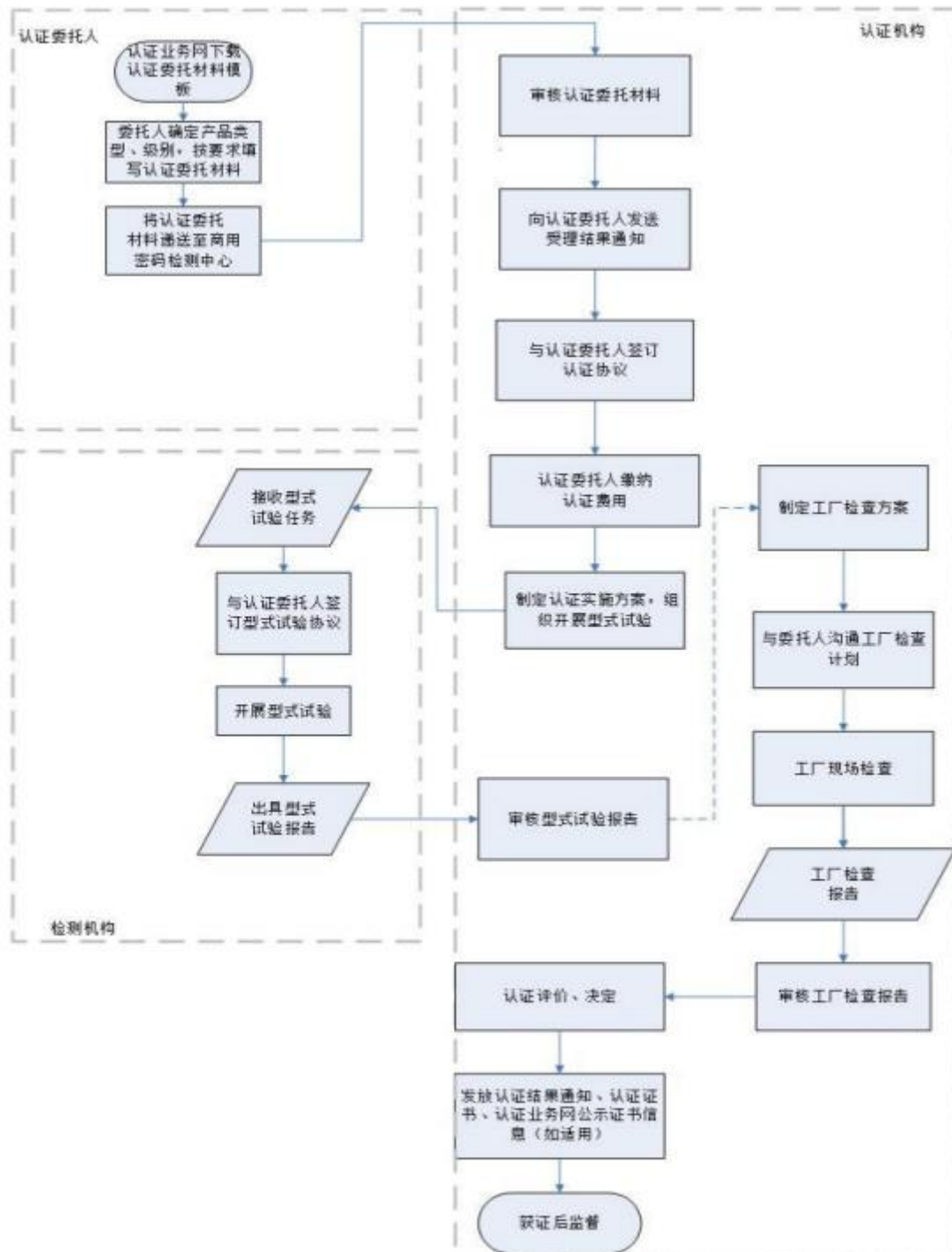


商用密码产品检测认证流程说明

1. 文件模板

文件模板获取链接如下：<https://service.scctc.org.cn/xzzx/rzyw/wjmb/>

2. 商用密码产品检测认证流程



3. 收费标准

收费公示

日期: 2022-11-13 字号: 大 中 小 分享:   

国推商用密码产品认证收费标准

序号	费用名称	金额	备注
1	申请费	500元/认证单元	认证机构在受理商用密码产品认证申请时向申请单位收取申请费。商用密码产品认证申请费收费标准为每个认证单元500元。
2	审核费	2500元/人-日	认证机构按照认证产品的工厂检查要求，对申请单位进行工厂检查时向申请认证单位收取审核费。商用密码产品认证审核费标准为每个检查员每个工作日2500元。
3	审定与注册费（含证书费）	800元/认证单元	认证机构在对符合认证要求的产品进行评定并颁发商用密码产品认证证书时，向申请认证单位收取审定与注册费。商用密码产品审定与注册费（含证书费）收费标准为每个认证单元800元。
4	监督审核费	2500元/人-日	认证机构在对获得认证证书的企业进行监督审核时收取监督审核费。商用密码产品监督审核费收费标准为每个检查员每个工作日2500元。
5	年金（含标志使用费）	100元/证书	为保证产品质量、保持证书有效，对同一申请单位获得的商用密码产品认证证书收取年金。商用密码产品认证年金统一按每个认证证书每年100元。

检测费用以检测合同为准。

4. 项目进度安排

1) 任务分发

任务内容：业务受理人员接收商用密码检测认证中心的型式试验任务书。并将项目任务分发给产品检测技术负责人。

责任人：业务受理员

工期：1 天

规范动作：业务受理员通过发送邮件并电话或口头告知的方式，确保所有相关人员明确自己的任务和责任。

2) 任务下达

任务内容：技术负责人接收到任务后，向项目经理下达详细的任务指令。

责任人：技术负责人

工期：1 天

规范动作：技术负责人通过发送邮件并电话或口头告知的方式，向项目经理明确任务要求、时间节点和交付标准，下发《任务通知书》。

3) 项目计划

任务内容：项目经理负责编制项目计划，并与销售和客户进行首次会议沟通。

责任人：项目经理

工期：3 天

规范动作：项目经理组织首次会议，与销售和客户共同讨论项目计划，向技术负责人提交初步计划。随后，项目经理还需要与客户进行进一步的沟通会，确保计划得到客户的认可。同时，项目经理负责组建项目团队，包括测评工程师、技术专家、项目审核组等。

4) 文档审查及不符合项发送及沟通

任务内容：对送检文档进行初步审查，拟定不符合项，与客户进行再次沟通。

责任人：测评工程师

工期：5 天

规范动作：项目经理及测评工程师完成文档的初步审查，将不符合项以邮件或书面形式发送给客户，并与客户完成不符合项的沟通。

5) 现场调试和测试

任务内容：测评工程师负责项目的现场调试和测试工作。

责任人：测评工程师

工期：20 天（可根据项目成熟度及技术人员配合程度调整）

规范动作：测评工程师与技术人员进行现场调试，为期 5 天。调试完成后，进行为期 15 天的测试工作，确保项目各项指标符合要求。项目经理负责解决一些复杂问题、并协调资源，及时解决问题。

6) 报告编写

任务内容：测评工程师负责编写项目报告。

责任人：测评工程师

工期：5 天

规范动作：测评工程师在 5 天内完成整套项目报告的编写，确保报告内容完整、准确、清晰。

7) 报告审核

任务内容：项目审核组和技术负责人负责对项目报告进行审核。

责任人：项目审核组、技术负责人和授权签字人

工期：5 天

规范动作：项目审核组、技术负责人和授权签字人在 5 天内完成项目报告的审核工作，确保报告的技术内容准确无误。

8) 报告签发

任务内容：项目经理负责将审核通过的签字的全套报告提交至商用密码检测认证中心。

责任人：项目经理

工期：2 天

规范动作：项目经理在 2 天内完成报告的签发工作，确保客户的报告及时提交至商用密码检测认证中心。

9) 回访

任务内容：项目经理或其他相应人员负责对客户进行回访，了解客户满意度。

责任人：项目经理或其他相应人员

工期：1 天

规范动作：项目经理或其他相应人员在 1 天内完成客户回访工作，收集客户反馈，确保客户满意度达到预期水平。

表 1 项目进度方案表

序号	任务内容	责任人	工期(天)	规范动作
1	任务分发	业务受理员	1	业务受理：发送邮件并电话或口头告知
2	任务下达	技术负责人/技术专家	1	任务下达：发送邮件并电话或口头告知
3	项目计划	项目经理	3	首次会议（和销售）+提交计划+客户沟通会
4	文档审查及不符合项发送及沟通	测评工程师	5	不符合发出和客户再次沟通，5 天内完成沟通

5	现场调试和测试	测评工程师	20	调试时间为 5 天，测试时间为 15 天
6	报告编写	测评工程师	5	5 天内完成整套报告编写
7	报告审核	项目审核组、技术负责人/技术专家和授权签字人	5	5 天内完成报告的审核
8	报告签发	项目经理	2	2 天内完成报告的签发
9	回访	项目经理或其他相应人员	1	完成客户满意度调查

10) 任务周期计划

总工期（不包含问题整改）：

整个检测周期计划的总工期为：1（任务分发）+1（任务下达）+3（项目计划）+5（文档审查及不符合项发送及沟通）+20（现场测试）+5（报告编写）+5（报告审核）+2（报告签发）+2（工厂检查）+1（回访）=45 天。

11) 注意事项

各责任人在执行任务时，应严格按照规范动作进行，确保任务质量和效率。如遇特殊情况导致任务延期，应及时通知相关人员并调整计划。项目经理应负责整个检测周期计划的协调和管理，确保各项任务按时完成。

5. 资源保障

(1) 人员配置

项目管理部门

为确保项目的顺利实施与交付，我司拥有专业的密码产品检测部门。该部门将全面统筹协调本项目的各项工作，从项目启动到最终交付，确保每个环节都得到有效管理和控制，保证项目高效、有序进行。

专业技术团队

拥有一支由 1 名项目经理 1 名技术专家（团队成员）和 4 名测评工程师（团队成员），

共 6 名技术人员构成的高学历专业技术团队。团队成员均具备丰富的行业经验和专业技能，能够应对项目中的各种挑战和问题。

项目经理：拥有具有丰富经验和专业技能的项目经理能担任此关键任务。项目经理将负责项目的总体规划、资源协调、人员管理等工作，确保项目顺利实施。同时，项目经理还需具有丰富的资质咨询及认证行业工作经验，能够牵头制定项目检测工作计划，并负责沟通协调，解决复杂问题。

技术专家：由行业资深技术专家和相关专业博士组成，保障项目两部分检测顺利进行，着重对项目第一部分包括但不限于基于格的密码算法、基于编码的密码算法、基于多变量的密码算法、基于哈希的密码算法及国际标准密码算法等内容提供技术支撑和技术把控。

测评工程师：将根据项目需求提供技术支持和解决方案，确保项目的技术实现符合要求；并负责将项目计划转化为实际行动，确保项目按照计划顺利进行。

团队建设与人才培养

我司高度重视团队建设和人才培养。我司定期组织内部培训和技能提升活动，提高团队成员的专业素质和综合能力。同时，我司还将鼓励团队成员之间互相学习和交流，促进知识的共享和团队的整体进步。

服务团队人员配置

服务团队配备 1 名项目经理，该项目经理将作为项目的主要负责人，全面负责项目的管理工作。项目经理将负责以下职责：

- 1) .负责组织协调沟通会议，确保双方之间的信息畅通，及时解决项目中的各种问题。
- 2) .负责解决一些复杂问题，并协调资源，确保问题能够及时得到解决，保证项目的顺利进行。
- 3) .根据要求，对项目团队的人员进行调度安排，确保项目团队能够高效地完成各项任务。
- 4) .完成产品技术文档的审查工作，协助对不符合项问题进行沟通确认并整改，确保项目的技术实现符合要求。

(2) 设备与工具

确保针对项目中各类密码检测工具的系统化、高效化的资源部署与利用，以支持 SSL VPN 密码检测、服务器密码机密码检测工具、以及算法正确性、随机数质量检测工具等检测工具的稳定运行和高效工作。



1) 硬件资源:

高性能服务器: 用于部署核心检测系统和处理大量检测任务, 确保系统运行的稳定性和处理速度。

专用密码卡/模块: 针对 PCI-E/PCI 密码卡等特定检测工具, 提供专用硬件支持, 确保密码检测的高效性和安全性。

存储设备: 配置大容量、高可靠性的存储设备, 用于保存检测数据、日志以及备份文件。

网络设备: 包括路由器、交换机等, 构建稳定、高效的网络环境, 支持各检测工具之间的数据传输和通信。

2) 软件资源:

操作系统: 选择稳定、安全的操作系统作为平台基础, 如 Linux 或 Windows Server。

检测工具软件: 部署相应的检测工具软件, 包括 SSL VPN、服务器密码机、服务器密码机等各类型密码检测工具。

数据库系统: 配置高性能的数据库系统, 用于存储和管理检测数据、用户信息、配置参数等。

安全管理软件: 部署防火墙、入侵检测系统等安全管理软件, 保障系统安全稳定运行。

(3) 项目设备资源部署

1) 硬件部署:

根据实际需求, 合理配置服务器、存储设备、网络设备以及专用密码卡/模块的数量和性能。

部署网络设备, 构建稳定、高效的网络环境, 确保各检测工具之间的数据传输和通信畅通无阻。

2) 软件部署:

安装操作系统和数据库系统，并进行必要的配置和优化。

部署检测工具软件，并进行参数设置和初始化配置。

安装安全管理软件，配置安全策略，确保系统安全稳定运行。

(4) 资源监控与优化

1) 性能监控：

建立性能监控机制，实时监测系统的运行状况和性能指标，如 CPU 利用率、内存占用率、网络带宽等。

根据监控数据，及时发现并解决性能瓶颈，优化系统性能。

2) 安全管理：

定期对系统进行安全检查，发现并修复潜在的安全漏洞和隐患。

加强用户权限管理，确保只有授权用户能够访问和操作系统。

3) 资源优化：

根据实际运行情况和业务需求，对硬件和软件资源进行动态调整和优化，提高资源利用率和系统性能。

定期进行维护和升级，保持稳定性和先进性。

6. 联系我们

姓名：万永泉

手机：139 2387 4393（微信同号）

电话：0755-89669007

邮箱：support@dxct.org

地址：深圳市坪山新区坪山街道行政二路招商花园城 9 栋