文档密级：公开

商用密码应用测评一体机系统

产品白皮书

豪密科技

V11

版权声明

免责声明

技术支持

如果您有任何宝贵意见或技术问题，请反馈：

地址：北京市海淀区国家网络安全产业园南区 2 号楼 1 层

电话：4000-181-171

邮箱：support@haomitech.cn

微信公众号：豪密科技

您也可联系豪密科技技术服务人员获得最新技术和产品信息。

目录

1 引言

密码是国之重器，是保障网络安全的核心技术和基础支撑，在网络安全防护中具有不可替代的重要作用。维护国家网络空间安全和数据安全，必须合规、正确、有效使用密码，必须大力推进商用密码应用安全性评估(下简称密评)。开展密评工作，密评工具必不可少。

2 产品概述

商用密码应用测评一体机系统是根据国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》研制的商用密码应用与安全性评估工作专用系统，能够针对流量文件、证书文件、签章文件等进行自动化精确解析，并进行合规性、正确性、有效性分析，为密评人员提供精准的判别依据；支持一体化的报告协同撰写功能，报告标准参考《商用密码应用安全性评估报告模板(2023 版)—系统密评报告》，能有效提升密评工作的效率及准确性，为密评单位节约成本。

商用密码应用测评一体机系统采用检测插件模式，可根据用户不同需求进行快速定制开发，满足不同行业的密评需求。

* 可搭配豪密数据分析工具箱使用（需单独付费）。

3 产品功能

产品功能如下图所示：

图 1 产品功能架构

图 2 功能菜单

3.1 密评报告协同编辑

系统集成密评报告在线编辑、生成模块。用户填写表单后，系统可自动生成密评报告 word 文档，多用户可针对密评报告填报开展协同编辑，提升报告撰写效率。

图 3 基本信息填报

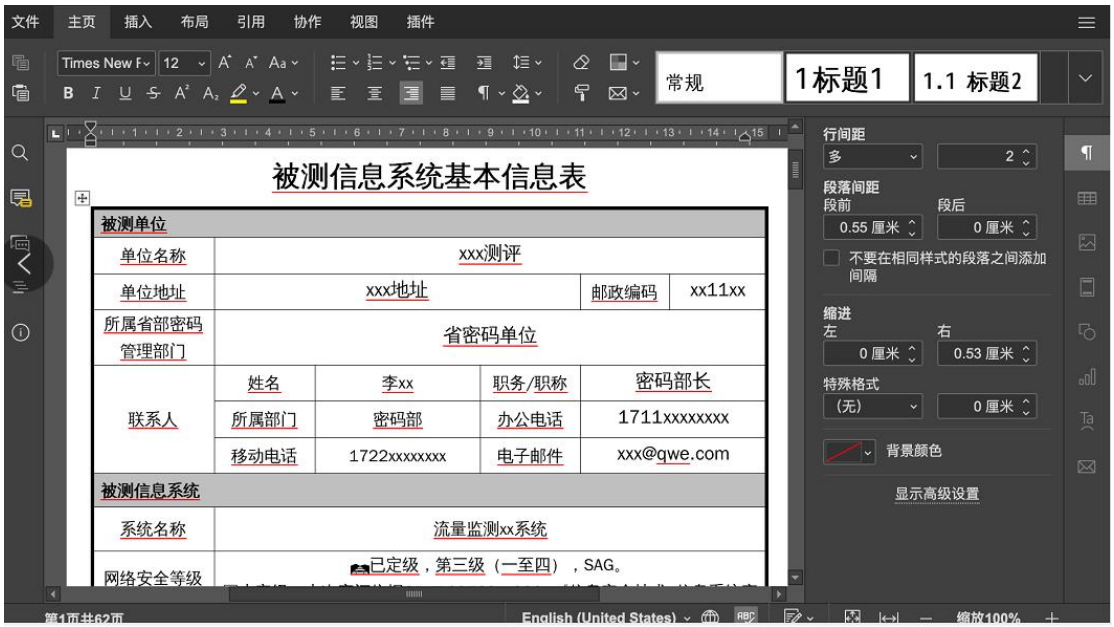
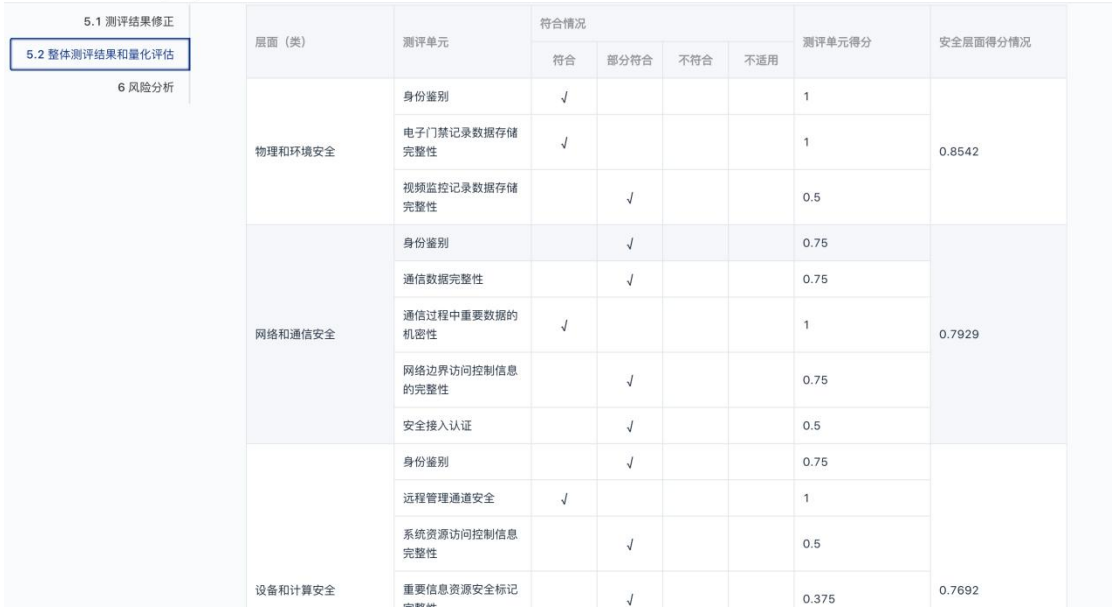


图 4 密评报告协同编辑

3.2 自动量化评估

用户针对测评对象进行测评结果记录评分后，系统会自动生成单元测评结果和量化评估表。量化评估方法依据《商用密码应用安全性评估量化评估规则》，根据不同等保级别自动进行加权计算。



层面（类）	测评单元	符合情况				测评单元得分	安全层面得分情况
		符合	部分符合	不符合	不适用		
物理和环境安全	身份鉴别	√				1	0.8542
	电子门禁记录数据存储完整性	√				1	
	视频监控记录数据存储完整性		√			0.5	
网络和通信安全	身份鉴别		√			0.75	0.7929
	通信数据完整性		√			0.75	
	通信过程中重要数据的机密性	√				1	
	网络边界访问控制信息的完整性		√			0.75	
	安全接入认证		√			0.5	
设备和计算安全	身份鉴别		√			0.75	0.7692
	远程管理通道安全	√				1	
	系统资源访问控制信息完整性		√			0.5	
	重要信息资源安全标记		√			0.375	

图 5 自动量化评估分析

在打完分后，系统可根据量化得分自动分析出相关风险项，并提

供问题描述、风险分析等相关描述模板可供参考和修改，方便用户进行快速分辨和内容编写。

图 6 风险分析自动生成

3.3 自动化分析检测

3.3.1 网络协议（含加密通信协议）自动化分析检测

针对主流网络协议的自动化分析检测是密评系统的核心功能之一，包括 SSL、IPSec、HTTP、FTP、SMTP、POP3 等。商用密码应用测评一体机系统依托多种流量检测策略，能够自动提取分析 SSL、IPSec 等协议的密钥协商信息、身份认证信息、数字证书、传输层会话载荷以及加密数据载荷等数据；支持自动提取并分析 HTTP、FTP、SMTP、POP3 等协议中的文件；能够过滤全流量敏感词，包括 ASCII、base64、unicode、utf8、gb2312、gbk 等编码格式；并将 IP 地址、端口、协议以及会话包数等会话信息进行统计展示。

图 7 网络协议检测分析

3.3.2 X509 证书自动化分析检测

商用密码应用测评一体机系统支持对 X509 证书进行自动化分析检测，包括证书格式检测、证书签名算法检测、证书签名哈希算法检测、证书自签名检测、证书有效期检测、证书密钥用途检测、证书公钥检测、证书链检测。

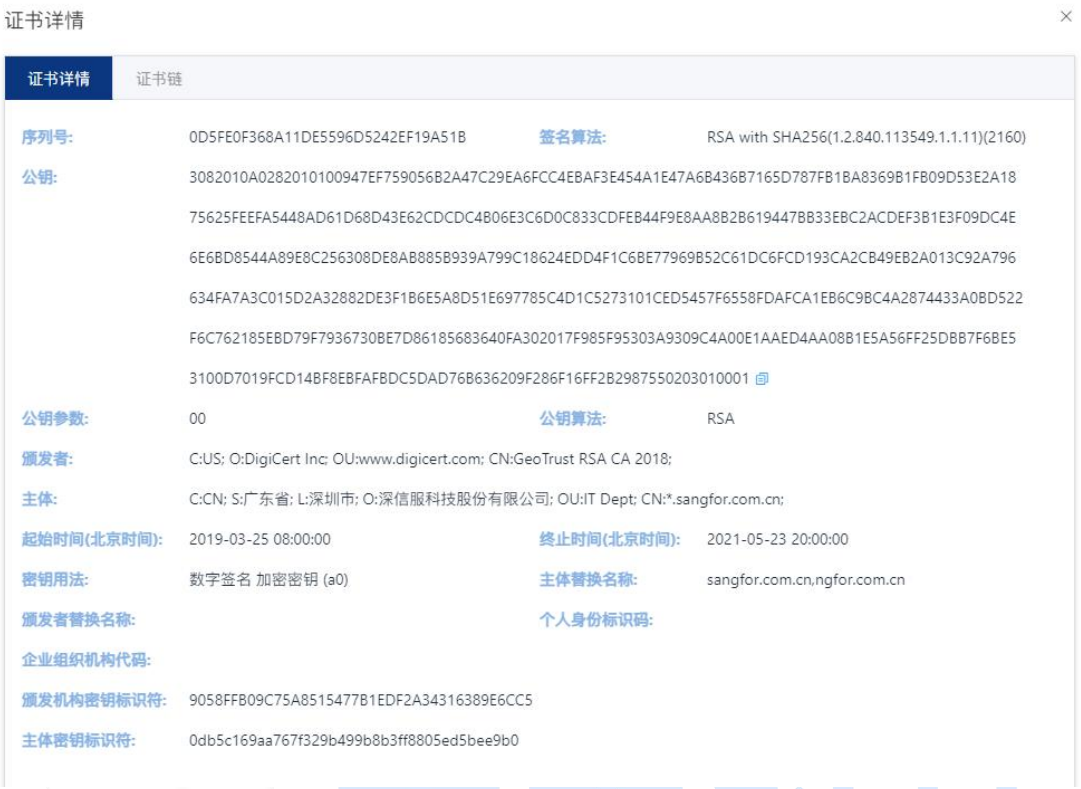


图 8 X509 证书检测分析

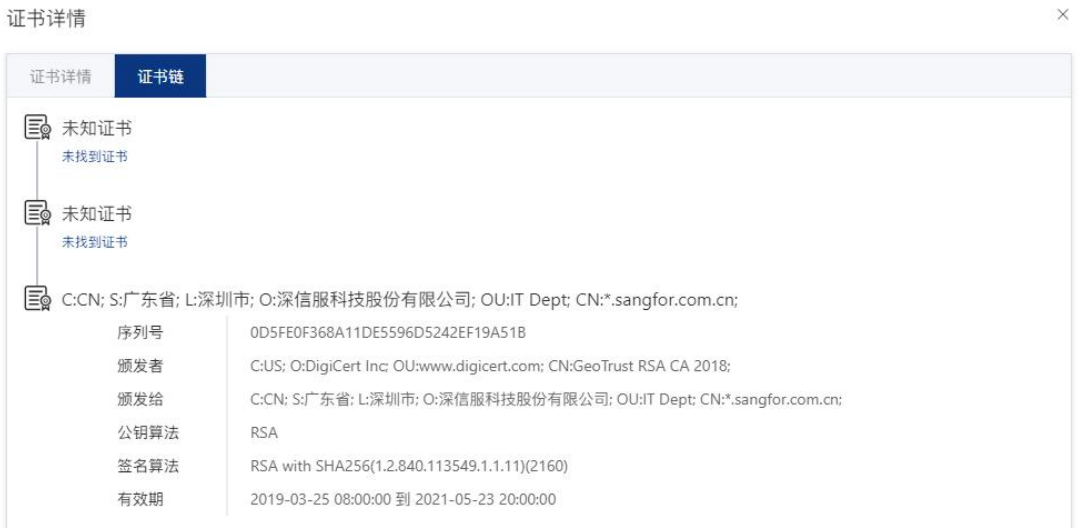


图 9 单证书链展示

3.3.3 签章文件自动化分析检测

商用密码应用测评一体机系统支持对签章文件进行自动化分析检测，包括对 OFD 文件格式检测、签章正确性（验章）检测、以及

印章相关检测（参考证书检测）。

下图为电子签章合规性检测结果图：

图 10 签章文件检测分析

3.3.4 随机性检测分析

商用密码应用测评一体机系统支持随机性检测功能，包括加密网络协议中的 Nonce 值、加密载荷的随机性检测。

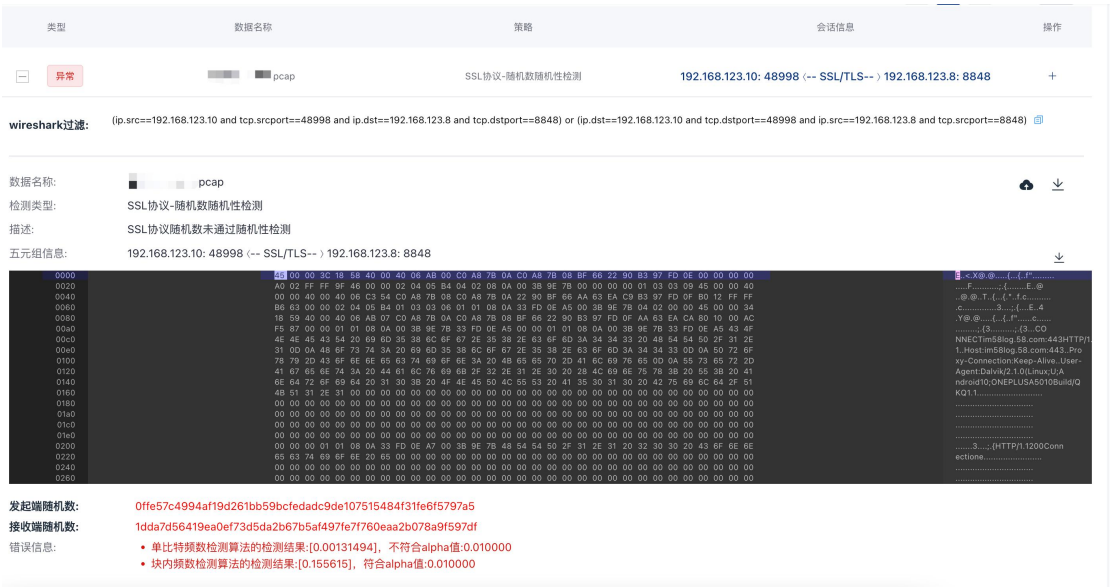


图 11 随机性检测分析

3.4 可私有化升级的知识库、资源库

商用密码应用测评一体机系统配套知识库、资源库。

知识库用于“结果分析”、“总体评价”、“安全问题”、“改进建议”等部分的话术积累，可用于指导新手密评人员启发思路、完善分析和评判思路，也可用于指导新入职机构的密评人员延续机构的报告内容、文法格式和分析思路，从而保障密评报告的质量稳定、风格统一、分析思路完整、判定风格一致；

图 12　知识库

资源库内置常用工具和模版等工具和文件，也支持私有化部署后内部不断升级补充，使密评人员共享密评机构内积累的密评资源。

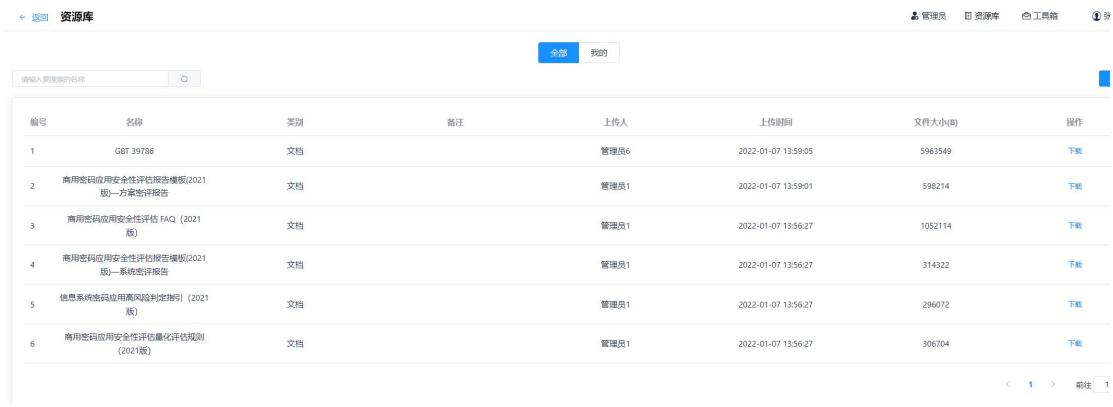


图 13 资源库

3.5 报告自动导出

支持多种内容形式的报告导出，包括测评方案阶段，备案表，包含附录 B 的整体报告导出等，可为用户提供阶段性的输出报告。

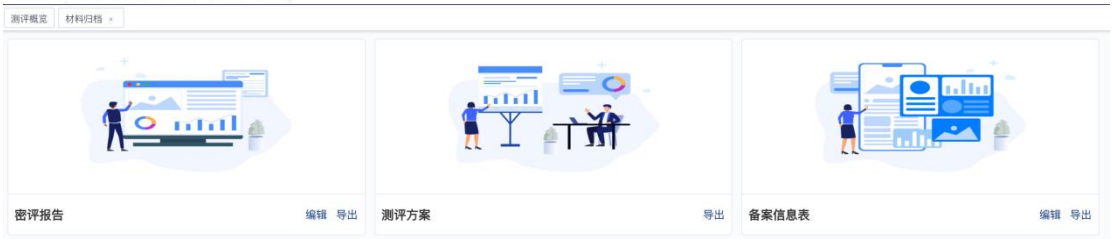


图 14 报告导出

3.6 易用性、引导性的密评填报

系统在密评人员开展系统资产填报之时即能自动化创建对应的测评对象；系统内置了测评方法、测评工具和测评工具检查点的填报内容，密评人员只需要修改或者补充；对于应用和数据安全层面的测评对象，系统也支持设定“身份鉴别”、“重要数据”、“不可否认性”这单项指标的子测评对象的设定；

除了上述的辅助性措施，系统还提供了更多的易用性、引导性设定，大大减少密评填报类型工作的重复性工作，促使密评人员将工作

精力聚焦在采集、分析、编制等重点工作上。并且可以自动同步总体性的评价，结果记录和测评结果等内容，为用户提供良好的测评体验，无需重复翻阅测评内容来做整体评价。

3.7 产品性能

- ✓ 系统平均响应时间不超过 5s；
- ✓ 并发用户数最高可达 30；
- ✓ 每秒响应事务数可达 15 TPS（Transactions Per Second）；

4 产品价值

4.1 分析结果准确智能

商用密码应用测评一体机系统是根据国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》研制的商用密码应用与安全性评估工作专用系统。系统功能涵盖了与密评相关的国标、行标以及指导文件所规定的主要检测范围，在工程实现上严格按照标准执行，对现场测评数据进行自动化智能分析，确保分析结果全面准确。

4.2 统一管理安全可控

商用密码应用测评一体机系统能够提供项目的全生命周期管理，提供“数据-任务-项目”各阶段的统一管理，降低业务风险。支持用户及项目权限划分，提升密评项目业务数据的安全性。

4.3 提升密评工作效率

商用密码应用测评一体机系统能够对用户上传的各类数据进行

自动化解析、分析与评估，给出评估结果、证据截图、相应报表，并支持用户在线协同编辑测评报告，一键生成报告，报告快速下载，简洁高效。整个流程中，用户操作简单，系统自动完成大部分分析工作，用户可快速定位相关问题，并将精力重点投入到对结果的分析和研判上，提升密评工作效率，达到事半功倍的效果。

4.4 持续赋能提升价值

商用密码应用测评一体机系统打破传统“工具集合”的思维模式，底层设计采用系统化的思维，工程实现上采用插件化的架构，内置了大量标准插件，能够满足用户常规的密评工作需求。在插件化架构的基础上，支持针对不同密评场景快速开展插件定制开发，不断提升系统的适用性和全面性，持续为用户创造价值。

5 产品形态

设备名	详细配置	数量	单位	备注
便携版硬件平台	CPU：Intel CPU 多核处理器； 内存：不低于 32G DDR4 硬盘：不低于 1T 接口：至少 1 个百兆或千兆或 2.5G 网卡	1	台	配套电源、配套线缆及相关配件

服务器版本

设备名	详细配置	数量	单位	备注
服务器版硬件平台	CPU：Intel CPU 双路，总核数不低于 10 核； 内存：不低于 32G DDR4 硬盘：不低于 2T，支持 RAID0/1/5/10 电源：配置冗余交流电源 接口：双口千兆网卡	1	台	配套电源、线缆及相关配件

图 15 产品形态图

6 应用场景

典型应用场景如下图所示：

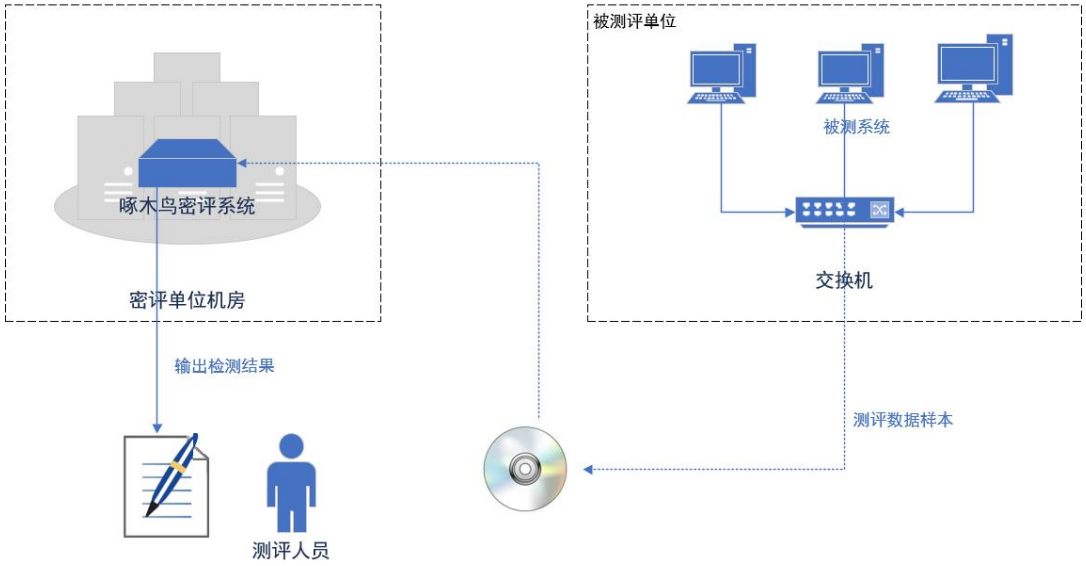


图 16 应用场景

7 公司简介

北京豪密科技有限公司，名称来源于 1931 年中国共产党第一本无线电通信密码“豪密”，致力于以密码和网络安全能力维护国家安全，向政企、军队、公安等特种用户提供产品和服务。公司管理团队和技术骨干主要来源于军队和国内著名高校研究所。凭借多年一线经验，持续研发创新，在密码和网络安全等方面形成了一批先进实用的技术和成果，主要产品包括：加密流量分析系统、密码实训平台、口令字破解系统、密码系统仿真平台、密码安全监测系统等。公司具有为特种行业服务的相关资质，总部位于海淀区北坞村路国家网络安全产业园，下设西安全资子公司和青岛全资子公司。秉承“专业靠谱”的理念，努力为国家安全服务。