密码算法提供的不安全密码服务。此外，应用系统未按规范要求使用密码服务、或者错误调用密码应用接口等等，这给信息系统带来了严重安全隐患。

## 密码应用不安全

1999年《商用密码管理条例》提出，任何单位或个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。虽然中央、地方、行业相继出台一些规定和配套制度、要求，但在一些地区和部门并未得到有效实施。一些单位重信息化建设、轻信息安全保护，信息系统密码使用不规范、不正确，在密钥管理、密码系统运行维护等方面存在风险。

# 密评工作容易遇到的问题

责任单位不够重视，历史遗留，对密评相关工作体系缺少认识等问题。

## 系统规划阶段未考虑密评

- 目前通过等保三级评估的系统,因等保和密评的差异性,大量已建系统在规划阶段并未考虑密码应用安全,几乎没有使用任何密码技术和密码产品,即便有也并不符合国家密码管理局的相关标准。
- 年代久远的老系统涉及到整体大改,将影响业务的正常运作。

## 责任单位不够重视

- 由于密码法的推行和普及的时间较短,责任单位还未意识到密评的必要性。
- 部门领导没有直接指示,密评工作被列为不重要项,开展进度缓慢。
- 涉及到经费问题。如今年刚刚做完等保改造或信息化建设,经费不足。

## 系统复杂涉及多方对接

- 涉及到被测责任单位\运维部\第三方开发商\密评差距评估\云平台等多个对象,整体密评改造难度偏大。整体密评改造难度偏大。
- 部分系统涉及到多端 (IOS\Android\PC\终端) 问题,结构复杂,改造范围大。

# 密评依据

PART. 02

# 密评标准



1

GB/T39786-2021 《信息系统密码应用基本要求》

2

《信息系统密码测评要求（试行）》

3

《商用密码应用安全性评估测评过程指南（试行）》

4

相关国家及行业标准、规范、指南（例如：《政务信息系统密码应用与安全性评估工作指南》（2020版）

5

通过评审的密码应用解决方案

# 相关标准、规范、指南

## 目录

1 GM/T 0070-2019 电子保单密码应用技术要求

---

2 GM/T 0071-2019 电子文件密码应用指南

---

3 GM/T 0072-2019 远程移动支付密码应用技术要求

---

4 GM/T 0073-2019 手机银行信息系统密码应用技术要求

---

5 GM/T 0074-2019 网上银行密码应用技术要求

---

6 GM/T 0075-2019 银行信贷信息系统密码应用技术要求

---

7 GM/T 0076-2019 银行卡信息系统密码应用技术要求

---

8 GM/T 0077-2019 银行核心信息系统密码应用技术要求

---

# 相关标准、规范、指南

## 目录

9 信息系统密码应用测评要求

---

10 信息系统密码应用测评过程指南

---

11 信息系统密码应用高风险判定指引

---

12 商用密码应用安全性评估量化评估规则

---

13 政务信息系统密码应用与安全性评估工作指南

---

14 <http://www.gmbz.org.cn/main/bzlb.html> (密码行业标准化技术委员会)

---



# GB/T39786测评指标解析

PART. 03

## 技术层面要求



- 物理与环境安全
- 网络与通信安全
- 设备与计算安全
- 应用与数据安全

## 管理制度要求



- 管理制度
- 人员管理
- 建设运行
- 应急处置

## 测评要求之物理与环境安全

### 1、身份鉴别 (高风险\*)

a) 测评指标：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。（L1-L4）

b) 测评对象：信息系统所在机房等重要区域及其电子门禁系统

### 2、电子门禁记录数据存储完整性

a) 测评指标：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。（L1-L4）

b) 测评对象：信息系统所在机房等重要区域及其电子门禁系统。

### 3、视频监控记录数据存储完整性

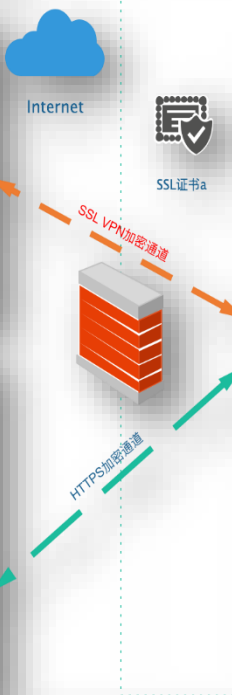
a) 测评指标：采用密码技术保证视频监控音像记录数据的存储完整性。（L3-L4）

b) 测评对象：信息系统所在机房等重要区域及其视频监控系统。

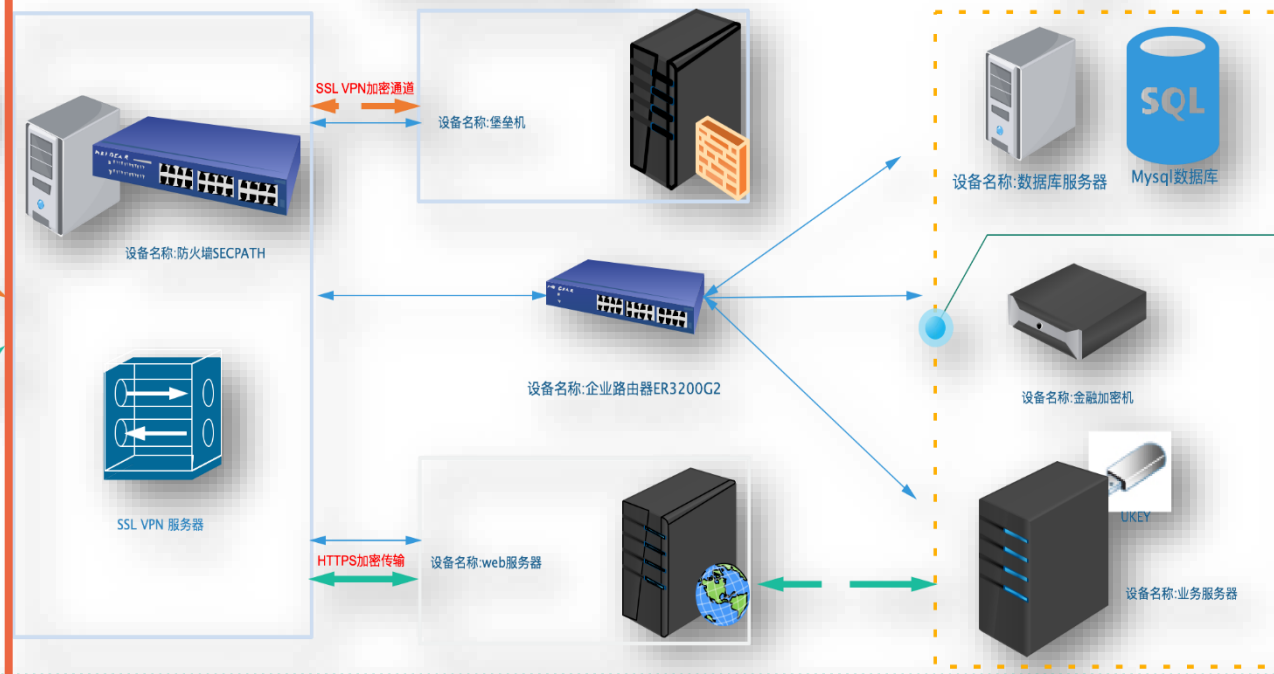
# 系统示例

## 密评实操演练平台(数据加密签名存储演示系统)

模拟公网环境



被测系统范围



核心区

运维网络线

业务网络线

物理通道

物理和环境安  
全覆盖范围

## 密码应用测评要求之网络和通信安全

### 1、身份鉴别（高风险\*）

#### a) 测评指标：

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。（L1-L3）

采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。（L4）

b) 测评对象：信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

### 2、通信数据完整性

a) 测评指标：采用密码技术保证通信过程中数据的完整性。（L1-L4）

b) 测评对象：信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

## 密码应用测评要求之网络和通信安全

### 3、通信过程中重要数据的机密性 **(高风险\*)**

- a) 测评指标：采用密码技术保证通信过程中重要数据的机密性。（L1-L4）
- b) 测评对象：信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

### 4、网络边界访问控制信息的完整性

- a) 测评指标：采用密码技术保证网络边界访问控制信息的完整性。（L1-L4）
- b) 测评对象：信息系统与网络边界外建立的网络通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品。

## 密码应用测评要求之网络和通信安全

### 5、安全接入认证

#### a) 测评指标

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，确保接入设备身份的真实性。（L3-L4）

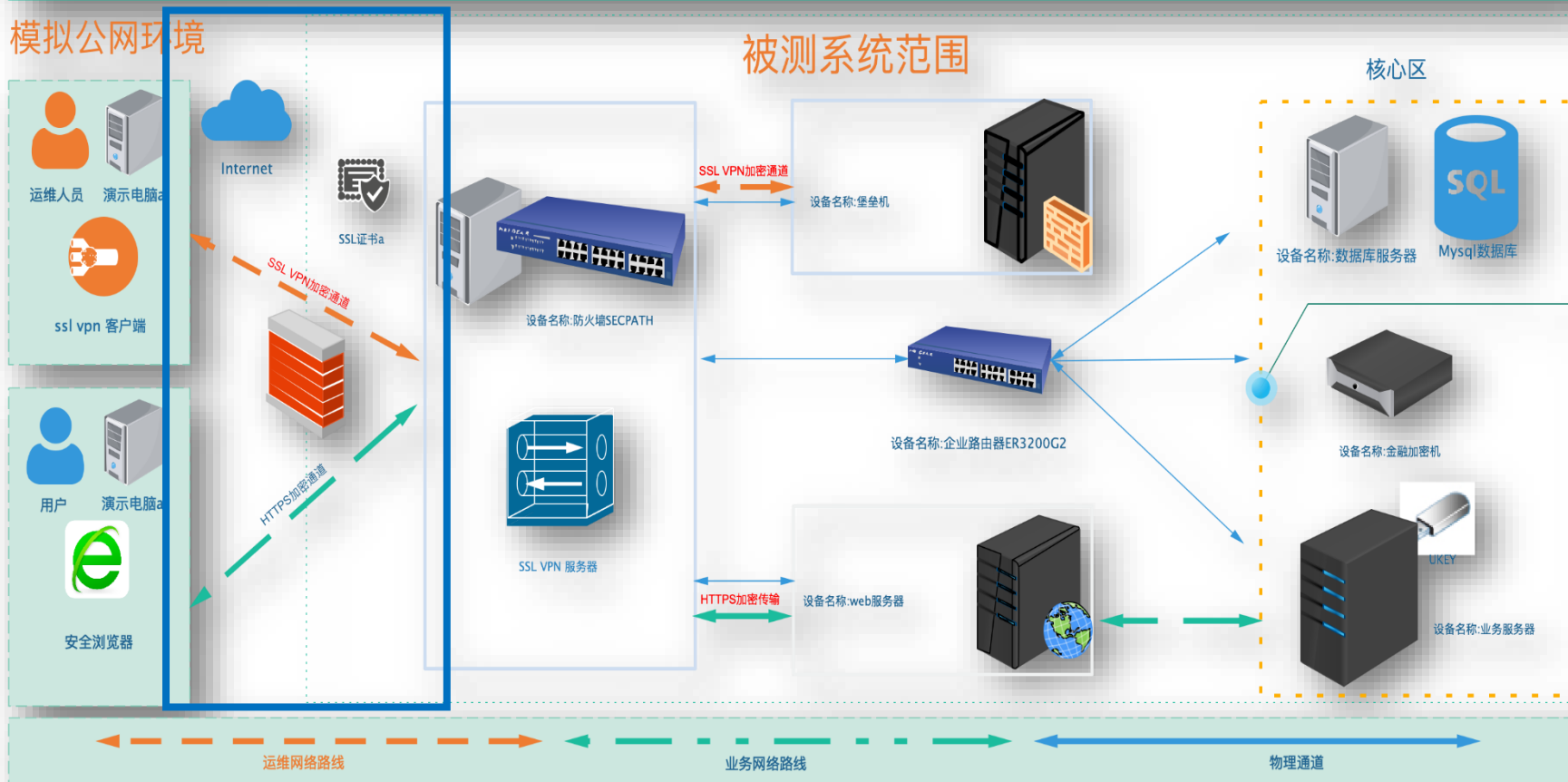
#### b) 测评对象

信息系统内部网络，以及提供设备入网接入认证功能的设备或组件、密码产品。



# 系统示例

## 密评实操演练平台(数据加密签名存储演示系统)



网络和通信安  
全覆盖范围

## 密码应用测评要求之设备和计算安全

### 1、身份鉴别（高风险\*）

- a) 测评指标：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。（L1-L4）
- b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供身份鉴别功能的密码产品。

### 2、远程管理通道安全（高风险\*）

- a) 测评指标：远程管理设备时，采用密码技术建立安全的信息传输通道。（L3-L4）
- b) 测评对象：通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供安全的信息传输通道的密码产品。

## 密码应用测评要求之设备和计算安全

### 3、系统资源访问控制信息完整性

- a) 测评指标：采用密码技术保证系统资源访问控制信息的完整性。（L1-L4）
- b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品

### 4、重要信息资源安全标记完整性

- a) 测评指标：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。（L3-L4）
- b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。

## 密码应用测评要求之设备和计算安全

### 5、日志记录完整性

- a) 测评指标：采用密码技术保证日志记录的完整性。（L1-L4）
- b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。

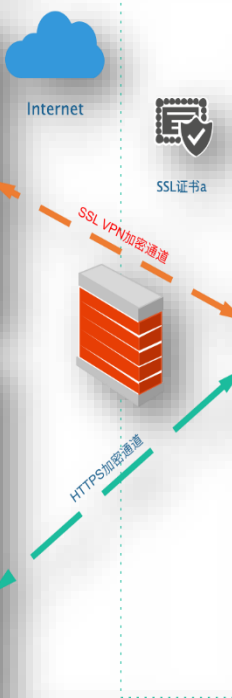
### 6、重要可执行程序完整性、重要可执行程序来源真实性

- a) 测评指标：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。  
(L3-L4)
- b) 测评对象：通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护和来源真实性功能的密码产品。

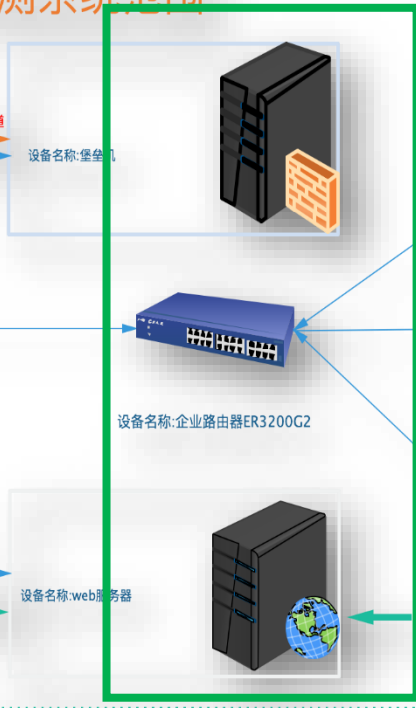
# 系统示例

## 密评实操演练平台(数据加密签名存储演示系统)

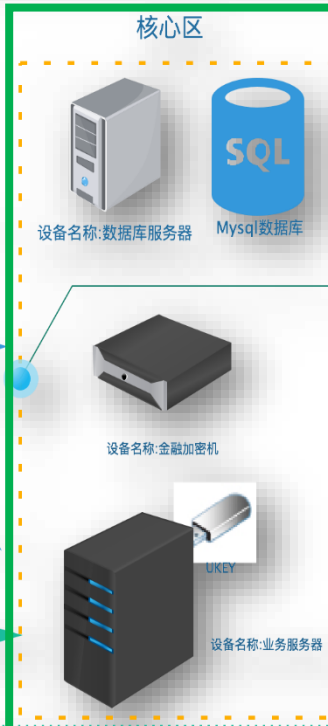
模拟公网环境



被测系统范围



核心区



运维网络路线

业务网络路线

物理通道

设备和计算安  
全覆盖外围

## 密码应用测评要求之应用和数据安全

### 1、身份鉴别 (高风险\*)

- a) 测评指标：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。（L1-L4）
- b) 测评对象：业务应用，以及提供身份鉴别功能的密码产品。

### 2、访问控制信息完整性

- a) 测评指标：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。（L1-L4）
- b) 测评对象：业务应用，以及提供完整性保护功能的密码产品。

### 3、重要信息资源安全标记完整性

- a) 测评指标：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。（L3-L4）
- b) 测评对象：业务应用，以及提供完整性保护功能的密码产品。

## 密码应用测评要求之应用和数据安全

### 4、重要数据传输机密性 (高风险\*)

- a) 测评指标：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。 (L1-L4)
- b) 测评对象：业务应用，以及提供机密性保护功能的密码产品。

### 5、重要数据存储机密性 (高风险\*)

- a) 测评指标：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。 (L1-L4)
- b) 测评对象：业务应用，以及提供机密性保护功能的密码产品。

### 6、重要数据传输完整性

- a) 测评指标：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。 (L1-L4)
- b) 测评对象：业务应用，以及提供完整性保护功能的密码产品。



## 密码应用测评要求之应用和数据安全

### 7、重要数据存储完整性 (高风险\*)

- a) 测评指标：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。（L1-L4）
- b) 测评对象：业务应用，以及提供完整性保护功能的密码产品。

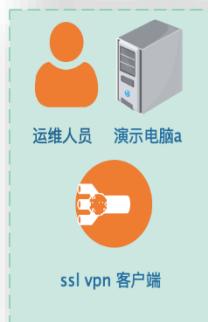
### 8、不可否认性 (高风险\*)

- a) 测评指标：在可能涉及法律责任认定的应用中，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。（L3-L4）
- b) 测评对象：业务应用，以及提供不可否认性功能的密码产品。

# 系统示例

## 密评实操演练平台(数据加密签名存储演示系统)

模拟公网环境



被测系统范围



核心区



运维网络路线

业务网络路线

物理通道

应用和数据安  
全覆盖外围

# 应对方法



## 物理与环境安全

- 电子门禁系统、视频监控系统、智能IC卡、服务器密码机、数据加密系统



## 网络与通信安全

- IPSec VPN、SSL VPN、安全认证网关、堡垒机



## 设备与计算安全

- 智能密码钥匙、服务器密码机、签名验签服务器



## 应用与数据安全

- 智能密码钥匙、动态令牌、服务器密码机、签名验签服务器、电子签章系统、时间戳服务器



## 密码应用测评要求之管理制度

- I. 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。（L1-L4）（高风险\*）
- II. 根据密码应用方案建立相应密钥管理规则。（L1-L4）
- III. 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。（L2-L4）
- IV. 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。（L3-L4）
- V. 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。（L3-L4）
- VI. 具有密码应用操作规程的相关执行记录并妥善保存。（L3-L4）

## 密码应用测评要求之人员管理

- I. 相关人员了解并遵守密码相关法律法规、密码应用安全管理制度。(L1-L4)
- II. 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。(L2-L4)
- III. 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；(L3-L4)
- IV. 对关键岗位建立多人共管机制；(L3-L4)
- V. 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；(L3-L4)
- VI. 相关设备与系统的管理和使用账号不得多人共用；(L3-L4)
- VII. 密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并应在任前对其进行背景调查。(L4)

## 密码应用测评要求之人员管理

- I. 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。（L2-L4）
- II. 定期对密码应用安全岗位人员进行考核。（L3-L4）
- III. 及时终止离岗人员的所有密码应用相关的访问权限、操作权限。（L1）
- IV. 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。（L2-L4）

## 密码应用测评要求之建设运行

- I. 依据密码相关标准和密码应用需求，制定密码应用方案。（L1-L4）（高风险\*）
- II. 根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照 GB/T AAAAA附录B。（L1-L4）
- III. 按照应用方案实施建设。（L1-L4）
- IV. 投入运行前进行密码应用安全性评估。（L1-L2）
- V. 投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行。（L3-L4）
- VI. 在运行过程中，严格执行既定的密码应用安全管理制度，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。（L3-L4）

## 密码应用测评要求之应急处置

- I. 根据密码产品提供的安全策略，由用户自主处置密码应用安全事件。（L1）
- II. 制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，按照应急处置措施结合实际情况及时处置。（L2）
- III. 制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置。（L3-L4）
- IV. 事件发生后，及时向信息系统主管部门进行报告。（L3）
- V. 事件发生后，及时向信息系统主管部门及归属的密码管理部门进行报告。（L4）
- VI. 事件处置完成后，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。（L3-L4）



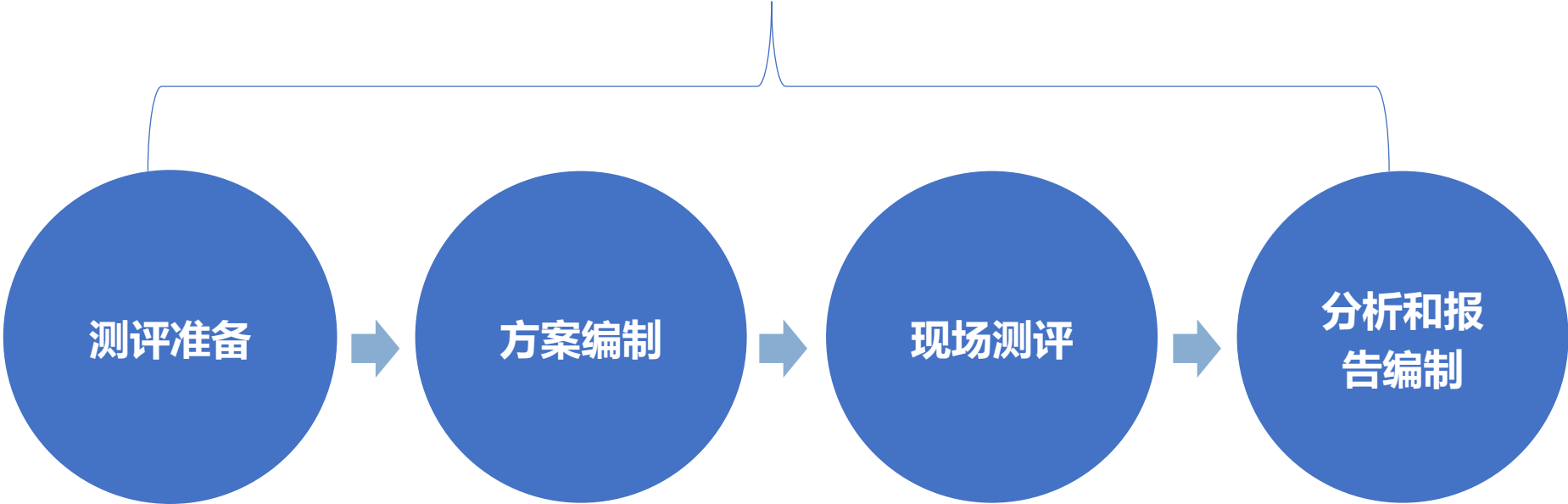
# 密评流程

---

**PART. 04**

# 密评实施过程

沟通与洽谈



# 测评准备

## 被测责任单位

1. 签订委托评估协议书
2. 签订保密协议
3. 提供被测系统详细资料 (包括但不限于被测系统总体描述文件、被测系统商用密码总体描述文件、安全保护等级定级报告、安全需求分析报告、安全总体方案、安全详细设计方案、用户指南、运行步骤、各种密码安全规章制度相关过程管理记录、配置管理文档、历史商用密码应用安全性测评报告、系统验收报告、密钥管理制度、人员管理制度、电子门禁系统技术文档、密码产品型号证书等)
4. 配合填写《信息系统商用密码应用情况调查表》  
《商用密码应用标准符合性自查表》等系统情况调查表格。

## 密评机构

1. 收集分析被测系统信息
2. 掌握被测系统详细情况
3. 准备评估工具

# 方案编制

## 被测责任单位

1. 组织商用密码从业单位编写密码应用方案
2. 配合密评机构意见修改完善密码应用方案
3. 出具完整的被测系统密码应用方案

## 密评机构

1. 根据密码应用方案编写实施方案
2. 根据密码应用方案确定系统测评指标
3. 根据密码应用方案确定测评检查点、
4. 根据密码应用方案确定系统密评方案

# 现场测评

## 被测责任单位

1. **做好测试环境准备、数据备份、资料准备、测试权限申请等内容，签订现场评估授权书**
2. **协调人员配合。密评项目负责人应确保现场测评过程中，信息系统相关人员（包括但不限于物理安全负责人、安全管理员、系统管理员、数据库管理员、应用系统管理员、安全审计员、密钥管理员、文档管理员、系统运维人员等）均能配合测评工作，接受密评机构访谈。**
3. **配合密评机构提供相关测评文档资料**
4. **配合密评机构采集系统测试结果**
5. **配合确认系统测评安全问题**
6. **场地环境准备**（提供召开现场测评启动会议、末次会议的会议室；提供独立的办公场所供测评组使用；提供必要的电源接入及被测系统的网络接入方式；提供互联网接入端口，以方便下载临时材料、查询相关资料等。）

## 密评机构

1. **召开测评现场首次会**（介绍测评工作，说明测评过程中具体的实施工作内容，测评时间安排，告知测评过程中可能存在的安全风险等）
2. **根据密评方案实施现场测评**（包括技术测评和安全管理测评部分）
3. **发现系统安全问题，汇总现场测评的测评记录**
4. **召开测评现场结束会**（确认系统测评结果、归还系统资料）

# 分析和报告编制

## 被测责任单位

1. 如系统存在高危风险安全问题，则根据系统整改建议进行系统整改
2. 查收系统测试报告

## 密评机构

1. 对现场测评获得的测评结果进行汇总  
分析（系统风险分析安全问题汇总）
2. 给出安全建设整改建议
3. 形成评估结论，编制评估报告
4. 出具测评报告

# 安全性评估结论



## 符合

- 信息系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分；

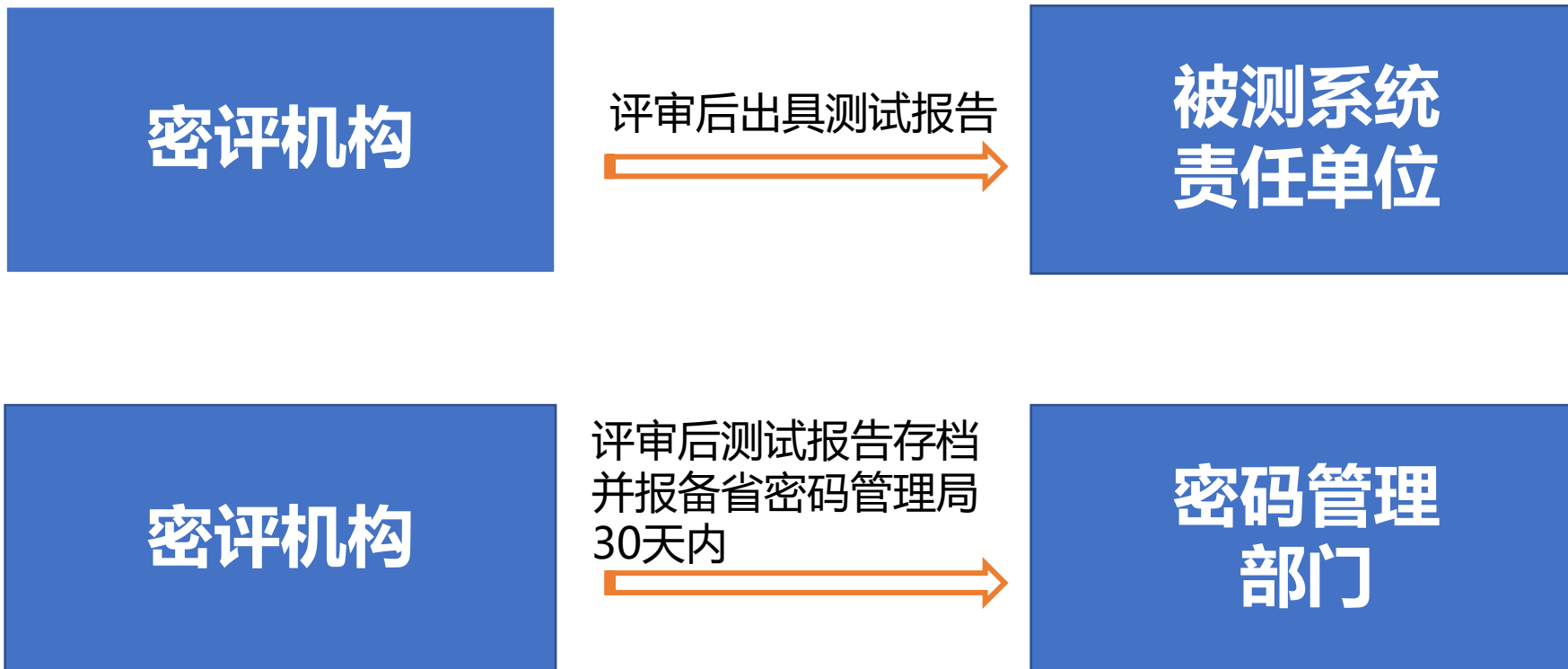
## 基本符合

- 信息系统中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题**不会导致信息系统面临高等级安全风险**，且综合得分**不低于阈值**；

## 不符合

- 信息系统中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题**会导致信息系统面临高等级安全风险**，或综合得分**低于阈值**。

# 密评完成





# 感谢聆听



天津市商用密码行业协会