ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0116—2021

信息系统密码应用测评过程指南

Testing and evaluation process guide for information system cryptography application

2021-10-19 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：国家密码管理局商用密码检测中心、中国科学院数据与通信保护研究教育中心、公安部三所（公安部信息安全等级保护评估中心）、上海交通大学、中国电子科技集团第十五研究所（信息产业信息安全测评中心）、深圳市网安计算机安全检测技术有限公司、国家信息技术安全研究中心、山东道普测评技术有限公司、北京信息安全测评中心。

本文件主要起草人：肖秋林、罗鹏、马原、贾世杰、银鹰、郑昉昱、张立花、黎水林、牛莹姣、刘健、杨宏志、吴冬宇、张晓溪、陈亚男。

信息系统密码应用测评过程指南

1 范围

本文件规定了信息系统密码应用的测评过程，规范了测评活动及其工作任务。

本文件适用于商用密码应用安全性评估机构、信息系统责任单位开展密码应用安全性评估工作。

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 25069—2010 信息安全技术 术语

GM/T 0115 信息系统密码应用测评要求

GM/Z 4001 密码术语

信息系统密码应用高风险判定指引

3 术语和定义

GB/T 25069—2010 和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

测评方 testing and evaluation agency

对信息系统开展密码应用安全性评估(简称“密评”)的主体。

注：具体可以是商用密码应用安全性评估机构或信息系统责任单位。

3.2

被测单位 agency under testing and evaluation

信息系统责任单位。

3.3

商用密码应用安全性评估人员 commercial cryptography application security evaluation staff

测评方中从事测评活动的人员。

注：简称“密评人员”。

4 概述

4.1 基本原则

测评方对信息系统开展密码应用安全性评估时，应遵循以下原则。

a) 客观公正性原则

测评实施过程中，测评方应保证在符合国家密码管理部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。

b) 可重用性原则

测评工作可重用已有测评结果，包括商用密码检测认证结果和密码应用安全性评估的测评结果等。所有重用结果都应以已有测评结果仍适用于当前被测信息系统为前提，并能够客观反映系统当前的安全状态。

c） 可重复性和可再现性原则

按照同样的要求，使用同样的测评方法，在同样的环境下，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果。可重复性和可再现性的区别在于，前者关注同一密评人员测评结果的一致性，后者则关注不同密评人员测评结果的一致性。

d） 结果完善性原则

在正确理解 GM/T 0115 各个要求项内容的基础之上，测评所产生的结果应客观反映信息系统的密码应用现状。测评过程和结果应基于正确的测评方法，以确保其满足要求。

4.2 测评风险识别

测评工作的开展可能会给被测信息系统带来一定风险，测评方应在测评开始前及测评过程中及时进行风险识别。在测评过程中，面临的风险主要包括以下方面。

a） 验证测试可能影响被测信息系统正常运行

在现场测评时，需对设备和系统进行一定的验证测试工作，部分测试内容需上机查看信息，可能对被测信息系统的运行造成不可预期的影响。

b） 工具测试可能影响被测信息系统正常运行

在现场测评时，根据实际需要可能会使用一些测评工具进行测试。测评工具使用时可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响，进而对被测信息系统中的服务器和网络通信造成一定影响甚至损害。

c） 可能导致被测信息系统敏感信息泄露

测评过程中，可能泄露被测信息系统的敏感信息，如加密机制、业务流程、安全机制和有关文档信息等。

d） 其他可能面临的风险

在测评过程中，也可能出现影响被测信息系统可用性、机密性和完整性的风险。

4.3 测评风险规避

在测评过程中，可以通过采取以下措施规避风险。

a） 签署委托测评协议书

在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式，明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等，使得测评双方对测评过程中的基本问题达成共识。

b） 签署保密协议

测评相关方应签署合乎法律规范的保密协议，规定测评相关方在保密方面的权利、责任与义务。

c） 签署现场测评授权书

现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，采取适当的方法进行风险规避，并针对可能出现的事件制定应急处理方案。

d） 现场测评要求

需进行验证测试和工具测试时，应避开被测信息系统业务高峰期，在系统资源处于空闲状态时进行测试，或配置与被测信息系统一致的模拟/仿真环境，在模拟/仿真环境下开展测评工作；需进行上机验证测试时，密评人员应提出需要验证的内容，由被测单位的技术人员进行实际操作。整个现场测评过程，由被测单位和测评方相关人员进行监督。

测评工作完成后，密评人员应交回在测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并将测评现场环境恢复至测评前状态。

4.4 测评过程

4.4.1 测评过程概述

在测评活动开展前，需要对被测信息系统的密码应用方案进行评估，通过评估的密码应用方案可以作为测评实施的依据。

测评过程包括4项基本测评活动：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。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。测评过程如图1所示。

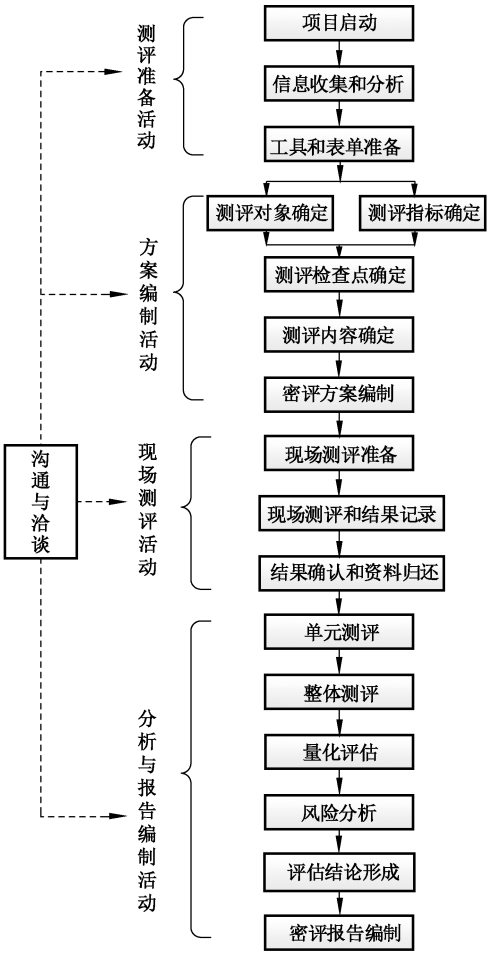

图1 测评过程工作流程图

4.4.2 测评准备活动

测评准备活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密评方案做好准备。

4.4.3 方案编制活动

方案编制活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测

评指标、测评检查点及测评内容等，形成密评方案，为实施现场测评提供依据。

4.4.4 现场测评活动

现场测评活动是开展测评工作的核心活动，主要任务是根据密评方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

4.4.5 分析与报告编制活动

分析与报告编制活动是给出测评工作结果的活动，主要任务是根据密评方案和 GM/T 0115 的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成密评报告。

5 测评准备活动

5.1 测评准备活动的工作流程

测评准备活动的目标是顺利启动测评项目，准备测评所需的相关资料，为编制密评方案提供条件。测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。

5.2 测评准备活动的主要任务

5.2.1 项目启动

在项目启动任务中，测评方组建测评项目组，获取被测单位及被测信息系统的基本情况，从基本资料、人员、计划安排等方面为整个测评项目的实施做准备。

——输入：委托测评协议书、保密协议等。

任务描述：

a) 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，测评方组建测评项目组，做好人员安排，并编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等内容。

b) 测评方要求被测单位提供基本资料，为全面初步了解被测信息系统做好资料准备。

——输出：项目计划书。

5.2.2 信息收集和分析

测评方使用调查表格、查阅被测信息系统资料等方式，了解被测信息系统的构成和密码应用情况，为编写密评方案和开展现场测评工作奠定基础。

——输入：调查表格。

任务描述：

a) 测评方收集测评所需资料，包括被测信息系统总体描述文件、被测信息系统密码应用总体描述文件、网络安全等级保护定级报告、安全需求分析报告、安全总体方案、安全详细设计方案、密码应用方案、相关密码产品的用户操作指南、各种密码应用安全规章制度，以及相关过程管理记录和配置管理文档等。

b) 测评方将被测信息系统基本情况调查表格提交给被测单位，协助并督促被测信息系统相关人员准确填写调查表格。

c) 测评方收回填写完成的调查表格，并分析调查结果，了解和熟悉被测信息系统的实际情况。分

析的内容包括被测信息系统的基本信息、行业特征、密码管理策略、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、被测信息系统网络安全保护等级、用户范围、用户类型、被测信息系统所处的运行环境及面临的威胁等。以上信息可以采信自查结果、上次网络安全保护等级测评报告或商用密码应用安全性评估报告中的可信结果。

d) 如果调查表格中有填写不准确、不完善或存在相互矛盾的情况，密评人员应与填表人进行沟通和确认。必要时，测评方应安排现场调查，与被测信息系统相关人员进行沟通和确认，以确保调查信息的正确性和完整性。

——输出：完成的调查表格，各种与被测信息系统相关的技术资料。

5.2.3 工具和表单准备

测评项目组成员在进行现场测评之前，应熟悉与被测信息系统相关的各种组件、校准测评工具、准备各类表单等。测评过程中使用的测评工具应符合国家密码管理部门相关管理政策要求和密码相关国家标准、行业标准的要求。

——输入：完成的调查表格、各种与被测信息系统相关的技术资料。

任务描述：

a) 校准本次测评过程中将用到的测评工具。

b) 如果具备条件，建议密评人员模拟被测信息系统搭建测评环境，进行前期准备和验证，为方案编制活动、现场测评活动提供必要的条件。

c) 准备并打印表单，主要包括：现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等。

——输出：选用的测评工具清单，打印的各类表单，如现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等。

5.3 测评准备活动的输出文档

测评准备活动的输出文档及其内容如表 1 所示。

表 1 测评准备活动的输出文档及其内容

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等
信息收集和分析	完成的调查表格，各种与被测信息系统相关的技术资料	被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况和相关部门及角色等
工具和表单准备	选用的测评工具清单，打印的各类表单，如现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等	测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录、会议签到信息等

6 方案编制活动

6.1 方案编制活动的工作流程

方案编制活动的目标是整理及分析测评准备活动中获取的被测信息系统相关资料，为现场测评活

动提供最基本的文档和指导方案。

方案编制活动包括测评对象确定、测评指标确定、测评检查点确定、测评内容确定及密评方案编制五项主要任务。

6.2 方案编制活动的主要任务

6.2.1 测评对象确定

根据已经了解到的被测信息系统信息，分析整个被测信息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，确定本次测评的测评对象。

——输入：完成的调查表格、各种与被测信息系统相关的技术资料。

任务描述：

a） 识别被测信息系统的基本情况

根据从调查表格获得的被测信息系统情况，识别出被测信息系统的物理环境、网络拓扑结构和外部边界连接情况、业务应用系统，以及与其相关的重要的计算机硬件设备、网络安全设备、密码产品和使用的密码服务等，并识别与上述内容相关的密码应用情况。

b） 描述被测信息系统

对识别出的被测信息系统的基本情况进行整理，并对被测信息系统进行描述。描述被测信息系统时，一般以被测信息系统的网络拓扑结构为基础，采用总分式的描述方法，首先说明整体结构，其次描述外部边界连接情况和边界主要设备，最后介绍被测信息系统的网络区域组成、主要业务功能及相关的设备节点，同时务必描述在这些方面所识别的密码应用情况。

c） 确定测评对象

根据被测信息系统的重要程度及其相关设备和组件等情况，明确核心资产在被测信息系统内的流转，从而确定与密码相关的测评对象。

被测单位需要确定被测信息系统需要保护的核心资产，以及相应的威胁模型和安全策略。核心资产可以是业务应用、业务数据或者业务应用的某些设备、组件。核心资产及其他需要保护的配套数据（如审计信息、配置信息、访问控制列表等）、敏感安全参数（主要指密钥）的威胁模型和安全策略等均由被测单位根据密码应用方案、网络安全等级保护定级报告等确定，并由测评方进行核查和确认。

d） 资产和威胁评估

资产的价值根据资产的重要性和关键程度确定。资产价值分为高、中、低三个等级。价值越高的资产遭到威胁时将导致越高的风险。资产价值高低的界定，可由被测单位根据密码应用方案、网络安全等级保护定级报告等继承和确定，并由测评方进行核查和确认。

对于各类资产和其他敏感信息，测评方与被测单位需要分析其可能面临的威胁及威胁发生的频率。威胁发生的频率分为高、中、低三个等级，威胁发生频率越高意味着资产的安全越有可能受到威胁。可能面临的威胁以及威胁发生的频率，可由被测单位根据密码应用方案、网络安全等级保护定级报告等继承和确定，并由测评方进行核查和确认。

e） 描述测评对象

测评对象包括机房、业务应用软件、主机和服务器、数据库、网络安全设备、密码产品、密码服务、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）及安全管理制度类文档和记录表单类文档等。在对每类测评对象进行描述时一般采用列表的方式，如对硬件设备进行描述时，应包括测评对象所属区域、设备名称、用途、设备信息等内容。

——输出：密评方案的测评对象部分。

6.2.2 测评指标确定

根据已经了解到的被测信息系统定级结果，确定出本次测评的测评指标。

——输入：完成的调查表格、GM/T 0115、通过评估的密码应用方案、相关行业标准或规范。

任务描述：

a) 根据被测信息系统的调查表格，获得被测信息系统的定级结果，并根据 GM/T 0115 选择相应等级对应的测评指标。

b) 根据被测信息系统相关的行业标准或规范，以及被测信息系统密码应用需求，确定特殊测评指标。

c) 对于核心资产、物理环境及其他需要保护的数据（如密钥、鉴别数据等），应按照被测信息系统的安全策略、相关标准要求进行逐项确认。通过确认在核心资产、物理环境及其他需要保护的数据全生命周期流转过程中所涉及的密码算法、密码技术、密码产品、密码服务等，明确密钥生存周期管理相关的要求，并对照已通过评估的密码应用方案逐项确认各项指标的适用性。

d) 如果确无密码应用方案，则需要对所有不适用项进行逐条核查、评估，详细论证其安全需求、不适用的具体原因，以及是否采用了可满足安全要求的其他替代性风险控制措施来达到等效控制。

——输出：密评方案的测评指标部分。

6.2.3 测评检查点确定

测评过程中，需要对一些关键安全点进行现场检查确认，以防止密码产品、密码服务虽然被正确配置，但是未接入被测信息系统之类的情况发生。可通过抓包测试、查看关键设备配置等方法，确认密码算法、密码技术、密码产品和密码服务的合规性、正确性和有效性。这些检查点应在方案编制时确定，并且充分考虑到检查的可行性和风险，最大限度地避免对被测信息系统的影响，尤其应避免对在线运行业务系统造成影响。

——输入：被测信息系统详细网络结构，选用的密码算法、密码技术、密码产品、密码服务等详细信息，通过评估的密码应用方案和 GM/T 0115。

任务描述：

a) 关键设备检查是现场测评的重要环节，关键设备一般为承载核心资产流转、进行密钥管理的设备。密评人员应列出需要接受现场检查的关键设备和检查内容，包括：涉及密码的部分是否使用国家密码管理部门认可的密码算法、密码技术、密码产品和密码服务等；相关配置是否与密码应用需求相符；是否满足 GM/T 0115 中的相关条款要求等。

b) 在使用工具进行测评时（测评工具包括但不限于：协议分析工具、算法合规性检测工具、随机性检测工具和数字证书格式合规性检测工具等），应在保证被测信息系统正常、安全运行的情况下，确定测试路径和工具接入点，并结合网络拓扑图，采用图示的方式描述测评工具的接入点、测试目的、测试途径和测试对象等相关内容。当从被测信息系统边界外接入时，测试工具一般接在系统边界设备（通常为交换机）上；从系统内部不同网段接入时，测试工具一般接在与被测对象不在同一网段的内部核心交换机上；从系统内部同一网段接入时，测试工具一般接在与被测对象在同一网段的交换机上。当测评工具接入被测信息系统条件不成熟时，测评方应与被测单位协商、配合，生成必要的离线数据。

——输出：密评方案的测评检查点部分。

6.2.4 测评内容确定

测评实施前，需确定现场测评的具体实施内容，即单元测评内容。

——输入：完成的调查表格，密评方案的测评对象、测评指标及测评检查点部分，通过评估的密码应用方案 和 GM/T 0115。

任务描述：

依据通过评估的密码应用方案和GM/T 0115，首先将已经得到的测评指标与测评对象结合起来，其次将测评对象与具体的测评方法结合起来。具体做法是将各层面上的测评指标结合到具体的测评对象上，并说明具体的测评方法，构成若干个可以具体实施测评的单元。然后，结合已选定的测评指标和测评对象，概要说明现场单元测评实施的工作内容；涉及现场测试部分时，应根据确定的测评检查点，编制相应的测试内容。在密评方案中，现场单元测评实施内容通常以表格的形式给出，表格内容包括测评指标、测评内容描述等。

——输出：密评方案的单元测评实施部分。

6.2.5 密评方案编制

密评方案是测评工作实施的基础，用于指导测评工作的现场实施活动。密评方案应包括但不限于以下内容：项目概述、测评对象、测评指标、测评检查点以及测评实施等。

——输入：委托测评协议书，项目计划书，完成的调查表格，通过评估的密码应用方案和GM/T 0115，密评方案中测评对象、测评指标、测评检查点、测评内容等部分。

任务描述：

a) 根据委托测评协议书和完成的调查表格，提取项目来源、被测单位整体信息化建设情况及被测信息系统与其他系统之间的连接情况等。

b) 结合被测信息系统的实际情况，根据通过评估的密码应用方案和GM/T 0115，明确测评活动所要依据和参考的与密码算法、密码技术、密码产品和密码服务等相关的标准规范。

c) 依据委托测评协议书和被测信息系统的情况，估算现场测评工作量，具体可根据配置检查的节点数量、工具测试的接入点及测试内容等情况进行估算。

d) 根据测评项目组成员分工，编制工作安排。

e) 根据以往测评经验以及被测信息系统规模，编制具体测评实施计划，包括现场工作人员的分工和时间安排。在进行时间安排时，应尽量避开被测信息系统的业务高峰期，避免给被测信息系统的正常运行带来影响。同时，在测评计划中应将具体测评工作所需的人员、资料、场所等保障要求一并提出，以确保现场测评工作的顺利开展。

f) 汇总上述内容及方案编制活动中其他任务获取的内容，形成密评方案。

g) 密评方案经测评方内部评审通过后，提交被测单位签字确认。

——输出：经过评审和确认的密评方案文本。

6.3 方案编制活动的输出文档

方案编制活动的输出文档及其内容如表2所示。

表2 方案编制活动的输出文档及其内容

任务	输出文档	文档内容
测评对象确定	密评方案的测评对象部分	被测信息系统的整体结构、边界、网络区域、核心资产、面临的威胁、测评对象等
测评指标确定	密评方案的测评指标部分	被测信息系统相应等级对应的适用和不适用的测评指标
测评检查点确定	密评方案的测评检查点部分	测评检查点、检查内容及测评方法
测评内容确定	密评方案的单元测评实施部分	单元测评实施内容
密评方案编制	经过评审和确认的密评方案文本	项目概述、测评对象、测评指标、测评检查点、单元测评实施内容、测评实施计划等

7 现场测评活动

7.1 现场测评活动的工作流程

现场测评活动的目标是通过与被测单位进行沟通和协调，依据密评方案实施现场测评工作，获取分析与报告编制活动所需且足够的证据和资料。现场测评活动包括三项主要任务：现场测评准备、现场测评和结果记录、结果确认和资料归还。

7.2 现场测评活动的主要任务

7.2.1 现场测评准备

本任务启动现场测评工作，以保证测评方能够顺利实施测评。

——输入：现场测评授权书、经过评审和确认的密评方案、风险告知书等。

任务描述：

a) 召开测评现场首次会，测评方介绍测评工作，进一步明确测评计划和方案中的内容，说明测评过程中具体实施的工作内容、测评时间安排、测评过程中可能存在的安全风险等；

b) 测评方与被测单位确认现场测评所需的各种资源，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相关数据；

c) 被测单位签署现场测评授权书和风险告知书；

d) 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。

——输出：会议记录，更新确认的密评方案，签署过的测评授权书和风险告知书等。

7.2.2 现场测评和结果记录

本任务主要是测评方根据密评方案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。

——输入：更新确认后的密评方案、测评结果记录表格、各种与被测信息系统相关的技术资料。

任务描述：

a) 测评方安排密评人员在约定的测评时间，通过与被测信息系统有关人员（个人/群体）的访谈、文档审查、实地察看，以及在测评检查点进行配置检查和工具测试等方式，测评被测信息系统是否达到了相应等级的要求。

b) 对于已经取得相应证书的密码产品，测评时不对其本身进行重复检测，主要进行符合性核验和配置检查，对于存在符合性疑问的，可联系密码产品审批部门或相应的检测认证机构加以核实。

c) 进行配置检查时，根据被测单位出具的商用密码产品认证证书（复印件）、安全策略文档或用户手册等，先确认实际部署的密码产品与声称情况的一致性，再查看配置的正确性，并记录相关证据。如果存在不明确的问题，可由被测单位通知密码产品厂商现场提供证据（如密码产品送检文档等）。

d) 进行工具测试时，需根据被测信息系统的实际情况选择测试工具，在配置检查无法提供有力证据的情况下，应通过工具测试的方法抓取并分析被测信息系统相关数据。以下列出了数据采集和分析的几种方式。

   1) 需要重点采集被测信息系统与外界通信的数据以及被测信息系统内部传输和存储的数据，分析使用的密码算法、密码协议、关键数据结构（如数字证书格式）是否合规，检查传输的口令、用户隐私数据等重要数据是否进行了保护（如对密文进行随机性检测、查看关键字段是否以明文出现），验证杂凑值和签名值是否正确；在条件允许的情况下，可以重放采

集的关键数据(如身份鉴别数据)验证被测信息系统是否具备防重放攻击的能力,或者修改传输的数据验证被测信息系统是否对传输数据进行了完整性保护。

2) 为了验证密码产品是否被正确、有效地使用,可采集密码产品和其调用者之间的通信数据,通过采集的密码产品调用指令和响应报文,分析密码产品的调用是否符合预期(如密码计算请求是否实时发起,数据内容和长度是否符合逻辑);若无法在密码产品和调用者之间接入测试工具(如密码产品是软件密码模块),且被测信息系统无法提供源代码等有关证据的情况下,可通过逆向分析等方法对被测信息系统应用程序进行逆向分析,探究应用程序内部组成结构及工作原理,核查应用程序调用密码功能的合理性。

3) 在不影响被测信息系统正常运行的情况下,探测 IPSec VPN 和 SSL VPN 等密码协议所对应的特定端口服务是否开启,利用漏洞扫描、渗透测试等工具对被测信息系统进行分析,查看被测信息系统是否存在与密码相关的安全漏洞。

e) 密评人员根据现场测评结果填写完成测评结果记录表格。

——输出:各类测评结果记录。

7.2.3 结果确认和资料归还

——输入:测评结果记录、工具测试完成后的电子输出记录。

任务描述:

a) 密评人员在现场测评完成之后,应首先汇总现场测评的测评记录,对遗漏和需要进一步验证的内容实施补充测评;

b) 召开测评现场结束会,测评方与被测单位对测评过程中得到各类测评结果记录进行现场沟通和确认;

c) 测评方归还测评过程中借阅的所有文档资料,将测评现场环境恢复至测评前状态,并由被测单位文档资料提供者签字确认。

——输出:经过被测单位确认的各类测评结果记录。

7.3 现场测评活动的输出文档

现场测评活动的输出文档及其内容如表 3 所示。

表 3 现场测评活动的输出文档及其内容

任务	输出文档	文档内容
现场测评准备	会议记录、更新确认的密评方案、签署过的测评授权书和风险告知书等	工作计划和内容安排、双方人员的协调、被测单位应提供的配合与支持等
现场测评和结果记录	各类测评结果记录	访谈、文档审查、实地察看和配置检查、工具测试的记录及测评结果
测评结果确认和资料归还	经过被测单位确认的各类测评结果记录	测评活动中发现的问题、问题的证据和证据源、每项测评活动中被测单位配合人员的书面认可文件

8 分析与报告编制活动

8.1 分析与报告编制活动的工作流程

现场测评工作结束后,测评方应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成评

估结论，并编制密评报告。

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。分析与报告编制活动包括单元测评、整体测评、量化评估、风险分析、评估结论形成及密评报告编制六项主要任务。

8.2 分析与报告编制活动的主要任务

8.2.1 单元测评

本任务主要是针对各测评指标中的各个测评对象，客观、准确地分析测评证据，对每个测评对象分别进行测评实施和结果判定。汇总各测评单元涉及的所有测评对象的测评实施结果，得出各测评单元的判定结果，并以表格的形式逐一列出。

——输入：经过被测单位确认的各类测评结果记录、GM/T 0115。

任务描述：

a) 按照 GM/T 0115 的规定，针对各测评单元涉及的各个测评对象，将实际获得的多个测评结果与预期的测评结果相比较，分别判断每个测评结果与预期结果之间的符合性，综合判定该测评对象的测评结果，从而得到每个测评对象对应的测评结果，包括符合、不符合、部分符合和不适用四种情况。

b) 按照 GM/T 0115 的规定，汇总各测评单元涉及的所有测评对象的测评实施结果，对各测评单元进行结果判定，判别原则如下：

   1) 测评单元包含的所有测评对象的测评结果均为符合，则对应测评单元结果判定为符合；

   2) 测评单元包含的所有测评对象的测评结果均为不符合，则对应测评单元结果判定为不符合；

   3) 测评单元包含的所有测评对象的测评结果均为不适用，则对应测评单元结果判定为不适用；

   4) 测评单元包含的所有测评对象的测评结果不全为符合或不符合，则对应测评单元结果判定为部分符合。

——输出：密评报告的单元测评部分。

8.2.2 整体测评

本任务针对测评结果为部分符合和不符合的测评对象，采取逐条判定的方法，给出整体测评的具体结果。

——输入：密评报告的单元测评部分。

任务描述：

a) 针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他单元的测评对象能否和它发生关联关系，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果；

b) 针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他层面的测评对象能否和它发生关联关系，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果；

c) 结合单元测评的结果汇总和整体测评结果，将物理和环境安全、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、应急处置等层面中各个测评对象的测评结果再次汇总分析，统计符合情况。

——输出：密评报告的单元测评结果修正部分。

8.2.3 量化评估

本任务综合单元测评结果和整体测评结果，计算修正后的各测评指标的各个测评对象的测评结果得分、各测评单元得分、各安全层面得分和整体得分，并对被测信息系统的密码应用情况安全性进行总体评价。

——输入：密评报告的单元测评的结果汇总及整体测评部分。

任务描述：

a) 根据整体测评结果，计算修正后的各测评指标的各个测评对象的测评结果符合程度得分；

b) 根据各个测评对象的符合程度得分，计算各测评单元得分；

c) 根据各测评单元得分，计算各安全层面得分；

d) 根据各安全层面得分，计算整体得分；

e) 根据各测评单元、各层面和整体得分，总体评价被测信息系统已采取的有效保护措施和存在的密码应用安全问题情况。

——输出：密评报告中整体测评结果和量化评估部分，以及总体评价部分。

8.2.4 风险分析

本任务依据相关规范和标准，采用风险分析的方法，分析测评结果中存在的安全问题以及可能对被测信息系统安全造成的影响。

——输入：完成的调查表格、密评报告的整体测评结果和量化评估部分、相关风险评估标准。

任务描述：

a) 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。

b) 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，对被测信息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。

c) 综合前两步分析结果，测评方根据自身经验和《信息系统密码应用高风险判定指引》等相关标准要求，对被测信息系统面临的密码应用安全风险进行赋值，风险值的取值范围为高、中和低。

d) 结合被测信息系统的网络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进行评价。如果存在高风险项，则认为被测信息系统面临高风险；同时也需要考虑多个中低风险叠加后可能导致的高风险问题。

——输出：密评报告的风险分析部分。

8.2.5 评估结论形成

本任务在测评结果汇总、量化评估以及风险分析的基础上，形成评估结论。

——输入：密评报告中被测信息系统的综合得分和总体评价部分、风险分析部分。

任务描述：

根据被测信息系统的综合得分和风险分析结果，得出评估结论。评估结论分为以下三种情况。

a) 符合：被测信息系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。

b) 基本符合：被测信息系统中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致被测信息系统面临高等级安全风险，且综合得分不低于阈值。

c) 不符合：被测信息系统中存在安全问题，部分符合和不符合项的统计结果不全为0，而且存在的安全问题会导致被测信息系统面临高等级安全风险，或者综合得分低于阈值。

——输出：密评报告的评估结论部分。

8.2.6 密评报告编制

本任务根据分析与报告编制活动的各项任务输出形成密评报告。密评报告应符合信息系统密码应用安全性评估报告模板要求，包括但不限于以下内容：测评项目概述、被测系统情况、测评范围与方法、单元测评、整体测评、量化评估、风险分析、评估结论、总体评价、安全问题及改进建议等。其中，概述部分描述被测信息系统的总体情况、测评目的和依据等。

——输入：完成的调查表格、密评方案、单元测评的结果汇总部分、整体测评部分、总体评价部分、风险分析部分、评估结论部分等。

任务描述：

a) 密评人员整理各项任务输出，编制密评报告相应部分。对每一个定级的被测信息系统应单独形成一份密评报告。

b) 针对被测信息系统存在的安全问题，提出相应改进建议，并编制密评报告安全文件及改进建议部分。

c) 采取列表方式给出现场测评文档清单和测评记录，以及对各个测评项的测评结果判定情况，编制密评报告单元测评的结果记录、整体测评结果、风险分析和评估结论等部分内容。

d) 密评报告编制完成后，测评方应根据委托测评协议书、被测单位提交的相关文档、测评原始记录和其他辅助信息，对密评报告进行内部评审。

e) 密评报告通过内部评审后，由授权签字人进行签发，提交被测单位。

——输出：经过评审和确认的密评报告。

8.3 分析与报告编制活动的输出文档

分析与报告编制活动的输出文档及其内容如表4所示。

表4 分析与报告编制活动的输出文档及其内容

任务	输出文档	文档内容
单元测评	密评报告的单元测评部分	汇总统计各测评指标的各个测评对象的测评结果，给出单元测评结果
整体测评	密评报告的单元测评结果修正部分	分析被测信息系统整体安全状况及对各测评对象测评结果的修正情况
量化评估	密评报告中整体测评结果和量化评估部分，以及总体评价部分	综合单元测评和整体测评结果，计算得分，并对被测信息系统的密码应用情况安全性进行总体评价
风险分析	密评报告的风险分析部分	分析被测信息系统存在的安全问题风险情况
评估结论形成	密评报告的评估结论部分	对测评结果进行分析，形成评估结论
密评报告编制	经过评审和确认的密评报告	测评项目概述、被测系统情况、测评范围与方法、单元测评、整体测评、量化评估、风险分析、评估结论、总体评价、安全问题及改进建议等