商用密码应用安全性评估
测评工具指引

中国密码学会密评联委会

二〇二四年十一月

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 2
3.1 术语和定义 2
3.2 缩略语 3
4 测评工具类别 3
4.1 概述 3
4.2 密码应用安全测评工具 4
4.3 密码应用安全测评辅助工具 5
4.4 密评报告编制工具 5
4.5 密评项目管理工具 5
5 测评工具安全要求 5
5.1 总体要求 5
5.2 部署和使用 6
5.3 维护和更新 6
5.4 卸载和更换 6
6 测评工具技术要求 6
6.1 密码应用安全测评工具 6
6.2 密码应用安全测评辅助工具 14
6.3 密评报告编制工具 17
6.4 密评项目管理工具 17
7 信息系统商用密码应用安全测评工具使用指引 18
7.1 概述 18
7.2 物理和环境安全测评工具使用指引 18
7.3 网络和通信安全测评工具使用指引 19
7.4 设备和计算安全测评工具使用指引 20
7.5 应用和数据安全测评工具使用指引 21
附　录　A （资料性） 密码应用安全测评工具使用示例 24
A.1 密码算法校验工具使用示例 24
A.1.1 算法校验场景示例 24
A.1.2 密码算法校验工具测试实施示例 25
A.2 协议分析工具使用示例 28
A.2.1 协议分析场景示例 28
A.2.2 协议分析工具测试实施示例 28
A.3 数字证书校验工具使用示例 31
A.3.1 数字证书校验场景示例 31
A.3.2 数字证书校验工具测试实施示例 32
A.4 随机数检测工具使用示例 32

A.4.1 随机数检测场景示例 32
A.4.2 随机数检测工具测试实施示例 33
A.5 电子签章校验工具使用示例 36
A.5.1 电子签章校验场景示例 36
A.5.2 电子签章校验工具测试实施示例 36
附 录 B （资料性） 密码算法校验工具参考表 39
B.1 对称密码算法 39
B.2 密码杂凑算法 41
B.3 消息鉴别码（MAC）算法 41
B.4 非对称密码算法 44
附 录 C （资料性） 密码应用安全测评辅助工具使用示例 48
C.1 源代码审计工具使用示例 48
C.1.1 源代码审计场景示例 48
C.1.2 源代码审计测试实施示例 48
C.2 编码转换工具使用示例 50
C.2.1 编码转换工具场景示例 50
C.2.2 编码转换工具测试实施示例 50
C.3 APDU 报文分析工具使用示例 52
C.3.1 APDU 报文分析工具场景示例 52
C.3.2 APDU 报文分析工具测试实施示例 52
参考文献 54

前言

本文件不涉及推荐或推广任何特定产品或服务，未经中国密码学会授权，任何单位或个人不得将本文件用于商业宣传、广告推广、产品销售或其他任何商业性活动。

本文件根据商用密码应用安全性评估实际需要给出了测评工具的逻辑分类，难免存在不完善不恰当之处。实际研制、使用测评工具，可选取本文件给出的某类测评工具的专门功能、部分或全部测评工具进行研制集成，或基于新技术、新应用、新业态对测评工具的种类及其功能进行扩展。欢迎对商用密码应用安全性评估测评工具的种类和功能提出进一步丰富的意见，并向中国密码学会密评联委会反馈更新本文件。

本文件由中国密码学会密评联委会提出并归口。

本文件起草单位：国家信息技术安全研究中心、中国科学院数据与通信保护研究教育中心、商用密码检测认证中心、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、工业和信息化部电子第五研究所、智巡密码(上海)检测技术有限公司、北京数字认证股份有限公司、国家网络与信息系统安全产品质量检验检测中心、公安部网络安全等级保护评估中心、深圳市网安计算机安全检测技术有限公司、公安部第一研究所信息安全等级保护测评中心、中科安永科技有限公司、福建金密网络安全测评技术有限公司、广州竞远安全技术股份有限公司、西部安全认证中心有限责任公司、宁夏泽新信息技术服务有限公司、北京银联金卡科技有限公司、上海市信息安全测评认证中心、浙江东安检测技术有限公司、江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心）、教育部教育管理信息中心、沈阳赛宝科技服务有限公司、天津云安科技发展有限公司、云南云盾信息安全测评有限公司、新疆量子通信技术有限公司、浙江省电子信息产品检验研究院、中互金认证有限公司、长春市博鸿科技服务有限责任公司、成都创信华通信息技术有限公司、天津恒御科技有限公司、广西网信信息技术有限公司、长沙中安密码检测有限公司、国家信息中心(国家电子政务外网管理中心)、安徽科测信息技术有限公司。

本文件主要起草人：吴冬宇、贾世杰、张帆、牛莹姣、李佳曦、付饶、陈天宇、李慧玲、吕娜、赵礼鹏、刘琛、高锐、刘军荣、王佳欢、丁漪、韦冠杰、周刊、郑亚杰、高松、林宣耿、钱文飞、徐琪、贾徽徽、马卫局、邓诗智、周世杰、冀利刚、邓福彪、吴震、王学进、管彩霞、刘学朋、孙少波、陈德海、王正临、刘学锐、李永忠、李瑞、张涛、钱行冠、于少军、徐雁飞、聂晓力、王海洋、李若甫、陈志刚、唐天日、黄水华、史汝辉、刘烨、苏欧煜、秦体红、姜玉琳、高嵩、路剑华、刘丽、韦博华、王惠君、刘云飞、梁浩然、梁宇轩、董宁博、张世俊、王天昊、俞宸捷、倪辰、卢秋如、吴晓刚、黄凌锋、孙成坤、兰长亮、周海涛、桑妤、修凤洲、梅文孝、刘芝影、冯晓钰。

本文件由张振峰、陈武平、秦小龙、阎亚龙、罗鹏、马原、王宏、刘健、刘尚焱、汪宗斌、郑昉昱等专家负责审核。

有关问题和建议，可发送邮箱至mplwh@cacrne.org.cn。

商用密码应用安全性评估测评工具指引

1 范围

本文件根据商用密码应用安全性评估工作中测评工具的使用需求，在对测评工具进行分类基础上提出了测评工具研制要求，并给出测评工具使用指引和使用示例。

本文件可为商用密码应用安全性评估测评工具的研制、使用提供参考。

本文件所涉及的商用密码应用安全性评估测评工具输出结果仅可用于辅助密评人员进行测评结果判定，信息系统密码应用安全风险应综合深入分析各类网络与信息系统的密码保障措施而确定。

本文件所涉及的商用密码应用安全性评估测评工具应当根据相关标准文件等的更新而及时升级，以确保测评工具的准确性。

注：本文件中对于“应”的条款，建议按照相关指标要求予以实现，对于“可”的条款，可按照相关指标要求自行决定是否实现。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 15843.3—2023 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15852.1—2020 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 15852.2—2012 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 15852.3—2019 信息技术 安全技术 消息鉴别码 第3部分：采用泛杂凑函数的机制

GB/T 17964—2021 信息安全技术 分组密码算法的工作模式

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 25069—2022 信息安全技术 术语

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 32918.1—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GB/T 32918.4—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 32918.5—2017 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义

GB/T 33133.1—2016 信息安全技术 祖冲之序列密码算法 第1部分：算法描述

GB/T 33133.2—2021 信息安全技术 祖冲之序列密码算法 第2部分：保密性算法

GB/T 33133.3—2021 信息安全技术 祖冲之序列密码算法 第3部分：完整性算法

GB/T 33190—2016 电子文件存储与交换格式 版式文档

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制

GB/T 36968—2018 信息安全技术 IPSec VPN技术规范

GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范

GB/T 38635.1—2020 信息安全技术 SM9标识密码算法 第1部分:总则

GB/T 38635.2—2020 信息安全技术 SM9标识密码算法 第2部分:算法

GB/T 38636—2020 信息安全技术 传输层密码协议（TLCP）
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
GB/T 43206—2023 信息安全技术 信息系统密码应用测评要求
GM/T 0005—2021 随机性检测规范
GM/T 0015—2023 数字证书格式
GM/T 0017—2023 智能密码钥匙密码应用接口数据格式规范
GM/T 0023—2023 IPSec VPN网关产品规范
GM/T 0024—2023 SSL VPN技术规范
GM/T 0025—2023 SSL VPN网关产品规范
GM/T 0035.2—2014 射频识别系统密码应用技术要求 第2部分：电子标签芯片密码应用技术要求
GM/T 0047—2016 安全电子签章密码检测规范
GM/T 0112—2021 PDF格式文档的密码应用技术要求
GM/T 0116—2021 信息系统密码应用测评过程指南
GM/T 0129—2023 SSH密码协议规范
GM/Z 4001—2013 密码术语

3 术语、定义和缩略语

GB/T 25069《信息安全技术 术语》、GB/T 39786《信息安全技术 信息系统密码应用基本要求》、GB/T 43206《信息安全技术 信息系统密码应用测评要求》和GM/Z 4001《密码术语》界定的，以及下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1 密码算法校验工具 cryptographic algorithm verification tool

是指用于验证以密码行业标准或国家标准形式公布的商用密码算法、常见国外密码算法正确性的工具。

3.1.2 协议分析工具 protocol analysis tool

是指用于捕获、解析网络通信数据包，验证通信协议版本、通信协议交互过程、身份鉴别算法、密钥交换算法、数据机密性和完整性保护算法以及数字证书等内容正确性的工具。

3.1.3 数字证书校验工具 digital certificate verification tool

是指用于验证数字证书结构、数字证书有效期、数字证书状态和证书链等内容正确性的工具。

3.1.4 随机数检测工具 random number test tool

是指用于检测二元序列随机性的工具。

3.1.5 电子签章校验工具 electronic seal signature verification tool

是指用于验证电子签章和电子印章结构、印章有效性、制章者和签章者证书、签名值、签章时间、原文杂凑值和时间戳等内容正确性的工具。

3.1.6 端口扫描工具 port scanning tool

是指用于探测和识别服务器、主机、密码设备等开放端口情况的工具。

3.1.7 逆向分析工具 reverse analysis tool

是指将可执行程序进行反汇编、反编译等操作，将可执行程序转换成汇编代码或高级编程语言，用于分析可执行程序内部组成结构及工作原理的工具。

3.1.8 源代码审计工具 source code auditing tool

是指用于检测源代码中的安全漏洞及密码应用缺陷的工具。

3.1.9 密码应用缺陷验证工具 cryptography application defect verification tool

是指未经授权绕过信息系统安全防护机制，来达成对信息系统密码应用缺陷的分析利用的工具。

3.2 缩略语

下列缩略语适用于本文件。

IPSec：互联网安全协议（IP Security）

SSL：安全套接层（Secure Sockets Layer）

TLS：传输层安全协议（Transport Layer Security Protocol）

SSH：安全交互（Secure Shell）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

APDU：应用协议数据单元（Application Protocol Data Unit）

CRL：证书撤销列表（Certificate Revocation List）

OCSP：在线证书状态查询协议（Online Certificate Status Protocol）

PKCS：公钥加密标准（Public-Key Cryptography Standards）

SCT：签名证书时间戳（Signed Certificate Timestamp）

4 测评工具类别

4.1 概述

商用密码应用安全性评估中涉及的测评工具包括密码应用安全测评工具、密码应用安全测评辅助工具、密评报告编制工具和密评项目管理工具等，通常包括软件系统和必要的配套硬件。

密码应用安全测评工具主要直接对密码功能进行检测，包括但不限于密码算法校验工具、协议分析工具、数字证书校验工具、随机数检测工具、电子签章校验工具等；密码应用安全测评辅助工具主要围绕密码应用安全检测需要，实现辅助检测功能，包括但不限于端口扫描工具、逆向分析工具、源代码审计工具、密码应用缺陷验证工具、其他工具等；密评报告编制工具主要为商用密码检测机构密评人员提供测评结果分析、量化评估、密评报告撰写等功能；密评项目管理工具主要为商用密码检测机构提供密评项目管理功能、数据分析功能。商用密码应用安全性评估测评工具体系如图1所示：

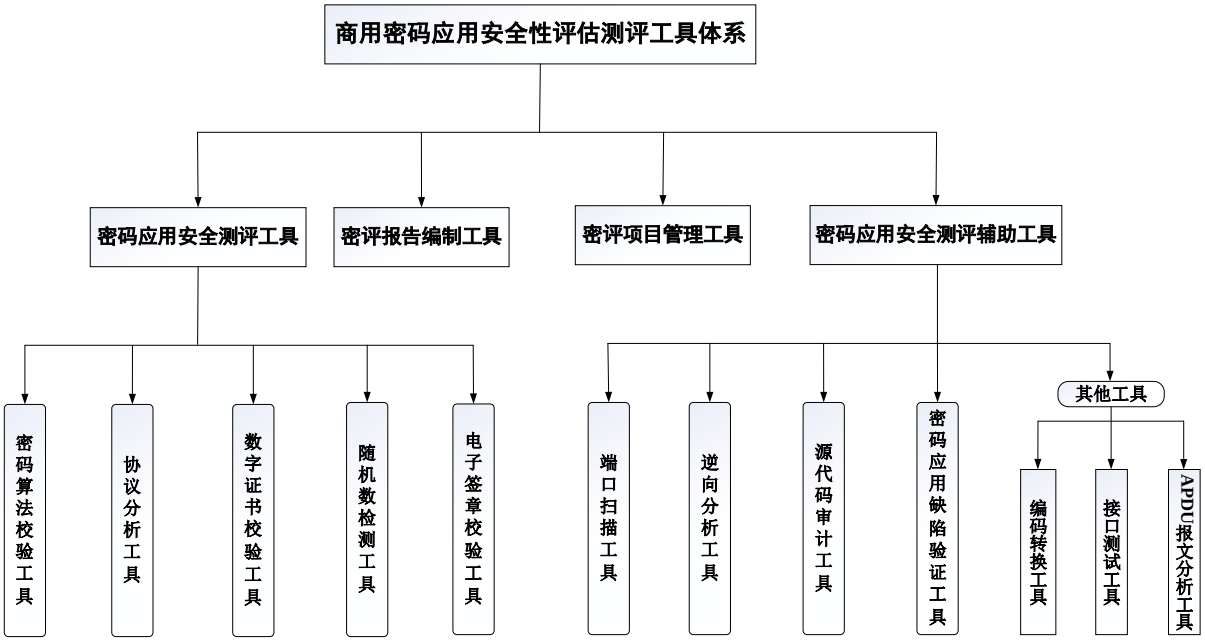


图1 商用密码应用安全性评估测评工具体系

4.2 密码应用安全测评工具

4.2.1 密码算法校验工具

密码算法校验工具能够实现对密码算法的校验，能够校验密码算法输入、输出参数的值、长度等是否符合国家和行业相关的标准、规范。校验的对象包括但不限于商用密码算法、常见国外密码算法，校验功能包括但不限于加密解密、签名验签、密码杂凑等。

4.2.2 协议分析工具

协议分析工具能够实现对通信协议的分析。分析的对象包括但不限于IPSec协议、SSL/TLS协议、TLCP协议、SSH协议，分析功能包括但不限于协议类型、协议版本、密钥交换过程、密码算法识别等。

4.2.3 数字证书校验工具

数字证书校验工具能够实现对数字证书的校验。校验的对象包括但不限于遵循GM/T 0015《数字证书格式》标准的数字证书，校验功能包括但不限于数字证书格式检查、数字证书状态检查、证书链验证、CRL结构检查等。

4.2.4 随机数检测工具

随机数检测工具能够实现对二元序列的随机性检测。支持检测二进制文件、pcap文件等样本格式，检测方法遵循GM/T 0005《随机性检测规范》相关要求，检测功能包括但不限于样本数据随机性检测、密文数据随机性检测、通信数据包密文数据自动化提取和随机性检测、生成检测报告等。

4.2.5 电子签章校验工具

电子签章校验工具能够实现对电子签章的校验。校验的对象包括但不限于遵循GB/T 38540《信息安全技术 安全电子签章密码技术规范》、GM/T 0112《PDF格式文档的密码应用技术要求》标准的PDF格式、OFD格式签章文件，校验功能包括但不限于文件读取、数字签名解析验证、电子印章解析验证、电子签章解析验证等。

4.3 密码应用安全测评辅助工具

4.3.1 端口扫描工具

端口扫描工具能够实现对服务器、主机、密码设备等开放端口的识别。用于辅助分析被测信息系统密码服务是否被正确调用。

4.3.2 逆向分析工具

逆向分析工具能够实现对可执行程序内部组成结构及工作原理的分析。分析的对象为源代码编译后的可执行程序，功能包括但不限于反汇编、反编译、静态分析、动态调试等。

4.3.3 源代码审计工具

源代码审计工具能够实现对应用程序/软件源代码的自动化审计分析。功能包括但不限于密码应用缺陷检测、安全漏洞检测等。

4.3.4 密码应用缺陷验证工具

密码应用缺陷验证工具能够实现对信息系统的密码应用缺陷的分析与利用。

4.3.5 其他工具

其他工具包括但不限于编码转换工具、接口测试工具、APDU报文分析工具等。

编码转换工具能够实现对字符串在不同编码格式、不同字符集、字节序之间的转换。功能包括但不限于常见编码格式间的转换、常见字符集间的转换、编码格式识别、编码解析等。

接口测试工具能够实现对密码服务和管理接口的安全性测试。

APDU报文分析工具能够实现APDU指令的抓取和分析，确认指令格式和内容是否符合预期。

4.4 密评报告编制工具

密评报告编制工具能够实现为商用密码检测机构密评人员提供方案密评报告编制、信息系统密评报告编制等功能。

4.5 密评项目管理工具

密评项目管理工具能够实现对商用密码检测机构开展密评项目过程的管理，并提供密评数据统计分析等功能。

5 测评工具安全要求

5.1 总体要求

a) 合规与正确性要求：测评工具设计和研制应符合国家相关法律法规要求，遵循国家和行业相关的标准、规范，测评工具的管理、校准遵循国家密码管理局的相关规定，以保证工具测评结果的合规性、正确性。
b) 完备性要求：涉及密码算法、协议分析的测评工具，在支持符合国家和行业相关标准、规范的密码算法、协议基础上，还应支持常见国外密码算法、协议。
c) 易用性要求：测评工具应结合商用密码应用安全性评估实际需求，提供简洁、直观的操作界面，支持各类常见测评数据格式的快速识别、验证。

d) 兼容性与可靠性要求：测评工具应支持常见的操作系统，支持当前主流硬件配置、软件配置、网络计算环境等，并经过充分的测试和验证，保证测评工具的稳定性和可靠性。
e) 可用性要求：测评工具应满足测评时效性要求，及时输出测评结果。
f) 文档支持要求：测评工具研制完成后，应提供完整的说明文档，如用户操作规程、技术文档等，方便用户了解和使用。

5.2 部署和使用

a) 安装部署要求：软件形态测评工具应提供标准或自定义安装选项，允许用户选择安装路径、组件、语言等；硬件形态测评工具部署应提供操作手册，并明确接入配置要求。
b) 身份鉴别要求：若测评工具具有缓存、存储重要数据或其他敏感信息等功能，应提供用户身份鉴别功能，应具有连续登录失败次数限制，口令长度、复杂度和更换周期等安全要求。
c) 安全使用要求：应采取必要的安全措施和技术手段保证测评工具自身的安全性，如工具应具有自身完整性校验功能，定期对工具进行安全漏洞扫描和漏洞修复，保证测评工具在使用过程中不会对被测系统造成安全威胁。
d) 数据安全要求：在使用测评工具进行取证、分析等过程中，应保证被测信息系统重要数据或其他敏感信息（包括但不限于源代码、通信数据包、数字证书、电子签章等）的安全性，避免数据泄露，防止数据被篡改、损坏或丢失。
e) 审计日志要求：测评工具应提供日志记录功能，记录测试工作日期、时间、类型、操作主体、测试结果等信息，便于定期进行审计操作。
f) 培训要求：应定期对密评人员进行工具使用培训，使其能够正确、有效的使用测评工具开展测评工作。

5.3 维护和更新

a) 工具维护要求：应定期对工具进行维护和安全性检查，保证测评工具为最新版本，及时修复测评工具中发现的问题。
b) 工具升级要求：测评工具更新升级时，应留存更新升级日志；若测评工具使用第三方开源应用组件代码，应对已公布的有关第三方开源应用组件/代码漏洞进行定期修复，并及时对测评工具进行改进升级。
c) 文档更新要求：当测评工具进行更新升级后，应同步更新测评工具相关文档，如用户操作规程、技术文档等。

5.4 卸载和更换

a) 卸载要求：软件形态的测评工具应提供易于使用的卸载程序，以便用户快速卸载测评工具，卸载完成后应确保与测评工具相关的所有残留文件和注册表项、服务等信息被完全删除；软件形态的测评工具应在卸载时提供选项由用户选择是否保留日志记录（硬件形态的测评工具应提供日志记录导出功能，由用户自行选择是否保留日志记录）。
b) 更换要求：硬件形态的测评工具在更换时，应保证被更换的测评工具中不保存任何历史测试数据、过程记录等内容；使用单位可妥善保管被更换测评工具日志记录。

6 测评工具技术要求

6.1 密码应用安全测评工具

6.1.1 密码算法校验工具

6.1.1.1 对称密码算法校验

对称密码算法主要实现数据加密、解密功能。在进行对称密码算法校验时应确定所使用的明文/密文数据格式、密钥、工作模式、数据填充方式等信息。其中，数据格式应支持字符串、十六进制、二进制、Base64等编码格式。

支持的密码算法

常见的对称密码算法及其对应的密钥长度要求、依据的标准等信息如表28所示。

密码算法校验工具应至少支持以下常见对称密码算法：SM4、AES、DES、3DES。

表28中ZUC序列密码算法包括两种算法，加密算法128-EEA3和完整性保护算法128-EIA3，可分别实现数据机密性和完整性保护。

支持的工作模式

常见分组密码算法工作模式所涉及的参数、参数输入长度要求、是否需要进行数据填充以及依据的标准等信息如表 29 所示。

密码算法校验工具应至少支持以下工作模式：ECB、CBC、CTR、GCM。

支持的数据填充方式

基于分组的对称密码算法计算过程中涉及的数据填充方式、不同填充方式对应的填充过程以及示例等信息如表30所示。

密码算法校验工具应至少支持以下常见数据填充方式：不填充、Zero填充、PKCS#7填充、ISO 10126填充、ISO/IEC 7816-4填充、ANSI X9.23填充。

6.1.1.2 密码杂凑算法校验

密码杂凑算法的作用是实现计算数据杂凑值功能。本节对密码杂凑算法校验功能进行说明，包括：支持的密码杂凑算法、算法输入长度要求、算法输出长度以及依据的标准等信息，具体情况如表31所示。

在进行密码杂凑算法校验时应确定所使用的数据格式、是否增加盐值等信息。密码杂凑算法校验功能应支持字符串、十六进制、二进制、Base64等编码格式。若计算过程中增加盐值，还应明确盐值与原计算消息的组合方式，比如将盐值放在原计算消息前，或者将盐值放在原计算消息后。

密码算法校验工具应至少支持以下常见密码杂凑算法：SM3、MD5、SHA-1、SHA-2系列算法、SHA-3系列算法。

6.1.1.3 消息鉴别码（MAC）算法校验

消息鉴别码（MAC）算法校验应支持基于分组密码算法（如SM4算法）的MAC算法校验功能（如CBC-MAC，CMAC以及GMAC）和带密钥的杂凑算法的MAC算法校验功能（即HMAC算法，如HMAC-SM3）。

本节对消息鉴别码（MAC）算法校验功能进行说明，包括：支持的MAC算法、算法输入参数、输入参数要求、算法输出、输出长度要求以及依据的标准等信息，具体情况如表32所示。

消息鉴别码（MAC）算法过程中涉及的消息填充及相应示例等信息如表33所示。

密码算法校验工具应至少支持以下常见MAC算法：CBC-MAC算法、HMAC算法。

6.1.1.4 非对称密码算法校验

支持的密码算法

非对称密码算法主要实现数据加解密、数字签名、密钥协商、密钥封装等功能。在进行非对称密码算法校验时应确定所使用的明文/密文数据及其编码格式、密钥等信息。其中，编码格式应支持字符串、十六进制、二进制、Base64等。

算法校验过程涉及的算法名称、公钥长度、私钥长度及其依据的标准等信息如表34所示。

密码算法校验工具应至少支持以下非对称密码算法：SM2、SM9、RSA。

SM2 密码算法

SM2密码算法校验功能包括密钥生成、验证公钥、加密、解密、签名、验签、密钥交换等功能。算法校验过程中涉及的算法功能、输入参数及输入参数长度要求、输出参数及输出参数长度要求等信息如表35所示。

SM9 密码算法

SM9密码算法校验功能包括密钥生成、加密、解密、签名、验签、密钥交换、密钥封装、密钥解封等功能。算法校验过程中涉及的算法功能、输入参数及输入参数长度要求、输出参数及输出参数长度要求等信息如表36所示。

RSA 密码算法

RSA密码算法校验功能包括密钥生成、加密、解密、签名、验签等功能。常用的RSA密码算法校验过程中涉及的算法功能、输入参数及输入参数长度要求、输出参数及输出参数长度要求等信息如表37所示。RSA加密、解密、签名、验签涉及的填充方式参见相关标准。

6.1.2 协议分析工具

6.1.2.1 IPSec 协议分析

支持的协议类型

IPSec协议分析功能应支持的协议类型，依据标准及主要功能如表1所示。

表1 IPSec协议分析功能支持协议类型及依据标准

序号	依据标准	功能
1	GB/T 36968 《信息安全技术 IPSec VPN技术规范》	①对ISAKMP进行识别和解析 ②对ESP、AH协议进行识别
2	RFC 2408:Internet Security Association and Key Management Protocol （ISAKMP）	对基于IKEv1的ISAKMP协议进行识别和解析
3	RFC 4306: Internet Key Exchange （IKEv2） Protocol	对基于IKEv2的ISAKMP协议进行识别和解析
4	RFC 5282:Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 （IKEv2） Protocol	
5	RFC 2406: IP Encapsulating Security Payload （ESP）	对ESP协议进行识别
6	RFC 2402: IP Authentication Header	对AH协议进行识别

功能要求

a) 数据包分析
   1) 应支持隧道模式和传输模式下的数据包解析；
   2) 能够对IPSec数据包进行解析，解析内容包括：

（1）协议类型及版本：能够解析IPSec协议的不同类型及版本，例如AH协议、ESP协议以及IKE协议等；

（2）SA属性信息：能够解析IPSec协议在IKE协议中协商的SA，包括加密算法、密码杂凑算法、认证方式和公钥算法、密钥协商数据等信息；

（3）数字证书检测：支持对密钥协商过程中传递的数字证书提取（签名证书和加密证书），并按照6.1.3节要求对数字证书进行解析；

（4）重复性检测：检测Nonce载荷、密钥交换过程的临时公钥等参数是否固定或重复使用。

3) 能够对密钥交换阶段进行合规性分析，分析内容包括：

（1）分析密钥交换阶段协议是否包括第一阶段和第二阶段；

（2）分析密钥交换各阶段是否完整；

（3）分析加密的临时密钥（可选）、Nonce、身份标识（ID）、数字证书（签名证书和加密证书）、数字签名等载荷是否完整；

（4）分析第一阶段协商的SA中密钥生存周期载荷值，分析工作密钥的最大更新周期是否符合GB/T 36968《信息安全技术 IPSec VPN技术规范》和GM/T 0023《IPSec VPN网关产品规范》中的相关条款要求；

（5）分析是否采用数字证书方式完成身份鉴别。

4) 能够对安全报文封装协议进行合规性分析，分析内容包括：

（1）分析是否单独使用AH协议；

（2）分析AH协议与ESP协议嵌套使用时，是否禁用了ESP协议中的验证操作；

（3）分析单独使用ESP协议时，是否启用了ESP协议中的验证操作。

b) 结果输出

IPSec协议分析工具应支持将分析结果生成报告，报告内容包括但不限于：

1) 源IP/端口、目的IP/端口、协议版本、加密算法、密码杂凑算法、第一阶段鉴别方式、数字证书、重复性检测结果等方面信息；

2) 工具应输出分析结论。

6.1.2.2 SSL/TLS 协议分析

支持的协议类型

SSL/TLS协议分析功能应支持的协议类型及依据标准如表2所示。

表2 SSL/TLS协议分析功能支持协议类型及依据标准

序号	支持协议	依据标准
1	TLCP	GB/T 38636 《信息安全技术 传输层密码协议（TLCP）》
2	TLS v1.0	RFC 2246:The TLS Protocol Version 1.0
3	TLS v1.1	RFC 4346:The Transport Layer Security （TLS） Protocol Version 1.1
4	TLS v1.2	RFC 5246:The Transport Layer Security （TLS） Protocol Version 1.2
5	TLS v1.3	RFC 8446:The Transport Layer Security （TLS） Protocol Version 1.3

功能要求

a) 数据包分析

1) 能够对握手阶段协议进行分析，分析内容包括：

（1）协议类型及版本：应支持6.1.2.2.1的协议类型，并解析其中的协议版本；

（2）算法套件：解析加密算法、杂凑算法、密钥交换算法等信息；

（3）数字证书检测：支持提取握手阶段协议中传递的数字证书，并按照6.1.3节要求对数字证书进行解析。

（4）重复性检测：检测握手阶段客户端随机数、服务端随机数、密钥交换过程的临时公钥等参数是否固定或重复使用。

2) 能够分析记录层协议采用的协议类型。

b) 结果输出

1) 工具应输出协议解析结果，包括：源IP/端口、目的IP/端口、握手协议阶段协议版本、算法套件、身份鉴别类型、单向身份鉴别/双向身份鉴别、数字证书、记录层协议类型、重复性检测结果等信息；

2) 工具应输出分析结论。

6.1.2.3 SSH 协议分析

支持的协议类型

SSH协议分析功能应支持的协议类型及依据标准如表3所示。

表3 SSH协议分析功能支持协议类型及依据标准

序号	支持协议	依据标准
1	SSH	GM/T 0129《SSH密码协议规范》
2	SSH2.0	RFC 4251:The Secure Shell （SSH） Protocol Architecture
3		RFC 4253:The Secure Shell （SSH） Transport Layer Protocol
4	SSH1.0	暂无

功能要求

a) SSH

1) 数据包分析

（1）协议类型及版本：通过客户端和服务端交换的“版本标识字符串”识别协商的协议版本；

（2）算法套件：通过客户端和服务端交换的“SSH_MSG_KEXINIT”识别协商的密钥交换算法（kex_algorithms）、对称加密算法（encryption_algorithms）、MAC算法（mac_algorithms）等内容；

（3）数字证书检测：通过客户端和服务端交换的“SSH_MSG_KEX_REQUEST”和“SSH_MSG_KEX_REPLY”，识别服务端的签名证书和加密证书，并按照6.1.3节要求对数字证书进行解析；

（4）重复性检测：检测Cookie、密钥交换过程的临时公钥等参数是否固定或重复使用。

2) 结果输出

（1）工具应输出源IP/端口、目的IP/端口、协议版本、算法套件、身份鉴别类型、数字证书、重复性检测结果等信息；

（2）工具应输出分析结论。

b) SSH2.0

1) 数据包分析

（1）协议类型及版本：通过客户端和服务端交换的“协议版本交换”识别协商的协议版本；

（2）算法套件：通过客户端和服务端交换的“Key Exchange Init”识别协商的密钥交换算法（kex_algorithms）、对称加密算法（encryption_algorithms）、MAC算法（mac_algorithms）等内容，并显示服务端支持的各类型算法列表；

（3）公钥信息：通过客户端和服务端交换的“Key Exchange Reply”，识别KEX host key的类型，明确公钥信息和签名值。

2) 结果输出

（1）工具应输出源IP/端口、目的IP/端口、协议版本、算法套件、身份鉴别类型、公钥等信息；

（2）工具应输出分析结论。

c) SSH1.0

通过客户端和服务端交换的“协议版本交换”识别协商的协议版本。

6.1.3 数字证书校验工具

6.1.3.1 支持的数字证书格式

数字证书校验功能应支持数字证书格式检查，检查依据如表4所示。

表4 数字证书格式检查依据标准

序号	依据标准
1	GM/T 0015《数字证书格式》
2	RFC 5280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List （CRL） Profile

6.1.3.2 功能要求

a) 数字证书格式检查

1) 功能描述

解析数字证书格式内容，检测数字证书是否符合相关标准。

2) 输入要求

输入参数：被测数字证书

3) 结果输出

（1）描述数字证书格式是否符合所依据的标准；

（2）解析数字证书，内容包括：证书版本、序列号、使用者、颁发者、颁发日期、截止日期、签名算法、哈希算法、公钥算法、公钥长度、公钥值（十六进制编码）、公钥参数、授权信息访问、证书策略、使用者密钥标识符、授权密钥标识符、SCT列表、密钥用法、基本约束、指纹、自定义扩展等。

b) 数字证书状态检查

1) 功能描述

数字证书状态检查包括检测数字证书有效期和证书撤销状态，其中证书撤销状态检测支持CRL、OCSP两种方式。

2) 输入要求

（1）CRL检查：

输入参数1：被测数字证书

输入参数2：CRL文件

（2）OCSP检查：

输入参数1：被测数字证书

输入参数2：OCSP地址

3) 结果输出

检测结果显示被测数字证书状态。

c) 证书链验证

1) 功能描述

验证证书链，检测数字证书是否在一个由一系列可信任证书构成的证书序列中，并通过验证数字证书中的数字签名，检查数字证书是否由受信任的CA颁发。通过验证证书链，可以确保数字证书的合法性和完整性。

2) 输入要求

输入参数1：被测数字证书

输入参数2：被测数字证书的根证书

3) 结果输出

检测结果显示信任链验证结果。

d) CRL结构检查

1) 功能描述

CRL结构检查包括以下内容：

（1）检测CRL是否符合格式标准；

（2）验证CRL本身的有效性验证，包括：CRL上的数字签名是否正确；当前是否处于有效期；

（3）检查被测数字证书是否在CRL撤销列表中。

2) 输入要求

输入参数1：CRL

输入参数2：被测数字证书的序列号

3) 结果输出

（1）描述CRL撤销列表格式是否符合所依据标准的证书撤销列表格式。

（2）解析CRL撤销列表，解析内容包含：版本、颁发者、生效日期、下一次更新日期、签名算法、授权密钥标识符、指纹、吊销列表（被吊销证书的序列号、吊销日期、吊销理由）。

（3）给出CRL本身的有效性结论，包括CRL上的数字签名是否正确，当前是否处于有效期。

（4）被测数字证书是否在CRL撤销列表中。

6.1.4 随机数检测工具

6.1.4.1 支持的样本格式

随机数检测工具应支持的样本格式包括但不限于二进制文件、pcap文件等。

6.1.4.2 功能要求

a) 随机数检测工具的检测方法应遵循GM/T 0005《随机性检测规范》相关要求；

b) 随机数检测工具应支持检测样本数据的随机性；

c) 随机数检测工具应支持检测使用加密算法对数据进行机密性保护后的密文数据的随机性；

d) 随机数检测工具应支持检测IPSec、TLS、TLCP等协议中密文数据的随机性，密文数据应从通信数据包中自动提取；

e) 随机数检测工具应具备良好的可扩展性，能够方便地添加新的测试项目或调整现有测试项目的参数；

f) 随机数检测工具应能够生成详细的检测报告，检测报告的内容包括但不限于检测过程、检测指标、检测结果等。

6.1.5 电子签章校验工具

6.1.5.1 支持的电子签章格式

a) 支持的文件格式

电子签章校验功能应支持的文件格式如表 5 所示。

表 5 电子签章校验功能支持的文件格式

序号	支持的文件格式	说明
1	PDF格式	一种常用的电子文档格式
2	OFD格式	一种电子文件格式标准

b) 依据的标准

电子签章校验功能依据的标准如表 6 所示。

表 6 电子签章校验功能依据的标准

序号	依据标准
1	GM/T 0047《安全电子签章密码检测规范》
2	GB/T 38540《信息安全技术 安全电子签章密码技术规范》
3	GB/T 33190《电子文件存储与交换格式版式文档》
4	GM/T 0112《PDF格式文档的密码应用技术要求》

6.1.5.2 功能要求

a) 解析和检测内容

1) 数字签名算法解析和检测

解析采用的数字签名算法，检测采用的算法和签名数据结构是否符合相关标准要求。

2) 电子印章解析和验证功能

（1）正确提取电子印章数据，检测数据格式是否满足相关标准要求；

（2）验证电子印章数据格式是否符合相关标准数据格式要求；

（3）提供电子印章签名值验证功能，根据印章信息数据、制章人证书和签名算法验证电子印章签名信息中签名值是否正确；

（4）提供制章人证书有效性验证功能，包括：制章人证书信任链验证、制章人证书有效期验证、制章人证书是否被吊销、密钥用法是否正确等；

（5）提供电子印章的有效期验证功能，根据印章属性中的印章有效起始日期和有效终止日期，验证电子印章是否过期。

3) 电子签章解析和验证功能

（1）正确提取电子签章数据，检测数据格式是否满足相关标准要求；

（2）提供电子签章签名值验证功能，能够基于待验证数据验证电子签章签名值是否正确。待验证数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识；

（3）提供签章人证书验证功能，验证签章人证书有效性，包括：签章人证书信任链验证、签章人证书有效期验证、签章人证书是否被吊销、密钥用法是否正确等；

（4）提供签章人证书是否在电子印章签章人证书列表中的验证功能；

（5）提供电子签章时间有效期验证功能。能够根据签章人数字证书有效期和电子签章中的时间信息，判断签章时间的有效性；

（6）提供电子签章原文杂凑验证功能，如果签章原文改变或电子签章数据中的原文杂凑值改变，都会导致验证失败；

（7）提供电子印章有效性验证功能和签章时间是否处于印章有效期内的验证功能。

b) 结果输出

（1）解析电子印章和电子签章采用的数字签名算法；
（2）生成电子印章数据，包括电子印章版本号、印章类型、印章名称、制作日期、印章有效起始日期、印章有效终止日期和制章人等相关信息；
（3）生成电子签章数据，包括电子签章版本号、时间信息、文档日期、签章人等相关信息；
（4）应对每个验证项目给出明确的“通过”或“未通过”的结果。

6.2 密码应用安全测评辅助工具

6.2.1 端口扫描工具

6.2.1.1 端口开放检测

端口扫描工具应能通过扫描服务器、主机、密码设备等端口开放状态，枚举服务器、主机、密码设备等的开放端口。如利用端口扫描工具，探测 IPSec VPN 服务对应的 UDP 500、4500 端口，SSL VPN 服务常用的 TCP 443 端口是否正常开启；是否开启了不必要的可能被攻击利用的端口，如 SSH、RDP、FTP 等协议使用的端口。

6.2.1.2 服务类型及版本检测

端口扫描工具应能检测远程设备上的网络服务以确定应用程序名称和版本号。

6.2.2 逆向分析工具

6.2.2.1 基础功能

a）逆向分析工具应具备基本的反汇编、反编译、代码分析和调试功能；
b）逆向分析工具的调试功能应至少包含静态分析和动态调试功能，其中动态调试功能应包含断点分析功能；
c）逆向分析工具应支持多种（至少2种）编程语言和软件格式，以满足不同类型软件的分析需求。

6.2.2.2 扩展性

逆向分析工具应具备一定的可扩展性，能够支持用户自定义插件或脚本，满足特定需求。

6.2.3 源代码审计工具

6.2.3.1 密码应用缺陷检测

a）源代码审计工具应支持检测是否使用了不安全的密码算法；
b）源代码审计工具应支持检测是否使用了不安全的随机数发生器、可预测或固定的随机数生成器种子；
c）源代码审计工具应支持检测是否使用了可预测的或固定的密钥、或基于相同口令或盐值用于密钥派生；
d）源代码审计工具应支持检测是否使用了不安全的SSL/TLS、SSH等协议以及不安全的配置（如未验证数字证书有效性）；
e）源代码审计工具应具备对SDF、SKF等接口调用的代码审计功能；
f）源代码审计工具可支持自动定位存在密码应用安全性问题的位置，便于用户快速定位问题，开展人工审计；
g）源代码审计工具可支持根据密评人员自身需求进行自定义规则的开发，以满足特定的代码审计需求。

6.2.3.2 安全漏洞检测

源代码审计工具应能够识别源代码中的常见安全漏洞，包括但不限于缓冲区溢出、注入攻击、跨站攻击（跨站脚本攻击XSS、跨站伪造攻击CSRF）等，可提供修复建议。

6.2.3.3 支持审计多种编程及标记语言

源代码审计工具应支持多种主流编程语言，包括但不限于Java/JSP、C/C++、VB/C#、PHP、Python、Golang、JS、TS、SQL等，以及常用标记语言，包括但不限于如XML等，以应对被测目标的多样性。

6.2.4 密码应用缺陷验证工具

6.2.4.1 密码应用缺陷识别

密码应用缺陷验证工具应能够辅助密评人员识别被测信息系统中的密码应用缺陷，包括但不限于不安全的密码算法、密码协议和密钥管理，不安全的随机数发生器，身份鉴别机制、完整性校验机制的设计和实现缺陷等。

6.2.4.2 密码应用缺陷利用

密码应用缺陷验证工具应能够辅助密评人员针对识别到的密码应用缺陷，从攻击者视角综合利用各种攻击技术手段，对被测信息系统可能遭受的攻击路径进行非破坏性质的攻击性测试，参考GB/T 20984《信息安全技术 信息安全风险评估方法》、GM/T 0116《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》等标准、指引，综合分析、确定密码应用缺陷风险等级，支撑信息系统密码应用安全性评估结果风险判定。

6.2.5 其他工具

6.2.5.1 编码转换工具

a）格式转换：编码转换工具应具备不同编码格式之间的相互转换功能，包括但不限于Base16（十六进制编码）、Base64、字符串等编码格式之间的相互转换；
b）字符集转换：编码转换工具应具备不同字符集之间的相互转换功能，包括但不限于UTF-8、UTF-16、UTF-16LE、UTF-16BE、GBK、GB2312、GB18030、ISO-8859-1至ISO-8859-15之间的相互转换；
c）字节序转换：编码转换工具应具备大端小端模式字节序转换功能；
d）编码格式识别：编码转换工具应具备针对不同编码格式的自动识别功能；
e）编码解析：编码转换工具应具备编码解析功能，包括但不限于ASN.1编码解析。

6.2.5.2 接口测试工具

a）接口身份鉴别安全性测试：应具备密码服务和管理接口身份鉴别的安全性测试功能，能够测试接口身份鉴别机制是否存在安全问题；
b）接口授权安全性测试：应具备密码服务和管理接口授权的安全性测试功能，能够测试是否能非授权访问接口并获取资源；
c）接口组件安全性测试：应具备接口所使用第三方组件的安全性测试功能，能够测试接口所使用第三方组件是否存在密码应用缺陷、安全漏洞、漏洞修复状况等；
d）接口敏感信息保护测试：应具备密码服务和管理接口是否泄露敏感信息的测试功能，敏感信息包括但不限于密钥、口令明文、敏感配置参数等；
e）接口连接有效期测试：应具备接口连接有效期的测试功能，能够测试接口连接的持续时间；

f）接口攻击防护测试：如以SDK形式提供密码服务和管理接口，则应具备SDK防静态逆向分析的测试功能，测试手段包括但不限于静态反汇编、字符串分析、导入导出函数识别、配置文件分析等，以验证是否能获得有关SDK实现方式的技术细节；可具备SDK防动态调试的测试功能，测试手段包括但不限于挂接动态调试器、动态跟踪程序、篡改文件、动态修改内存代码等，以验证是否能控制程序行为。

6.2.5.3 APDU 报文分析工具

APDU是应用层协议的数据单元，是一种标准的数据格式，用于在应用层协议之间进行通信。由命令APDU和响应APDU两部分组成，命令APDU用于发送指令，响应APDU用于接收响应信息。标准APDU指令报文由4个部分组成：标准头部、命令数据、数据长度和错误检查和确认。

a）应具备设备选择的功能：包括自动设备识别、手动选择设备。

b）应具备 APDU 报文捕获功能：包括抓取智能密码钥匙、智能 IC 卡等传输的 APDU 报文和保存。

c）可具备 APDU 报文发送和接收功能：包括单条指令的发送接收功能和多条指令的发送接收功能。

d）应具备 APDU 报文解析功能：工具在进行 APDU 报文分析时，应按照十六进制的编码格式对报文进行解析，并分析报文格式和内容是否符合预期。具体要求如下：

（1）依据标准

对各类APDU报文解析所依据的标准如表7所示。

表7 各类APDU报文解析依据标准

序号	功能	依据标准
1	智能密码钥匙的APDU报文解析	GM/T 0017 《智能密码钥匙密码应用接口数据格式规范》
2	接触式智能IC卡的APDU报文解析	ISO/IEC 7816-4 《Organizatioin, security and commands for interch ange》
3	接触卡片的通讯协议报文解析	ISO/IEC 7816-3 《Cards with contacts - Electronic dignals and tran smission protocols》
4	非接触式智能IC卡的APDU报文解析	ISO/IEC 7816-4 《Organizatioin, security and commands for interch ange》
5	非接触卡片的通讯协议报文解析	ISO/IEC 14443-4 《Contactless integrated circuit cards - Proximity cards - Transmission protocol》
6	金融行业的金融IC卡APDU报文解析	ISO/IEC 7816-4 《Organizatioin, security and commands for interch ange》 JR/T 0025.5《中国金融集成电路（IC）卡规范 第5部分：借记贷记应用卡片规范》
7	射频识别系统的卡片指令报文解析	ISO/IEC 7816-4 《Organizatioin, security and commands for interch ange》 GM/T 0035.2 《射频识别系统密码应用技术要求 第2部分：电子标签芯片密码应用技术要求》

（2）功能要求

1）命令APDU报文解析

能够解析出必备的4字节命令头：CLA INS P1 P2；

能够解析出有条件的可变长度命令主体；

能够根据提取出指令报文的值，按照对应的智能密码钥匙/智能IC卡的指令格式解析出请求报文，包括使用的密码算法，以及输入的重要数据内容及格式是否正确，如算法参数设置、数字证书格式、加解密模式等。

2）响应APDU报文解析

能够解析出有条件的可变长度主体；

能够解析出必备的2字节状态字：SW1 SW2；

能够判别报文是否正常响应，按照对应的智能密码钥匙/智能IC卡的指令格式解析出响应报文数据内容，并分析响应数据是否符合对应的密码算法及数据格式要求，如密文数据、杂凑结果、数字证书等的长度、格式、组织方式等。

3）结果输出

工具应输出APDU报文解析结果，包括：设备ID、设备信息、使用的算法、关键操作信息数据等方面信息；工具应输出分析结论。

6.3 密评报告编制工具

6.3.1 基础功能

a）密评报告编制工具可具备方案密评报告编制功能：

1）方案密评报告工具可支持系统基本信息表、系统各安全层面保护对象、各层面安全控制措施描述、指标适用情况及论证说明、改进建议、密评活动有效性证明记录等内容的编制功能；

2）方案密评报告编制功能可支持自动生成完整的方案密评报告，输出的方案密评报告应符合中国密码学会密评联委会最新发布的方案密评报告模板，并满足报告模板的格式要求；

3）方案密评报告编制功能可支持密码应用方案的插入和格式修订；

4）方案密评报告编制功能可支持密码应用方案对应的初步量化评估结果。

b）密评报告编制工具应具备系统密评报告编制功能：

1）密评报告编制工具应支持系统基本信息、测评结果记录、密评活动有效性证明记录等内容的编制功能；

2）密评报告编制工具应具备量化评估功能，量化评估规则应符合中国密码学会密评联委会最新发布的《商用密码应用安全性评估量化评估规则》文件要求；

3）密评报告编制工具应支持自动生成完整的系统密评报告，输出的系统密评报告应符合中国密码学会密评联委会最新发布的系统密评报告模板的格式要求。

c）密评报告编制工具可支持密评人员间协同撰写密评报告，支持报告撰写完成后自动生成和导出。

d）密评报告编制工具可支持报告自动查错功能。

e）密评报告编制工具应支持报告模板导入和更新功能。

f）密评报告编制工具应支持报告模板的可编辑功能，能够满足云平台、有特殊指标要求的信息系统等密评报告的编制需求。

g）密评报告编制工具可支持数据互通功能，能够支持同一信息系统的方案密评报告、系统密评报告中相同数据的复用。

6.3.2 扩展性

密评报告编制工具可保留二次开发接口，支持用户二次开发扩展功能，满足特定需求。

6.4 密评项目管理工具

6.4.1 基础功能

a）密评项目管理工具应具备项目基本信息管理功能，项目基本信息包括但不限于：网络与信息系统名称、网络安全等级保护级别、系统责任单位（运营者）、委托单位、合同金额、前次密评

情况、评估结论、系统得分、服务领域、密评时间、密评备案部门、项目合同/委托书、密评报告等。

b）密评项目管理工具应支持用户权限划分，针对密评项目组长、密评人员、管理员等不同角色设置不同权限。

c）密评项目管理工具应具备密评人员信息管理功能，密评人员信息包括但不限于：密评人员基本信息、密评人员参与的项目、项目角色、实施密评活动人员组成、密评人员资格情况、现场测评时间等。

d）密评项目管理工具可具备密评任务管理功能，可对密评项目执行节点、任务执行情况等进行跟踪分析。

e）密评项目管理工具应具备密评结果备案管理功能，备案信息模板应符合国家密码管理局最新发布的模板要求。

f）密评项目管理工具应具备项目信息导入导出功能。

6.4.2 统计分析

密评项目管理工具可具备密评数据统计分析功能。

a） 密评项目管理工具可支持从信息系统密评结论、综合得分、行业领域、地区、通过率、年份等维度对信息系统密评结果进行统计分析。

b） 密评项目管理工具可支持对信息系统密评结果、安全问题、遗留风险等维度进行统计分析，可跟踪密评项目逐年改造节点，增加密评项目延续性。

c） 密评项目管理工具可支持对统计分析结果进行可视化展示，能够以表格、直方图等形式，按照年份体现每年参与项目的数量、行业分布、被测系统等级等情况。

7 信息系统商用密码应用安全测评工具使用指引

7.1 概述

使用商用密码应用安全性评估测评工具开展密评工作时，应在不影响被测系统正常运行的情况下，依据测评方案中确定的测评对象、测评指标、测评工具接入点及测评内容实施，各测评单元、测评对象的测评结果还需结合访谈、文档审查、实地查看、配置检查等多种测评方法，进行综合判定。

7.2 物理和环境安全测评工具使用指引

物理和环境安全测评中各测评单元测评工具使用指引如表8所示。

表 8 物理和环境安全测评工具推荐表

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	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；	密码算法校验工具 APDU 报文分析工具 密码应用缺陷验证工具	1)密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 2)APDU 报文分析工具可用于分析门禁卡与读卡器之间的APDU 报文； 3)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
电子门禁记录数据存储完整性	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；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验电子门禁记录数据存储完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析电子门禁记录数据存储完整性保护相关代码；

测评单元	测评内容	测评工具推荐建议	工具说明
			3)接口测试工具可用于测试密码相关接口的安全性。
视频监控记录数据存储完整性	采用密码技术保证视频监控音像记录数据的存储完整性。	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验视频监控记录数据存储完整性 保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析视频监控记录数据存储完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。

7.3 网络和通信安全测评工具使用指引

网络和通信安全测评中各测评单元测评工具使用指引如表9所示。

表 9 网络和通信安全测评工具推荐表

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	采用密码技术对通信实体进行单向或双向身份鉴别，保证通信实体身份的真实性；	端口扫描工具 数字证书校验工具 协议分析工具 密码算法校验工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性； 3)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 4)密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
通信数据完整性	采用密码技术保证通信过程中数据的完整性；	端口扫描工具 协议分析工具 密码算法校验工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 3)密码算法校验工具可用于校验通信数据完整性保护所使用密码算法的合规性、正确性； 4)密码应用缺陷验证工具可用于识别、利用通信过程中数据的完整性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
通信过程中重要数据的机密性	采用密码技术保证通信过程中重要数据的机密性；	端口扫描工具 协议分析工具 密码算法校验工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 3)密码算法校验工具可用于校验通信过程中重要数据的机密性保护所使用密码算法的合规性、正确性； 4)密码应用缺陷验证工具可用于识别、利用通信过程中重要数据的机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 5)随机数检测工具可用于检测 IPSec、TLS、TLCP 等协议中密文数据的随机性。

测评单元	测评内容	测评工具推荐建议	工具说明
网络边界访问控制信息的完整性	采用密码技术保证网络边界访问控制信息的完整性；	端口扫描工具 密码算法校验工具 源代码审计工具 接口测试工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)密码算法校验工具可用于校验网络边界访问控制信息的完整性保护所使用密码算法的合规性、正确性。 3)源代码审计工具可用于分析网络边界访问控制信息的完整性保护相关代码； 4)接口测试工具可用于测试密码相关接口的安全性。
安全接入认证	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。	端口扫描工具 数字证书校验工具 协议分析工具 密码算法校验工具 源代码审计工具 接口测试工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性； 3)协议分析工具可用于分析设备接入通道涉及的协议类型、协议版本、密钥交换过程、密码算法等；分析安全接入认证的工作机制； 4)密码算法校验工具可用于校验安全接入认证所使用密码算法的合规性、正确性； 5)源代码审计工具可用于分析安全接入认证相关代码； 6)接口测试工具可用于测试密码相关接口的安全性； 7)密码应用缺陷验证工具可用于识别、利用安全接入认证存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

7.4 设备和计算安全测评工具使用指引

设备和计算安全测评中各测评单元测评工具使用指引如表10所示。

表 10 设备和计算安全测评工具推荐表

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	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；	端口扫描工具 数字证书校验工具 协议分析工具 密码算法校验工具 源代码审计工具 接口测试工具 APDU 报文分析工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性； 3)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析对登录设备的用户进行身份鉴别的工作机制； 4)密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5)源代码审计工具可用于分析身份鉴别相关代码； 6)接口测试工具可用于测试密码相关接口的安全性； 7)APDU 报文分析工具可用于分析密码卡、智能密码钥匙等的 APDU 报文； 8)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
远程管理通道安全	远程管理设备时，采用密码技术建立安全的信息传输通道；	端口扫描工具 数字证书校验工具 协议分析工具 密码算法校验工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性；

测评单元	测评内容	测评工具推荐建议	工具说明
		密码应用缺陷验证工具	3)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 4)密码算法校验工具可用于校验远程管理通道所使用密码算法的合规性、正确性； 5)密码应用缺陷验证工具可用于识别、利用远程管理通道存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 6)随机数检测工具可用于检测 IPSec、TLS、TLCP 等协议中密文数据的随机性。
系统资源访问控制信息完整性	采用密码技术保证系统资源访问控制信息的完整性；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验系统资源访问控制信息完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析系统资源访问控制信息完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
重要信息资源安全标记完整性	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；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验重要信息资源安全标记完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析重要信息资源安全标记完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
日志记录完整性	采用密码技术保证日志记录的完整性；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验日志记录完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析日志记录完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
重要可执行程序完整性、重要可执行程序来源真实性	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。	数字证书校验工具 密码算法校验工具 源代码审计工具 接口测试工具 逆向分析工具	1)数字证书校验工具可用于校验数字证书有效性； 2)密码算法校验工具可用于校验重要可执行程序完整性和来源真实性保护所使用密码算法的合规性、正确性； 3)源代码审计工具可用于分析重要可执行程序完整性和来源真实性保护相关代码； 4)接口测试工具可用于测试密码相关接口的安全性； 5)逆向分析工具可用于分析重要可执行程序完整性和来源真实性保护的工作机制。

7.5 应用和数据安全测评工具使用指引

应用和数据安全测评中各测评单元测评工具使用指引如表11所示。

表 11 应用和数据安全测评工具推荐表

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	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；	端口扫描工具 数字证书校验工具 协议分析工具 密码算法校验工具 源代码审计工具 接口测试工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性； 3)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析对登录用户进行身份鉴别的工作机制；

测评单元	测评内容	测评工具推荐建议	工具说明
		APDU 报文分析工具 密码应用缺陷验证工具	4)密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5)源代码审计工具可用于分析身份鉴别相关代码； 6)接口测试工具可用于测试密码相关接口的安全性； 7)APDU 报文分析工具可用于分析智能密码钥匙等的 APDU 报文。 8)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
访问控制信息完整性	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；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验访问控制信息完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析访问控制信息完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
重要信息资源安全标记完整性	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；	密码算法校验工具 源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验重要信息资源安全标记完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析重要信息资源安全标记完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
重要数据传输机密性	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；	端口扫描工具 协议分析工具 密码算法校验工具 源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析重要数据传输机密性保护的工作机制； 3)密码算法校验工具可用于校验重要数据传输机密性保护所使用密码算法的合规性、正确性； 4)源代码审计工具可用于分析重要数据传输机密性保护相关代码； 5)接口测试工具可用于测试密码相关接口的安全性； 6)编码转换工具可用于对所采集数据进行编码转换、编码解析等； 7)密码应用缺陷验证工具可用于识别、利用重要数据传输机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 8)随机数检测工具可用于检测使用加密算法对数据进行机密性保护后的密文数据的随机性。
重要数据存储机密性	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；	密码算法校验工具 源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1)密码算法校验工具可用于校验重要数据存储机密性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析重要数据存储机密性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性； 4)编码转换工具可用于对所采集数据进行编码转换、编码解析等；

测评单元	测评内容	测评工具推荐建议	工具说明
			5)密码应用缺陷验证工具可用于识别、利用重要数据存储机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 6)随机数检测工具可用于检测使用加密算法对数据进行机密性保护后的密文数据的随机性。
重要数据传输完整性	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；	端口扫描工具 协议分析工具 密码算法校验工具 电子签章校验工具 源代码审计工具 接口测试工具 编码转换工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析重要数据传输完整性保护的工作机制； 3)密码算法校验工具可用于校验重要数据传输完整性保护所使用密码算法的合规性、正确性； 4)电子签章校验工具可用于校验电子签章数据传输完整性保护的合规性、正确性； 5)源代码审计工具可用于分析重要数据传输完整性保护相关代码； 6)接口测试工具可用于测试密码相关接口的安全性； 7)编码转换工具可用于对所采集数据进行编码转换、编码解析等。
重要数据存储完整性	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；	密码算法校验工具 电子签章校验工具 源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1)密码算法校验工具可用于校验重要数据存储完整性保护所使用密码算法的合规性、正确性； 2)电子签章校验工具可用于校验电子签章数据存储完整性保护的合规性、正确性； 3)源代码审计工具可用于分析重要数据存储完整性保护相关代码； 4)接口测试工具可用于测试密码相关接口的安全性； 5)编码转换工具可用于对所采集数据进行编码转换、编码解析等； 6)密码应用缺陷验证工具可用于识别、利用重要数据存储完整性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
不可否认性	在可能涉及法律责任认定的应用中，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。	密码算法校验工具 电子签章校验工具 源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1)密码算法校验工具可用于校验不可否认性保护所使用密码算法的合规性、正确性； 2)电子签章校验工具可用于校验在进行电子签章操作时，不可否认性保护的合规性、正确性； 3)源代码审计工具可用于分析不可否认性保护的相关代码； 4)接口测试工具可用于测试密码相关接口的安全性； 5)编码转换工具可用于对所采集数据进行编码转换、编码解析等； 6)密码应用缺陷验证工具可用于识别、利用不可否认性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

附　录　A
（资料性）
密码应用安全测评工具使用示例

某网络安全等级保护第三级的信息系统网络拓扑图如图2所示，基于该信息系统现状给出相应测评工具使用示例。

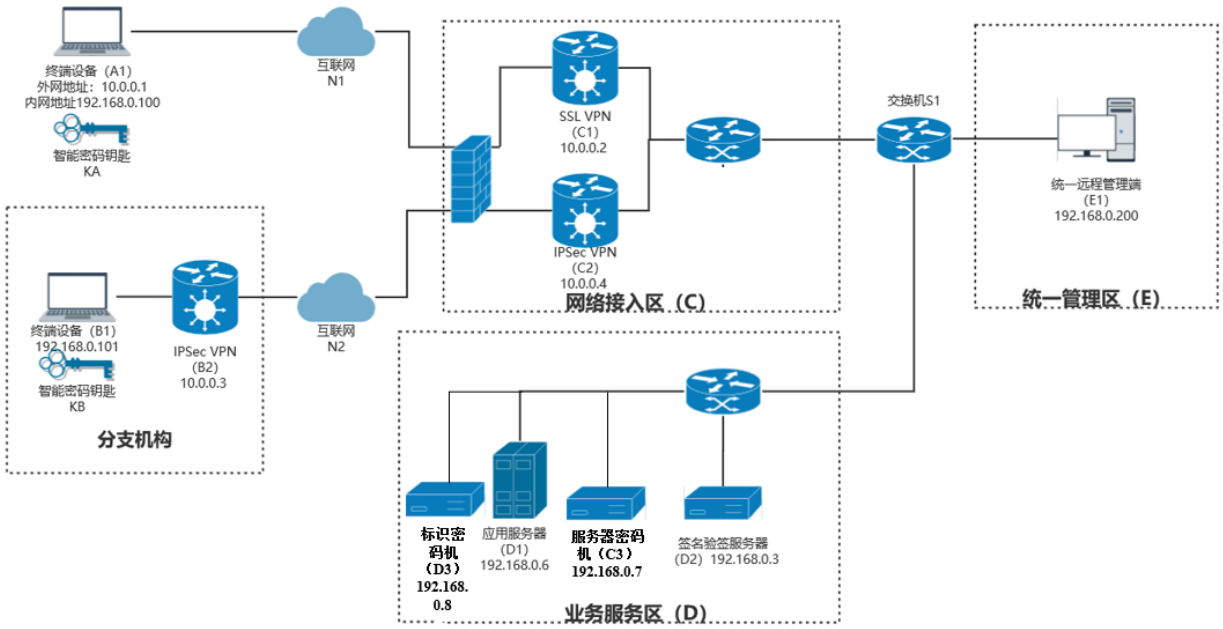


图2 某信息系统网络拓扑图

A.1　密码算法校验工具使用示例

A.1.1　算法校验场景示例

信息系统可能涉及到算法校验的场景如下：

a)　业务应用：

1) 用户每次关键操作需要调用自己的智能密码钥匙进行SM2签名；应用服务器（D1）调用签名验签服务器（D2）进行校验。该关键操作信息连同签名一起存放在应用服务器（D1）的数据库中。
2) 用户每次关键操作需要调用自己的智能密码钥匙进行SM9签名；应用服务器（D1）调用标识密码机（D3）进行校验。

b)　数据存储：

1) 用户口令（password）使用SM3算法进行杂凑计算后，将得到完整的杂凑值（h=SM3(password||salt)）存放在应用服务器（D1）的数据库中。
2) 应用服务器（D1）的数据库中，用户的单条记录（包括口令杂凑值、身份证号、手机号等密文值、角色、权限等）使用HMAC-SM3算法计算后，把得到的MAC值一并存放在该条目中。

A.1.2 密码算法校验工具测试实施示例

A.1.2.1 密码杂凑算法校验

a） 操作过程

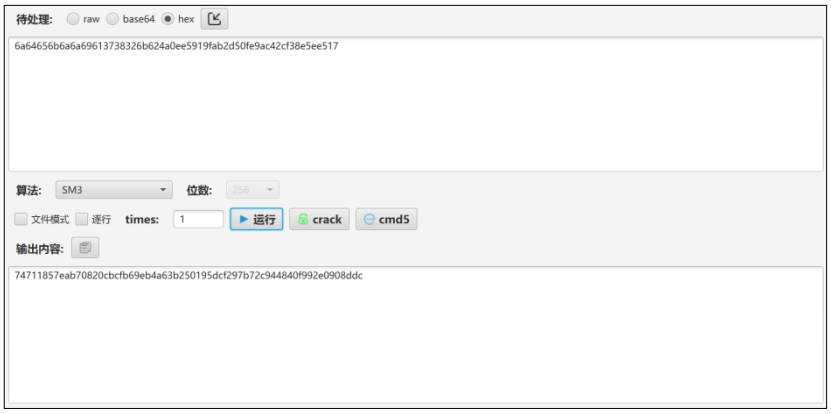
针对b)数据存储：1)用户口令（password）使用SM3算法进行杂凑计算后，将得到完整的杂凑值（h=SM3(password||salt)）存放在应用服务器（D1）的数据库中。密评人员向被测信息系统方收集用于算法校验的相关信息：

表12 密码杂凑算法校验收集信息表

值	选项	描述
原文	必选	请用户配合从应用服务器（D1）的数据库中取出用户口令（password），需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
盐值（Salt）/位置	可选	请用户配合取出与password对应的Salt，需要确认编码格式，使用编码转换工具，将最终可识别数据输入到工具中。 Salt、Salt位置在前或在后为可选参数，若采用密码杂凑算法加盐的方式保护数据，则此值必选。
杂凑值	可选	采用工具比对或人工比对，若采用工具比对，则请用户配合从应用服务器（D1）的数据库中取出杂凑值，需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。

b） 工具示例

表 13 密码杂凑算法校验工具示例表

场景	工具示例	结果
密评人员获取口令原文、盐值，选择编码方式，进行SM3运算，得到杂凑值。		经人工比对杂凑值，结果比对一致，验证通过。

A.1.2.2 消息鉴别码（MAC）算法校验

a） 操作过程

针对b）数据存储：2)应用服务器（D1）的数据库中，用户的单条记录（包括口令杂凑值、身份证号、手机号等密文值、角色、权限等）使用HMAC-SM3算法计算后，把得到的MAC值一并存放在该条目中。密评人员向被测信息系统方收集用于算法校验的相关信息：

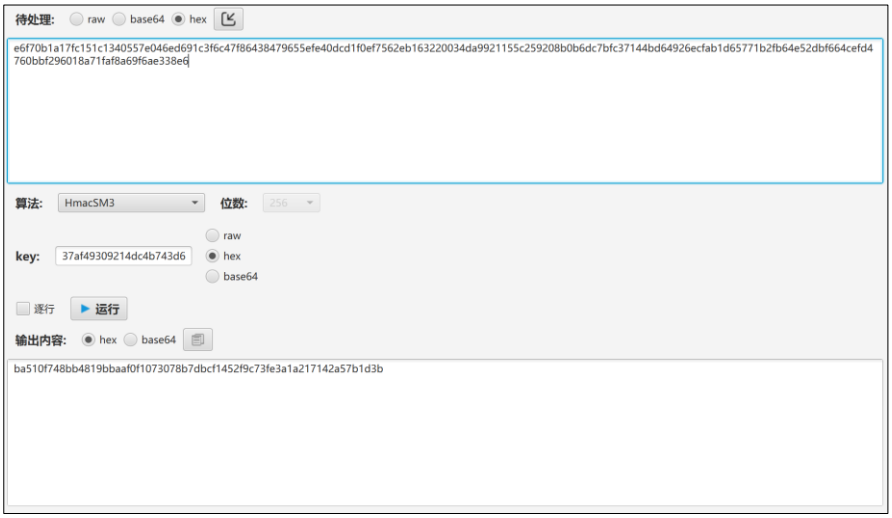
表14 消息鉴别码算法校验收集信息表

值	选项	描述
原文	必选	请用户配合从应用服务器（D1）的数据库中取出用户的单条记录，需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
消息鉴别码（MAC）算法	必选	CBC-MAC、CMAC、HMAC等。

值	选项	描述
密钥	必选	在实际测评中，如无法获取生产密钥，可尝试使用测试密钥。
填充模式	可选	如涉及使用填充模式，根据实际情况选择填充模式。
消息鉴别码	可选	采用工具比对或人工比对，若采用工具比对，则请用户配合从应用服务器（D1）的数据库中取出MAC值，需要确认编码格式，使用编码转换工具，将最终可识别数据输入到工具中。

b） 工具示例

表 15 消息鉴别码算法校验工具示例表

场景	工具示例	结果
密评人员获取原文、密钥，选择编码方式，进行HMAC-SM3运算，得到MAC值。		经人工比对MAC值，结果比对一致，验证通过。

A.1.2.3 非对称密码算法校验

A.1.2.3.1 SM2 密码算法（签名验签）

a） 操作过程

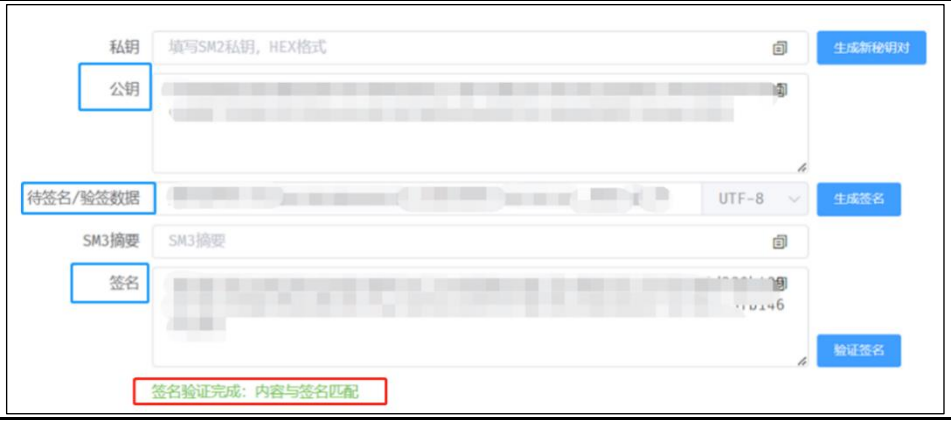
针对 a）业务应用：1）用户每次关键操作需要调用自己的智能密码钥匙进行 SM2 签名；应用服务器（D1）调用签名验签服务器（D2）进行校验。该关键操作信息连同签名一起存放在应用服务器（D1）的数据库中。密评人员向被测信息系统方收集用于算法校验的相关信息：

表 16 SM2 密码算法校验收集信息表

值	选项	描述
签名原文	必选	请用户配合从应用服务器（D1）的数据库中取出关键操作信息，需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
签名值	必选	请用户配合从应用服务器（D1）的数据库中取出签名值，需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
公钥	可选	验签时，将用户智能密码钥匙中的证书或公钥导入到工具中。
私钥	可选	签名时，在实际测评中，如无法获取生产私钥，可尝试使用测试私钥。
User ID	可选	确认用户标识值（通常采用默认值）。

b） 工具示例

表 17 SM2 密码算法校验工具示例表

场景	工具示例	结果
密评人员得到签名原文、签名值和公钥，输入到工具中进行验签。		经工具测试，验签通过。

A.1.2.3.2 SM9 密码算法（签名验签）

a） 操作过程

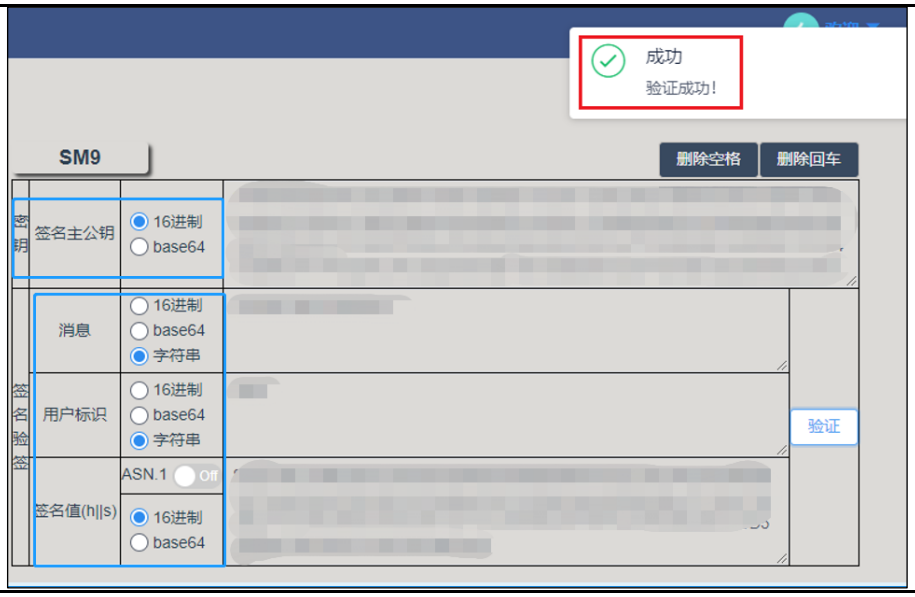
针对 a）业务应用：2）用户每次关键操作需要调用自己的智能密码钥匙进行 SM9 签名；应用服务器（D1）调用标识密码机（D3）进行校验。密评人员向被测信息系统方收集用于算法校验的相关信息：

表 18 SM9 密码算法校验收集信息表

值	选项	描述
签名值	必选	需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
签名原文	必选	需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
用户标识	可选	确认用户标识值，需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。
签名主公钥	可选	需要确认编码格式，使用编码转换工具进行转换，将最终可识别数据输入到工具中。

b） 工具示例

表 19 SM9 密码算法校验工具示例表

场景	工具示例	结果
密评人员得到签名主公钥、签名原文、用户标识、签名值，输入工具进行验签。		经工具测试，验证签名通过。

A.2 协议分析工具使用示例

A.2.1 协议分析场景示例

信息系统可能涉及到协议分析的场景如下：

a) 网络接入：

1) 远程办公用户（A1）安装SSL VPN客户端，通过SSL VPN网关（C1）接入到单位内网。通过TLCP协议建立客户端与服务端的连接，实现通信实体的身份鉴别、通信数据的机密性和完整性保护。
2) 分支机构用户（B1）在本地部署IPSec VPN（B2），在单位部署IPSec VPN（C2）。通过IPSec协议建立IPSec VPN（B2）与IPSec VPN（C2）的连接，实现通信实体的身份鉴别、通信数据的机密性和完整性保护。

b) 管理和运维：

1) 管理和运维人员终端（E1）通过SSH协议对服务器进行远程管理和运维。

A.2.2 协议分析工具测试实施示例

a）操作过程

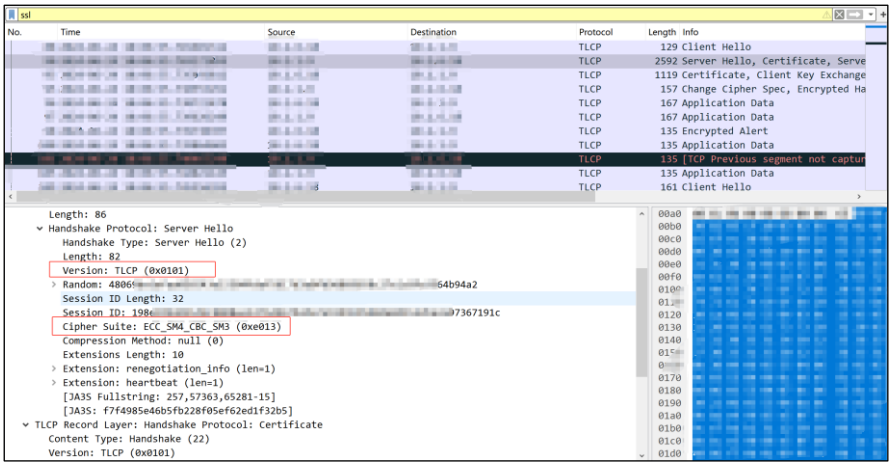
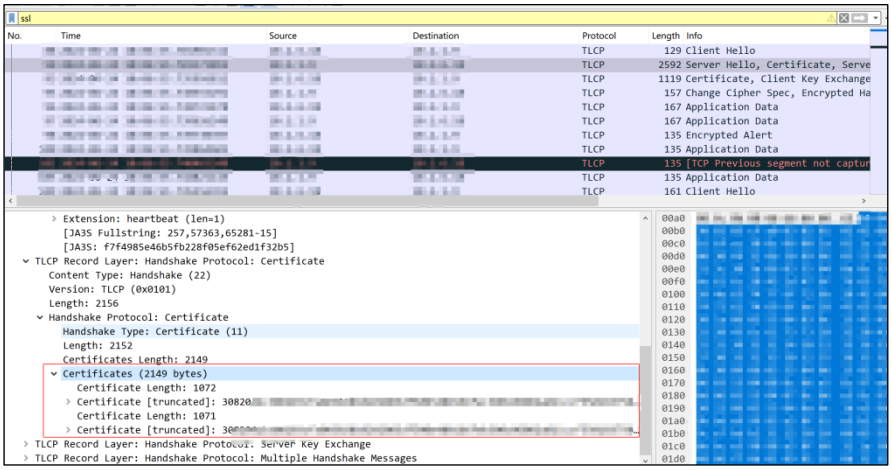
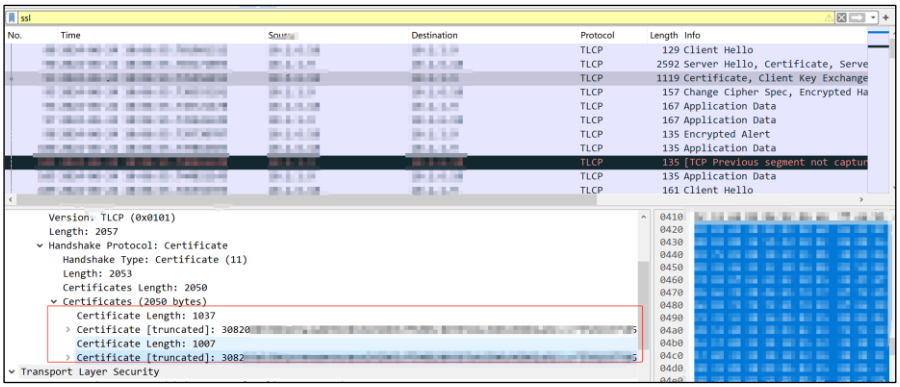
针对示例场景，密评人员向被测信息系统方收集用于协议分析的相关信息：

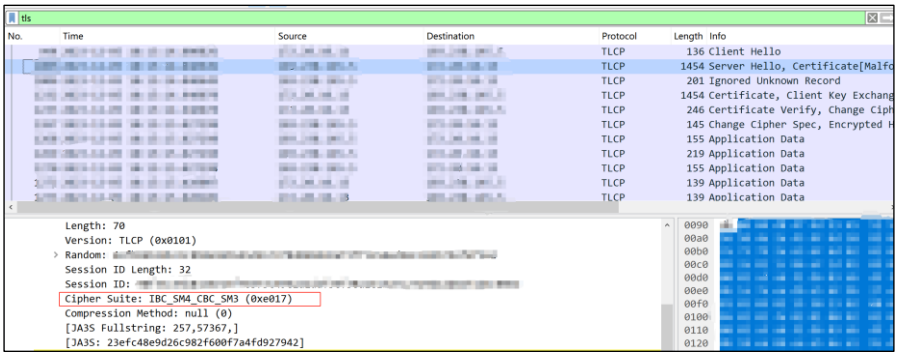
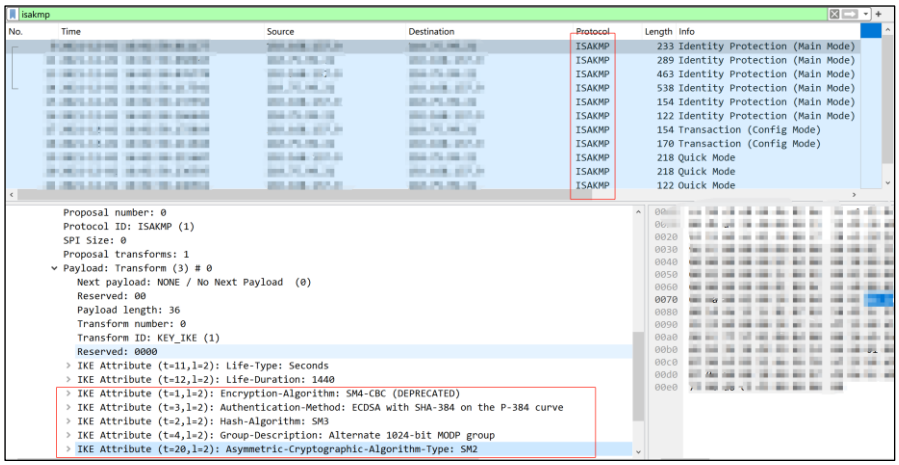
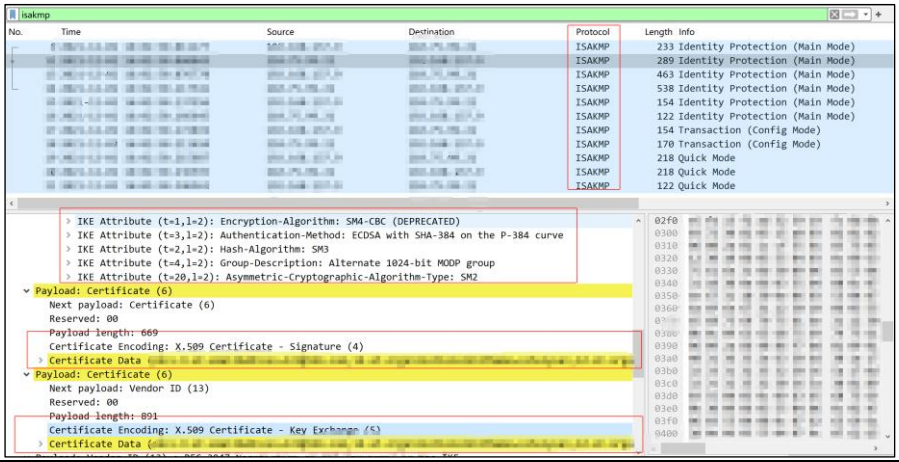
表 20 协议分析工具收集信息表

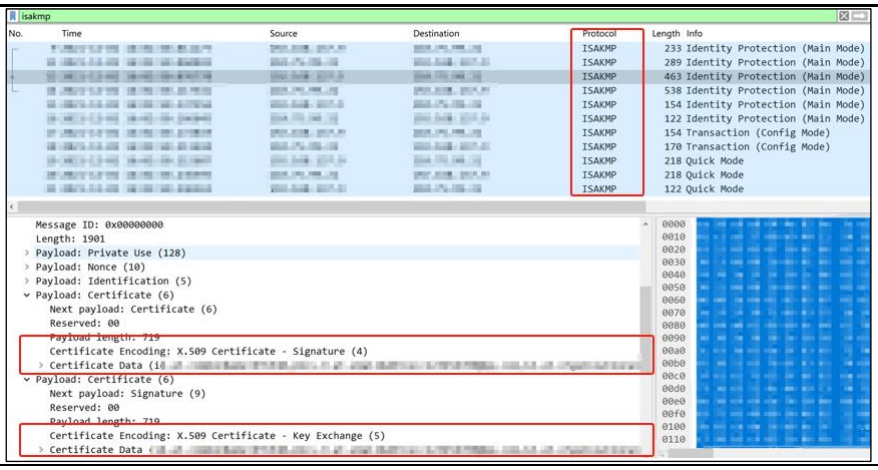
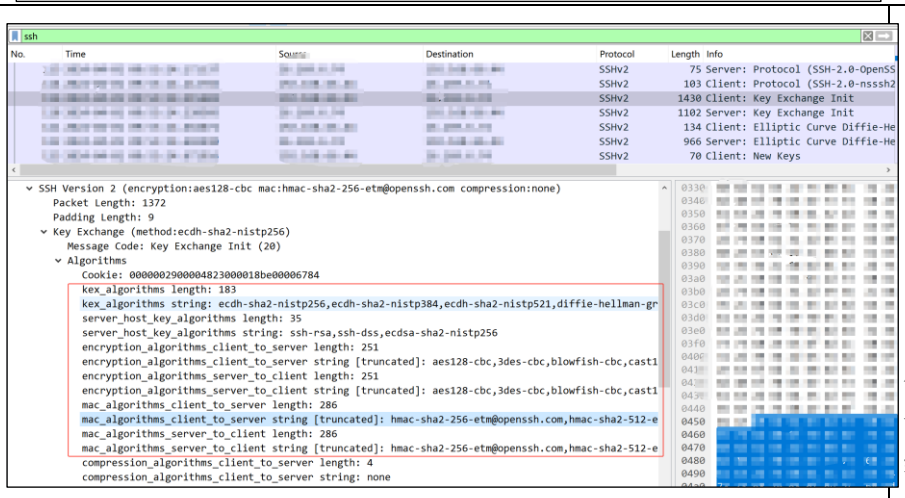
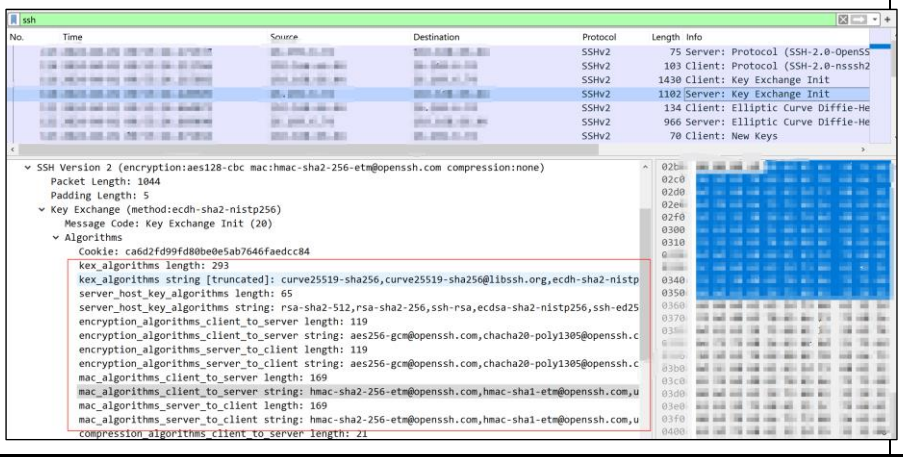
值	选项	描述
流量数据包	必选	a）网络接入： 1）密评人员在被测信息系统方现场收集离线数据流量，在A1或者C1（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。 2）密评人员在被测信息系统方现场收集离线数据流量，在B2或者C2（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。 b)管理和运维： 密评人员在被测信息系统方现场收集离线数据流量，在E1（也可能是交换机上获取镜像流量），获取流量包后，使用离线协议分析工具打开。
源IP/端口	可选	流量分析必要因素
目的IP/端口	可选	流量分析必要因素
采用协议	可选	流量分析必要因素
关键字	可选	协议相关的关键字

b）工具示例

表 21 协议分析工具示例表

场景	工具示例	结果
密评人员在被测信息系统方现场收集离线数据流量，在A1或者C1（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。	  	通过部署 SSL VPN，使用 TLCP 协议建立客户端与服务端的连接，使用 ECC_SM4_CBC_SM3 密码算法套件，可进一步通过数字证书校验工具校验数字证书的有效性。

场景	工具示例	结果
密评人员在被测信息系统方现场收集离线数据流量，在A1或者C1（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。		通过部署 SSL VPN，使用 TLCP 协议建立客户端与服务端的连接，使用 IBC_SM4_CBC_SM3 密码算法套件。
密评人员在被测信息系统方现场收集离线数据流量，在B2或者C2（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。	 	通过部署 IPSec VPN，使用 IPSec 协议建立 IPSec VPN 之间的连接，使用 SM2、SM3、SM4 密码算法，可进一步通过数字证书校验工具校验数字证书的有效性。

场景	工具示例	结果
		
密评人员在被测信息系统方现场收集离线数据流量，在E1（也可能是交换机上获取镜像流量）获取流量包后，使用离线协议分析工具打开。	 	使用SSH（V2）协议建立运维终端与服务器之间的连接，使用国外密码算法。

A.3 数字证书校验工具使用示例

A.3.1 数字证书校验场景示例

信息系统可能涉及到数字证书校验的场景如下：

a) 网络接入：

1) 远程办公用户（A1）安装SSL VPN客户端，通过SSL VPN网关（C1）接入到单位内网。通过TLCP协议建立客户端与服务端的连接，实现通信实体的身份鉴别、通信数据的机密性和完整性保护。
2) 分支机构用户（B1）在本地部署IPSec VPN（B2），在单位部署IPSec VPN（C2）。通过IPSec协议建立IPSec VPN（B2）与IPSec VPN（C2）的连接，实现通信实体的身份鉴别、通信数据的机密性和完整性保护。

b) 应用用户登录：

1) 远程办公用户（A1）和分支机构用户（B1）均配发了智能密码钥匙（KA和KB），智能密码钥匙中存放了SM2数字证书和对应私钥，用户登录应用时，使用用户名+口令和智能密码钥匙+PIN码方式进行身份鉴别。

c) 关键操作行为：

1) 用户具有对合同进行签章的权限，可以利用智能密码钥匙配合签章软件对合同进行电子签章，使用的算法为SM2和SM3。

A.3.2 数字证书校验工具测试实施示例

a) 操作过程

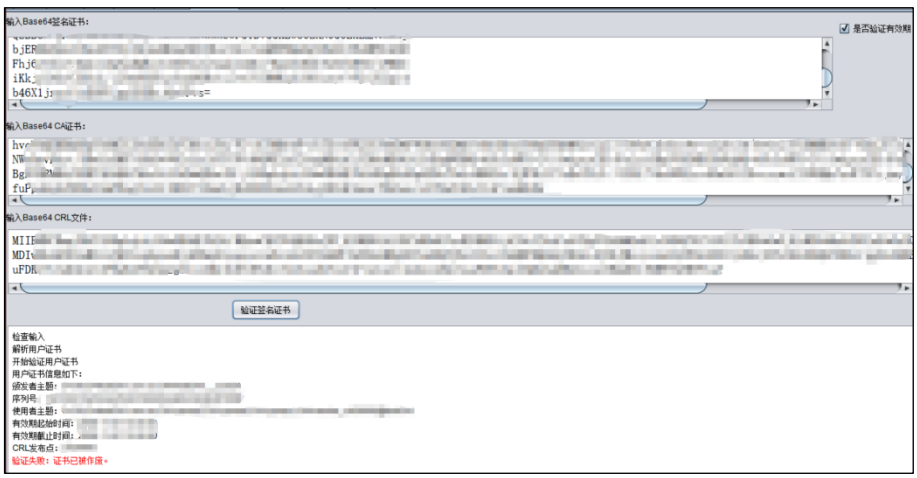
针对示例场景，密评人员向被测信息系统方收集用于数字证书校验的相关信息：

表 22 数字证书校验工具收集信息表

值	选项	描述
数字证书	必选	综合利用访谈、人工分析、配置核查、工具测试等方式获取数字证书。
CA证书链	必选	综合利用访谈、人工分析、配置核查、工具测试等方式获取CA证书。
CRL文件	可选	可通过CRL方式查询证书撤销状态。

b）工具示例

表 23 数字证书校验工具示例表

场景	工具示例	结果
密评人员输入数字证书、CA证书、CRL文件，校验证书有效性。		数字证书已作废。

A.4 随机数检测工具使用示例

A.4.1 随机数检测场景示例

信息系统可能涉及到随机数检测的场景如下：

a) 检测取自合规或者不合规的随机数发生器产生的随机数的随机性；

b) 检测使用加密算法对数据进行机密性保护后的密文数据的随机性；

c) 检测 IPSec、TLS、TLCP 等协议中密文数据的随机性。

A.4.2 随机数检测工具测试实施示例

a) 操作过程

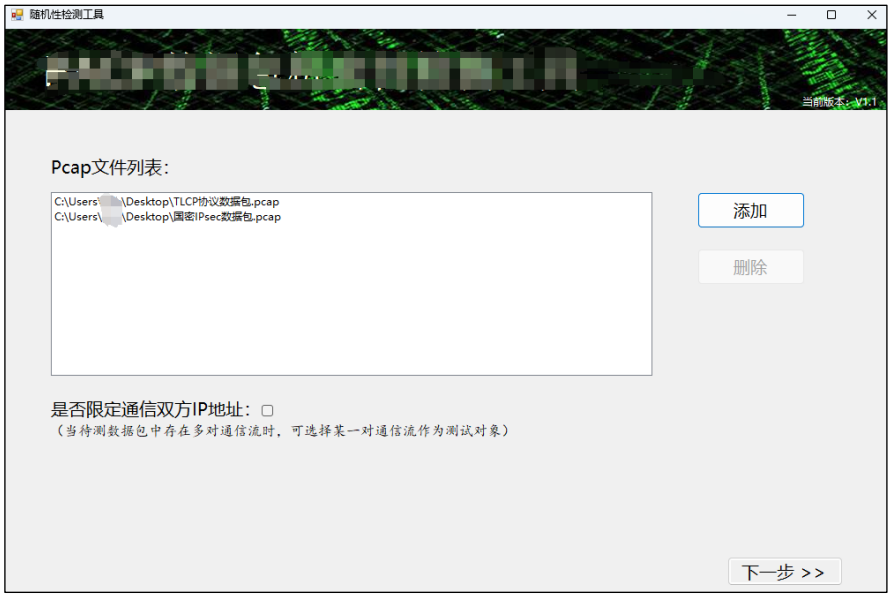
针对示例场景，密评人员向被测信息系统方收集用于检测的随机数相关信息：

表 24 随机数检测工具收集信息表

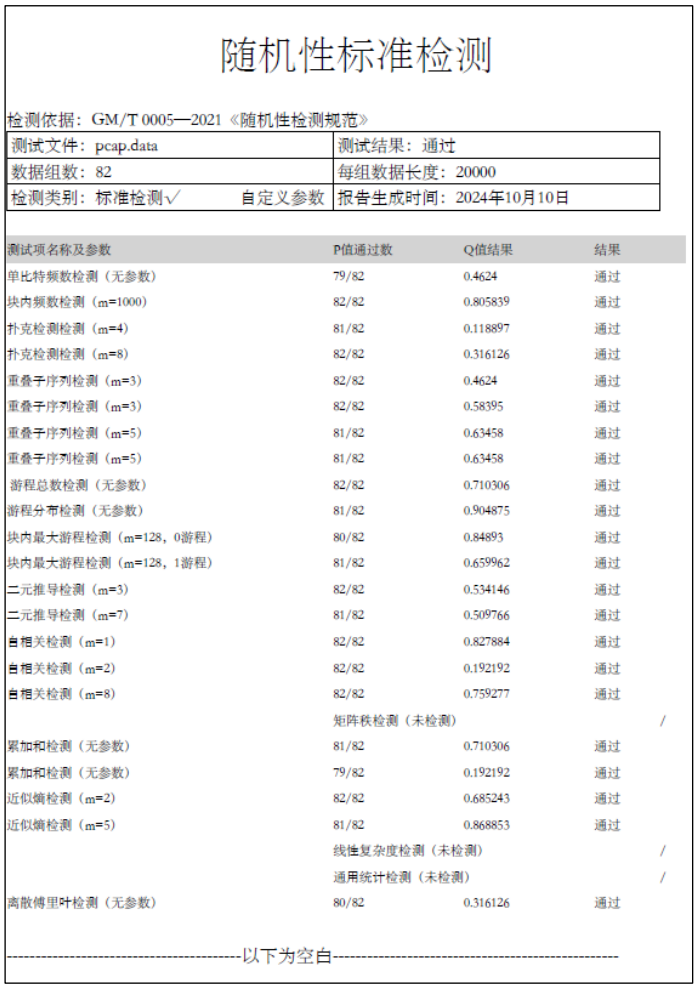
值	选项	描述
随机数样本数据文件	必选	获取被测信息系统随机数样本，数据库中密文数据，或者IPSec、TLS/TLCP等通信数据包。

b) 工具示例

表 25 随机数检测工具示例表

场景	示例	结果
从通信数据包中自动提取密文数据后进行随机数检测		从通信数据包中自动提取密文数据后，确定随机数分组比特长度、组数等信息，确定随机数检测项目，根据 GM/T 0005《随机性检测规范》输出检测结果。

场景	示例	结果
	 随机性检测工具 正在解析文件 ----------1.通信数据解析---------- C:\Users\ \Desktop\TLCP协议数据包.pcap 开始执行通信数据解析... SSL/TLS包数量：516 IPsec包数量：0 ----------2.通信数据解析---------- C:\Users\ \Desktop\国密IPsec数据包.pcap 开始执行通信数据解析... SSL/TLS包数量：0 IPsec包数量：1752 数据解析完毕! 分组长度: 20000, 组数: 82 返回 下一步 >>  随机性检测工具 国家标准分组设置 随机数测试平台（国密标准）v1.1是一款随机数统计检测软件，依据2021版《随机性检测规范》进行实现，共有15项检测。每次检测需要若干组等长度数据。标准长度有2*10^4、10^6和10^8比特三种，标准测试组数为1000组。数据存储为二进制文件格式。测试结果评价标准为一级检测P值通过率和二级检测Q值数值。当15项检测全部通过时，认定待测数据通过该测试；否则，认定待测数据无法通过该测试。 使用标准分组长度 20000 组数 82 使用自定义分组长度 1000000 << 上一步 下一步 >>  国家标准检测项目 全选检测项 是否使用自定义参数（多个参数请用英文逗号分开） 1、单比特频数检测 2、块内频数检测 10 子序列长度m 3、扑克检测 4,8 子序列长度m 4、重叠子序列检测 3,5 子序列长度m 5、游程总数检测 6、游程分布检测 7、块内最大游程检测 8、二元推导检测 3,7 二元推导K次 9、自相关检测 2,8 左移位数d 10、矩阵秩检测 11、累加和检测 12、近似熵检测 2,5 子序列长度m 13、线性复杂度检测 500,1000 子序列长度m 14、Maurer通用统计检测 15、离散傅里叶检测 << 上一步 下一步 >>	

场景	示例	结果
		

随机性标准检测

检测依据：GM/T 0005—2021《随机性检测规范》

测试文件：pcap.data	测试结果：通过
数据组数：82	每组数据长度：20000
检测类别：标准检测√　　自定义参数	报告生成时间：2024年10月10日

测试项名称及参数	P值通过数	Q值结果	结果
单比特频数检测（无参数）	79/82	0.4624	通过
块内频数检测（m=1000）	82/82	0.805839	通过
扑克检测检测（m=4）	81/82	0.118897	通过
扑克检测检测（m=8）	82/82	0.316126	通过
重叠子序列检测（m=3）	82/82	0.4624	通过
重叠子序列检测（m=3）	82/82	0.58395	通过
重叠子序列检测（m=5）	81/82	0.63458	通过
重叠子序列检测（m=5）	81/82	0.63458	通过
游程总数检测（无参数）	82/82	0.710306	通过
游程分布检测（无参数）	81/82	0.904875	通过
块内最大游程检测（m=128，0游程）	80/82	0.84893	通过
块内最大游程检测（m=128，1游程）	81/82	0.659962	通过
二元推导检测（m=3）	82/82	0.534146	通过
二元推导检测（m=7）	81/82	0.509766	通过
自相关检测（m=1）	82/82	0.827884	通过
自相关检测（m=2）	82/82	0.192192	通过
自相关检测（m=8）	82/82	0.759277	通过
	矩阵秩检测（未检测）		/
累加和检测（无参数）	81/82	0.710306	通过
累加和检测（无参数）	79/82	0.192192	通过
近似熵检测（m=2）	82/82	0.685243	通过
近似熵检测（m=5）	81/82	0.868853	通过
	线性复杂度检测（未检测）		/
	通用统计检测（未检测）		/
离散傅里叶检测（无参数）	80/82	0.316126	通过

----------以下为空白----------

A.5 电子签章校验工具使用示例

A.5.1 电子签章校验场景示例

信息系统可能涉及到电子签章验证的情况如下：

a) 业务应用：用户具有对合同进行签章的权限，可以利用智能密码钥匙配合签章软件对合同进行电子签章，使用的算法为 SM2 和 SM3。

A.5.2 电子签章校验工具测试实施示例

a) 操作过程

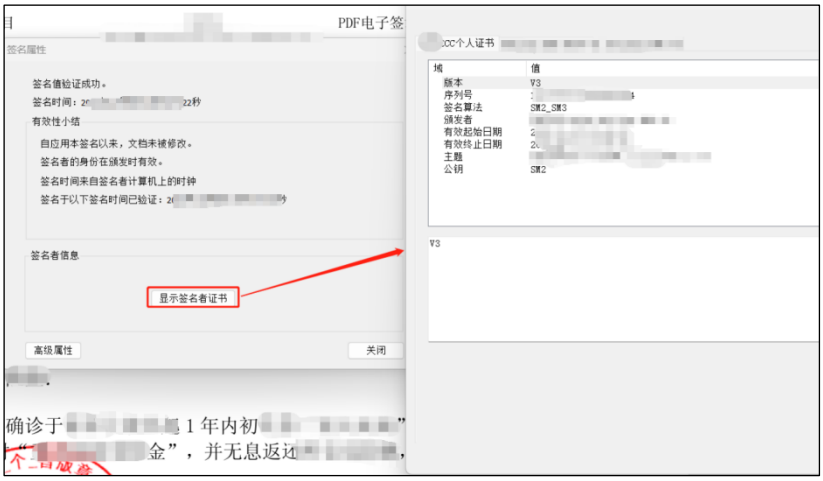
针对示例场景，密评人员向被测信息系统方收集用于电子签章校验的相关信息：

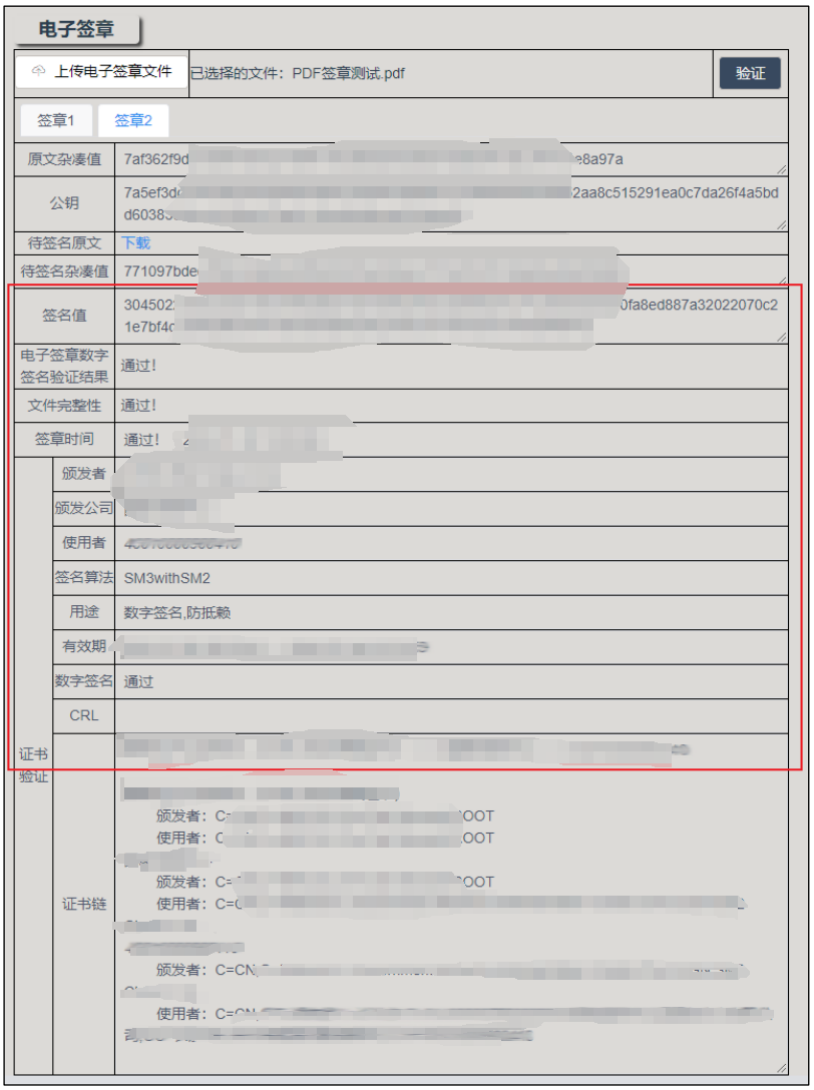
表 26 电子签章校验工具收集信息表

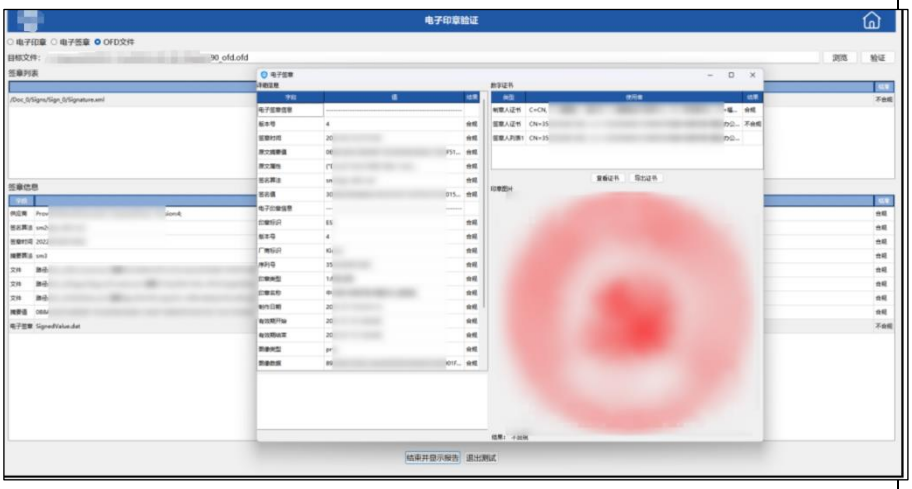
值	选项	描述
电子签章文件	必选	获取被测信息系统电子签章文件

b) 工具示例

表 27 电子签章校验工具示例表

场景	示例	结果
PDF 签章		电子签章文件校验通过。

场景	示例	结果
		
OFD 签章		电子签章文件校验通过。

场景	示例	结果
		

电子签章

上传电子签章文件 | 已选择的文件：OFD签章测试.ofd | 验证

签章1 | 签章2 | 签章3

原文杂凑值	b08ad99e3 ... h32a1cb
公钥	b264d1 ... fc425ee7441e4032db5c50e 69c07
待签名原文	下载
待签名杂凑值	481fd9
签名值	97488 ... 5db0618 67e4
电子签章数字签名验证结果	通过！
文件完整性	通过！
签章时间	通过！ (
证书验证 颁发者	
证书验证 颁发公司	
证书验证 使用者	
证书验证 签名算法	SM3withSM2
证书验证 用途	数字签名,防抵赖,密钥加密,密钥协议
证书验证 有效期	
证书验证 数字签名	通过
证书验证 CRL	
证书链	颁发者: 使用者: 颁发者: 使用者

附 录 B
（资料性）
密码算法校验工具参考表

B.1 对称密码算法

表28 对称密码算法校验功能要求表

算法名称	密钥长度（比特）	依据标准
SM4	128	GB/T 32907《信息安全技术 SM4分组密码算法》
ZUC	128	GB/T 33133.2《信息安全技术 祖冲之序列密码算法 第2部分：保密性算法》 GB/T 33133.3《信息安全技术 祖冲之序列密码算法 第3部分：完整性算法》
AES	128、192、256	ISO/IEC 18033-3《Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers》
DES	64（由于加入错误检查比特，密钥实质长度为56）	
3DES	128（2TDEA，实质长度为112）、192（3TDEA，实质长度为168）	

表29 基于分组的对称密码算法支持的工作模式表

工作模式	涉及的参数及参数长度要求	是否需要数据填充	依据标准
ECB	无	需要	GB/T 17964《信息安全技术 分组密码算法的工作模式》
CBC	初始向量IV，IV长度为一个分组的长度	需要	
CFB	初始向量IV，IV长度为一个分组的长度	可能需要 （具体情况可参考标准GB/T 17964《信息安全技术 分组密码算法的工作模式》 附录A.3）	
OFB	初始向量IV，IV长度为一个分组的长度	可能需要 （具体情况可参考标准GB/T 17964《信息安全技术 分组密码算法的工作模式》 附录A.4）	
CTR	计时器Counter，Counter长度为一个分组的长度	不需要	
XTS	加密调整值TWeak，TWeak长度为一个分组的长度	不需要	
CCM	**参数1**：S，S长度为120-8w比特； **参数2**：w，w为信息长度域的长度（以字节为单位），应在集合{2,3,4,5,6,7,8}中选取； **参数3**：tag（标志，与加密后的消息拼接，用于提供数据完整性保护），tag的长度为t（以比特为单位），t应在集合{32,48,64,80,96,112,128}中选取。	需要	GB/T 36624《信息技术 安全技术 可鉴别的加密机制》

工作模式	涉及的参数及参数长度要求	是否需要数据填充	依据标准
	备注：CCM工作模式应使用分组长度为128位的分组密码算法		
GCM	**参数1**：S，S可为任意长度； **参数2**：A，A可为任意长度，在工具开发时可明确定义输入长度上限； **参数3**：tag（标志，与加密后的消息拼接，用于提供数据完整性保护），tag的长度为t，t的取值应是8的整数倍，且满足96≤t≤128（在特定情况下t的值也可以为32或64）。 备注：GCM工作模式应使用分组长度为128位的分组密码算法	不需要	

表30 支持的数据填充方式表

填充方式	填充过程	示例
不填充	无	略
Zero填充	在输入后填充a个字节0x00，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。如果输入为空串或其最后一个分组正好为分组长度，则不填充。	以SM4密码算法为例，以Hex格式编码：输入为0011223344556677889900000000000000；若输入为00112233445566778899AABBCCDDEEFF，则填充后为00112233445566778899AABBCCDDEEFF。
PKCS#7填充	在输入后填充a个字节“a”，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。如果输入为空串或其最后一个分组正好为分组长度，则填充b个字节“b”，其中“b”表示一个分组所需要的字节数。	以SM4密码算法为例，以Hex格式编码：输入为0011223344556677889906060606060606；若输入为00112233445566778899AABBCCDDEEFF，则填充后为00112233445566778899AABBCCDDEEFF10101010101010101010101010101010。
PKCS#5填充	PKCS#5填充是PKCS#7填充的子集，只是分组长度固定为8字节。	以DES密码算法为例，以Hex格式编码：输入为0011223344，则填充后为0011223344030303。
ISO 10126填充	在输入后填充a - 1个随机字节，然后填充1个字节“a”，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。	以SM4密码算法为例，以Hex格式编码：输入为0011223344556677889900000000000000；若输入为00112233445566778899AABBCCDDEEFF，则填充后可能为00112233445566778899AABBCCDDEEFF27ac3cbde9f215f6d80e1e4b46b0fb10。
ISO/IEC 7816-4填充	在输入后填充1个字节0x80，然后填充a - 1个字节0x00，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。	以SM4密码算法为例，以Hex格式编码：输入为0011223344556677889900000000000000；若输入为00112233445566778899AABBCCDDEEFF，则填充后为00112233445566778899AABBCCDDEEFF80000000000000000000000000000000。

填充方式	填充过程	示例
ANSI X9.23填充	在输入后填充a - 1个字节0x00，然后填充1个字节“a”，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。	以SM4密码算法为例，以Hex格式编码：输入为0011223344556677889900000000000006；若输入为00112233445566778899AABBCCDDEEFF，则填充后为00112233445566778899AABBCCDDEEFF00000000000000000000000000000010。

B.2 密码杂凑算法

表31 密码杂凑算法校验功能要求表

算法名称		输入长度要求	输出长度（比特）	依据标准
SM3		小于2^64比特	256	GB/T 32905《信息安全技术 SM3 密码杂凑算法》
MD5		无限制	128	RFC 1321:The MD5 Message-Digest Algorithm
SHA-1		小于2^64比特	160	ISO/IEC 10118-3《Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions》
SHA-2	SHA-224	小于2^64比特	224	
	SHA-256		256	
	SHA-384	小于2^128比特	384	
	SHA-512		512	
	SHA-512/224		224	
	SHA-512/256		256	
SHA-3	SHA3-224	无限制	224	
	SHA3-256		256	
	SHA3-384		384	
	SHA3-512		512	

B.3 消息鉴别码（MAC）算法

表32 消息鉴别码（MAC）算法校验功能要求表

MAC算法	输入参数及要求	输出及输出长度（比特）	依据标准
CBC-MAC	**参数1：**数据串，其比特长度L≥0，如果选择填充模式3，则0≤L<2^n，其中n为分组密码的分组长度； **参数2：**选择填充模式（可使用填充方法1、2和3）； **参数3：**选择分组密码算法； **参数4：**密钥，密钥比特长度为对应分组算法密钥长度。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
EMAC	**参数1：**数据串，其比特长度L≥0，如果选择填充模式3，则0≤L<2^n，其中n为分组密码的分组长度； **参数2：**选择填充模式（可使用填充方法1、2和3）； **参数3：**选择分组密码算法； **参数4：**密钥K、K’，比特长度均等于对应分组算法密钥的长度，K和K’可由同一个主密钥（分组密码密钥）通过密钥诱导方法生成，应满足K和K’高概率不相同。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
ANSI retail MAC	**参数1：**数据串，其比特长度L≥0，如果选择填充模式3，则0≤L<2^n，其中n为分组密码的分组长度； **参数2：**选择填充模式（可使用填充方法1、2和3）； **参数3：**选择分组密码算法； **参数4：**密钥K、K’，两个密钥应独立选取，比特长度均等于对应分组算法密钥的长度。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
MacDES	**参数1：**数据串，其比特长度L≥2n，如果选择填充模式3，则0≤L<2^n，其中n为分组密码的分组长度； **参数2：**选择填充模式（可使用填充方法1、2和3，填充的分组数不应小于2）； **参数3：**选择分组密码算法； **参数4：**密钥K和K’，两个密钥应独立选取，比特长度均等于对应分组算法密钥的长度。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
CMAC	**参数1：**明文字符串，其长度L≥0； **参数2：**选择填充模式（可使用填充方法4）； **参数3：**选择分组密码算法； **参数4：**密钥K，长度等于对应分组算法密钥的长度。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
LMAC	**参数1：**数据串，其比特长度L≥0，如果选择填充模式3，则0≤L<2^n，其中n为分组密码的分组长度； **参数2：**选择填充模式（可使用填充方法1、2和3）； **参数3：**选择分组密码算法； **参数4：**密钥K、K’，比特长度均等于对应分组算法密钥的长度，K和K’可由同一个主密钥（分组密码密钥）通过密钥诱导方法生成，应满足K和K’高概率不相同。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》

MAC算法	输入参数及要求	输出及输出长度（比特）	依据标准
TrCBC	**参数1：**数据串，其比特长度L≥0； **参数2：**选择填充模式（可使用填充方法4）； **参数3：**选择分组密码算法； **参数4：**密钥，密钥比特长度等于对应分组算法密钥长度。	MAC算法的输出长度为m，满足：0<m≤n，其中n为分组密码的分组长度。	GB/T 15852.1《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》
GMAC	**参数1：**输入消息，其比特长度L≤128*2^64； **参数2：**分组长度为128比特的分组密码算法； **参数3：**主密钥K； **参数4：**临时值比特串，其比特长度为任意长度。	MAC算法的输出长度为m，满足：m为8的整数倍，96≤m≤128 （在特定场合下，m=32和m=64仍允许使用，具体参考GB/T 15852.3-2019）。	GB/T 15852.3《信息技术 安全技术 消息鉴别码 第3部分：采用泛杂凑函数的机制》
HMAC	**参数1：**选择杂凑函数，杂凑函数应从ISO/IEC 10118-3中的专用杂凑函数1、2、3和7中选取。使用的专用杂凑函数也可以为SM3算法； **参数2：**输入消息。其比特长度L不大于2^64-1； **参数3：**密钥。密钥比特长度k应该满足L2≤k≤L1，其中L1为输入到轮函数的比特串的比特长度，L2为杂凑值的比特长度。	m（m≤L2，其中L2为杂凑值的比特长度）。	GB/T 15852.2《信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制》

表33 消息鉴别码（MAC）算法填充方法表

序号	填充方法分类	填充方法	示例
1	填充方法1	在数据比特串*D*的右侧填充“0”，尽可能少填充（甚至不填充），使填充后比特串的长度是分组长度*n*的正整数倍。	明文字符串： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 填充后输出： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 00 00 00 00 00 00 00
2	填充方法2	在数据比特串*D*的右侧填充一个比特“1”，然后在所得到的比特串右侧填充“0”，尽可能少填充（甚至不填充），使填充后的比特串的长度是*n*的正整数倍。	明文字符串： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 填充后输出： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 80 00 00 00 00 00 00
3	填充方法3	在数据比特串*D*的右侧填充“0”，尽可能少填充（甚至不填充），使填充后比特串的长度是*n*的正整数倍。然后在所得	明文字符串： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20

序号	填充方法分类	填充方法	示例
		到的数据比特串左侧填充一个分组L。分组L由尽可能少的“0”和数据比特串D的长度L_D的二进制表示组成，其中位于L_D二进制表示的左侧的“0”尽可能少，且使L的长度为n比特。L最右端的比特和L_D的二进制表示中的最低位相对应。 填充后的数据串D的比特长度应小于$2n$。	填充后输出： 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C8 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 00 00 00 00 00 00 00
4	填充方法4	如果输入MAC算法的数据比特串D的比特长度是n的正整数倍，则不需要填充。否则，在数据比特串D的右侧填充一个“1”比特，然后在所得到的比特串右侧填充“0”，尽可能少填充（甚至不填充），使填充后的比特串的长度是n的正整数倍。	明文字符串： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 填充后输出： 54 68 69 73 20 69 73 20 74 68 65 20 74 65 73 74 20 6D 65 73 73 61 67 65 20 80 00 00 00 00 00 00 00

B.4 非对称密码算法

表34 非对称密码算法校验功能要求表

算法名称		公钥长度	私钥长度	依据标准
SM2		512比特，包含两个坐标分量，每个坐标分量长度为256比特	256比特	GB/T 32918.1《信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则》 GB/T 32918.2《信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法》 GB/T 32918.3《信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议》 GB/T 32918.4《信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法》 GB/T 32918.5《信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义》
SM9	签名验签	主公钥1024比特，包含两个坐标分量，每个坐标分量长度为512比特	用户签名私钥512比特，包含两个坐标分量，每个坐标分量长度为256比特	GB/T 38635.1《信息安全技术 SM9标识密码算法 第1部分:总则》 GB/T 38635.2《信息安全技术 SM9标识密码算法 第2部分:算法》
	加密解密	加密主公钥512比特，包含两个坐标分量，每个坐标分量长度为256比特	用户加密私钥1024比特，包含两个坐标分量，每个坐标分量长度为512比特	

算法名称		公钥长度	私钥长度	依据标准
	密钥交换	加密主公钥512比特，包含两个坐标分量，每个坐标分量长度为256比特	用户加密私钥de_A、de_B，其中de_A和de_B都为1024比特，包含两个坐标分量，每个坐标分量长度为512比特	
	密钥封装	加密主公钥512比特，包含两个坐标分量，每个坐标分量长度为256比特	用户加密私钥1024比特，包含两个坐标分量，每个坐标分量长度为512比特	
RSA	RSA-1024	（n,e），其中，n为1024比特	（d,p,q），d长度为1024比特	RFC 8017:PKCS #1:RSA Cryptography Specifications Version 2.2
	RSA-2048	（n,e），其中，n为2048比特	（d,p,q），d长度为2048比特	
	RSA-3072	（n,e），其中，n为3072比特	（d,p,q），d长度为3072比特	

表35 SM2密码算法校验功能要求表

SM2算法功能	输入参数及输入参数长度要求（比特）	输出参数及输出参数长度要求（比特）
密钥生成	私钥d，长度为256比特	公钥（x,y），其中x和y均为256比特
验证公钥	公钥（x,y），其中x和y均为256比特	公钥在曲线上/公钥不在曲线上
加密	**参数1**：公钥（x,y），x和y均为256比特 **参数2**：明文M，M长度为m_len	密文C，长度为768+m_len
解密	**参数1**：私钥d，d为256比特 **参数2**：密文C，密文C，768+m_len	明文M，长度为m_len
签名	**参数1**：私钥d，d为256比特 **参数2**：待签名原文M **参数3**：用户ID	签名值（r,s），其中r和s均为256比特
验签	**参数1**：公钥（x,y）， x和y均为256比特 **参数2**：待验签消息M **参数3**：签名值（r,s），r和s均为256比特 **参数4**：用户ID	验证通过/验证不通过
密钥交换	**用户A参数**：用户标识Z_A，私钥d_A，公钥P_A=（x_A,y_A） **用户B参数**：用户标识Z_B，私钥d_B，公钥P_B=（x_B,y_B），其中Z_A、Z_B、d_A、d_B、x_A、y_A、x_B、y_B均为256比特	用户A发送至用户B数据： R_A=（x_1,y_1）、S_A 用户B发送至用户A数据： R_B=（x_2,y_2）、S_B，其中x_1、y_1 、x_2、y_2、S_A和S_B均为256比特

表36 SM9密码算法校验功能要求表

SM9 算法功能	输入参数及参数输入长度要求	输出参数及参数输输出长度
系统签名主密钥和用户签名密钥产生	**参数1**：系统私钥ks，ks长度为256比特 **参数2**：用户公钥ID_A	签名主公钥P_{pub-s}，签名私钥ds_A
签名	**参数1**：待签名原文M **参数2**：主公钥P_{pub-s} ，P_{pub-s}的两个坐标分量长度均为512比特 **参数3**：用户公钥ID_A **参数4**：用户签名私钥ds_A，ds_A的两个坐标分量长度均为256比特	签名（h,S），其中h长度为256比特，S长度为512比特
验签	**参数1**：待验签消息M **参数2**：主公钥P_{pub-s}，P_{pub-s}的两个坐标分量长度均为512比特 **参数3**：用户公钥ID_A	验证通过/验证不通过

系统加密主密钥和用户加密密钥产生	**参数1：**系统私钥ke，ke长度为256比特 **参数2：**用户公钥ID_A，ID_B	加密主公钥P_{pub-e}、用户私钥d_A、d_B
加密	**参数1：**明文M **参数2：**公钥$ID_{B:}$ **参数3：**加密主公钥P_{pub-e}，P_{pub-e}的两个坐标分量长度均256比特	密文C
解密	**参数1：**密文C **参数2：**用户私钥$d_{B,}$ d_B的两个坐标分量均为512比特	明文M
密钥封装	**参数1：**用户标识ID_B **参数2：**加密主公钥P_{pub-e}， P_{pub-e}的两个坐标分量长度均为256比特	封装密文C，被封装的密钥K
密钥解封	**参数1：**封装密文C **参数2：**用户标识ID_B **参数3：**用户私钥$d_{B:}d_B$的两个坐标分量均为512比特	被封装的密钥K

表37 常用RSA密码算法校验功能要求表

常用RSA算法功能		输入参数及输入参数长度要求	输出参数及输出参数长度
密钥生成	RSA-1024	**参数1：**公钥（n,e） **参数2：**私钥p和q，p和q的长度为512比特	私钥（d,p,q），d长度为1024比特
	RSA-2048	**参数1：**公钥（n,e） **参数2：**私钥p和q，p和q的长度为1024比特	私钥（d,p,q），d长度为2048比特
	RSA-3072	**参数1：**公钥（n,e） **参数2：**私钥p和q， p和q的长度为1536比特	私钥（d,p,q），d长度为3072比特
加密	RSA-1024	**参数1：**明文M，M长度为1024比特 **参数2：**公钥（n,e），n长度为1024比特	密文C，为1024比特
	RSA-2048	**参数1：**明文M，M长度为2048比特 **参数2：**公钥（n,e），n长度为2048比特	密文C，为2048比特
	RSA-3072	**参数1：**明文M，M长度为3072比特 **参数2：**公钥（n,e），n长度为3072比特	密文C，为3072比特
解密	RSA-1024	**参数1：**密文C，C长度为1024比特 **参数2：**私钥（d,p,q），d长度为1024比特	明文M，为1024比特
	RSA-2048	**参数1：**密文C，C长度为2048比特 **参数2：**私钥（d,p,q），d长度为2048比特	明文M，为2048比特
	RSA-3072	**参数1：**密文C，C长度为3072比特 **参数2：**私钥（d,p,q），d长度为3072比特	明文M，为3072比特
签名	RSA-1024	**参数1：**待签名原文M **参数2：**私钥（d,p,q）	签名值S
	RSA-2048	**参数1：**待签名原文M **参数2：**私钥（d,p,q）	签名值S
	RSA-3072	**参数1：**待签名原文M **参数2：**私钥（d,p,q）	签名值S
验签	RSA-1024	**参数1：**待验签消息M **参数2：**签名值S **参数3：**公钥（n,e）	验签通过/验签不通过

常用RSA算法功能		输入参数及输入参数长度要求	输出参数及输出参数长度
	RSA-2048	**参数1：**待验签消息M **参数2：**签名值S **参数3：**公钥（n,e）	验签通过/验签不通过
	RSA-3072	**参数1：**待验签消息M **参数2：**签名值S **参数3：**公钥（n,e）	验签通过/验签不通过

附 录 C
（资料性）
密码应用安全测评辅助工具使用示例

C.1 源代码审计工具使用示例

C.1.1 源代码审计场景示例

C.1.1.1 适用场景

信息系统可能涉及到源代码审计的场景如下：

表 38 源代码审计场景示例表

序号	测试对象	场景	可能涉及的指标
1	重要用户信息数据（账户名、姓名、手机号、邮箱、卡号）	采用对称加密算法对重要用户信息数据提供存储机密性保护。	1）应用和数据安全：重要数据存储机密性。
		采用基于密码杂凑算法的消息认证码方式进行真实性、完整性保护。	1）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； 2）网络和通信安全：身份鉴别、网络边界访问控制信息的完整性； 3）设备与计算安全：身份鉴别、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； 4）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、重要数据传输完整性，重要数据存储完整性。

C.1.1.2 具体示例

某信息系统声称对如下数据做了相关密码保护。

特别声明：示例仅用于说明工具使用，并不一定完全合规且无任何实现倾向性。

表 39 源代码审计重要数据示例表

序号	重要数据	保护措施
1	重要用户信息数据	基于非固定口令和盐值派生的密钥，采用 SM4 算法对信息系统的用户信息进行加密存储。
2	重要用户信息数据	基于 SM3 算法的消息认证码机制对信息系统的用户信息、日志记录进行完整性保护。

C.1.2 源代码审计测试实施示例

C.1.2.1 重要数据存储机密性

a） 操作过程

密评人员向被测信息系统方收集用于源代码审计的相关信息，并开展访谈：

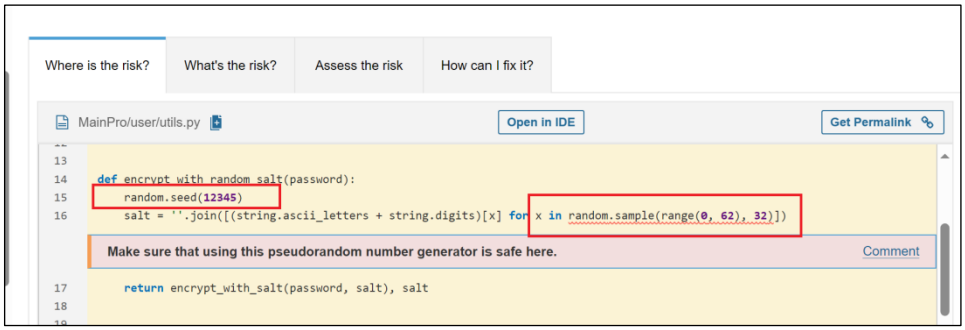
表 40 源代码审计测试（存储机密性）收集信息表

收集信息/操作	选项	描述

源代码	必选	获取能证明提供重要数据存储机密性保护的源代码，源代码必须与被测信息系统的当前版本完全一致。
访谈	必选	访谈被测信息系统的系统管理员、安全主管，获知重要数据存储机密性保护的方式。

b） 工具示例

表 41 源代码审计测试工具（存储机密性）示例表

场景	工具示例	结果
密评人员获得能证明重要数据存储机密性保护的源代码文件，输入工具进行源代码审计。	 工具发现并给出存在问题的伪随机数生成器（PRNG）工作相关代码的位置，密评人员快速定位问题位置，并查看工具给出的关键提示信息。 如图，伪随机数生成器（PRNG）用了固定的种子，导致出现可预测的随机数。	经源代码审计，发现使用不安全的伪随机数生成器。

C.1.2.2 重要数据存储完整性

a） 操作过程

密评人员向被测信息系统方收集用于源代码审计的相关信息，并开展访谈：

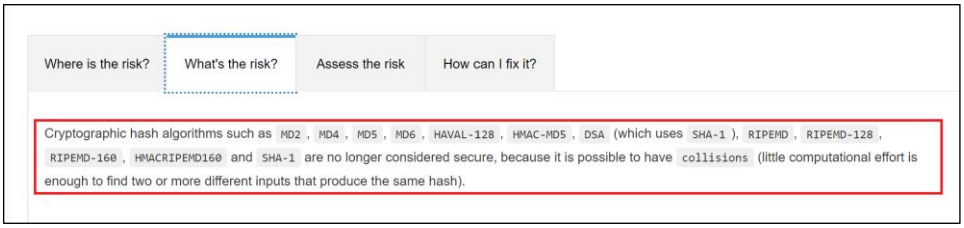
表 42 源代码审计测试（存储完整性）收集信息表

收集信息/操作	选项	描述
源代码	必选	获取能证明提供重要数据存储完整性保护的源代码，源代码必须与被测信息系统的当前版本完全一致。
访谈	必选	访谈被测信息系统的系统管理员、安全主管，获知重要数据存储完整性保护的方式。

b） 工具示例

表43 源代码审计测试工具（存储完整性）示例表

场景	工具示例	结果
密评人员获得能证明重要数据存储完整性保护的源代码文件，输入工具进行源代码审计。		经源代码审计，发现使用了不合规的 MD5 算法。

场景	工具示例	结果
	工具发现并给出存在问题的算法应用相关代码的位置，密评人员快速定位问题位置，并查看工具给出的关键提示信息，如上图工具给出的问题线索，结合密评人员的人工审计，进一步确认该函数参与了对客户数据的完整性保护。  工具尽可能给出建设性建议，基于上述建议并结合密评人员的人工审计，给出整改建议，如采用 HMAC-SM3 算法进行完整性保护。	

C.2 编码转换工具使用示例

C.2.1 编码转换工具场景示例

C.2.1.1 适用场景

信息系统可能涉及到编码转换工具的场景如下：

表 44 编码转换工具场景示例表

序号	测试对象	场景	可能涉及的指标
1	重要数据	采用非对称加密算法对重要数据进行机密性保护。	1）应用和数据安全：重要数据传输机密性、重要数据存储机密性。
		采用签名算法对重要数据进行完整性、不可否认性保护。	1）物理和环境安全：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； 2）网络和通信安全：网络边界访问控制信息的完整性； 3）设备与计算安全：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； 4）应用和数据安全：访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输完整性、重要数据存储完整性、不可否认性。

C.2.1.2 具体示例

某信息系统声称对如下数据实现了存储机密性、完整性保护。

特别声明：示例仅用于说明工具使用，并不一定完全合规且无任何实现倾向性。

表45 编码转换工具重要数据示例表

序号	重要数据	保护措施
1	个人敏感信息（身份证号）	采用 SM2 算法对信息系统的个人敏感信息进行加密存储。
2	个人敏感信息（身份证号）	采用 SM2 算法对信息系统的个人敏感信息进行签名验签。

C.2.2 编码转换工具测试实施示例

C.2.2.1 重要数据存储机密性

a） 操作过程

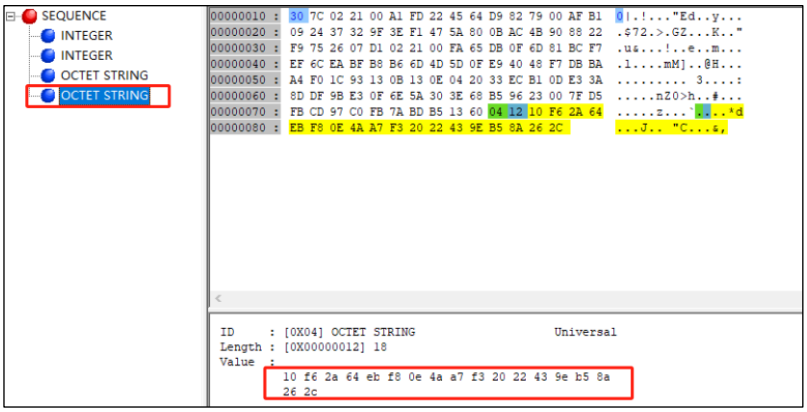
对被测系统相关人员进行访谈，确认被测系统使用的加密算法，核查被测系统提供的用于对个人敏感信息（身份证号）进行存储加密的代码以及密文值：

表46 编码转换工具（存储机密性）收集信息表

收集信息/操作	选项	描述
访谈	必选	访谈被测系统相关人员，获取个人敏感信息（身份证号）存储机密性保护所使用的加密算法。
核查加密算法代码	必选	核查被测系统提供的个人敏感信息（身份证号）存储机密性保护所使用的加密算法代码。
核查密文值	必选	核查被测系统提供的个人敏感信息（身份证号）存储机密性保护的加密结果。

b） 工具示例

表47 编码转换工具测试（存储机密性）示例表

场景	工具示例	结果
密评人员获得个人敏感信息（身份证号）存储机密性保护所使用的加密算法代码和密文值，将密文值输入工具进行解码。	 首先将十六进制字符串的密文值通过编码转换工具转换为 Base64 编码的密文值，并将 Base 64 编码的密文值通过编码转换工具进行 ASN.1 解码。 参考 GB/T 35276《信息安全技术 SM2 密码算法使用规范》，核查密文值的 ASN.1 结构。	经核查，SM2Cipher 的 HASH 长度为 32 字节，CipherText 长度为 18 字节，密文值符合 GB/T 35276《信息安全技术 SM2 密码算法使用规范》的 SM2 密文结构。

C.2.2.2 重要数据存储完整性

a） 操作过程

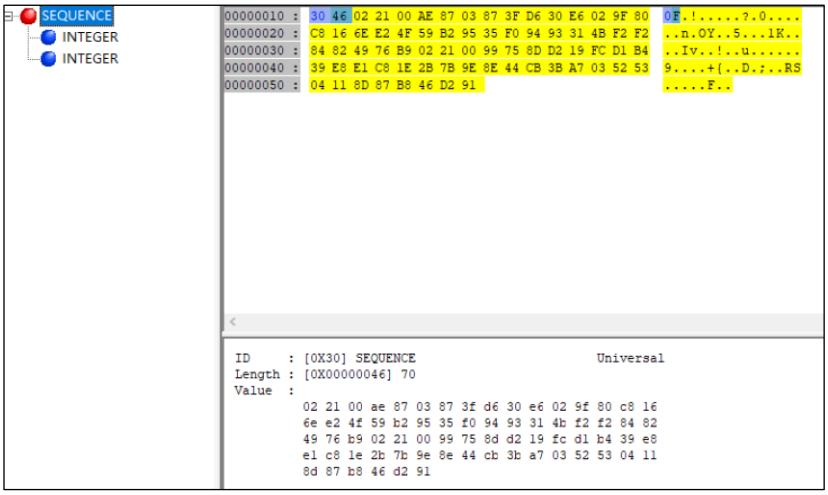
对被测系统相关人员进行访谈，确认被测系统使用的签名算法，核查被测系统提供的用于对个人敏感信息（身份证号）进行存储完整性保护的签名代码以及签名值。

表 48 编码转换工具（存储完整性）收集信息表

操作	选项	描述
访谈	必选	访谈被测系统相关人员，获取个人敏感信息（身份证号）存储完整性保护所使用的签名算法。
核查签名算法代码	必选	核查被测系统提供的个人敏感信息（身份证号）存储完整性保护所使用的签名算法代码。
核查签名值	必选	核查被测系统提供的个人敏感信息（身份证号）存储完整性保护的签名结果。

b） 工具示例

表49 编码转换工具测试（存储完整性）示例表

场景	工具示例	结果
密评人员获得个人敏感信息（身份证号）存储完整性保护所使用的签名算法代码和签名值，将签名值输入工具进行解码。	 首先将十六进制字符串的签名值通过编码转换工具转换为Base64编码的签名值，并将Base64编码的签名值通过编码转换工具进行ASN.1解码。 参考GB/T 35276《信息安全技术 SM2密码算法使用规范》，核查签名值的ASN.1结构。	经核查，签名值符合GB/T 35276《信息安全技术 SM2密码算法使用规范》的SM2签名值结构。

C.3 APDU报文分析工具使用示例

C.3.1 APDU报文分析工具场景示例

C.3.1.1 适用场景

信息系统可能涉及到APDU报文分析工具的场景如下：

表50 APDU报文分析工具场景示例表

序号	测试对象	场景	可能涉及的指标
1	身份鉴别对象、关键操作行为	使用智能密码钥匙进行身份鉴别、不可否认性保护	1）网络和通信安全：身份鉴别。 2）设备和计算安全：身份鉴别。 3）应用和数据安全：身份鉴别、不可否认性。
2		使用智能IC卡进行身份鉴别	1）物理和环境安全：身份鉴别。 2）设备和计算安全：身份鉴别。

C.3.1.2 具体示例

某信息系统声称用户使用智能密码钥匙+PIN码，采用符合GB/T 15843.3《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》的身份鉴别机制登录应用系统，实现对用户的身份鉴别。

特别声明：示例仅用于说明工具使用，并不一定完全合规且无任何实现倾向性。

表51 APDU报文分析工具用户示例表

序号	用户	身份鉴别方式
1	用户	用户使用智能密码钥匙+PIN码，采用符合GB/T 15843.3《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》的身份鉴别机制登录应用系统，实现对用户的身份鉴别。

C.3.2 APDU报文分析工具测试实施示例

C.3.2.1 身份鉴别

a） 操作过程

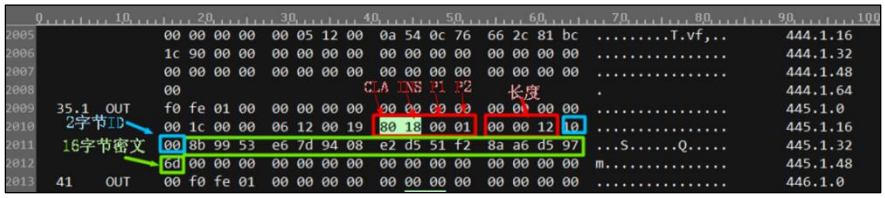
用户使用智能密码钥匙，输入PIN码，登录应用系统。

表52 APDU报文分析工具测试操作信息表

操作	选项	描述
校验PIN码	必选	校验用户输入的PIN码。

b） 工具示例

表53 APDU报文分析工具测试示例表

场景	工具示例	结果
用户使用智能密码钥匙，输入PIN码，登录应用系统，使用APDU报文分析工具抓包并分析，确认校验PIN码的指令格式和内容是否符合预期。	 代码 | 长度(byte) | 值(Hex) | 描 述 CLA | 1 | 80 | — INS | 1 | 18 | — P1 | 1 | 00 | — P2 | 1 | XX | PIN 类型(0x00 为管理员 PIN,0x01 为用户 PIN) Lc | 3 | 000012 | — DATA | 18 | XX...XX | 应用 ID(2 字节)+ 加密的校验数据(16 字节) Le | — | — | 不存在 参考 GM/T 0017《智能密码钥匙密码应用接口数据格式规范》分析抓包数据，发现数据符合校验 PIN 码的指令格式，即 CLA 为 80、INS 为 18、P1 为 00、P2 为 01、Lc 为 000012、DATA 为 10008B9953E67D9408E2D551F28AA6D5976D。其中 2 字节应用 ID 为 1000，16 字节校验数据密文为 8B9953E67D9408E2D551F28AA6D5976D。	经核查，校验PIN码的指令格式符合GM/T 0017《智能密码钥匙密码应用接口数据格式规范》。

参考文献

[1] ISO/IEC 7816-3《Cards with contacts - Electronic dignals and transmission protocols》

[2] ISO/IEC 7816-4《Organizatioin, security and commands for interchange》

[3] ISO/IEC 10118-3《Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions》

[4] ISO/IEC 14443-4《Contactless integrated circuit cards - Proximity cards - Transmission protocol》

[5] ISO/IEC 18033-3《Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers》

[6] RFC 1321:The MD5 Message-Digest Algorithm

[7] RFC 2246:The TLS Protocol Version 1.0

[8] RFC 2402:IP Authentication Header

[9] RFC 2406:IP Encapsulating Security Payload （ESP）

[10] RFC 2408:Internet Security Association and Key Management Protocol （ISAKMP）

[11] RFC 4251:The Secure Shell （SSH） Protocol Architecture

[12] RFC 4253:The Secure Shell （SSH） Transport Layer Protocol

[13] RFC 4306:Internet Key Exchange （IKEv2） Protocol

[14] RFC 4346:The Transport Layer Security （TLS） Protocol Version 1.1

[15] RFC 5246:The Transport Layer Security （TLS） Protocol Version 1.2

[16] RFC 5280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List （CRL） Profile

[17] RFC 5282:Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 （IKEv2） Protocol

[18] RFC 8017:PKCS #1:RSA Cryptography Specifications Version 2.2

[19] RFC 8446:The Transport Layer Security （TLS） Protocol Version 1.3