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，报告模板为 2023 年版。

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>是否为关键信息基础设施</td><td colspan="5">☐已认定，所属安全保护工作部门：_____
☐未认定</td></tr>
<tr><td rowspan="2">网络安全等级保护定级和备案情况</td><td colspan="5">☐已定级备案，第___级（一至四），S__A__G__
备案证明编号：
本次被测信息系统与等级保护定级系统是否一致：
☐是 ☐否，变化情况说明：</td></tr>
<tr><td colspan="5">☐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>商用密码应用安全性评估情况</td><td colspan="5">☐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><td rowspan="2">系统是否依赖不在本系统范围内的云平台运行</td><td colspan="2">☐是，
云平台名称：</td><td colspan="3">☐云平台已评估☐云平台正在评估☐云平台未评估
密评机构名称：
评估时间： 评估结论：</td></tr>
<tr><td colspan="5">☐否</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，方案重点解决的系统密码应用需求和密码实现等内容。}*
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

1 系统概述

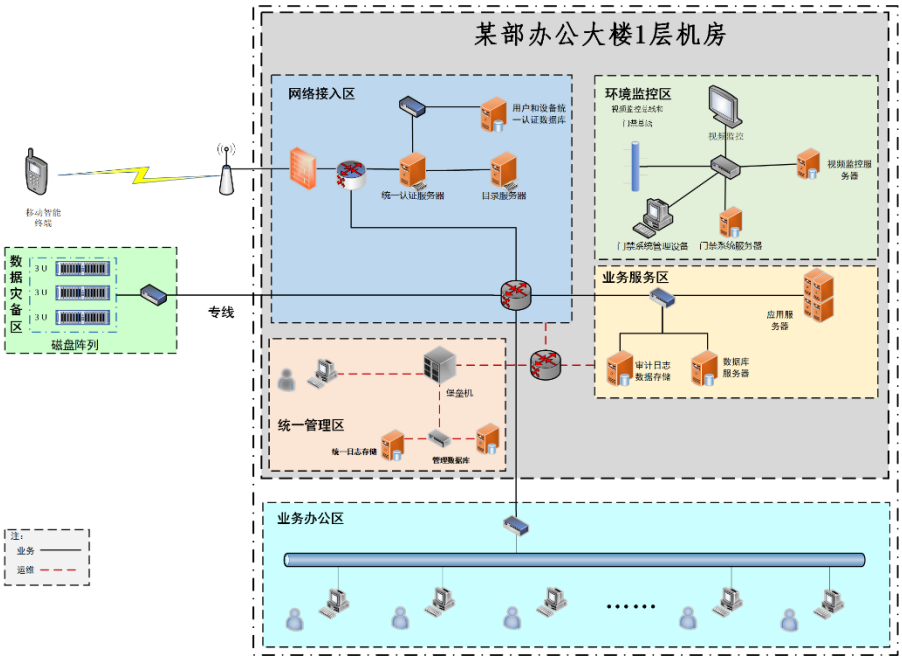

图 1 系统网络拓扑图

{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、与其他系统的互联关系（网络互联、数据互通等情况）、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}*

序号	安全层面	保护对象
7		……
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		{服务器密码机等整机类密码产品}
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

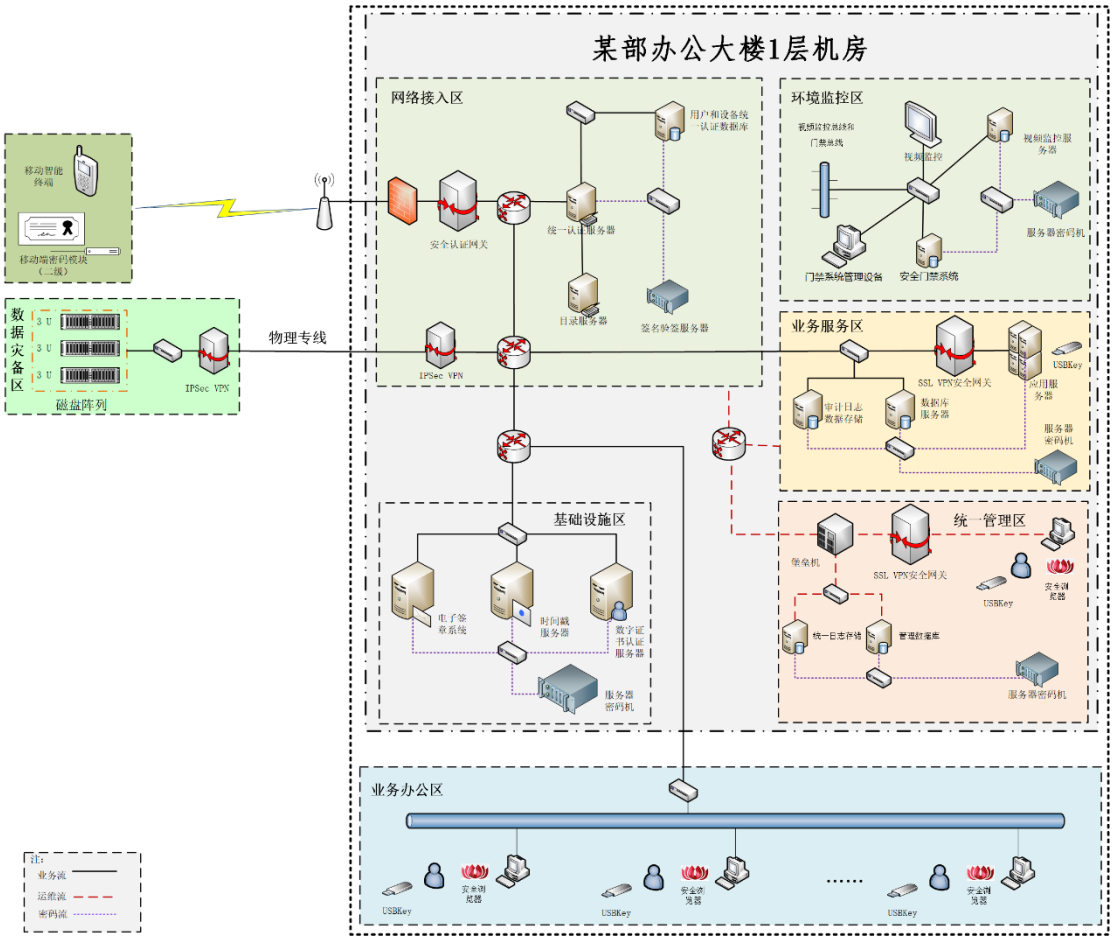

图 2 系统密码应用部署图

{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 □不适用	
	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 □不适用	
	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	可	□适用	

	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。		□不适用	
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 □不适用	
	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 □不适用	
	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 □不适用	
	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 □不适用	
	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 □不适用	
	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	宜	□适用 □不适用	

	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。			
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 □不适用	
	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 □不适用	
	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 □不适用	
	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 □不适用	
	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 □不适用	
	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 □不适用	
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 □不适用	
	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，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任； 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 □不适用	
	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	应	□适用 □不适用	

	行专门培训，确保其具备岗位所需专业技能；			
	8.6 d）应定期对密码应用安全岗位人员进行考核；	应	□适用 □不适用	
	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 □不适用	
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 □不适用	
	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 □不适用	
	8.7 c）应按照应用方案实施建设；	应	□适用 □不适用	
	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 □不适用	
	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 □不适用	
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 □不适用	
	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 □不适用	
	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 □不适用	
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身份鉴别，保证通信实体身份的真实性。	*{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}*

安全层面	指标要求	评估结果	未通过原因说明
	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}*

安全层面	指标要求	评估结果	未通过原因说明
	重要数据传输完整性	□通过 □未通过	*{具体风险分析}*
	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}*

安全层面	指标要求	评估结果	未通过原因说明
	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}*
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]。

[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。

5 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 份提交委托单位，X 份由密评机构留存。

附录 A 密评活动有效性证明记录[2]

A.1密评委托证明[3]

表 A-1 委托证明文件

文件类型	合同/任务书/……	**签订时间**	20XX 年 XX 月 XX 日
委托单位			
委托金额	XXXX 元/——	**方案密评单价**	XXXX 元/——
{*委托证明扫描件/照片*}			

[2] 相关证明材料请提供盖章、签字版本的扫描件或照片。

[3] 主要指合同、任务书或其他委托证明文件扫描件，文件内容、页数过多的，只需提供服务内容、收费金额、签字盖章等关键页。运营者自行开展密评的，无须提供。

A.2密评活动证明[4]

表 A-2 密评活动证明

方案评估起止时间	20XX 年 XX 月 XX 日-20XX 年 XX 月 XX 日
密评人员	
{*活动证明扫描件/照片*}	
{*活动证明扫描件/照片*}	

[4] 主要指密评人员与委托方相关人员通信记录（如电话、邮件、信息等）、会议记录等测评证明依据，有任一证明即可。

A.3密评活动质量文件

表 A-3 密评报告评审

报告评审时间	20XX 年 XX 月 XX 日
{*方案评估报告评审记录扫描件/照片*}	

A.4密评人员资格证明[5]

表 A-4 密评人员资格情况

序号	姓名	角色	密评人员考试通过时间
1		{*组长、密评报告编制人*}	20XX 年 XX 月
2		{*组员*}	20XX 年 XX 月
3		{*组员*}	20XX 年 XX 月
4		{*密评报告审核人*}	20XX 年 XX 月
5		{*密评报告批准人*}	20XX 年 XX 月

表 A-5 密评人员考核成绩证明

{*成绩扫描件/照片*}	{*成绩扫描件/照片*}

[5] 本次实施密评活动人员中至少 2 名通过密评人员考试的成绩证明扫描件；同时提供密评报告编制人、审核人、批准人（授权签字人）通过密评人员考试的成绩证明扫描件。

A.5系统定级匹配证明

表 A-6 系统定级备案证明

系统等保定级备案名称	
系统等保定级备案时间	20XX 年 XX 月 XX 日
{*信息系统安全等级保护备案证明扫描件/照片*}	

附：《XXXX 系统密码应用方案》