商用密码产品认证实施细则

签名验签服务器

国家密码管理局商用密码检测中心

2020 年 6 月

目 录

1 适用范围.....1
2 认证依据.....1
3 认证模式.....1
4 认证单元划分.....1
5 认证的基本环节.....1
6 认证实施.....1
6.1 认证委托.....1
6.1.1 认证委托及受理.....1
6.1.2 认证委托资料要求.....2
6.2 型式试验.....2
6.2.1 制定型式试验方案.....2
6.2.2 型式试验样品要求.....2
6.2.3 样品及相关资料的处置.....2
6.2.4 型式试验报告的提交.....2
6.3 初始工厂检查.....2
6.3.1 检查内容.....2
6.3.1.1 生产和保障能力.....2
6.3.1.2 产品一致性.....3
6.3.2 初始工厂检查时间.....3
6.4 认证评价与决定.....3
6.5 获证后监督.....3
6.5.1 获证后监督的频次和方式.....3
6.5.2 获证后监督审查的内容.....3
6.5.3 获证后监督的记录.....3
6.5.4 获证后监督结果评价.....4
7 认证时限.....4
8 认证证书.....4
8.1 认证证书的保持.....4
8.2 认证证书覆盖产品的变更.....4
8.2.1 变更委托.....4
8.2.2 变更评价与批准.....4
8.2.3 证书有效期.....4
8.3 认证证书覆盖产品的扩展.....4
8.3.1 认证证书覆盖产品扩展委托.....4
8.3.2 认证证书覆盖产品的扩展评价与批准.....4
8.3.3 证书有效期.....5
8.4 认证证书的注销、暂停和撤销.....5
8.5 认证证书的使用.....5
9 认证标志.....5
10 认证责任.....5

1 适用范围

本细则依据《商用密码产品认证规则》（以下简称认证规则）编制，作为认证规则的配套文件，与认证规则共同使用，适用于签名验签服务器产品认证。

2 认证依据

GM/T 0029《签名验签服务器技术规范》
GM/T 0028《密码模块安全技术要求》
GM/T 0065《商用密码产品生产和保障能力建设规范》
GM/T 0066《商用密码产品生产和保障能力建设实施指南》

签名验签服务器产品中的密码算法应为符合 GM/T 0001《祖冲之序列密码算法》、GM/T 0002《SM4 分组密码算法》、GM/T 0003《SM2 椭圆曲线公钥密码算法》、GM/T 0004《SM3 密码杂凑算法》、GM/T 0009《SM2 密码算法使用规范》、GM/T 0010《SM2 密码算法加密签名消息语法规范》、GM/T 0044《SM9 标识密码算法》等国家密码管理要求的密码算法。

签名验签服务器产品的随机数检测应遵循 GM/T 0005《随机性检测规范》、GM/T 0062《密码产品随机数检测要求》。

上述标准如未特别注明年代号，原则上应执行其最新版本（包括所有的修改单）。

3 认证模式

签名验签服务器产品认证模式为：
型式试验+初始工厂检查+获证后监督
认证机构可对获证产品生产企业的扩项产品认证委托，减免初始工厂检查环节。

4 认证单元划分

原则上应按签名验签服务器产品型号的不同划分认证单元。同一认证单元内有多个版本的产品时，认证委托人应提交不同版本间的差异说明，必要时还应进行补充差异试验。

5 认证的基本环节

认证的基本环节包括认证委托、型式试验、初始工厂检查、认证评价与决定、获证后监督。

6 认证实施

6.1 认证委托

6.1.1 认证委托及受理

认证委托人应按认证机构要求提交认证委托资料，认证机构于收到委托资料后 5 个工作日内完成资料形式化审核并给出审核意见。若认证委托人提交的资料齐全且符合规定形式，

认证机构向认证委托人发送认证受理通过通知。若认证委托人首次提交的认证委托资料不齐全或不符合规定形式，认证机构通知认证委托人补正资料；若认证委托人提交的补正资料仍不齐全或不符合规定形式，认证机构通知认证委托人受理不通过并说明理由。

6.1.2 认证委托资料要求

认证委托人委托认证时，应提交的认证委托资料，包括但不限于：

（1）认证委托书
（2）具有独立法人资格的证明材料
（3）商用密码产品生产和保证能力自我评估表
（4）技术工作总结报告
（5）安全性设计报告
（6）密码模块分级检测申请材料
（7）用户手册
（8）生产一致性证明文件
（9）产品实物图
（10）其他需要的文件

6.2 型式试验

6.2.1 制定型式试验方案

认证机构根据认证委托资料制定型式试验方案并通知认证委托人，将型式试验方案及相关委托资料转交检测机构。型式试验方案包括型式试验的样品要求和数量、检测标准项目、检测机构信息等。

6.2.2 型式试验样品要求

认证委托人按型式试验方案提供样品至检测机构，并保证样品与实际生产产品一致；必要时，认证机构也可采用生产现场抽样的方式获得样品。

6.2.3 样品及相关资料的处置

检测机构应对型式试验全过程作出完整记录，并妥善管理、保存、保密相关资料，确保在认证有效期内检测结果可追溯。认证委托人可在认证结束后取回型式试验样品。

6.2.4 型式试验报告的提交

型式试验结束后，检测机构应在 5 个工作日内向认证机构和认证委托人出具型式试验报告，出具型式试验报告时间计算在型式试验周期内。

6.3 初始工厂检查

6.3.1 检查内容

认证机构进行初始工厂检查的内容为生产能力、质量保障能力、安全保障能力、服务保障能力，以及产品一致性检查等。

初始工厂检查的场所范围原则上覆盖产品的设计研发环境和生产加工环境。

6.3.1.1 生产和保障能力

由认证机构依据 GM/T 0065《商用密码产品生产和保障能力建设规范》和 GM/T 0066

《商用密码产品生产和保障能力建设实施指南》等标准规范实施审核和检查。

6.3.1.2 产品一致性

初始工厂检查时，在生产现场对委托认证的产品进行一致性检查。重点检查以下内容：

(1）认证产品的铭牌、包装上所标明的及运行时所显示的产品名称、型号、版本号与型式试验报告上所标明的内容是否一致；

(2）认证产品所用的软件、硬件与型式试验合格的样品是否一致；

(3）非认证的产品是否违规标贴了认证标识。

6.3.2 初始工厂检查时间

由认证机构根据认证实施需要安排初始工厂检查。人日数根据所委托认证产品的认证单元数量确定，并适当考虑工厂的规模及产品的安全级别，一般每个场所为 4 至 6 个人日。

6.4 认证评价与决定

认证机构对型式试验、初始工厂检查结论和相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书并允许使用认证标志；对暂不符合认证要求的，可要求认证委托人限期（通常情况下不超过 3 个月）整改，整改后仍不符合的则书面通知认证委托人终止认证。

6.5 获证后监督

6.5.1 获证后监督的频次和方式

为保证产品持续符合标准要求，在认证有效期内，认证机构持续进行获证后监督，监督频次一般为一年一次，认证机构可根据实际情况调整监督频次。获证后监督可采用工厂检查或文件审查的方式。在证书有效期内，认证机构至少开展一次工厂检查。认证机构可采取事先不通知的方式对获证方实施监督。

获证方如出现以下情形之一，认证机构可视情况增加获证后监督审查的频次：

（1） 获证产品出现严重质量问题，或者用户提出投诉并经查实为获证方责任时；

（2） 认证机构有足够理由，对获证产品与本规则中规定的标准要求的符合性提出质疑时；

（3） 有足够信息表明获证方因组织机构、生产条件、质量管理体系等发生变更，从而可能影响产品质量时。

6.5.2 获证后监督审查的内容

获证后监督可采用工厂检查或文件审查的方式。必要时可在生产现场或市场抽样，对产品进行检测。

工厂检查时，主要对生产能力、质量保障能力、安全保障能力、服务保障能力，以及认证产品一致性进行检查。文件审查时，认证委托人应向认证机构提交生产一致性证明文件，自测报告等资料。如需进行抽样检测时，抽样检测的样品应在获证方的产品中（包括生产线、仓库、市场）随机抽取。型式试验的检测项均可以作为监督时的检测项，认证机构可根据具体情况选取部分或全部进行检测。

6.5.3 获证后监督的记录

认证机构对获证后监督进行记录并归档留存，以保证认证过程和结果具有可追溯性。

6.5.4 获证后监督结果评价

认证机构对获证后监督结论和相关资料信息进行综合评价。评价通过的，可继续保持认证证书、使用认证标志；不通过的，认证机构根据相应情形做出暂停或者撤销认证证书的处理。

7 认证时限

认证时限是指自委托被正式受理之日起至颁发认证证书时止所实际发生的工作日。整改时间不计算在内。因委托人未及时提交材料、未能及时递送样品、不能按计划接受工厂检查、未及时缴纳费用等原因导致认证时间的延长时，不计算在内。

认证委托、初始工厂检查、认证评价与决定三个基本环节，安全等级第一级、第二级的一般在 30 个工作日内完成，安全等级第三级、第四级的一般在 40 个工作日内完成。

型式试验环节，安全等级第一级的一般在 30 个工作日内完成，安全等级第二级的一般在 60 个工作日内完成，安全等级第三级的一般在 80 个工作日内完成，安全等级第四级的一般在 120 个工作日内完成。

8 认证证书

8.1 认证证书的保持

认证证书有效期为 5 年，并通过认证机构的获证后监督保持效力。证书到期需延续使用的，认证委托人应在有效期届满前 6 个月内提出认证委托。认证机构采用获证后监督的方式对符合认证要求的委托换发新证书。

8.2 认证证书覆盖产品的变更

8.2.1 变更委托

获证后的产品或其生产者（制造商）、生产企业等发生变化时，认证委托人应向认证机构提出变更委托。

8.2.2 变更评价与批准

认证机构根据变更的内容，对委托资料进行审核，确定是否可以批准变更。如需样品检测和/或工厂检查，应在检测和/或检查合格后方能批准。

8.2.3 证书有效期

变更后，证书有效期与原证书一致。

8.3 认证证书覆盖产品的扩展

8.3.1 认证证书覆盖产品扩展委托

认证委托人需要增加已经获得的认证证书覆盖的产品范围时，应向认证机构提出扩展委托，并提供扩展产品和获证产品之间的差异说明。

8.3.2 认证证书覆盖产品的扩展评价与批准

认证机构可采用委托资料审核、补充差异试验和/或工厂检查的方式核查原认证结果对

扩展产品的有效性。核查通过的，由认证机构换发新证书。

8.3.3 证书有效期

扩展后，证书有效期与原证书一致。

8.4 认证证书的注销、暂停和撤销

认证证书的暂停、注销和撤销依据有关规定执行。认证机构采用适当方式对外公布被暂停、注销和撤销的产品认证证书。

8.5 认证证书的使用

认证证书可以展示在文件、网站、通过认证的工作场所、销售场所、广告和宣传资料或广告宣传等商业活动中，但不得利用认证证书和相关文字、符号，误导公众认为认证证书覆盖范围外的产品、服务、管理体系获得认证。宣传认证结果时不得损害认证机构的声誉。

9 认证标志

标志的图案如下图。

标志的样式和使用应符合《商用密码产品认证规则》。

10 认证责任

认证机构对其做出的认证结论负责。
检测机构对检测结果和检测报告负责。
认证机构及其所委派的工厂检查员对工厂检查结论负责。
认证委托人对其所提交的委托资料及样品的真实性、合法性负责。