ICS 35.040
L 80

备案号：

天津市商用密码团体标准

T/TCCIA 0004-2023

天津市商用密码应用安全性评估服务工作规范（试行版）

Service Specification for Commercial Cryptography Application Security Evaluation

天津市商用密码行业协会 发布

目　录

前　言

商用密码应用安全性评估工作已成为法定要求，测评实施过程的规范性直接决定着评估结论的可靠性。在实际测评中，实施密评的机构或单位应根据GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》等标准采用恰当的测评实施方法开展商用密码应用安全性评估工作，保证商用密码应用的规范性。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。

本文件由天津市商用密码行业协会提出并归口。

本文件起草单位：天津光电安辰信息技术股份有限公司、南开大学、中汽研软件测评（天津）有限公司、天津恒御科技有限公司、天津鲲奥世达科技有限公司、天津联信达软件技术有限公司、天津市兴先道科技有限公司、天津云安科技发展有限公司、中互金认证有限公司、天津赢达信科技有限公司、天津灵创智恒软件技术有限公司、天津数字认证有限公司。

本文件主要起草人：胡双喜、刘哲理、汪定、邵学彬、赵振东、王泽、穆慧、刘立民、苏明、李文宝、张秋璞、李忠献、崔悦。

天津市商用密码应用安全性评估服务工作规范（试行版）

1 范围

本文件主要依据GB/T 43206—2023《信息安全技术 信息系统密码应用测评要求》和 GM/T 0116—2021《信息系统密码应用测评过程指南》，结合密码应用技术和管理测评指标，给出测评准备阶段、测评方案编制阶段、现场测评阶段等环节的规范要求，对商用密码应用安全性评估的测评实施工作提供指导。

本文件适用于规范在天津提供服务的商用密码应用安全性检测机构、信息系统运营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 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》
- GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》
- GM/T 0116-2021《信息系统密码应用测评过程指南》
- 《关于进一步加强商用密码应用安全性评估结果备案工作的通知》（第454号）
- 《信息系统密码应用高风险判定指引》
- 《商用密码应用安全性评估量化评估规则》
- 《商用密码应用安全性评估报告模板》
- 《商用密码应用安全性评估测评实施指引》
- 《信息系统密码应用方案》（如有）

3 术语和定义

3.1 商用密码应用安全性评估

商用密码应用安全性评估，简称“密评”，是指按照有关法律法规和标准规 范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性和有效性进行检测分析和评估验证的活动。

3.2 检测机构

经国家密码管理局认定，依法取得商用密码检测机构资质，从事网络与信息系统商用密码应用安全性评估活动，向社会出具具有证明作用的商用密码安全性评估数据、结果的机构。

3.3 被测单位

信息系统责任单位或运营单位。（商用密码应用责任单位、信息系统的建设单位或运维单位）。

3.4 商用密码应用安全性评估人员

通过国家密码管理局或其授权机构组织的考核，取得商用密码应用安全评估人员证书从事测评活动的人员，简称“密评人员”。

3.5 天津市商用密码行业协会

天津市商用密码行业协会，简称“商密协会”。

3.6 天津市商用密码测评与产品检测专业委员会

天津市商用密码测评与产品检测专业委员会，是天津市商用密码行业协会下设的非独立法人机构，简称“专委会”。主要职能为普及商用密码检测相关的法律法规，组织本地检测机构不断提升测评能力，配合相关管理部门对本市密评项目实施质量监督，具体职责包括但不限于：备案信息核验、过程监督、项目材料及报告抽查与评审等。

4 密评项目服务要求

按照国家和天津市密评管理相关要求，参照相关省市做法，商密协会制定天津市商用密码应用安全性评估服务工作规范。

4.1 机构备案

检测机构在天津市开展密评业务前，应当向商密协会办理信息登记备案，提交《商用密码应用安全性评估机构信息登记表》，并承诺遵守《商用密码应用安全性评估行业自律公约》及相关的监管要求。

4.1.1 备案要求

检测机构应对其提交备案材料的真实性、完整性及合法性承担主体责任。商密协会收到备案材料后，应当对备案信息的完整性、规范性进行核对。发现检测机构存在提供虚假备案材料情形的，可依规采取通报、约谈、限期整改等措施；相关检测机构经整改仍不符合要求的，商密协会应当将有关情况报送上级密码管理部门，由其依法处理。

在天津市以外地区注册的检测机构，在天津市行政区域内开展密评业务前，除应履行本标准4.1条规定的备案义务外，还应当向天津市商用密码协会提交以下材料：

《商用密码检测机构资质证书》复印件（应清晰载明“商用密码应用安全性评估”业务范围），并加盖机构公章；

拟在天津市从事密评业务的人员清单及其《商用密码应用安全评估人员证书》彩色扫描件；

项目本地化技术服务保障方案（内容应包括：常驻天津技术人员名单、缴纳社会保险的证明材料，以及本地化服务承诺等）。

4.1.2 备案路径

检测机构应当将电子备案文件发送至商密协会指定邮箱。商密协会收到材料后，应定期将不涉及检测机构商业秘密及个人隐私的基本情况通报给专委会，由专委会共同确认。经专委会确认后，协会应在3个工作日内通过指定邮箱向检测机构发送备案确认通知；备案材料不完整的，协会应当一次性告知需要补正的全部内容。

4.1.3 备案有效期

备案确认通知有效期为一年，自备案确认通知载明的日期起算。有效期届满后，检测机构如需在天津市行政区域内继续开展商用密码应用安全性评估业务，应当于有效期届满前三十日内重新办理备案。

4.2 项目实施人员的服务要求

天津市及天津市以外地区注册的商用密码检测机构，在天津本地实施商用密码应用安全性评估项目时，为保障服务水平与质量，应严格遵守以下相关工作要求。

4.2.1 持证上岗要求

检测机构应当指派具备相应资格的人员实施密评项目。现场实施人员应当持有有效的商用密码应用安全性评估人员测评能力考核合格证，评估项目的现场实施人员不得少于2名。

检测机构不得采用人员挂靠或聘用兼职人员的方式开展商用密码应用安全性评估业务。

项目所涉及的其他密码业务服务人员，应当参加商密协会组织的密码业务培训，持有培训考核合格后由协会或其他合规机构颁发的相应证书（如密码技术应用员证书、天津市商用密码培训证书等）。

4.2.2 项目实施人员要求

检测机构应当根据项目实际需要合理确定项目实施周期，确保评估工作的充分性与规范性。

在测评过程中，检测机构应当对实施人员的主要工作节点进行必要的过程记录。过程记录可采用现场签到、工作日志、系统打卡等形式。检测机构应当将项目实施过程中的相关纸质材料（包括但不限于原始记录、过程文档、现场见证材料等）妥善留档备查，确保测评行为可追溯。

检测机构及项目实施人员应当积极配合密码管理部门及商密协会组织开展的现场核查、质量监督、行业自律检查等工作。实施人员应如实提供项目实施过程中的相关记录材料。

4.2.3 继续教育要求

密评人员或项目实施人员每年需完成不少于40学时继续教育，内容涵盖密码最新知识的要求、政策法规更新等。

检测机构应保留培训记录及考核成绩，保存期限不少于3年。

4.3 工作证明材料留存

天津市以外地区检测机构在天津实施密评项目后，检测机构应根据商用密码应用安全性评估报告要求提供项目实施周期内的差旅证明，包括但不限于与被测单位的工作记录、差旅机票、差旅火车票、住宿发票、餐饮票、城市打车票等佐证材料。

4.3.1 测评的工作记录

项目实施人员应当对测评过程中的主要工作节点进行记录，记录形式包括但不限于工作照片、被测单位出入记录、现场签到记录等。相关记录应当作为项目过程文件一并归档备查。

4.4 项目实施监督检查

专委会配合密码管理部门对天津市行政区域内密评项目的实施过程适时开展抽查。被抽查的检测机构应当予以配合，如实提供相关资料。重点核查内容包括但不限于项目实施周期、项目费用、服务质量等方面是否存在明显不合理情形，以及是否存在违规测评、虚假测评等行为。

4.5 项目档案管理

4.5.1 档案管理区域要求

检测机构需设立独立的办公区域和档案管理区域。档案管理区域应当采取相应的安全保护措施，包括但不限于：

a) 设置独立区域并配备专用门锁；

b) 档案柜应当独立配备柜锁，并按柜建立档案台账；

c) 在档案管理区域出入口配备视频监控装置，监控记录保存期限不少于6个月；

d) 建立档案管理区域出入记录制度。

4.5.2 项目归档内容要求

项目归档材料应当包括但不限于：

a) 项目过程文档（含测评原始记录、工作记录、过程记录材料等）；

b) 商用密码应用安全性评估报告；

c) 其他与项目实施相关的重要文件。

4.5.3 项目归档时间要求

测评原始记录、商用密码应用安全性评估报告及相关过程文档的保存期限不得少于6年，自项目完成之日起计算。

5 密评项目实施流程

根据国家密码管理局《关于进一步加强商用密码应用安全性评估结果备案工作的通知》（第 454 号）等相关文件要求，信息系统责任单位和运营单位应直接委托检测机构实施密评服务。

5.1 测评准备阶段服务

5.1.1 项目启动服务

检测机构和被测单位召开信息系统项目启动会议。

被测单位介绍系统基本情况（业务功能、等保定级情况、密码应用情况等）和项目安排（项目周期和当前项目进度）。

检测机构介绍商用密码应用安全性评估服务内容和服务方式。

会议形成会议纪要和签到表，作为项目过程文档。

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，检测机构组建测评项目组。做好人员安排，并编制项目计划书。项目计划书将包含项目概述、工作依据、技术思路、工作内容和项目组织等内容。

5.1.2 信息收集和分析服务

对于新建信息系统，信息收集和分析分为两部分：规划建设期间相关信息收集和分析、建设完成后相关信息收集和分析。

在信息系统规划建设期间，通过参加项目例会、线上沟通讨论等方式，了解系统建设进度和情况，涉及密码应用方面的建设，对其中可能影响密码应用合规性、正确性、有效性的问题，及时向被测单位进行风险提示，并给出合适的建议。

沟通结果和调研内容，形成可查询的记录，如邮件或纸质材料。在系统建设完成后，检测机构提供信息系统基本情况调研表，协助并督促被测单位填写调研表格，对信息系统的功能、部署环境、服务方式、用户类型等进行调研，同时对其定级报告、等级证明进行查阅。

对于调研情况不准确、不完善或存在相互矛盾的情况，现场实施人员将与被测单位相关人员进行沟通和确认。进行的沟通结果和调研内容，形成可查询的记录，如邮件或纸质材料。

5.1.3 工具和表单提供服务

检测机构根据系统当前现状，准备测评所需要的工具和相关表单。

工具准备：工具通常包括协议分析工具、密码算法验证工具、端口扫描工具、签名验签工具等。

表单准备：至少包括现场测评授权书、风险告知书、保密协议、文档交接单、会议记录表单、会议签到表单等。

5.1.4 测评准备阶段输出文档服务

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、现场测评授权书、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。

5.2 测评方案编制阶段服务

测评方案主要由检测机构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。

5.2.1 测评对象确定服务

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。

5.2.2 测评指标确定服务

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。

5.2.3 测评检查点确定服务

对一些关键安全点设置检查点，进行现场检查确认，以验证密码产品、密码服务是否被正确部署与应用，避免出现配置正确但实际未生效等情况。通过抓包测试、查看关键设备配置等方法，来确认密码算法、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。

5.2.4 测评内容确定服务

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，确定现场测评的具体实施内容，即单元测评内容。涉及现场测试部分时，根据确定的测评检查点，编制相应的测试内容。

5.2.5 测评方案编制服务

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；确定测评活动依据和参考的标准规范；依据委托书和系统情况估算工作量；编制具体测评实施计划，包括人员分工和时间安排；汇总以上内容，形成测评方案。

5.2.6 测评方案评审及确认服务

编制的测评方案进行内部评审后，提交被测单位签字确认。

5.2.7 测评方案编制阶段输出文档服务

测评方案编制活动的输出文档及其内容如表2所示。

表2 测评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	测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	测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	测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	测评方案的单元测评实施部分	单元测评实施内容。
测评方案编制	经过评审和确认的测评方案文本	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。

5.3 现场测评阶段服务

现场测评阶段服务主要是检测机构和被测单位进行沟通和协调，依据测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。

5.3.1 提供合规检测机构资质和密评人员服务

实施测评服务的主体应具备国家密码管理局下发的《商用密码检测机构资质证书（商用密码应用安全性评估业务）》（详见附录 A）。

检测机构在项目实施人员中至少有2名通过商用密码应用安全性评估人员测评能力考核，并在开展测评服务时提供商用密码应用安全性评估人员测评能力考核通过的证明（详见附录 B）。

5.3.2 现场测评准备服务

1、召开测评现场首次会，检测机构结合测评方案介绍测评工作，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，并对测评方案进行签字确认。以上会议留存会议纪要及签到表。

2、检测机构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数据。

3、被测单位签署（签字或盖章）保密协议、现场测评授权书和风险告知书。

4、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。

5.3.3 现场测评和结果记录服务

1、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。

2、密评人员根据现场测评结果填写完成测评结果记录表格。

5.3.4 结果确认和资料归还服务

1、现场测评完成之后，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。

2、召开测评现场结束会，检测机构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。以上会议留存会议纪要及签到表。

3、检测机构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。确认的文档包括会议纪要及签到信息表、现场核查记录表、文档交接单等。

5.3.5 现场测评阶段输出文档服务

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。

5.4 分析与报告编制阶段服务

现场测评工作结束后，检测机构将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。

5.4.1 单元测评服务

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，结论包括符合、不符合、部分符合和不适用四种情况。

5.4.2 整体测评服务

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，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。

5.4.3 量化评估服务

综合单元测评结果和整体测评结果，根据《商用密码应用安全性评估量化评 估规则》，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。

5.4.4 风险分析服务

密评人员依据密评的相关规范和标准，依据《信息系统密码应用高风险判定指引》，采用风险分析的方法分析测评结果中存在的安全问题可能对被测系统安全造成的影响。

5.4.5 评估结论服务

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。

密评结论（含量化评估、风险评估、不适用指标项等）应按照现行标准和文件要求完整准确给出，其中报告的评估结论共计有三种：符合、基本符合、不符合。

系统评估结论符合性判断规则如下：

综合得分100分，结论为符合；

综合得分小于100分、不低于60 分，且系统密码应用无高风险，结论为基本符合；否则，结论为不符合。

5.4.6 密评报告编制服务

根据分析与报告编制活动的各项任务输出形成密评报告。

报告内容要求：

1）密评报告选择的密评等级应与被测系统网络安全等级保护定级要求一致。

2）密评报告编制人、审核人、批准人（授权签字人）均应通过密评人员考核，加盖单位公章或密评/报告专用章。

3）密评报告中，业务情况、拓扑图，以及各个层面的密码应用情况描述应清晰、明确、易于理解。

4）密评报告应参照现行密评报告模板编制，内容完整，格式统一，排版清晰；无目录、页码、文字等方面的错误；特定对象名称（如单位名称、系统名称、系统等级等）前后一致。

5）密评报告所附测评记录应详实，不能全部为文字描述而无关键图片证据（如网络数据包或数字证书解析结果、重要数据存储状态、物理环境等的照片或截图）。

6）密评报告中的安全问题和改进建议应具体、清晰，不存在简单套用模板的情况。

7）密评报告编制完成后,检测机构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。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。

5.4.7 分析与报告编制阶段输出文档服务

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。

5.5 运行阶段售后服务

5.5.1 密码应用方案评估服务

商用密码应用方案评估报告服务，需协助出具方案评估报告（如应用系统客户需要），并需配合协助落实方案合规性审核及备案。

5.5.2 密码应用培训服务

在符合合同约定的前提下，信息系统责任单位或运营单位可根据项目实际需要，向检测机构提出密码应用培训要求。检测机构一年内可按需提供不少于2次现场培训，每次培训时长不少于1小时，两次培训时间间隔不少于6个月。

培训实施人员应持有有效的“商用密码应用安全性评估人员测评能力考核合格证”。检测机构留存培训记录（包括培训时间、地点、参训人员、培训内容等）及现场照片等过程材料，并在每次培训结束后5个工作日内，按照要求将培训情况报告提交至商密协会。

5.5.3 密码应用改进咨询服务

提供对被测对象的密码应用方案设计与规划的咨询，对被测单位提供现场答疑和整个项目评估服务周期内的咨询服务。

5.5.4 持续密码应用服务

在符合合同约定的前提下，信息系统责任单位或运营单位可根据项目实际需要，与检测机构协商确定密码应用服务的具体内容与频次。检测机构应当安排持有有效“商用密码应用安全性评估人员测评能力考核合格证”的人员提供服务。

每次现场服务结束后，检测机构应当在5个工作日内将服务证明（包括但不限于服务时间、地点、内容、人员及现场照片等过程材料）提交至商密协会。

持续密码应用服务的服务期自项目启动之日起计算，至下一年度该项目再次开展商用密码应用安全性评估工作时终止。如下一年度未开展评估工作，则服务期自项目启动之日起满365日终止。

5.5.5 限时响应专业服务

检测机构应建立限时响应服务机制，为用户提供7×24小时电话技术支持。对于现场支持服务，应根据问题的紧急程度和影响范围，在与用户约定的时限内响应并到达现场。

6 测评结果备案服务

6.1 密评报告备案服务

测评完成后，检测机构和被测单位应分别按照密码相关法律法规要求，将测评结果向相应密码管理部门进行备案。检测机构完成商用密码应用安全性评估工作后，应协助被测单位在密评报告出具之日起 30 日内完成向天津市国家密码管理局密评结果备案工作。

6.2 密评服务标准对照表备案服务

测评完成后，按照密评服务标准要求提交信息系统商用密码应用安全性评估服务对照表（详见附录 C）至相关商密协会。对于持续支持服务的条款，更新后按照要求及时提交。

附录A 商用密码检测机构资质证书（商用密码应用安全性评估业务）样例

商用密码检测机构资质证书

机构名称：

统一社会信用代码：

注册地址：

证书编号：

有效期至：

业务范围：

商用密码应用安全性评估

国家密码管理局

2024年11月11日

附录B 商用密码应用安全性评估人员测评能力考核（样例）

商用密码应用安全性评估
人员测评能力考核

编　　号：

姓　　名：

身份证号：

所在单位：

持证人参加 2020 年第 1 期全国商用密码应用安全性评估人员测评能力考核，成绩 [redacted] 分。

考核 合格 。

国家商用密码应用安全性评估
人员测评能力考核小组
2020 年 1 月 17 日

商用密码应用安全性评估
人员测评能力考核

编　　号：

姓　　名：

身份证号：

所在单位：

持证人参加商用密码应用安全性评估人员测评能力考核，成绩 85 分。考核 优秀 。

国家商用密码应用安全性评估
人员测评能力考核小组
2022 年 7 月 8 日

商用密码应用安全性评估从业人员
考核成绩

准考证号：[redacted]

姓　　名：[redacted]

身份证号：[redacted]

报考单位：[redacted]

持证人参加商用密码应用安全性评估从业人员考核，成绩[redacted]分。考核合格。

国家密码管理局商用密码管理办公室

2023 年 8 月 16 日

附录C 信息系统商用密码应用安全性评估服务对照表

序号	服务阶段	服务项目	服务内容	服务结果	是否完成
1	测评准备	项目启动	在项目启动任务中，检测机构组建密评项目组，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。	1、完成项目计划书的输出	□是 □否
				2、提供项目启动会议，考试合格的项目经理1人和项目组成员至少2人到场的证明，全部人员需要持证上岗	□是 □否
2		信息收集和分析	检测机构使用调查表格、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。	1、完成调查表格的输出	□是 □否
				2、完成系统等保报告、备案证明等收集	□是 □否
3		工具和表单准备	密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、调试测评工具、准备各种表单等。	1、选用的测评工具清单输出	□是 □否
				2、完成客户签字的现场测评授权书收集	□是 □否
				3、完成客户签字的风险告知书收集	□是 □否
				4、完成密评人员签字后的保密承诺书输出	□是 □否
				5、完成启动会签到表输出	□是 □否
4	方案编制	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。	1、测评方案中包含测评对象部分	□是 □否
5		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。	1、测评方案中包含测评指标部分	□是 □否

序号	服务阶段	服务项目	服务内容	服务结果	是否完成
6		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，来确认密码算法、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。	1、测评方案中包含测评检查点部分	□是 □否
7		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。	1、测评方案中包含单元测评实施部分	□是 □否
8		测评方案编制	测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。测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、测评检查点以及单元测评实施等。	1、完成测评方案的评审过程记录表输出	□是 □否
				2、完成测评方案输出	□是 □否
9	**现场测评**	现场测评准备	本任务启动现场测评，以保证检测机构能够顺利实施测评。	1、完成客户签字后的测评方案输出	□是 □否
				2、完成现场测评签到表输出	□是 □否
10		现场测评和结果记录	本任务主要是根据测评方案及现场测评准备的结果，测评方安排密评人员在现场完成测评工作。	1、完成密评过程原始记录输出	□是 □否
				2、完成被测系统问题确认单输出	□是 □否
11		结果确认和资料归还	结果确认和资料归还。	1、完成经过被测单位确认的各类测评结果记录输出	□是 □否
12	**报告编制**	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。	1、密评报告中包含所有测评的单元测评部分	□是 □否

序号	服务阶段	服务项目	服务内容	服务结果	是否完成
13		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。	1、密评报告中包含单元测评结果修正部分	□是 □否
14		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。	1、密评报告中包含整体测评结果和量化评估部分，以及总体评价部分	□是 □否
15		风险分析	密评人员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可能对被测系统安全造成的影响。	1、密评报告中包含风险分析部分	□是 □否
16		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。	1、密评报告中包含评估结论部分	□是 □否
17		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：概述、被测信息系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、量化评估、风险分析、评估结论、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。	1、完成密评报告的评审过程记录表输出	□是 □否
				2、完成确认后的密评报告输出	□是 □否
18	**总结**	报告总结会	项目报告总结会议。	1、完成末次会签到表的输出	□是 □否

序号	服务阶段	服务项目	服务内容	服务结果	是否完成
19	**密码应用方案评估**	商用密码应用方案评估服务	商用密码应用方案评估报告服务，需出具方案评估报告（如需要），并需配合协助落实方案合规性审核及 备案。	1、完成商用密码应用方案评估报告出具（如需要）	□是 □否
				2、协助完成商用密码应用方案合规性审核及备案（如需要）	□是 □否
20	**密码应用培训**	商用密码应用培训服务	检测机构对密码应用要求和密码评估开展相关培训，培训内容包括密码标准要求、密评工作要求等内容，培训服务年度内次数不少于2次，每次不少1小时，培训场地由被测单位和检测机构共同确定。	1、培训后5 个工作日内提交开展现场培训的培训计划、培训课件、培训签到表到商密协会	□是 □否
				2、提供培训老师的现场培训记录证明	□是 □否
21	**密码应用咨询**	商用密码应用咨询服务	提供对被测对象的密码应用方案设计与规划的咨询，对被测单位提供现场答疑和整个项目评估服务周期内的咨询服务	1、提供密评咨询访谈记录表	□是 □否
22	**持续密码应用改进**	持续密码应用改进服务	项目合同服务结束前，建议每2个月至少需有1名持证合格密评人员保证1天在使用方进行密码方面服务工作，每次服 务后需在5个工作日内提供服务证明。	1、每次服务后5 个工作日内提供服务证明到商密协会	□是 □否
				2、提供培训服务老师的现场改 进服务记录证明	□是 □否
23	**限时响应**	限时响应专业服务	现场支持服务接到用户电话一般问题6小时反馈问题结果，严重问题3小时到达现场，提供7*24小时电话服务。	1、提供加盖公章的限时响应的服务能力承诺书	□是 □否
24	**测评结果备案**	密评报告提交备案服务	确认所有信息填报完成后提交天津市国家密码管理局备案。	1、协助完成密评结果到密码主管部门备案	□是 □否
				2、完成将密码主管部门审核报备合格回执送达系统运营单位	□是 □否