

文档密级：公开



# 啄木鸟密评系统[单机版] 产品白皮书

豪密科技

V3

## 版权声明

本文中出现的任何文字叙述、文档格式、插图、图片、方法、过程等内容，除另有特别注明，版权均为豪密科技（指北京豪密科技有限公司、西安豪密网络科技有限公司）所有，受到有关产权及版权法保护。任何个人、机构未经豪密科技的书面授权许可，不得以任何方式复制或引用本文的任何片段。

## 免责声明

本文档仅用于为最终用户提供信息，其内容如有更改或撤回，均不另行通知。豪密科技已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，豪密科技均不对最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。

## 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](mailto: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.....                    | 1 |
| 2   | 产品概述.....                  | 1 |
| 3   | 产品功能及特点.....               | 2 |
| 3.1 | 覆盖全面且易用的辅助能力 .....         | 2 |
| 3.2 | 单机版不“单机”，密评协作不费力 .....     | 3 |
| 3.3 | 引导性、智能化信息填报 .....          | 4 |
| 3.4 | 测评证据集中管理、证据引用维护无忧 .....    | 5 |
| 3.5 | 从测评单元到整体量化评估结果的计算自动化 ..... | 5 |
| 3.6 | 采样数据自动化提取、分析与检测 .....      | 5 |
| 3.7 | 不断升级、独享性话术知识库 .....        | 6 |
| 3.8 | 密评成果一键导出 .....             | 6 |
| 4   | 使用方式.....                  | 6 |
| 5   | 产品特点.....                  | 6 |

# 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(简称密评)。开展密评工作，密评工具必不可少。

## 2 产品概述

HM-ZMN-TS002 啄木鸟密评系统[单机版](以下简称“密评系统”)是严格遵照国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》要求研制的商用密码应用与安全性评估工作专用系统，为密评工作的规范性、统一性、流程化、便捷性提供易用性工具及技术辅助手段。密评系统全面覆盖测评准备、方案编制、现场测评、分析与报告编制等主要活动，辅助密评人员开展测评方案以及基于《商用密码应用安全性评估报告模板(2023 版)——系统密评报告》的密评报告的填写和一键生成，结合我司多年累积的行业经验发掘活动中的易错点相应给出自动化、规范化的指导意见，同时利用技术手段通过智能化、易用的智能管理功能解决填报、修改阶段繁杂耗时的机械性工作负荷，从而释放密评人员去做更重要、更核心的测评分析工作。

系统具备解析多种现场测评采样数据，诸如流量数据、证书文件、签章文件等，自动提取并展示密码应用元数据，涵盖还原的 IPSec/SSL/TLS/TLCP 等加密协议会话、证书签名/签名算法/摘要算法/

有效期/CN/用途等、印章/制章元属性等，自动生成密码应用合规性判定导引结果。为密评人员开展现场测评活动时快速提供线索性信息。

密评系统为单机版软件，配置有安装包，安装方便快捷，可独立运行于 64 位 Win10、Win11 操作系统上，密评业务过程不依赖互联网。

\* 建议搭配 HM-ZMN-TS001 豪密数据分析工具箱使用，该产品可用于密码应用数据验证。

### 3 产品功能及特点

产品功能如下图所示：



图 1 产品功能架构

#### 3.1 覆盖全面且易用的辅助能力

单机版系统提供的密评报告编制能力覆盖测评准备活动一直到分析与报告编制活动中的所有编制信息，编制细节精细且全面，诸

如内置基本信息表、系统资产等诸多模版可供导入；提供图、文和表格编制能力以支持承载业务情况、网络拓扑图及描述和密码应用情况（含工作流程和密钥体系）的编制；提供测评方案、密评报告以及备案表等编制和导出。现场测评活动中也提供了对离线数据的不合规性自动解析和判定，辅助密评人员快速找寻证据线索。

单机版系统内置了对重要数据的有效性检查和提醒，诸如系统资产填报完成情况、系统使用密码产品情况、物理安防设施/数据库管理系统所在位置等等均内置自检能力；对于系统资产、现场测评结果记录等数据还拥有误操作防护能力，防止数据在误操作或者反复横向参考时发生丢失。

考虑密评机构的分布和客户服务区域，单机版系统内置了全局测评配置能力，随着测评业务的发展，全局测评积累的信息越多，新开展的密评项目在准备阶段就越省心省力。

### 3.2 单机版不“单机”，密评协作不费力

单机版系统虽离线运行在密评人员的工作机上，却不是信息孤岛，完全支持分工模式下的协同工作。多个单机版之间可通过被测系统的信息共享能力完成协作，支持分工开展编制的多个密评人员将信息汇聚到一起，在任一单机版系统平台上完成所有编制。共享过程中所传递的编制信息数据存储为加密的自研文件格式，因此协作过程中信息始终被安全保护。

### 3.3 引导性、智能化信息填报

报告编制人员基于 word 格式填报密评报告时容易因为个体经验差异、思路全面性、证据截图管理及引用习惯等主观因素导致无论是内部的编制组的自查审校阶段，还是送审整改阶段均造成了相当繁重的工作量，评审人日常任务繁重，评审过程更需要投入十二分力气查漏定错，编制组在自查和整改时也要面临牵一发而动全身，付出改一处要刷一遍全文的工作量，随着被测系统的测评内容多少，这种情况愈加明显，工作量急剧增加，甚至影响密评项目无法及时结项，更不论释放密评小组开展新的项目了。

单机版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”单项指标的子测评对象的设定；

单机版系统提供现场测评结果记录模版，模版与测评等级、安全层面和 DAK 量化情况紧密对应，不同的条件拥有不同的模版，让编制过程既全面又省力。

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

### 3.4 测评证据集中管理、证据引用维护无忧

现场测评阶段累积的证据图片是很多的，当证据图片插入到测评结果记录中进行引用之后，无论是重新编号、记录文字的文法调整还是语言组织形式的调整都将会使密评报告的编辑和更新的工作量成倍的增长。密评工具提供智能化的证据图片管理，将编制人员从繁重的调整工作中解脱出来，关注证据图片的组织和使用即可。

### 3.5 从测评单元到整体量化评估结果的计算自动化

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》，根据不同等级级别自动进行加权计算。

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、风险分析等相关模板。

### 3.6 采样数据自动化提取、分析与检测

密评系统支持对加密网络协议开展会话还原、密码应用元数据提取和展示，以及合规性自动分析；

密评系统也支持对 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；

密评系统还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)。

### 3.7 不断升级、独享性话术知识库

密评系统提供知识库功能，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、判定风格一致性；

### 3.8 密评成果一键导出

支持密评业务流程中最重要输出成果的导出，包括测评方案，备案表，以及包含附录 A、附录 B 的密评报告。

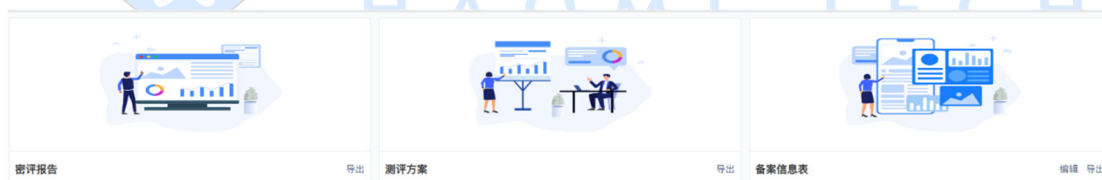


图 2 报告导出

## 4 使用方式

产品以软件方式提供，直接安装即可使用，无需连接互联网。

## 5 产品特点

本产品为单机形态软件，可在离线环境下使用，具有功能全面、系统兼容性高、简便易用等特点。