商用密码培训与模拟测评环境
白 皮 书

一、环境背景

商用培训与模拟测评环境是一套由密码设备、网络设备、密码应用终端，以及培训与模拟测评系统组成的实装环境，能够模拟典型的合规、不合规密码应用场景，测评人员实际场景采集流量数据、设备日志和数据库数据，并分析数据，研判测评结果，撰写密评报告，实现对测评主要环节的密评实操训练。同时，通过与密评正确答案的对比，及时评判测评人员训练成绩，提升训练效果。

本环境结合啄木鸟密评工具，“真实环境+密评工具”，共同构成完整的密评模拟测评与培训系统。纸上得来终觉浅，绝知此事要躬行。使用该系统开展实操培训，可以使得测评人员接触密码设备，了解典型密码应用过程，尽快熟悉密评全流程，熟练掌握密评工具和方法，丰富密评经验，缩小“理论知识”与“实操技能”之间的差距，从“密评小白”，快速成长为 “实操达人”。

环境的简要使用流程如下：

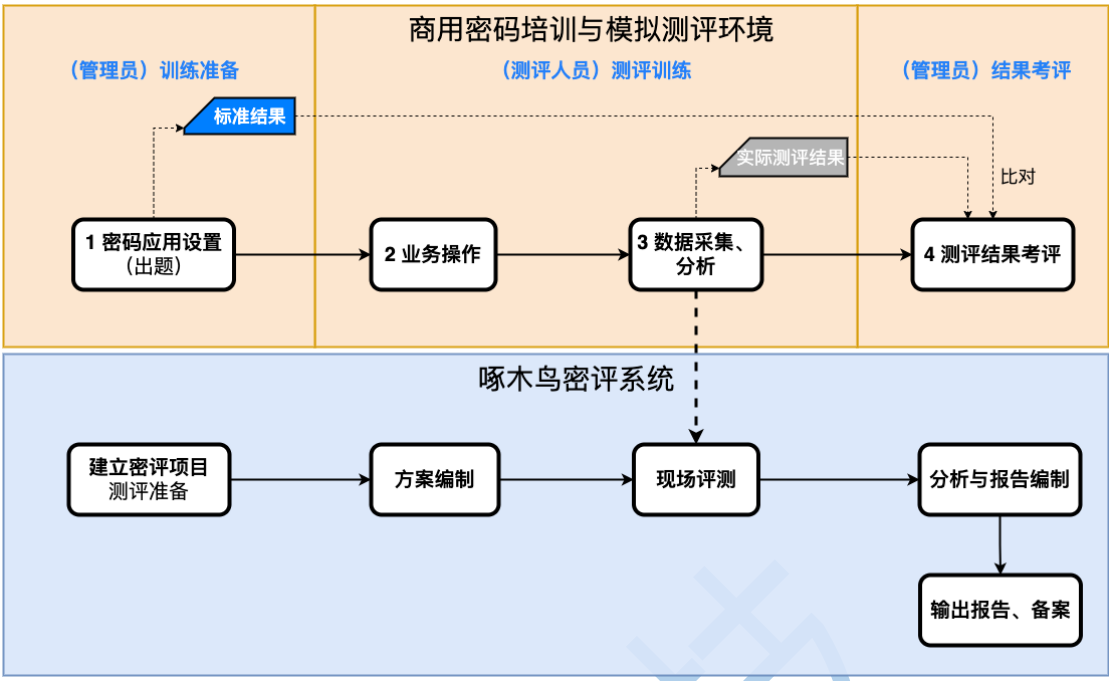

图 1-密评培训与模拟测评环境使用流程

二、典型仿真场景

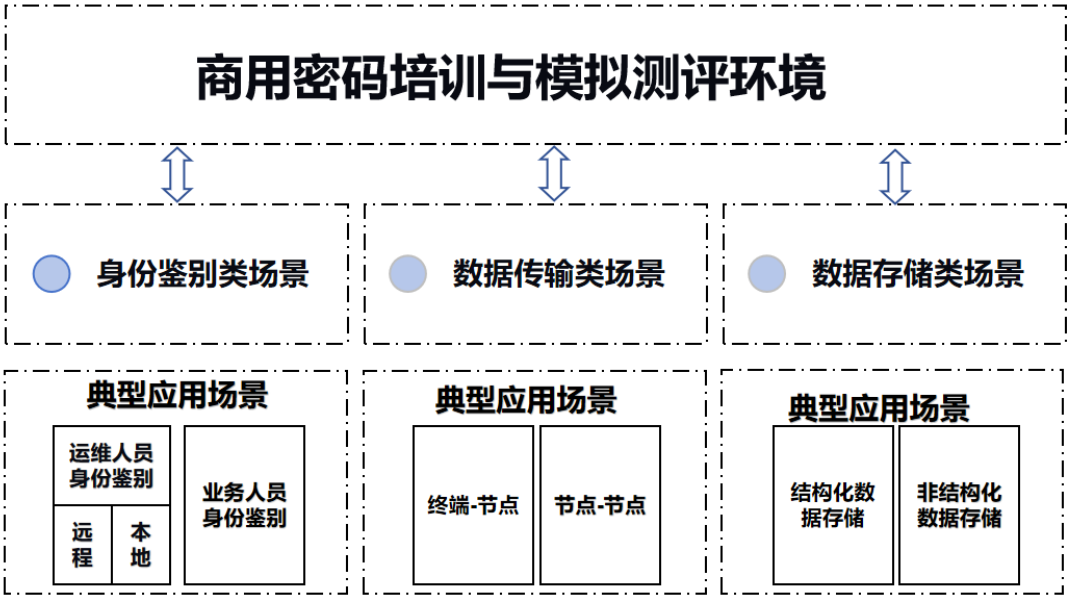

图 2-环境仿真场景

1. 身份鉴别类

1.1 运维人员身份鉴别

1）本地运维：运维人员通过 Ukey+国密数字证书登录堡垒机进行身份鉴别。

2）远程运维：运维人员通过国密 SSL VPN 接入，和堡垒机形成单一运维通道进行后端设备运维。

1.2 系统用户身份鉴别

1）网络和通信层身份鉴别：基于国密数字证书的单向、双向国密 SSL 通道的身份鉴别。

2）应用和数据层身份鉴别：基于国密数字证书的系统应用登录的身份鉴别。

2. 数据传输类

2.1 终端-站点安全通信

用户通过支持国密算法的 SSL VPN 接入内网，保证通信实体身份鉴别、数据机密性和完整性。

2.2 站点-站点安全通信

站点之间通过 IPSEC VPN 进行传输链路保护，保证站点之间身份鉴别、数据传输机密性、完整性。

3. 数据存储类

3.1 结构化数据

通过国密 SM2\SM3\SM4 对数据库数据完成机密性、完整性保护。通过调用合规的密码设备接口，完成字段级、记录级保护。包括访问控制列表、权限控制列表、管理/业务日志等信息。

3.2 非机构化数据

对应用系统中文件进行机密性、完整性保护。主要包括各类系统配置文件、业务文件、重要音视频文件、日志等。

三、环境拓扑

培训与模拟测评环境由模拟外网终端、模拟分支机构、网络接入区、业务区、密码服务区、内网办公区、统一管理区、证书服务区 8 个区域组成。

模拟外网终端，使用本地客户端和智能密码钥匙，通过网络接入区的网关认证，安全接入内网；模拟分支机构经过本地 IPSec VPN 与总部 IPSec VPN 建立安全网络通道，接入内网；网络接入区负责外部网络安全接入；业务区部署密码应用系统；密码服务区部署密码设备，向业务区提供调用服务；内网办公区终端从内部访问业务应用；统一管理区实现设备的管理和运维。

环境拓扑图如下图所示：

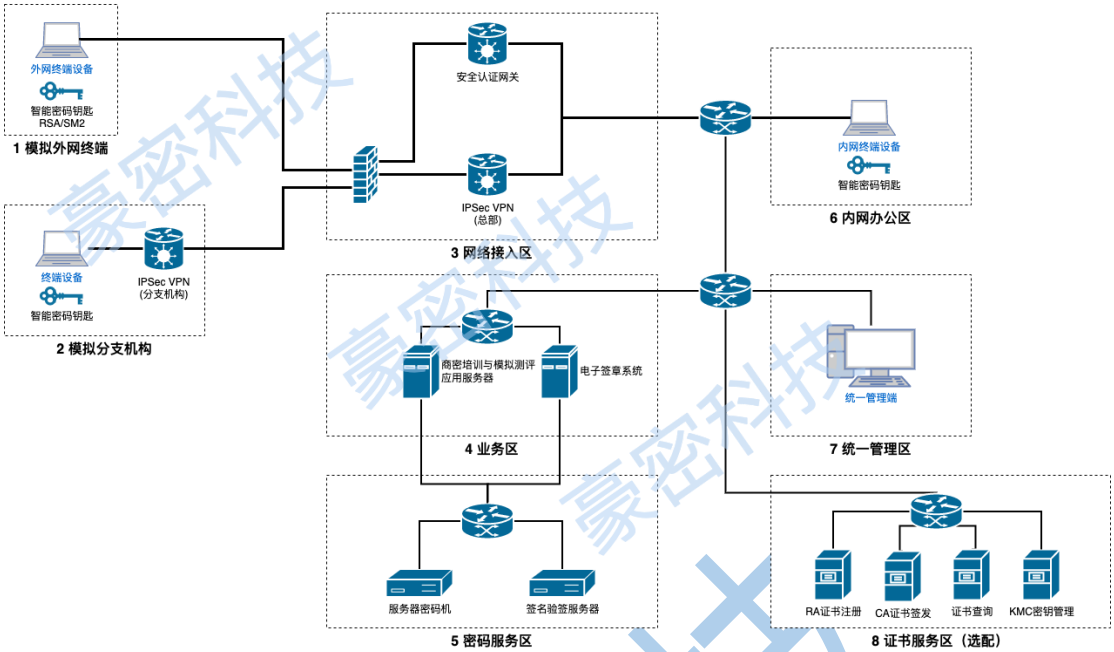

图 3-环境拓扑

四、产品形态

图 4-培训与模拟测评环境设备

图 5-培训与模拟测评系统界面

环境组成清单：

序号	设备名称	用途	数量	型号
1	培训与模拟测评系统（软件）	模拟典型密码应用场景，实现主流密码设备接入，支持合规和不合规的典型密码应用配置，从环境中采集数据，支撑密评机构人员实操训练、模拟测评	1 套	HMP-210
2	安全网关	远程用户安全接入内网	1 台	
3	IPSec VPN	分支机构安全接入内网	2 台	
4	智能密码钥匙 ukey	终端加密和用户身份鉴别	20 个	
5	签名验签服务器	数据签名验签	1 台	
6	服务器密码机	应用服务加解密计算	1 台	
7	电子签章系统	电子签章（带签章客户端）	1 台	
8	OFD/PDF 阅读器（软件）	电子签章的文档处理客户端	5 套	
9	交换机	模拟测评环境的网络连接	1 台	

五、密码应用配置

系统支持管理员对环境做各类合规、不合规的密码应用配置，以模拟不同的密码应用情况。测评人员在系统中做业务操作并采集数据、进行分析。支持的密码应用配置包括：

安全层面	指标	测评对象	合规应用	不合规应用
网络和通信	身份鉴别	终端-节点	UKey+国密数字证书双因素认证	套件中身份鉴别使用非国密算法
		节点-节点		
	数据通信机密性	通信链路	算法套件中使用 SM4 国密算法	明文传输或使用不合规加密算法
	数据通信完整性	通信链路	算法套件中使用 SM3 国密算法	明文传输或使用不合规杂凑算法
应用和数据	身份鉴别	终端用户	“口令+国密数字证书”双因素认证	仅使用口令认证、口令+不合规证书认证、使用过期证书和黑名单证书
	数据传输机密性	传输数据	SM4 数据加密传输	明文传输
	数据传输完整性	传输数据	SM3 数据完整性	未做完整性保护
	数据存储机密性	口令	SM3 数据完整性	明文存储 不合规杂凑
		其它敏感数据	SM4-ECB/CBC 数据加密存储	使用 3DES、AES128 加密，或不合理使用 ECB 模式及错误设置 IV 向量
	数据存储完整性	关键数据记录	国密 HMAC 数据完整性	未做完整性保护、使用普通 MAC 或不合规的 HAMC 做完整性保护
	抗抵赖	关键业务记录	国密签名验签	未采取签名验签或不合规的签名验签

六、系统特色

本环境是密评实验室建设必备的基础设施，包括内部培训与模拟测评的软硬件环境、专业测评工具，满足机构技术培训、测评验证和测评考核需要。具有以下特点：

1）真设备、真应用、真测评。实现主流密码设备接入和调用，通过一套完整密码应用系统覆盖多种密码应用场景，支持密评人员从环境中采集网络数据、日志数据和数据库数据，贴近实战开展分析测评，迅速提升密评实操能力。

2）多种场景、灵活配置、贴近实际。支持密码算法、参数及应用方式设置，灵活选择典型合规、不合规选项，模拟出不同的密码应用场景。

3）密评主要环节全覆盖。综合使用“模拟环境+密评工具”，完整实现了密评测评准备、方案编制、现场测评、分析与报告编制输出的全过程。