商用密码应用安全性评估量化评估规则

中国密码学会密评联委会

二〇二〇年十二月

目　录

商用密码应用安全性评估量化评估规则

1. 范围

本文件依据 GB/T AAAAA《信息安全技术 信息系统密码应用基本要求》和 GM/T BBBB《信息系统密码应用测评要求》，对信息系统的密码应用情况给出定量评估结果。

本文件适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

2. 规范性引用文件

1) GB/T AAAAA《信息安全技术 信息系统密码应用基本要求》
2) GM/T BBBB《信息系统密码应用测评要求》

3. 原则

本文件按如下原则设计量化评估规则：

1) 遵循法律法规和最新相关指导性文件的总体要求；
2) 遵循 GB/T AAAAA 和 GM/T BBBB；
3) 鼓励使用密码技术；
4) 特别鼓励使用合规的密码算法/技术/产品/服务；
5) 优先在网络和通信安全层面、应用和数据安全层面进行密码技术应用。

4. 量化评估框架

参考 GM/T BBBB，本规则从三个方面进行量化评估：

- 密码使用安全（*Cryptography **D**eployment security*）是指，密码技术是否被正确、有效使用，以满足信息系统的安全需求，有效提供机密性、完整性、真实性和不可否认性的保护；
- 密钥管理安全（***K**ey management security*）是指，密钥管理的全生命周期是否安全，用于密码计算或密钥管理的密码产品/密码服务是否安全。
- 密码算法/技术安全（*Cryptography **A**lgorithm/Technique security*）是指，信息系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，信

息系统中使用的密码技术是否遵循密码相关国家标准和行业标准或经国家密码管理部门核准。

5. 量化规则

（1）各测评对象的测评结果量化规则

密码应用技术要求中，第 i 个安全层面的第 j 测评单元的第 k 测评对象 $T_{i,j,k}$，其量化评估结果 $S_{i,j,k}\in\{0, 0.25, 0.5, 1\}$，其中 0 表示不符合，1 表示符合，其它表示部分符合。$S_{i,j,k}$ 的取值分别见表 1。**通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标**不单独评价。

密码应用管理要求不针对各个测评对象的测评结果进行量化评估。

（2）测评单元的测评结果量化规则

第 i 个安全层面的第 j 测评单元 $U_{i,j}$ 的量化评估结果 $S_{i,j}$ 为该测评单元内所有 $n_{i,j}$ 个测评对象测评结果的算术平均值（四舍五入，取小数点后 4 位），即：

$$S_{i,j}=\frac{\sum_{1\le k\le n_{i,j}} S_{i,j,k}}{n_{i,j}}$$

密码应用管理要求中，第 i 个安全层面的第 j 测评单元，根据 GM/T BBBB 给出判定结果 $S_{i,j}$，符合为 1 分，不符合为 0 分，部分符合为 0.5 分。

（3）安全层面的测评结果量化规则

本文件为每个测评单元分配了相应的权重$w_{i,j}$，如表 2 所示。第 i 个安全层面 L_i 的量化评估结果 S_i 为该安全层面内所有 n_i 个适用测评单元测评结果 $S_{i,j}$ 的加权平均值（四舍五入，取小数点后 4 位），即：

$$S_i=\frac{\sum_{1\le j\le n_i} w_{i,j}S_{i,j}}{\sum_{1\le j\le n_i} w_{i,j}}$$

若某测评指标不适用，则不参与量化评估过程，不适用的判定方式参见 GM/T BBBB）。

（4）整体测评结果量化规则

本文件为每个安全层面分配了相应的权重w_i，如表 2 所示。量化评估结果 S 为所有 n 个安全层面测评结果 S_i 的加权平均值（四舍五入，取小数点后 2 位），即：

$$S=\frac{\sum_{1\le i\le n} w_i\cdot S_i}{\sum_{1\le i\le n} w_i}\times 100$$

若某个安全层面的所有测评指标都不适用，则该安全层面不参与量化评估过程。

6. 整体结论判定

整体量化评估结果S为100分，则判定被测信息系统**符合**GB/T AAAAA相应等级要求；*S*低于100分、不低于阈值，且经风险评估发现没有高风险，则判定被测信息系统**基本符合**GB/T AAAAA 相应等级要求；否则，判定被测信息系统**不符合** GB/T AAAAA 相应等级要求。

表 1 量化评估表

符合情况	涉及情况			示例	分值 $S_{i,j,k}$
	密码使用安全 ***D***	密码算法/技术合规性 ***A***	密钥管理安全 ***K***		
符合	√	√	√	全部符合相关的要求	1
部分符合	√	×	√	使用认证合格的密码产品，但使用的密码算法/技术不合规	0.5
	√	√	×	使用未经认证或不满足安全等级要求的密码产品，但使用的密码算法/技术合规	
	√	×	×	使用未经认证或不满足安全等级要求的密码产品，且使用的密码算法/技术不合规	0.25
不符合	×	/	/	使用的密码技术无法满足信息系统的安全需求，或未使用密码技术等	0

表 2 测评指标权重表

序号	测评单元			安全层面权重（w_i）	指标权重 $w_{i,j}$			
					第一级	第二级	第三级	第四级
1	密码技术应用要求	物理和环境安全	身份鉴别	10	0.4	0.7	1	1
2			电子门禁记录数据存储完整性		0.4	0.4	0.7	1
3			视频记录数据存储完整性		/	/	0.7	1
4		网络和通信安全	身份鉴别	15	0.4	0.7	1	1
5			通信数据完整性		0.4	0.4	0.7	1
6			通信过程中重要数据的机密性		0.4	0.7	1	1
7			网络边界访问控制信息的完整性		0.4	0.4	0.7	1
8			安全接入认证		/	/	0.4	0.7
9		设备和计算安全	身份鉴别	15	0.4	0.7	1	1
10			远程管理通道安全		/	/	1	1
11			系统资源访问控制信息完整性		0.4	0.4	0.7	1
12			重要信息资源安全标记完整性		/	/	0.7	1
13			日志记录完整性		0.4	0.4	0.7	1

14			重要可执行程序完整性、重要可执行程序来源真实性		/	/	0.7	1
15		应用和数据安全	身份鉴别	30	0.4	0.7	1	1
16			访问控制信息完整性		0.4	0.4	0.7	1
17			重要信息资源安全标记完整性		/	/	0.7	1
18			重要数据传输机密性		0.4	0.7	1	1
19			重要数据存储机密性		0.4	0.7	1	1
20			重要数据传输完整性		0.4	0.7	1	1
21			重要数据存储完整性		0.4	0.7	1	1
22			不可否认性		/	/	1	1
23	安全管理	管理制度	具备密码应用安全管理制度	8	1	1	1	1
24			密钥管理规则		0.7	0.7	0.7	0.7
25			建立操作规程		/	0.7	0.7	0.7
26			定期修订安全管理制度		/	/	0.7	0.7

27			明确管理制度发布流程		/	/	0.7	0.7
28			制度执行过程记录留存		/	/	0.7	0.7
29		人员管理	了解并遵守密码相关法律法规和密码管理制度	8	0.7	0.7	0.7	0.7
30			建立密码应用岗位责任制度		/	1	1	1
31			建立上岗人员培训制度		/	0.7	0.7	0.7
32			定期进行安全岗位人员考核		/	/	0.7	0.7
33			建立关键岗位人员保密制度和调离制度		0.7	0.7	0.7	0.7
34		建设运行	制定密码应用方案	8	1	1	1	1
35			制定密钥安全管理策略		1	1	1	1
36			制定实施方案		0.7	0.7	0.7	0.7
37			投入运行前进行密码应用安全性评估		1	1	1	1
38			定期开展密码应用		/	/	0.7	0.7

			安全性评估及攻防对抗演习					
39		应急处置	应急策略	6	1	1	1	1
40			事件处置		/	/	0.7	0.7
41			向有关主管部门上报处置情况		/	/	0.7	0.7