商用密码应用安全性评估报告模板

（2021 版）

中国密码学会密评联委会

二〇二一年十二月

说明

按照商用密码应用“三同步一评估”要求，信息系统需要同步规划、同步建设、同步运行密码保障系统，并进行商用密码应用安全性评估。在规划阶段，评估的对象是信息系统的密码应用方案；在建设和运行阶段，评估的对象是实际的信息系统。因此，本文件包括两个模板，分别为：

- 《XX 系统密码应用方案》商用密码应用安全性评估报告模板
- XX 系统商用密码应用安全性评估报告模板

报告编号：{}

《XXX 系统密码应用方案》

商用密码应用安全性评估报告

委托单位：_____

密评机构：_____

报告时间：_____

声 明

本报告是*{密评机构名称}*针对《XXX 系统密码应用方案》给出的商用密码应用安全性评估报告。

本报告评估结论的有效性建立在委托单位提供相关材料的真实性基础之上。

本报告中给出的评估结论仅对本次评估的《XXX 系统密码应用方案》的内容有效。评估工作完成后，当《XXX 系统密码应用方案》发生变更时，本报告不再适用。

本报告中给出的评估结论不能作为实际建设或运行系统的评估结论，也不能作为系统构成组件（或产品）的评估结论。

在任何情况下，若需引用本报告中的评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

本报告若无签字或机构盖章，均属无效。

{密评机构名称}（盖章）

年　　月　　日

基本信息表

<table>
<tr><th colspan="6">责任单位</th></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属省部密码管理部门</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><th colspan="6">信息系统</th></tr>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>网络安全等级保护定级情况</td><td colspan="5">☐已定级，第__级（一至四），S__A__G__。
☐未定级，本次密评依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第__级（一至四）信息系统要求</td></tr>
<tr><td>网络安全等级保护定级备案情况</td><td colspan="2">☐已备案
备案证明编号：
_____
☐未备案</td><td>本次被评信息系统与等级保护定级系统是否一致</td><td colspan="2">☐是
☐否，变化情况说明：
_____</td></tr>
<tr><td>网络安全等级保护测评情况</td><td colspan="2">☐已测评
测评机构名称：_____
测评时间：_____
测评结论：_____
☐正在测评
测评机构名称：_____
☐未测评</td><td>商用密码应用安全性评估情况</td><td colspan="2">☐已评估
密评机构名称：_____
评估时间：_____
评估结论：_____
☐正在评估
密评机构名称：_____
☐未评估</td></tr>
<tr><th colspan="6">密评机构</th></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>通信地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td rowspan="3">审核批准</td><td>编制人</td><td>（签字）</td><td>编制日期</td><td colspan="2"></td></tr>
<tr><td>审核人</td><td>（签字）</td><td>审核日期</td><td colspan="2"></td></tr>
<tr><td>批准人</td><td>（签字）</td><td>批准日期</td><td colspan="2"></td></tr>
</table>

商用密码应用安全性评估结论

方案名称	
方案简介	*{简要描述系统情况，方案内容。}*
评估情况简介	*{简要描述方案评估时间、范围、内容和过程（包括方案修改的交互过程，方案最后定稿的时间和版本）等。}*
评估结论	***{通过/不通过}***
不适用指标数目/总指标项数目	*{X/Y}*

改进建议

{评估结论为不通过时，具体修改意见为针对《XXXX 系统密码应用方案》中存在的XXX 问题（指出具体章节，具体问题），具体修改建议为XXX，需补充的材料为XXX。}

{评估结论为通过时：无意见/或进一步完善的参考建议意见为XXX。}

目录

声 明 I

基本信息表 I

商用密码应用安全性评估结论 II

改进建议 III

1 **系统概述** 1

2 **安全控制措施描述及指标适用情况** 4

3 **安全控制措施评估结果** 9

4 **方案评估结论** 12

附：《XXXX 系统密码应用方案》 13

1 系统概述

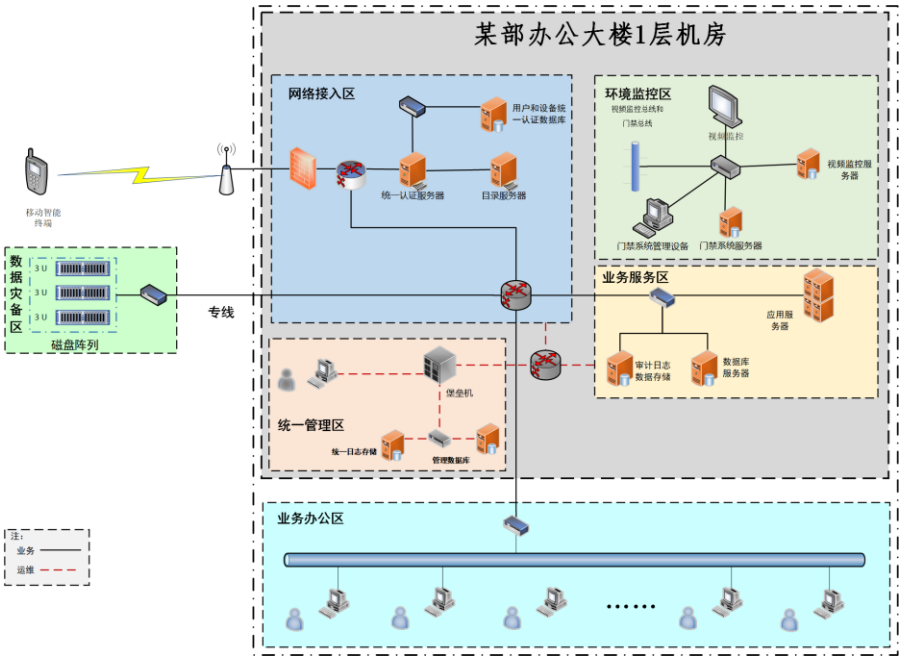

图 1 系统网络拓扑图

{该部分内容需包含系统网络拓扑、承载的业务情况等内容，梳理系统各安全层面保护对象（汇总到表 1 中）。}

*{系统网络拓扑应结合系统网络拓扑图（图 1 为示例），说明**系统体系架构、网络所在机房情况（物理机房的个数及其所在具体位置）、网络边界划分、跨网络访问的通信信道、设备组成及实现功能**等内容。承载的业务情况包含系统承载的**业务应用、业务功能、应用用户、重要数据以及关键的用户操作行为**等。}*

表 1 系统各安全层面保护对象汇总

序号	安全层面	保护对象
1	物理和环境安全	*{物理机房 1}*
2		*{物理机房 2}*
3		。。。
4		*{物理机房 n}*
5	网络和通信安全	*{通信信道 1}*
6		*{通信信道 2}*
7		。。。

序号	安全层面	保护对象
8		{通信信道 n}
9	设备和计算安全	{应用服务器}
10		{数据库服务器}
11		{数据库管理系统}
12		{服务器密码机等整理类密码产品}
13		{电子签章系统等系统类密码产品}
14		{堡垒机}
15	应用和数据安全	{应用 1}
16		{应用 2}
17		。。。
18		{应用 n}
19	管理制度	{管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）}
20	人员管理	{管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）}
21	建设运行	{密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档}
22		{管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）}
23	应急处置	{管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员）}

{进一步对应用和数据安全层面的保护对象进行梳理（汇总到表 2 中），重点

梳理各个应用具有身份鉴别（真实性）需求的应用用户，各个应用的重要数据及对应具体安全需求，各个应用具有不可否认性需求的操作行为。}

表 2 应用和数据安全层面保护对象

应用名称	类别	具体保护对象	安全需求
{应用 1}	应用用户	*{应用用户 1}*	真实性
		{应用用户 2}	真实性
		。。。	真实性
		{应用用户 n}	真实性
	重要数据	*{重要数据 1}*	□传输机密性 □存储机密性 □传输完整性 □存储完整性
		{重要数据 2}	□传输机密性 □存储机密性 □传输完整性 □存储完整性
		。。。	□传输机密性 □存储机密性 □传输完整性 □存储完整性
		{重要数据 n}	□传输机密性 □存储机密性 □传输完整性 □存储完整性
	操作行为	*{操作行为 1}*	不可否认性
		{操作行为 2}	不可否认性
		。。。	不可否认性
		{操作行为 n}	不可否认性
{应用 2}	应用用户	*{XX 应用用户}*	真实性
	重要数据	*{XX 重要数据}*	□传输机密性 □存储机密性 □传输完整性 □存储完整性
	操作行为	*{XX 操作行为}*	不可否认性
。。。	应用用户	*{XX 应用用户}*	真实性
	重要数据	*{XX 重要数据}*	□传输机密性

			□存储机密性 □传输完整性 □存储完整性
	操作行为	{XX 操作行为}	不可否认性
{应用 n}	应用用户	{XX 应用用户}	真实性
	重要数据	{XX 重要数据}	□传输机密性 □存储机密性 □传输完整性 □存储完整性
	操作行为	{XX 操作行为}	不可否认性

2 安全控制措施描述及指标适用情况

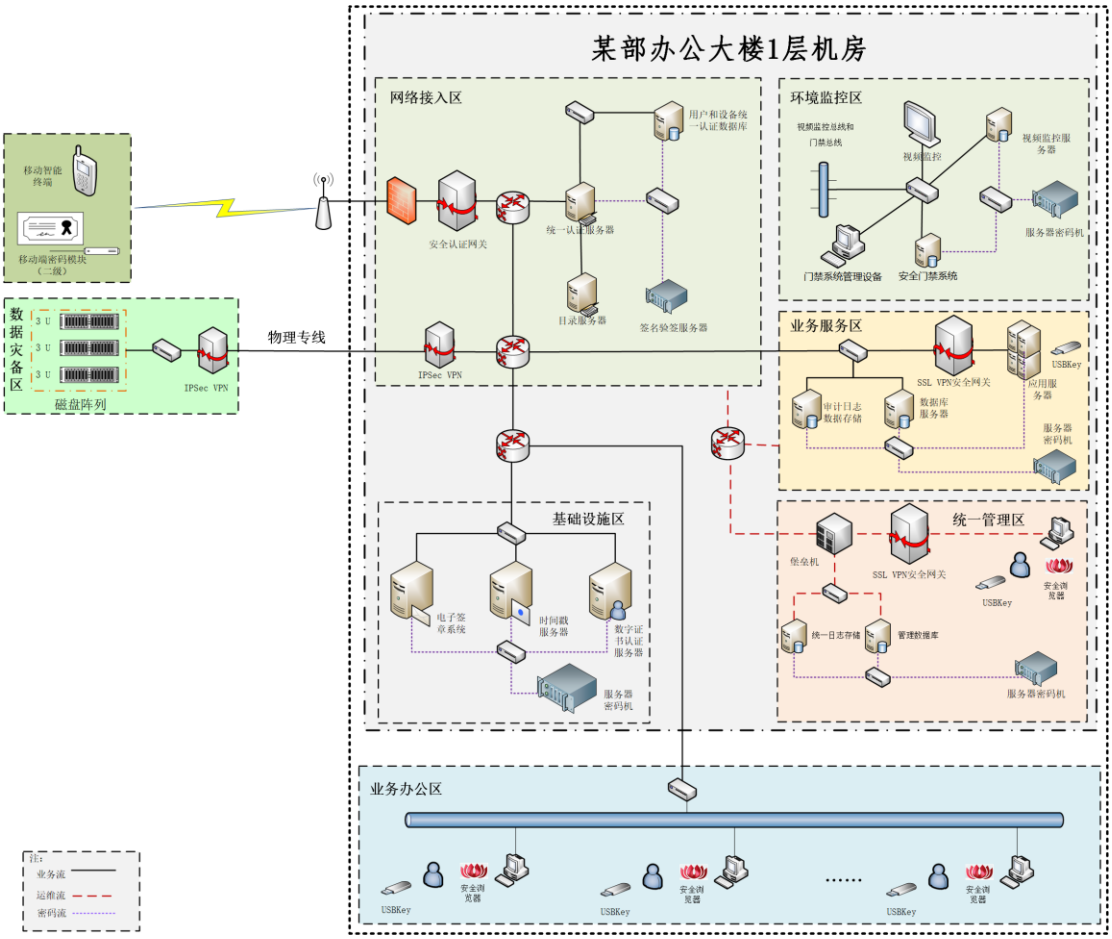

图 2 系统密码应用部署图

{结合系统密码应用部署图（图 2 为示例），概括总结每个安全层面中各个保护对象的安全控制措施（包含密码应用措施和/或风险替代措施），并汇总说明系统指标适用情况。}。

在物理和环境安全方面，XXX。

在网络和通信安全方面，XXX。

在设备和计算安全方面，XXX。

在应用和数据安全方面，XXX。

在管理制度方面，XXX。

在人员管理方面，XXX。

在建设运行方面，XXX。

在应急处置方面，XXX。

《XX 系统密码应用方案》依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第*{三}*级别要求进行设计，选取的指标总数为*{41}*项，其中确定的不适用指标*{XX}*项，具体见表 3。*{特殊指标{XX}项（见表 4）}*。*{以第三级别要求为例，按实际系统级别情况进行修改}*

表 3 指标适用情况及论证说明

安全层面	指标要求	应用要求	适用情况	不适用性论证说明
物理和环境安全	8.1 a）宜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；	宜	□适用 □不适用	*{无/XX 对象不适用，原因为 XX。}*
	8.1 b）宜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；	宜	□适用 □不适用	
	8.1 c）宜采用密码技术保证视频监控音像记录数据的存储完整性。	宜	□适用 □不适用	
网络和通信安全	8.2 a）应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；	应	适用	
	8.2 b) 宜采用密码技术保证通信过程中数据的完整性；	宜	□适用 □不适用	
	8.2 c) 应采用密码技术保证通信过程中重要数据的机密性；	应	适用	
	8.2 d) 宜采用密码技术保证网络边界访问控制信息的完整性；	宜	□适用 □不适用	
	8.2 e) 可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	可	□适用 □不适用	

	保接入的设备身份真实性。			
设备和计算安全	8.3 a) 应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；	应	适用	
	8.3 b) 远程管理设备时，应采用密码技术建立安全的信息传输通道；	应	适用	
	8.3 c) 宜采用密码技术保证系统资源访问控制信息的完整性；	宜	□适用 □不适用	
	8.3 d) 宜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；	宜	□适用 □不适用	
	8.3 e) 宜采用密码技术保证日志记录的完整性；	宜	□适用 □不适用	
	8.3 f) 宜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。	宜	□适用 □不适用	
应用和数据安全	8.4 a) 应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；	应	适用	
	8.4 b) 宜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；	宜	□适用 □不适用	
	8.4 c) 宜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；	宜	□适用 □不适用	
	8.4 d) 应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；	应	适用	
	8.4 e) 应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；	应	适用	
	8.4 f) 宜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；	宜	□适用 □不适用	
	8.4 g) 宜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；	宜	□适用 □不适用	
	8.4 h) 在可能涉及法律责任认定的应用中，宜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	宜	□适用 □不适用	

	行为的不可否认性和数据接收行为的不可否认性。			
管理制度	8.5 a）应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；	应	适用	
	8.5 b）应根据密码应用方案建立相应密钥管理规则；	应	适用	
	8.5 c）应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；	应	适用	
	8.5 d）应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；	应	适用	
	8.5 e）应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；	应	适用	
	8.5 f）应具有密码应用操作规程的相关执行记录并妥善保存。	应	适用	
人员管理	8.6 a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；	应	适用	
	8.6 b) 应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： 1) 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； 2) 对关键岗位建立多人共管机制； 3) 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，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4) 相关设备与系统的管理和使用账号不得多人共用。	应	适用	
	8.6 c) 应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	应	适用	

	业技能；			
	8.6 d) 应定期对密码应用安全岗位人员进行考核；	应	适用	
	8.6 e) 应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。	应	适用	
建设运行	8.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案；	应	适用	
	8.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录 A；	应	适用	
	8.7 c）应按照应用方案实施建设；	应	适用	
	8.7 d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；	应	适用	
	8.7 e）在运行过程中，应严格执行既定的密码应用安全管理制度，应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。	应	适用	
应急处置	8.8 a）应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，应立即启动应急处置措施，结合实际情况及时处置；	应	适用	
	8.8 b）事件发生后，应及时向信息系统主管部门进行报告；	应	适用	
	8.8 c）事件处置完成后，应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。	应	适用	
指标合计		**41 项**	**不适用指标合计**	***{XX 项}***

表 4 特殊指标及解释说明

序号	安全层面	指标要求	解释说明
1	网络和通信安全	9.2 a）应采用密码技术对通信实体进行双向	*{如系统在网络和通信层面对通信实体具有双向身份鉴别需求，三级*

		身份鉴别，保证通信实体身份的真实性。	*系统选用了四级指标。}*
2			
特殊指标合计			***{XX 项}***

3 安全控制措施评估结果

针对密码应用方案中各个安全层面保护对象所采取的安全控制措施（包含密码应用措施和/或风险替代措施）按指标进行评估，如表 5 所示。

若指标涉及的所有保护对象的相应安全控制措施有效（不存在高风险），且方案中描述的实施保障措施合理，则该指标的评估结果为通过；否则，该指标的评估结果为未通过。

表 5 安全控制措施评估结果

安全层面	指标要求	评估结果	未通过原因说明
物理和环境安全	身份鉴别	□通过 □未通过	*{具体风险分析}*
	电子门禁记录数据存储完整性	□通过 □未通过	*{具体风险分析}*
	视频监控记录数据存储完整性	□通过 □未通过	*{具体风险分析}*
网络和通信安全	身份鉴别	□通过 □未通过	*{具体风险分析}*
	通信数据完整性	□通过 □未通过	*{具体风险分析}*
	通信过程中重要数据的机密性	□通过 □未通过	*{具体风险分析}*
	网络边界访问控制信息的完整性	□通过 □未通过	*{具体风险分析}*

安全层面	指标要求	评估结果	未通过原因说明
	安全接入认证	□通过 □未通过	*{具体风险分析}*
设备和计算安全	身份鉴别	□通过 □未通过	*{具体风险分析}*
	远程管理通道安全	□通过 □未通过	*{具体风险分析}*
	系统资源访问控制信息完整性	□通过 □未通过	*{具体风险分析}*
	重要信息资源安全标记完整性	□通过 □未通过	*{具体风险分析}*
	日志记录完整性	□通过 □未通过	*{具体风险分析}*
	重要可执行程序完整性、重要可执行程序来源真实性	□通过 □未通过	*{具体风险分析}*
应用和数据安全	身份鉴别	□通过 □未通过	*{具体风险分析}*
	访问控制信息完整性	□通过 □未通过	*{具体风险分析}*
	重要信息资源安全标记完整性	□通过 □未通过	*{具体风险分析}*
	重要数据传输机密性	□通过 □未通过	*{具体风险分析}*
	重要数据存储机密性	□通过 □未通过	*{具体风险分析}*
	重要数据传输完整性	□通过 □未通过	*{具体风险分析}*

安全层面	指标要求	评估结果	未通过原因说明
	重要数据存储完整性	□通过 □未通过	*{具体风险分析}*
	不可否认性	□通过 □未通过	*{具体风险分析}*
管理制度	具备密码应用安全管理制度	□通过 □未通过	*{具体风险分析}*
	密钥管理规则	□通过 □未通过	*{具体风险分析}*
	建立操作规程	□通过 □未通过	*{具体风险分析}*
	定期修订安全管理制度	□通过 □未通过	*{具体风险分析}*
	明确管理制度发布流程	□通过 □未通过	*{具体风险分析}*
	制度执行过程记录留存	□通过 □未通过	*{具体风险分析}*
人员管理	了解并遵守密码相关法律法规和密码管理制度	□通过 □未通过	*{具体风险分析}*
	建立密码应用岗位责任制度	□通过 □未通过	*{具体风险分析}*
	建立上岗人员培训制度	□通过 □未通过	*{具体风险分析}*
	定期进行安全岗位人员考核	□通过 □未通过	*{具体风险分析}*
	建立关键岗位人员保密制度和调离制度	□通过 □未通过	*{具体风险分析}*

安全层面	指标要求	评估结果	未通过原因说明
建设运行	制定密码应用方案	□通过 □未通过	{具体风险分析}
	制定密钥安全管理策略	□通过 □未通过	{具体风险分析}
	制定实施方案	□通过 □未通过	{具体风险分析}
	投入运行前进行密码应用安全性评估	□通过 □未通过	{具体风险分析}
	定期开展密码应用安全性评估及攻防对抗演习	□通过 □未通过	{具体风险分析}
应急处置	应急策略	□通过 □未通过	{具体风险分析}
	事件处置	□通过 □未通过	{具体风险分析}
	向有关主管部门上报处置情况	□通过 □未通过	{具体风险分析}

4 方案评估结论

受{委托单位}委托，{密评机构名称}于 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日，依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》和 GM/T 0115—2021《信息系统密码应用测评要求》的第 XX{（一～四）}级相关要求，对《XX 系统密码应用方案》进行了商用密码应用安全性评估，结论为：***{通过/不通过}***[1]。

以下报告内容无正文

[1] 若所有指标的安全控制措施评估结果均为通过，且初步量化评估分数能够达到阈值要求，则方案评估结论为通过；否则为不通过。

附：《XXXX 系统密码应用方案》

报告编号：{}

XXXXX 系统

商用密码应用安全性评估报告

被测单位：_____

密评机构：_____

报告时间：_____

声 明

本报告是 XXXXX 系统的商用密码应用安全性评估报告。

本报告评估结论的有效性建立在被测单位提供相关证据的真实性基础之上。

本报告中给出的评估结论仅对被测信息系统当时的安全状态有效。被测信息系统发生变更后，应重新对其进行评估，本报告不再适用。

本报告中给出的评估结论不能作为对被测信息系统内部署的相关系统构成组件（或产品）的评估结论。

在任何情况下，若需引用本报告中的评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

{*密评机构名称*}（盖章）

年　　月　　日

被测信息系统基本信息表

<table>
<tr><th colspan="6">被测单位</th></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属省部密码管理部门</td><td colspan="5"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><th colspan="6">被测信息系统</th></tr>
<tr><td>系统名称</td><td colspan="5"></td></tr>
<tr><td>网络安全等级保护定级情况</td><td colspan="5">☐已定级，第级（一至四），SAG。
☐未定级，本次密评依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第级（一至四）信息系统要求</td></tr>
<tr><td>网络安全等级保护定级备案情况</td><td colspan="2">☐已备案
备案证明编号:
☐未备案</td><td>本次被测信息系统与等级保护定级系统是否一致</td><td colspan="2">☐是
☐否，变化情况说明:</td></tr>
<tr><td>网络安全等级保护测评情况</td><td colspan="5">☐已测评
测评机构名称:　　测评时间:
测评结论:
☐正在测评
测评机构名称:
☐未测评</td></tr>
<tr><td rowspan="3">系统服务情况</td><td>服务范围</td><td colspan="4">☐全国　　☐跨省（区、市）跨个
☐全省（区、市）　　☐跨地（市、区）跨个
☐地（市、区）内　　☐其他</td></tr>
<tr><td>服务领域</td><td colspan="4">☐电信　☐广电　☐经营性公众互联网　☐铁路　☐银行　☐海关　☐税务　☐民航　☐电力　　☐证券　☐保险　☐国防科技工业　☐公安　☐财政　☐人事劳动和社会保障　☐审计　☐商业贸易　☐国土资源　☐能源　☐交通　☐统计　☐工商行政管理　☐邮政　☐教育　☐文化　☐卫生　☐农业　☐水利　☐外交　☐发展改革　☐科技　☐宣传　☐质量监督检验检疫　　☐其他</td></tr>
<tr><td>服务对象</td><td colspan="4">☐单位内部人员　　☐社会公众人员
☐两者均包括☐其他</td></tr>
</table>

<table>
<tr><td rowspan="2">系统网络平台</td><td>覆盖范围</td><td colspan="4">□局域网　□城域网　□广域网　□其他</td></tr>
<tr><td>网络性质</td><td colspan="4">□业务专网　□互联网　□其他</td></tr>
<tr><td>系统服务用户数量</td><td colspan="5">大概数量级/被测系统处于建设阶段</td></tr>
<tr><td>系统是否已投入运行</td><td colspan="5">□是，投入运行时间：年 月
□否，目前情况：_____</td></tr>
<tr><td>系统互联情况</td><td colspan="5">□与其他行业系统连接□与本行业其他单位系统连接
□与本单位其他系统连接　　□其他</td></tr>
<tr><td rowspan="3">系统是否具有密码应用方案</td><td colspan="5">□有密码应用方案，且通过评审，评审通过时间：
评审方式：□专家评审　□密评机构评审，密评机构名称：</td></tr>
<tr><td colspan="5">□有密码应用方案，但未通过评审</td></tr>
<tr><td colspan="5">□无密码应用方案</td></tr>
<tr><td>系统使用的密码产品情况</td><td colspan="5">□系统使用的密码产品（台／套），独立使用（台／套），共享使用（台／套）；其中，取得认证证书的产品数量台／套，未取得认证证书的国内产品数量（台／套），国外产品数量（台／套）。
□系统未使用密码产品</td></tr>
<tr><td>系统使用的密码算法</td><td colspan="5">分组算法：□SM1 □SM4 □SM7 □AES □DES □3DES □其他
非对称算法：□SM2 □SM9 □RSA1024 □RSA2048 □其他
杂凑算法：□SM3 □SHA-1 □SHA-256 □SHA-384 □SHA-512 □MD5 □其他
序列算法：□ZUC □其他
其他算法：</td></tr>
<tr><td colspan="6">密评机构</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>通信地址</td><td colspan="3"></td><td>邮政编码</td><td></td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="2"></td></tr>
<tr><td>所属部门</td><td></td><td>办公电话</td><td colspan="2"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td rowspan="3">审核批准</td><td>编制人</td><td>（签字）</td><td>编制日期</td><td colspan="2"></td></tr>
<tr><td>审核人</td><td>（签字）</td><td>审核日期</td><td colspan="2"></td></tr>
<tr><td>批准人</td><td>（签字）</td><td>批准日期</td><td colspan="2"></td></tr>
</table>

商用密码应用安全性评估结论

系统名称			
系统简介			
测评情况简介	（简要描述测评范围和主要内容。建议不超过 200 字。）		
评估结论	{*符合/基本符合/不符合*}	**综合得分**	
不适用项数目/总测评指标项数目	{*X/Y*}	**高风险项数目**	

总体评价

本次信息系统商用密码应用安全性评估依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{*X*}级别要求，选取的测评指标总数为 XXX 项，其中不适用项为 XXX 项，特殊指标 XXX 项。测评结果为：符合项 XXX 项，部分符合项 XXX 项，不符合项 XXX 项。其中，在部分符合和不符合项中：高风险项 XXX 项，中风险项 XXX 项，低风险项 XXX 项。

1. 在物理和环境安全方面，XXX
2. 在网络和通信安全方面，XXX
3. 在设备和计算安全方面，XXX
4. 在应用和数据安全方面，XXX
5. 在管理制度方面，XXX
6. 在人员管理方面，XXX
7. 在建设运行方面，XXX
8. 在应急处置方面，XXX

通过对 XXXXX 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、管理制度、人员管理、建设运行和应急处置等方面的测评，该系统{*符合/基本符合/不符合*}GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{*X*}级别要求。

安全问题及改进建议

本次信息系统商用密码应用安全性评估依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{*X*}级别要求，发现被测信息系统存在以下安全问题。建议被测信息系统根据实际情况和以下给出的建议进行整改。

1. 物理和环境安全

问题描述：

改进建议：

2. 网络和通信安全

问题描述：

改进建议：

3. 设备和计算安全

问题描述：

改进建议：

4. 应用和数据安全

问题描述：

改进建议：

5. 管理制度

问题描述：

改进建议：

6. 人员管理

问题描述：

改进建议：

7. 建设运行

问题描述：

改进建议：

8. 应急处置

问题描述：

改进建议：

目录

声 明 I

被测信息系统基本信息表 I

商用密码应用安全性评估结论 III

总体评价 IV

安全问题及改进建议 V

1 **测评项目概述** 1

1.1 测评目的 1

1.2 测评依据 1

1.2.1 依据标准和规范 1

1.2.2 参考标准和规范 1

1.2.3 术语和缩略语 1

1.3 测评过程 1

1.3.1 测评准备阶段 2

1.3.2 方案编制阶段 3

1.3.3 现场测评阶段 3

1.3.4 分析与报告编制阶段 3

1.4 报告分发范围 4

2 **被测系统情况** 5

2.1 承载的业务情况 5

2.2 网络拓扑图及描述 5

2.3 密码应用情况 5

2.3.1 物理和环境安全密码应用情况 5

2.3.2 网络和通信安全密码应用情况 5

2.3.3 设备和计算安全密码应用情况 5

2.3.4 应用和数据安全密码应用情况 5

2.4 系统资产 5

2.4.1 物理环境 5

2.4.2 物理安防设施 6
2.4.3 密码产品 6
2.4.4 服务器/存储设备 6
2.4.5 网络及安全设备 6
2.4.6 数据库管理系统 7
2.4.7 关键业务应用 7
2.4.8 重要数据 7
2.4.9 安全管理文档 8
2.4.10 人员 8
2.5 密码服务 8
2.6 安全威胁 8
2.7 前次测评情况 10
3 测评范围与方法 11
3.1 测评指标 11
3.1.1 基本指标 11
3.1.2 特殊指标 14
3.1.3 不适用指标 14
3.2 测评方法及工具 14
3.2.1 现场测评方法 14
3.2.2 测评工具 15
3.2.3 测评工具检查点 15
3.3 测评对象和对应测评方式 15
3.3.1 测评对象确定方法 15
3.3.2 测评对象确定结果 15
4 单元测评 19
4.1 密码技术应用要求 19
4.1.1 物理和环境安全 19
4.1.2 网络和通信安全 19

4.1.3 设备和计算安全 20
4.1.4 应用和数据安全 20
4.2 安全管理 22
4.2.1 管理制度 22
4.2.2 人员管理 23
4.2.3 建设运行 24
4.2.4 应急处置 25
5 **整体测评** 26
5.1 测评结果修正 26
5.2 整体测评结果和量化评估 26
6 **风险分析** 29
7 **评估结论** 30
附录 A 测评结果记录 31
A.1. 物理和环境安全 31
A.2. 网络和通信安全 33
A.3. 设备和计算安全 35
A.4. 应用和数据安全 37
A.5. 管理制度 43
A.6. 人员管理 44
A.7. 建设运行 45
A.8. 应急处置 48

1 测评项目概述

1.1 测评目的

{*密评机构*}受{*被测单位*}的委托，于 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日，依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{*X*}级别要求，对{*被测单位*}的 XXXXX 系统从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面进行商用密码应用安全性评估，通过测评项目的实施，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。

1.2 测评依据

1.2.1 依据标准和规范

- GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》
- GM/T 0115—2021《信息系统密码应用测评要求》
- GM/T 0116—2021《信息系统密码应用测评过程指南》
- 《信息系统密码应用高风险判定指引》
- 《商用密码应用安全性评估量化评估规则》
- 《XXXXX 系统密码应用方案》（如有）

1.2.2 参考标准和规范

- 被测信息系统专用的标准（如 CA 系统所要参考的 GM/T 0034 等标准，金融 IC 卡信息系统所要参考的 PBOC 等标准）

1.2.3 术语和缩略语

1.3 测评过程

商用密码应用安全性评估过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。测评工作流程如图 1-1 所示。

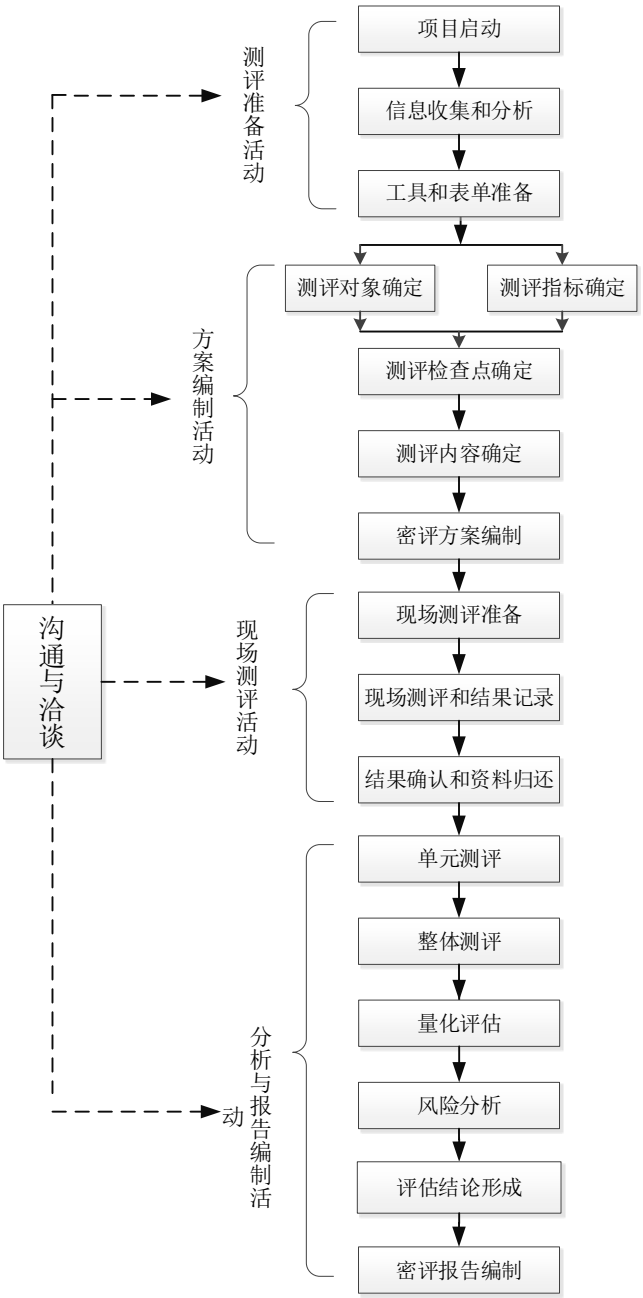

图 1-1 测评工作流程

1.3.1 测评准备阶段

根据测评双方签订的委托测评协议书和被测信息系统规模，密评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。密评机构通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和密码保护情况，为编写密评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测信息系统相关的各种组件、调试测评工具、准备各种表单等。

测评准备阶段时间：XX 年 XX 月 XX 日- XX 年 XX 月 XX 日。

测评项目组成员如表 1-1 所示：

表 1-1 测评项目组成员

角色	姓名	任务分工
项目负责人		
测评项目组成员		

1.3.2 方案编制阶段

根据已经了解到的被测信息系统情况，分析整个被测系统及其涉及的业务应用系统，以及与此相关的密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；确认测评过程中需要现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最大限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容；最终完成测评方案的编制。

方案编制阶段时间：XX 年 XX 月 XX 日- XX 年 XX 月 XX 日。

1.3.3 现场测评阶段

现场测评准备：召开测评现场首次会，密评机构介绍测评工作，交流测评信息，进一步明确测评计划和测评方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。测评双方确认现场测评需要的各种资源，包括被测单位的配合人员和需要提供的测评条件等，确认被测信息系统已备份过系统及数据。被测单位签署现场测评授权书。密评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

测评项目组根据密评方案以及现场测评准备的结果，安排密评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认；密评机构归还测评过程中借阅的所有文档资料，并由被测单位文档资料提供者签字确认。

现场测评阶段时间：XX 年 XX 月 XX 日- XX 年 XX 月 XX 日。

1.3.4 分析与报告编制阶段

在现场测评工作结束后，密评机构对现场测评获得的测评结果进行汇总分析，形成评估结论，并编制评估报告。

密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，有的测评对象的测评结果可能会有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。

分析与报告编制阶段时间：XX 年 XX 月 XX 日- XX 年 XX 月 XX 日。

1.4 报告分发范围

本报告一式 X 份，其中 X 份提交密码管理部门，X 份提交被测单位，X 份由密评机构留存。

2 被测系统情况

2.1 承载的业务情况

{*主要介绍信息系统承载的业务情况，重点说明业务的密码应用需求，具体的写法可以参考《商用密码应用与安全性评估》第五章*}

2.2 网络拓扑图及描述

{*主要介绍信息系统的完整网络拓扑，方便了解信息系统边界、资产等基本情况，具体的写法可以参考《商用密码应用与安全性评估》第五章*}

2.3 密码应用情况

2.3.1 物理和环境安全密码应用情况

{*介绍物理和环境安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由密码产品完成，且与信息系统承载的业务关联性较低，因此可以主要围绕所使用的密码产品展开介绍*}

2.3.2 网络和通信安全密码应用情况

{*介绍网络和通信安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由 VPN 等密码产品完成，因此可以主要围绕所使用的密码产品展开介绍*}

2.3.3 设备和计算安全密码应用情况

{*介绍设备和计算安全层面密码应用的大致情况。考虑到该层面的密码应用流程和密钥管理主要由密码产品完成，且与信息系统承载的业务关联性较低，因此可以主要围绕所使用的密码产品展开介绍*}

2.3.4 应用和数据安全密码应用情况

{*详细介绍应用和数据安全层面的密码应用情况。这部分是重点，与信息系统承载的业务息息相关，建议分为密码应用工作流程和密钥体系两方面分别介绍。具体的写法可以参考《商用密码应用与安全性评估》第五章*}

2.4 系统资产

2.4.1 物理环境

表 2-1 物理环境

序号	物理环境名称	物理位置	重要程度
1			

2.4.2 物理安防设施

表 2-2 物理安防设施

序号	产品名称	生产厂商和型号	所在物理环境名称	重要程度
1				
2				

2.4.3 密码产品

表 2-3 密码产品

序号	产品名称	生产厂商	商密产品认证证书编号	使用的密码算法	数量	用途
1						
2						
3						
4						

2.4.4 服务器/存储设备

表 2-4 服务器/存储设备

序号	设备名称	生产厂商	型号	操作系统版本	是否为虚拟设备	用途	数量	重要程度
1								
2								
3								

2.4.5 网络及安全设备

表 2-5 网络及安全设备

序号	设备名称	生产厂商	型号	用途 （包括涉及的密码技术）	数量	重要程度
1						
2						
3						
4						
5						

2.4.6 数据库管理系统

表 2-6 数据库管理系统

序号	数据库管理系统名称	版本	部署位置	主要功能	重要程度
1					
2					
3					
4					
5					

2.4.7 关键业务应用

表 2-7 关键业务应用

序号	应用名称	版本	部署位置	主要功能
1				
2				
3				
4				
5				

2.4.8 重要数据

表 2-8 重要数据

序号	数据	描述	所属应用	存储位置	安全需求
1					机密性/真实性/完整性
2					
3					

2.4.9 安全管理文档

表 2-9 安全管理文档

序号	文档名称	主要内容
1		
2		
3		

2.4.10人员

表 2-10 人员

序号	姓名	岗位/角色	职责说明	联系方式
1				
2				
3				

2.5 密码服务

表 2-11 密码服务

序号	密码服务名称	密码服务提供商
1		
2		

2.6 安全威胁

表 2-12 安全威胁

序号	威胁类别	威胁分类
TP1	物理和环境	非法人员进入物理环境，对软硬件设备和数据进行直接破坏
TP2		物理进出记录和视频记录遭到篡改，以掩盖非法人员进出情况

TN1	网络和通信	非法通信实体接入网络
TN2		通信数据在信息系统外部被非授权的截取、篡改
TN3		非法设备从外部接入内部网络，或网络边界被破坏
TD1	设备和计算	设备被非法人员登录
TD2		搭建的远程管理通道被非法使用，或传输的管理数据被非授权获取和篡改
TD3		设备资源被登录设备的其他用户获取
TD4		重要信息资源安全标记被非授权获取和篡改
TD5		设备日志记录被非法篡改，以掩盖非法操作
TD6		设备内重要程序和文件的来源不可信
TA1	应用和数据	应用被非法人员登录
TA2		应用资源被登录应用的其他用户获取
TA3		重要信息资源安全标记被非授权获取和篡改
TA4		传输或存储的数据被外部攻击者非法获取
TA5		某个应用传输或存储的数据被其他应用获取
TA6		应用日志记录被非法篡改，以掩盖非法操作
TA7		应用程序、重要应用配置等重要信息被非法修改
TA8		数据发送者或接收者不承认发送或接受到数据，或者否认所做的操作和交易
TK1	密钥管理和安全管理	生成的密钥缺少随机性，被攻击者猜测
TK2		密钥被非法获取
TK3		密钥被非法篡改，或密钥与实体之间的关联关系被非法篡改
TK4		密钥被非法使用
TK5		密钥备份和归档机制不健全，导致密钥泄露，或密钥被恢复到非法的设备中
TK6		密钥销毁不及时导致密钥泄露，或销毁的密钥被恶意恢复
TK7		安全管理制度和密钥管理策略等不完善，管理流程不健全，执行不到位，职责不明确，导致密钥泄露、数据泄露等风险

2.7 前次测评情况

本次测评是被测信息系统进行的第___次商用密码应用安全性评估，上次评估时间为___年____月____日，评估结论为：_____。

3 测评范围与方法

3.1 测评指标

3.1.1 基本指标

{根据被测信息系统密码应用安全要求等级，选择GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》中对应级别的安全要求作为本次测评工作的基本指标，在表3-1 中列出指标。}

表 3-1GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》{第三级别}要求基本指标

测评指标			测评指标描述	应用要求
技术要求	物理和环境安全	身份鉴别	8.1 a）宜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；	宜
		电子门禁记录数据存储完整性	8.1 b）宜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；	宜
		视频监控记录数据存储完整性	8.1 c）宜采用密码技术保证视频监控音像记录数据的存储完整性。	宜
	网络和通信安全	身份鉴别	8.2 a）应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；	应
		通信数据完整性	8.2 b)宜采用密码技术保证通信过程中数据的完整性；	宜
		通信过程中重要数据的机密性	8.2 c) 应采用密码技术保证通信过程中重要数据的机密性；	应
		网络边界访问控制信息的完整性	8.2 d)宜采用密码技术保证网络边界访问控制信息的完整性；	宜
		安全接入认证	8.2 e)可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，确保接入的设备身份真实性。	可
	设备和计算安全	身份鉴别	8.3 a)应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；	应
		远程管理通道安全	8.3 b)远程管理设备时，应采用密码技术建立安全的信息传输通道；	应
		系统资源访问控制信息完整性	8.3 c)宜采用密码技术保证系统资源访问控制信息的完整性；	宜
		重要信息资源安	8.3 d)宜采用密码技术保证设备中的重要信息资源安	宜

		全标记完整性	全标记的完整性；	
		日志记录完整性	8.3 e)宜采用密码技术保证日志记录的完整性；	宜
		重要可执行程序完整性、重要可执行程序来源真实性	8.3 f)宜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。	宜
	应用和数据安全	身份鉴别	8.4 a)应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；	应
		访问控制信息完整性	8.4 b)宜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；	宜
		重要信息资源安全标记完整性	8.4 c)宜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；	宜
		重要数据传输机密性	8.4 d)应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；	应
		重要数据存储机密性	8.4 e)应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；	应
		重要数据传输完整性	8.4 f)宜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；	宜
		重要数据存储完整性	8.4 g)宜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；	宜
		不可否认性	8.4 h)在可能涉及法律责任认定的应用中，宜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。	宜
管理要求	管理制度	具备密码应用安全管理制度	8.5 a）应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；	应
		密钥管理规则	8.5 b）应根据密码应用方案建立相应密钥管理规则；	应
		建立操作规程	8.5 c）应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；	应
		定期修订安全管理制度	8.5 d）应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；	应
		明确管理制度发布流程	8.5 e）应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；	应
		制度执行过程记	8.5 f）应具有密码应用操作规程的相关执行记录并妥	应

		录留存	善保存。	
	人员管理	了解并遵守密码相关法律法规和密码管理制度	8.6 a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；	应
		建立密码应用岗位责任制度	8.6 b)应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： 1) 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； 2) 对关键岗位建立多人共管机制； 3) 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，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4) 相关设备与系统的管理和使用账号不得多人共用。	应
		建立上岗人员培训制度	8.6 c) 应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；	应
		定期进行安全岗位人员考核	8.6 d) 应定期对密码应用安全岗位人员进行考核；	应
		建立关键岗位人员保密制度和调离制度	8.6 e)应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。	应
	建设运行	制定密码应用方案	8.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案；	应
		制定密钥安全管理策略	8.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录 B；	应
		制定实施方案	8.7 c）应按照应用方案实施建设；	应
		投入运行前进行密码应用安全性评估	8.7 d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；	应
		定期开展密码应用安全性评估及攻防对抗演习	8.7 e）在运行过程中，应严格执行既定的密码应用安全管理制度，应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。	应
	应急处	应急策略	8.8 a）应制定密码应用应急策略，做好应急资源准备，	应

	置		当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；	
		事件处置	8.8 b）事件发生后，应及时向信息系统主管部门进行报告；	应
		向有关主管部门上报处置情况	8.8 c）事件处置完成后，应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。	应
测评指标合计		41 项		

3.1.2 特殊指标

{*结合被测评单位要求、被测系统的实际安全需求以及安全最佳实践经验，以列表形式给出 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》未覆盖（如行业标准）或者高于 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》中被测系统相应等级的安全要求，其中标准需要在 1.2.2 中写明*}

3.1.3 不适用指标

鉴于信息系统的复杂性和特殊性，GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》的第{*X*}级要求中的个别项可能不适用于被测信息系统，对于这些不适用项及其不适用原因如表 3-2 所示：

表 3-2 不适用指标及说明

安全层面	测评指标	测评指标描述	不适用原因
物理和环境			
网络和通信			
设备和计算			
……			
不适用项合计			

3.2 测评方法及工具

3.2.1 现场测评方法

本次商用密码应用安全性评估使用的测评方法包括：

- 访谈：通过与被测单位的相关人员进行交谈和问询，了解被测信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

- 文档审查：审核被测单位提交的有关信息系统安全的各个方面的文档，如：被测系统总体描述文件，被测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，被测单位的信息化建设与发展状况以及联络方式；密码应用方案及评审意见，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，自查或上次评估报告等等。通过对这些文档的审核与分析确认测评的相关内容是否达到安全保护等级的要求；
- 实地查看：现场查看测评对象所处的环境、外观等情况；
- 配置检查：查看测评对象的相关配置；
- 工具测试：根据被测信息系统的实际情况，密评人员使用适合的技术工具对其进行测试。

3.2.2 测评工具

本次商用密码应用安全性评估使用的测评工具如表 3-3 所示：

表 3-3 测评工具

序号	工具名称	版本	生产厂商	工具说明
1				
2				
3				
4				
5				

3.2.3 测评工具检查点

{*描述在何处接入何种测评工具进行何种测试工作，可参考《商用密码应用与安全性评估》*

示例：检查点 A：检查点描述(并在图中标明)，在检查点 A 进行抓包，查看 XX 和 XX 之间的通信报文是否是加密的，算法标识是否为 XX。}

3.3 测评对象和对应测评方式

3.3.1 测评对象确定方法

依据《信息系统密码应用测评过程指南》的测评对象确定方法，根据被测信息系统的重要程度及其相关资产等的价值认定结果，明确核心资产在信息系统内的流转，从而确定与密码相关的测评对象。

3.3.2 测评对象确定结果

3.3.2.1 密码技术应用测评

3.3.2.1.1 物理和环境安全测评

表 3-4 物理和环境安全测评对象

序号	测评对象	测评方式	说明
1	XXXX 机房	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	
2	XXXX 机房	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	

3.3.2.1.2 网络和通信安全测评

表 3-5 网络和通信安全测评对象

序号	测评对象	测评方式	说明
1	外部客户端与 XXXXX 系统的通信信道	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	
2	集中管理通道	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	

3.3.2.1.3 设备和计算安全测评

表 3-6 设备和计算安全测评对象

序号	测评对象	测评方式	说明
1	密码产品/设备	□访谈 □文档审查 □实地查看	

		□配置检查 □工具测试	
2	通用服务器	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	
3	其他涉及设备	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	

3.3.2.1.4 应用和数据安全测评

表 3-7 应用和数据安全测评对象

序号	测评对象	测评方式	说明
1	XXX 应用	□访谈 □文档审查 □实地查看 □配置检查 □工具测试	

3.3.2.2 安全管理测评

表 3-8 安全管理测评对象

序号	测评单元	测评对象	测评方式	说明
1	管理制度	{*管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）*}	□访谈 □文档审查	
2	人员管理	{*管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）*}	□访谈 □文档审查	
3	建设运行	{*密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档*}	□访谈 □文档审查	
4		{*管理体系（包括安全管理制度类文档、记*	□访谈	

		录表单类文档、系统相关人员）}	□文档审查	
5	应急处置	{*管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员*）}	□访谈 □文档审查	

4 单元测评

4.1 密码技术应用要求

4.1.1 物理和环境安全

4.1.1.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-1 所示：

表 4-1 物理和环境安全测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）		
		身份鉴别	电子门禁记录数据存储完整性	视频监控记录数据存储完整性
1	*{XXXX 机房}*			
2	*{YYYY 机房}*			
单元测评结果（符合/部分符合/不符合/不适用）				

4.1.1.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.1.2 网络和通信安全

4.1.2.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-2 所示：

表 4-2 网络和通信安全测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）				
		身份鉴别	通信数据完整性	通信过程中重要数据的机密性	网络边界访问控制信息的完整性	安全接入认证
1	*{外部客户端与 XXXXX 系统的通信信道}*					
2	*{系统管理员*					

	从外部进行管理所使用的集中管理通道}					
单元测评结果（符合/部分符合/不符合/不适用）						

4.1.2.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.1.3 设备和计算安全

4.1.3.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-3 所示：

表 4-3 设备和计算安全测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）					
		身份鉴别	远程管理通道安全	系统资源访问控制信息完整性	重要信息资源安全标记完整性	日志记录完整性	重要可执行程序完整性、重要可执行程序来源真实性
1	*{密码产品/设备}*						
2	*{通用服务器}*						
3	*{其他涉及设备}*						
单元测评结果（符合/部分符合/不符合/不适用）							

4.1.3.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.1.4 应用和数据安全

4.1.4.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-4 所示：

表 4-4 应用和数据安全测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）							
		身份鉴别[1]	访问控制信息完整性	重要信息资源安全标记完整性	重要数据传输机密性[2]	重要数据存储机密性	重要数据传输完整性	重要数据存储完整性	不可否认性[3]
1	{*信息化办公系统应用*}								
2	其他								
单元测评结果（符合/部分符合/不符合/不适用）									

针对应用和数据安全层面身份鉴别情况进行说明和汇总，如表 4-5 所示：

表 4-5 应用和数据安全身份鉴别测评结果汇总

序号	应用用户	身份鉴别
1	{*OA 办公系统管理员用户*}	
2	{*OA 办公系统业务用户*}	
3	{*公文管理系统管理员用户*}	
4	{*公文管理系统业务用户*}	
单元测评结果（符合/部分符合/不符合/不适用）		

针对应用和数据安全层面重要数据的机密性和完整性保护情况进行说明和汇总，如表 4-6 所示：

[1]“身份鉴别”单元测评结果得出过程详见表 4-5。

[2]“重要数据传输机密性”“重要数据存储机密性”“重要数据传输完整性”“重要数据存储完整性”单元测评结果得出过程详见表 4-6。

[3]“不可否认性”单元测评结果得出过程详见表 4-7。

表 4-6 应用和数据安全重要数据测评结果汇总

序号	重要数据	传输机密性	存储机密性	传输完整性	存储完整性
1	{*OA 办公系统管理员用户登录口令*}				
2	{*OA 办公系统业务用户登录口令*}				
3	{*OA 办公系统业务报表*}				
4	{*OA 办公系统办公文件数据*}				
5	{*OA 办公系统业务日志*}				
6	{*公文管理系统管理员用户登录口令*}				
7	{*公文管理系统业务用户登录口令*}				
8	{*公文管理系统业务数据*}				
9	{*公文管理系统业务日志*}				
单元测评结果（符合/部分符合/不符合/不适用）					

针对应用和数据安全层面不可否认性情况进行说明和汇总，如表 4-7 所示：

表 4-7 应用和数据安全不可否认性测评结果汇总

序号	操作行为	不可否认性
1	{*OA 办公系统业务用户文件审批操作*}	
2	{*公文管理系统业务用户公文签发操作*}	
单元测评结果（符合/部分符合/不符合/不适用）		

4.1.4.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.2 安全管理

4.2.1 管理制度

4.2.1.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-8 所示：

表 4-8 管理制度测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）					
		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
1	{*管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）*}						
单元测评结果（符合/部分符合/不符合/不适用）							

4.2.1.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.2.2 人员管理

4.2.2.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-9 所示：

表 4-9 人员管理测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）				
		了解并遵守密码相关法律法规	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	建立关键岗位人员保密制度和调离制度

		和密码管理制度				
1	{管理体系(包括安全管理制度类文档、记录表单类文档、系统相关人员)}					
单元测评结果（符合/部分符合/不符合/不适用）						

4.2.2.2 结果分析

{主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。}

4.2.3 建设运行

4.2.3.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-10 所示：

表 4-10 建设运行测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）				
		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
1	{密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档}					
2	{管理体系(包括安全管理制度类文档、记录表单类文档、系统相关人员)}					
单元测评结果（符合/部分符合/不符合/不适用）						

4.2.3.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

4.2.4 应急处置

4.2.4.1 结果汇总

针对不同测评单元，对各个测评对象的测评结果进行汇总和统计，如表 4-11 所示：

表 4-11 应急处置测评结果汇总

序号	测评对象	测评指标符合情况（符合/部分符合/不符合/不适用）		
		应急策略	事件处置	向有关主管部门上报处置情况
1	{*管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员）*}			
单元测评结果（符合/部分符合/不符合/不适用）				

4.2.4.2 结果分析

{*主要对单元测评结果进行分析，简单介绍系统在该安全层面的符合情况，以及判定依据等。*}

5 整体测评

5.1 测评结果修正

针对各个“部分符合”及“不符合”测评指标要求的测评对象，分析与其相关的其他单元、其他层面的测评对象能否和它发生关联关系，发生何种的关联关系，这些关联关系产生的作用是否可以“弥补”该测评对象的不足，以及该测评对象的不足是否会影响与其有关联关系的其他测评对象的测评结果。

表 5-1 测评结果修正

序号	安全层面	测评单元	测评对象	经弥补前的测评结果/分值	经弥补后的测评结果/分值[4]	弥补原因及相关测评对象
1	{*应用和数据安全*}	{*重要数据传输机密性*}	对象 1	{*不符合/0*}	{*部分符合/0.5*}	{*示例：该测评对象在应用和数据安全层面明文传输，测评对象原始分值为0。在网络和通信安全层面，通过部署经商用密码检测认证的SSL VPN建立安全传输通道（国密SSL 协议），对传输数据进行机密性保护，分值为1 分，经网络和通信安全层面弥补后，该测评对象分值为0.5。*}
			对象 2	{*部分符合/0.25*}	{*部分符合/0.5*}	
2		测评单元 2	对象 1			
			……			
……		……	……			

5.2 整体测评结果和量化评估

[4]若测评对象 A 弥补了测评对象 B 的不足，测评对象 A 的分值为 P_A，测评对象 B 的弥补前分值为 P_B，则测评对象 B 弥补后的分值为 MAX(0.5×P_A, P_B)，即 0.5×P_A 和 P_B 之间的较大值。

修正后的整体测评结果和量化评估汇总如表 5-2 所示。其中，测评单元得分的计算过程参见附录 A。

表 5-2 整体测评结果

层面（类）	测评单元	符合情况				测评单元得分 $S_{i,j}$	安全层面得分情况 $S_i = \frac{\sum_{1\le j\le n_i} w_{i,j}S_{i,j}}{\sum_{1\le j\le n_i} w_{i,j}}$
		符合	部分符合	不符合	不适用		
物理和环境安全	身份鉴别						
	电子门禁记录数据存储完整性						
	视频监控记录数据存储完整性						
网络和通信安全	身份鉴别						
	通信数据完整性						
	通信过程中重要数据的机密性						
	网络边界访问控制信息的完整性						
	安全接入认证						
设备和计算安全	身份鉴别						
	远程管理通道安全						
	系统资源访问控制信息完整性						
	重要信息资源安全标记完整性						
	日志记录完整性						
	重要可执行程序完整性、重要可执行程序来源真实性						
应用和数据安全	身份鉴别						
	访问控制信息完整性						
	重要信息资源安全标记完整性						
	重要数据传输机密性						
	重要数据存储机密性						
	重要数据传输完整性						
	重要数据存储完整性						
	不可否认性						
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						
	建立关键岗位人员保密制度和调离制度						
建设运行	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	应急策略						
	事件处置						
	向有关主管部门上报处置情况						
合计							
符合情况		**符合**	**部分符合**	**不符合**	**不适用**	**综合得分** $\frac{\sum_{1\le i\le n} w_i \cdot S_i}{\sum_{1\le i\le n} w_i} \times 100$	

6 风险分析

具体地，根据威胁类型和威胁发生频率，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。根据资产价值的高低，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测系统的业务信息安全造成的影响程度，影响程度取值范围为高、中和低。综合以上的结果，密评机构根据自身经验和相关国家标准要求，对被测系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。结合被测系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。如果存在高风险项，则认为信息系统面临高风险；同时也需要考虑多个中低风险叠加可能导致的高风险问题。

{*根据《商用密码应用安全性评估高风险判定指引》判定系统是否存在高风险。经风险分析，系统存在高风险 X 项，中风险 X 项，低风险 X 项，具体见表 6-1：*}

表 6-1 风险分析

序号	安全层面	问题描述	关联威胁	风险分析	风险等级		
					高	中	低
1					1	0	0
2							
统计							

7 评估结论

{*综合上述几章节的测评与风险分析结果，根据符合性判定依据给出商用密码应用安全性评估结论。*}

通过对{*被测单位*}{*被测系统*}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、管理制度、人员管理、建设运行和应急处置等方面的测评，该系统综合得分为*{XX}*分，系统密码应用面临*{高/中/低}*风险，{*符合/基本符合/不符合*}GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的第*{X}*三级别要求[5]。

[5]评估结论判定规则如下：

- 综合得分 100 分，结论为符合；
- 综合得分小于 100 分、不低于 60 分，且系统密码应用无高风险，结论为基本符合；
- 否则，结论为不符合。

附录 A 测评结果记录

A.1. 物理和环境安全

表 A-1 物理和环境安全测评结果记录

测评单元	测评对象	结果记录	量化指标				测评单元得分 $S_{i,j} = \frac{\sum_{1 \le k \le n_{i,j}} S_{i,j,k}}{n_{i,j}}$
			密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K	测评对象评分 $S_{i,j,k}$	
身份鉴别	*{XXXX 机房}*	经访谈机房相关管理员、安全主管，审查电子门禁系统/视频监控系统相关技术文档，以及实地检查电子门禁系统和视频监控系统后核实：机房访问人员使用生物识别（指纹）方式实现机房进出的身份鉴别，如图 X-X。未使用商用密码技术对机房访问人员做身份鉴别。基本原理为登记指纹-刷指纹-将鉴别数据传给后台系统-比对是否与数据库中登记信息相同；登记或刷指纹的鉴别数据通过专线传至数据库。机房为双道门。电子门禁断电后，将处于全开状态。					
	{YYYY 机房}						

电子门禁记录数据存储完整性	*{XXXX 机房}*	未使用商用密码技术保护电子门禁系统进出记录完整性。但电子门禁系统的登录具有身份鉴别机制，登录后才可对访问记录操作，允许管理员删除访问记录，图 X-X。电子门禁系统登录时身份鉴别方式为用户名+口令，管理员口令设置为 8 位字符，更新周期为半年。					
	{YYYY 机房}						
视频监控记录数据存储完整性	*{XXXX 机房}*	未使用商用密码技术实现监控记录的完整性保护。采用 RAID5 的数据冗余技术（奇偶校验码）防止监控记录的丢失。视频监控设备被“面对面”放置，确保可以全方位监控机房内动态，图 X-X。监控记录可保存 90 天。视频监控系统登录时身份鉴别方式为用户名+口令，口令长度设置为 9 个字符，更新周期为半年。					
	{YYYY 机房}						

A.2. 网络和通信安全

表 A-2 网络和通信安全测评结果记录

测评单元	测评对象	结果记录	量化指标				测评单元得分 $S_{i,j} = \frac{\sum_{1 \le k \le n_{i,j}} S_{i,j,k}}{n_{i,j}}$
			密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K	测评对象评分 $S_{i,j,k}$	
身份鉴别	{*外部客户端与 XXXXX 系统的通信信道*}						
	{*系统管理员从外部进行管理所使用的集中管理通道*}						
通信数据完整性	{*外部客户端与 XXXXX 系统的通信信道*}						
	{*系统管理员从外部进行管理所使用的集中*						

	管理通道}						
通信过程中重要数据的机密性	{外部客户端与 XXXXX 系统的通信信道}						
	{系统管理员从外部进行管理所使用的集中管理通道}						
网络边界访问控制信息的完整性	{外部客户端与 XXXXX 系统的通信信道}						
	{系统管理员从外部进行管理所使用的集中管理通道}						
安全接入认证	{外部客户端与 XXXXX 系统的通信信道}						
	{系统管理员从外部进行管理所使用的集中管理通道}						

A.3. 设备和计算安全

表 A-3 设备和计算安全测评结果记录

测评单元	测评对象	结果记录	量化指标				测评单元得分 $S_{i,j} = \frac{\sum_{1 \le k \le n_{i,j}} S_{i,j,k}}{n_{i,j}}$
			密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K	测评对象评分 $S_{i,j,k}$	
身份鉴别	{*密码产品/设备*}						
	{*通用服务器*}						
	{*其他涉及设备*}						
远程管理通道安全	{*密码产品/设备*}						
	{*通用服务器*}						
	{*其他涉及设备*}						
系统资源访问控制信息完整性	{*密码产品/设备*}						
	{*通用服务器*}						
	{*其他涉及设备*}						
重要信息资源安全标记完整性	{*密码产品/设备*}						
	{*通用服务器*}						
	{*其他涉及设备*}						
日志记录完整性	{*密码产品/设备*}						
	{*通用服务器*}						

	{其他涉及设备}						
重要可执行程序完整性、重要可执行程序来源真实性	{密码产品/设备}						
	{通用服务器}						
	{其他涉及设备}						

A.4. 应用和数据安全

表 A-4 应用和数据安全测评结果记录

测评单元	测评对象	结果记录	量化指标				测评单元得分 $S_{i,j} = \frac{\sum_{1 \le k \le n_{i,j}} S_{i,j,k}}{n_{i,j}}$
			密码使用安全 D	密码算法/技术合规性 A	密钥管理安全 K	测评对象评分 $S_{i,j,k}$	
身份鉴别	*{OA 办公系统管理员用户}*						
	{OA 办公系统业务用户}						
	{公文管理系统管理员用户}						
	{公文管理系统业务用户}						
访问控制信息完整性	*{OA 办公系统}*						
	{公文管理系统}						
重要信息资源安全标记完整性	*{OA 办公系统}*						
	{公文管理系						

	统}						
重要数据传输机密性	{OA 办公系统管理员用户登录口令}						
	{OA 办公系统业务用户登录口令}						
	{OA 办公系统业务报表}						
	{OA 办公系统办公文件数据}						
	{OA 办公系统业务日志}						
	{公文管理系统管理员用户登录口令}						
	{公文管理系统业务用户登录口令}						
	{公文管理系统业务数据}						
	{公文管理系						

	统业务日志}						
重要数据存储机密性	*{OA 办公系统管理员用户登录口令}*						
	{OA 办公系统业务用户登录口令}						
	{OA 办公系统业务报表}						
	{OA 办公系统办公文件数据}						
	{OA 办公系统业务日志}						
	{公文管理系统管理员用户登录口令}						
	{公文管理系统业务用户登录口令}						
	{公文管理系统业务数据}						
	{公文管理系统业务日志}						

重要数据传输完整性	{OA 办公系统管理员用户登录口令}						
	{OA 办公系统业务用户登录口令}						
	{OA 办公系统业务报表}						
	{OA 办公系统办公文件数据}						
	{OA 办公系统业务日志}						
	{公文管理系统管理员用户登录口令}						
	{公文管理系统业务用户登录口令}						
	{公文管理系统业务数据}						
	{公文管理系统业务日志}						
重要数据存储完整性	{OA 办公系统						

	管理员用户登录口令}						
	{OA 办公系统业务用户登录口令}						
	{OA 办公系统业务报表}						
	{OA 办公系统办公文件数据}						
	{OA 办公系统业务日志}						
	{公文管理系统管理员用户登录口令}						
	{公文管理系统业务用户登录口令}						
	{公文管理系统业务数据}						
	{公文管理系统业务日志}						
不可否认性	*{OA 办公系统业务用户文件*						

	审批操作}						
	{公文管理系统业务用户公文签发操作}						

A.5. 管理制度

表 A- 5 管理制度测评结果记录

测评单元	测评对象	结果记录	测评指标符合情况（符合/部分符合/不符合/不适用）	测评单元得分 $S_{i,j}$
具备密码应用安全管理制度	{*管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）*}			
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				

A.6. 人员管理

表 A-6 人员管理测评结果记录

测评单元	测评对象	结果记录	测评指标符合情况（符合/部分符合/不符合/不适用）	测评单元得分 $S_{i,j}$
了解并遵守密码相关法律法规和密码管理制度	{*管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）*}			
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				
建立关键岗位人员保密制度和调离制度				

A.7. 建设运行

表 A-7 建设运行测评结果记录

测评单元	测评对象	结果记录	测评指标符合情况（符合/部分符合/不符合/不适用）	测评单元得分 $S_{i,j}$
制定密码应用方案	{*密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档*}			
	{*管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）*}			
制定密钥安全管理策略	{*密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防*			

	对抗演习报告、整改文档}			
	{管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）}			
制定实施方案	{密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档}			
	{管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）}			
投入运行前进行密码应用安全性评估	{密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档}			
	{管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）}			

定期开展密码应用安全性评估及攻防对抗演习	{*密码应用方案、密钥管理制度及策略类文档、密码实施方案、商用密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档*}			
	{*管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）*}			

A.8. 应急处置

表 A-8 应急处置测评结果记录

测评单元	测评对象	结果记录	测评指标符合情况（符合/部分符合/不符合/不适用）	测评单元得分 $S_{i,j}$
应急策略	{*管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员）*}			
事件处置				
向有关主管部门上报处置情况				