商用密码应用安全性评估量化评估规则

（2023 版）

2023 年 7 月 17 日发布　　2023 年 8 月 1 日实施

中国密码学会密评联委会

目 录

主要修订情况

版本	章节	主要修订内容
2020	/	首次制定
2021	第4章	● 将“密码使用安全”更名为“密码使用有效性” ● 将“密码算法/技术安全”更名为“密码算法/技术合规性”
	第5章	● 增加“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”的示例 ● 完善量化评估表的说法，并增加脚注 ● 更新安全层面和测评单元的权重值
2023	第1章	对适用范围的说法进行微调
	第3章	对原则的说法进行微调
	第4章	对框架的说法进行微调
	第5章	● 更名为“量化评估规则” ● 修改各测评对象的测评结果量化评估规则和量化评估表，增加密码算法/技术合规性修正参数和密钥管理安全修正参数，并增补《商用密码应用安全性评估报告模板（2023版）》中针对分值弥补的说明 ● 修改整体测评结果量化评估规则，使密码应用技术要求和密码应用管理要求两部分分值保持固定
	第6章	● 更名为“量化评估阈值” ● 增补《商用密码应用安全性评估报告模板（2023版）》中确定的阈值

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 39786—2021《信息安全技术信息系统密码应用基本要求》和 GM/T 0115—2021《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。

本文件适用于规范信息系统密码应用安全性评估，以及指导相关信息系统的规划、建设等工作。

2. 规范性引用文件

1) GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》
2) GM/T 0115—2021《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 39786—2021 和 GM/T 0115—2021；
3) 鼓励使用合规的密码算法/技术/产品/服务；
4) 优先在网络和通信安全层面、应用和数据安全层面推进密码技术应用。

4. 量化评估框架

参考 GM/T 0115—2021，本规则从三个方面进行量化评估：

- 密码使用有效性（*Cryptography **D**eployment effectiveness*）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；
- 密码算法/技术合规性（*Cryptography **A**lgorithm/Technique compliance*）是指，信息系统中使用的密码算法是否符合法律、行政法规、国家有关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通过国家密码管理部门审查鉴定。

- 密钥管理安全（***Key management security***）是指，密钥的全生命周期管理是否安全，用于密码计算或密钥管理的密码产品/密码服务是否安全。

5. 量化评估规则

（1）各测评对象的测评结果量化评估规则

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 $S_{i,j,k}\in[0, 1]$，其中 0 表示不符合，1 表示符合，其它表示部分符合。$S_{i,j,k}$ 的取值见表 1（涉及计算时，四舍五入，取小数点后 4 位）。**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。

涉及以下情况时，需要对测评对象的分值进行修正：

- 若测评对象 A 弥补了测评对象 B 的不足，测评对象 A 的分值为 P_A，测评对象 B 的弥补前分值为 P_B，则测评对象 B 弥补后的分值为 MAX(0.5×P_A, P_B)，即 0.5×P_A 和 P_B 之间的较大值（四舍五入，取小数点后 4 位）。

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评估规则

密码应用技术要求中，第 i 个安全层面的第 j 测评单元 $U_{i,j}$ 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 0115—2021 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评估规则

本文件为每个测评单元分配了相应的权重$w_{i,j}$，如表 4 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 个适用测评单元的测评结果 $S_{i,j}$ 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 0115—2021）。

（4）整体测评结果量化评估规则

本文件为每个安全层面分配了相应的权重w_i，如表 4 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：

$$S = \frac{\sum_{1 \le i \le 4} w_i \cdot S_i}{\sum_{1 \le i \le 4} w_i} \times 70 + \frac{\sum_{5 \le i \le 8} w_i \cdot S_i}{\sum_{5 \le i \le 8} w_i} \times 30$$

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。比如，如果信息系统中“物理和环境安全”层面所有测评指标都不适用，而其他各层面均有适用的测评指标，那么根据表 4 提供的安全层面权重，上述分值计算公式具体为：

$$S = \frac{\sum_{2 \le i \le 4} w_i \cdot S_i}{60} \times 70 + \frac{\sum_{5 \le i \le 8} w_i \cdot S_i}{30} \times 30。$$

6. 量化评估阈值

采用本文件进行量化评估时，GM/T 0115—2021“9. 评估结论”中的得分阈值为60分。

表 1 量化评估表

符合情况	涉及情况			示例	分值 $S_{i,j,k}$
	密码使用有效性 *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	√	×	√	密码使用有效，具备安全的密钥管理机制，但使用的密码算法/技术不符合法律、行政法规、国家有关规定和密码相关国家标准、行业标准的有关要求	$0.5R_a$
	√	√	×	密码使用有效，使用的密码算法/技术符合法律、行政法规、国家有关规定和密码相关国家标准、行业标准的有关要求，但是相关的密钥管理机制存在问题	$0.5R_k$
	√	×	×	密码使用有效，但使用的密码算法/技术不符合法律、行政法规、国家有关规定和密码相关国家标准、行业标准的有关要求，相关的密钥管理机制也存在问题	$0.25R_aR_k$
不符合	×	/	/	未使用密码技术，或由于未正确、有效使用密码技术导致无法满足信息系统的安全需求	0
注 1：在判定密码使用有效性、密码算法/技术合规性、密钥管理安全三个维度时，均进行独立判定，比如：在单独判定密码使用有效性维度时，不考虑由于密码算法/技术合规性和密钥管理安全导致的风险。 注 2：R_a 为密码算法/技术合规性修正参数，取值见表 2；R_k 为密钥管理安全修正参数，取值见表 3。					

表 2 密码算法/技术合规性修正参数 R_a 取值表

密码算法/技术使用情况	所使用的密码算法/技术与信息系统安全要求不匹配	所使用的密码算法/技术可以在一定程度上为信息系统提供安全保障	所使用的密码算法/技术可以较好地为信息系统提供安全保障
示例	安全强度小于 80 比特的密码算法/技术	安全强度大于等于 80 比特小于 112 比特的密码算法/技术	安全强度大于等于 112 比特的密码算法/技术
R_a	0.2	0.5	1

表 3 密钥管理安全修正参数 R_k 取值表

密码应用级别	第一级 第二级	第三级		第四级	
密钥管理安全情况	/	使用一级密码模块，且能够满足 GM/T 0115—2021 中“5.5 密钥管理安全性”的其他要求	其他情况	使用二级密码模块，且能够满足 GM/T 0115—2021 中“5.5 密钥管理安全性”的其他要求	其他情况
R_k	1 （不修正）	1.2	1 （不修正）	1.5	1 （不修正）

表 4 测评单元权重表

要求维度	安全层面序号 *i*	安全层面	测评单元序号 *j*	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
密码应用技术要求	1	物理和环境安全	（1）	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	0.7
			（3）	视频记录数据存储完整性		/	/	0.7	0.7
	2	网络和通信安全	（1）	身份鉴别	20	0.4	0.7	1	1
			（2）	通信数据完整性		0.4	0.4	0.7	1
			（3）	通信过程中重要数据的机密性		0.4	0.7	1	1
			（4）	网络边界访问控制信息的完整性		0.4	0.4	0.4	0.7
			（5）	安全接入认证		/	/	0.4	0.7
	3	设备和计算安全	（1）	身份鉴别	10	0.4	0.7	1	1
			（2）	远程管理通道安全		/	/	1	1
			（3）	系统资源访问控制信息完整性		0.4	0.4	0.4	0.7
			（4）	重要信息资源安全标记完整性		/	/	0.4	0.7
			（5）	日志记录完整性		0.4	0.4	0.4	0.7
			（6）	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

	4	应用和数据安全	（1）	身份鉴别	30	0.4	0.7	1	1
			（2）	访问控制信息完整性		0.4	0.4	0.4	0.7
			（3）	重要信息资源安全标记完整性		/	/	0.4	0.7
			（4）	重要数据传输机密性		0.4	0.7	1	1
			（5）	重要数据存储机密性		0.4	0.7	1	1
			（6）	重要数据传输完整性		0.4	0.7	0.7	1
			（7）	重要数据存储完整性		0.4	0.7	0.7	1
			（8）	不可否认性		/	/	1	1
密码应用管理要求	5	管理制度	（1）	具备密码应用安全管理制度	8	1	1	1	1
			（2）	密钥管理规则		0.7	0.7	0.7	0.7
			（3）	建立操作规程		/	0.7	0.7	0.7
			（4）	定期修订安全管理制度		/	/	0.7	0.7
			（5）	明确管理制度发布流程		/	/	0.7	0.7
			（6）	制度执行过程记录留存		/	/	0.7	0.7
	6	人员管理	（1）	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
			（2）	建立密码应用岗位责任制度		/	1	1	1
			（3）	建立上岗人员培训制度		/	0.7	0.7	0.7
			（4）	定期进行安		/	/	0.7	0.7

				全岗位人员考核					
			（5）	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
	7	建设运行	（1）	制定密码应用方案	8	1	1	1	1
			（2）	制定密钥安全管理策略		1	1	1	1
			（3）	制定实施方案		0.7	0.7	0.7	0.7
			（4）	投入运行前进行密码应用安全性评估		1	1	1	1
			（5）	定期开展密码应用安全性评估及攻防对抗演习		/	/	0.7	0.7
	8	应急处置	（1）	应急策略	6	1	1	1	1
			（2）	事件处置		/	/	0.7	0.7
			（3）	向有关主管部门上报处置情况		/	/	0.7	0.7