



# 中华人民共和国国家标准

GB/T 29829—2022

代替 GB/T 29829—2013

## 信息安全技术 可信计算 密码支撑平台功能与接口规范

Information security technology—Functionality and interface  
specification of cryptographic support platform for trusted computing

2022-04-15 发布

2022-11-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布

中 华 人 民 共 和 国  
国 家 标 准  
信 息 安 全 技 术 可 信 计 算  
密 码 支 撑 平 台 功 能 与 接 口 规 范  
GB/T 29829—2022

\*

中 国 标 准 出 版 社 出 版 发 行  
北 京 市 朝 阳 区 和 平 里 西 街 甲 2 号 (100029)  
北 京 市 西 城 区 三 里 河 北 街 16 号 (100045)

网 址 : [www.spc.org.cn](http://www.spc.org.cn)

服 务 热 线 : 400-168-0010

2022 年 4 月 第 一 版

\*

书 号 : 155066 · 1-70212

版 权 专 有 侵 权 必 究

## 目 次

前言 .....	XV
引言 .....	XVI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	3
5 可信计算密码支撑平台概述 .....	4
5.1 可信计算概述 .....	4
5.2 可信构件 .....	4
5.3 可信计算基 .....	4
5.4 可信边界 .....	5
5.5 可信传递 .....	5
5.6 可信授权 .....	5
6 可信计算密码支撑平台功能 .....	5
6.1 平台体系结构 .....	5
6.2 平台接口功能 .....	7
7 可信密码模块接口 .....	11
7.1 通用要求 .....	11
7.2 启动命令 .....	11
7.3 检测命令 .....	13
7.4 会话命令 .....	15
7.5 对象命令 .....	16
7.6 复制命令 .....	24
7.7 非对称算法命令 .....	28
7.8 对称算法命令 .....	32
7.9 随机数发生器命令 .....	33
7.10 杂凑/HMAC 命令 .....	34
7.11 证明命令 .....	40
7.12 临时 EC 密钥命令 .....	44
7.13 签名及签名验证命令 .....	46
7.14 度量命令 .....	48
7.15 增强授权命令 .....	50
7.16 分层命令 .....	60

7.17	字典攻击命令	66
7.18	管理功能命令	67
7.19	上下文管理命令	68
7.20	属性命令	71
7.21	NV 操作命令	72
8	证实方法	82
8.1	概述	82
8.2	符合性实现原理说明	82
附录 A (规范性)	数据结构	86
A.1	命令码	86
A.2	返回码	90
A.3	基本常量	94
A.4	结构定义	117
A.5	密码参数和结构	133
A.6	密钥/对象结构	138
A.7	NV 存储结构	143
A.8	上下文数据	147
附录 B (资料性)	可信密码模块证实实例	151
B.1	概述	151
B.2	启动命令输入输出实例	151
B.3	检测命令输入输出实例	151
B.4	会话命令输入输出实例	152
B.5	对象命令输入输出实例	152
B.6	复制命令输入输出实例	155
B.7	非对称算法命令输入输出实例	157
B.8	对称算法命令输入输出实例	158
B.9	HASH/HMAC/Event 命令输入输出实例	158
B.10	证书命令输入输出实例	160
B.11	临时 EC 命令输入输出实例	162
B.12	签名及签名验证命令输入输出实例	162
B.13	完整命令输入输出实例	163
B.14	增强授权命令输入输出实例	164
B.15	分层命令输入输出实例	166
B.16	字典攻击命令输入输出实例	167
B.17	管理功能命令输入输出实例	168
B.18	上下文管理命令输入输出实例	168
B.19	性能命令输入输出实例	170

B.20 NV 操作命令输入输出实例 .....	170
附录 C (资料性) 可信密码模块体系架构和功能原理 .....	174
C.1 TCM 的架构 .....	174
C.2 TCM 自身安全 .....	177
C.3 TCM 执行状态 .....	177
C.4 TCM 控制域 .....	179
C.5 主种子 .....	180
C.6 TCM 句柄 .....	181
C.7 TCM 对象名称 .....	182
C.8 PCR 操作 .....	183
C.9 TCM 命令/响应结构 .....	184
C.10 授权 .....	189
C.11 会话加密 .....	204
C.12 受保护的存储 .....	205
C.13 受保护的存储层次结构 .....	207
C.14 凭据保护 .....	213
C.15 对象属性 .....	215
C.16 对象结构元素 .....	215
C.17 对象创建 .....	217
C.18 对象加载 .....	220
C.19 对象创建参考实现 .....	220
C.20 上下文管理 .....	221
C.21 证明 .....	226
C.22 密码支持函数 .....	226
C.23 硬件可信度量根的核心时间序列 .....	227
C.24 时间组件 .....	227
C.25 非易失性存储器 .....	228
C.26 错误和返回码 .....	235
C.27 通用输入输出 .....	235
附录 D (资料性) 章条编号对照一览表 .....	236
附录 E (资料性) 可信密码模块应用案例 .....	239
E.1 基于 TCM 的信任链传递 .....	239
E.2 增强型 TCM 的可信启动 .....	239
E.3 基于 TCM 建立设备与服务的可信连接 .....	239
参考文献 .....	242
图 1 密码对平台功能的支撑关系图 .....	5

图 2 可信密码支撑平台技术结构 ..... 6

图 3 完整性度量流程 ..... 10

图 C.1 可信密码模块结构 ..... 174

图 C.2 可信密码模块命令执行流程图 ..... 176

图 C.3 命令或响应标头 ..... 185

图 C.4 标记值 ..... 187

图 C.5 响应的授权布局 ..... 187

图 C.6 没有内部封装只有外部封装的复制过程 ..... 210

图 C.7 带有内部封装和 TCM\_RH\_NULL 为 NP 的复制过程 ..... 210

图 C.8 没有内部封装和 TCM\_RH\_NULL 为 NP 的复制过程 ..... 211

图 C.9 保护组 ..... 212

图 E.1 信任链传递 ..... 239

图 E.2 可信链接框架设计 ..... 240

  

表 1 TCM2\_Startup()接口输入参数 ..... 12

表 2 TCM2\_Startup()接口输出参数 ..... 12

表 3 TCM2\_Shutdown()接口输入参数 ..... 12

表 4 TCM2\_Shutdown()接口输出参数 ..... 13

表 5 TCM2\_SelfTest()接口输入参数 ..... 13

表 6 TCM2\_SelfTest()接口输出参数 ..... 13

表 7 TCM2\_IncrementalSelfTest()接口输入参数 ..... 14

表 8 TCM2\_IncrementalSelfTest()接口输出参数 ..... 14

表 9 TCM2\_GetTestResult()接口输入参数 ..... 14

表 10 TCM2\_GetTestResult()接口输出参数 ..... 14

表 11 TCM2\_StartAuthSession()接口输入参数 ..... 15

表 12 TCM2\_StartAuthSession()接口输出参数 ..... 16

表 13 TCM2\_PolicyRestart()接口输入参数 ..... 16

表 14 TCM2\_PolicyRestart()接口输出参数 ..... 16

表 15 TCM2\_Create()接口输入参数 ..... 17

表 16 TCM2\_Create()接口输出参数 ..... 17

表 17 TCM2\_Load()接口输入参数 ..... 18

表 18 TCM2\_Load()接口输出参数 ..... 18

表 19 TCM2\_LoadExternal()接口输入参数 ..... 19

表 20 TCM2\_LoadExternal()接口输出参数 ..... 19

表 21 TCM2\_ReadPublic()接口输入参数 ..... 19

表 22 TCM2\_ReadPublic()接口输出参数 ..... 20

表 23 TCM2\_ActivateCredential()接口输入参数 ..... 21

表 24	TCM2_ActivateCredential()接口输出参数	21
表 25	TCM2_MakeCredential()接口输入参数	22
表 26	TCM2_MakeCredential()接口输出参数	22
表 27	TCM2_Unseal()接口输入参数	22
表 28	TCM2_Unseal()接口输出参数	23
表 29	TCM2_ObjectChangeAuth()接口输入参数	23
表 30	TCM2_ObjectChangeAuth()接口输出参数	24
表 31	TCM2_Duplicate()接口输入参数	24
表 32	TCM2_Duplicate()接口输出参数	25
表 33	TCM2_Rewrap()接口输入参数	25
表 34	TCM2_Rewrap()接口输出参数	26
表 35	TCM2_Import()接口输入参数	27
表 36	TCM2_Import()接口输出参数	27
表 37	TCM2_ZGen_2Phase()接口输入参数	28
表 38	TCM2_ZGen_2Phase()接口输出参数	28
表 39	TCM2_ECC_Encrypt()接口输入参数	29
表 40	TCM2_ECC_Encrypt()接口输出参数	29
表 41	TCM2_ECC_Decrypt()接口输入参数	30
表 42	TCM2_ECC_Decrypt()接口输出参数	30
表 43	TCM2_ECDH_ZGen()接口输入参数	31
表 44	TCM2_ECDH_ZGen()接口输出参数	31
表 45	TCM2_ECDH_KeyGen()接口输入参数	31
表 46	TCM2_ECDH_KeyGen()接口输出参数	32
表 47	TCM2_EncryptDecrypt()接口输入参数	32
表 48	TCM2_EncryptDecrypt()接口输出参数	33
表 49	TCM2_GetRandom()接口输入参数	33
表 50	TCM2_GetRandom()接口输出参数	34
表 51	TCM2_StirRandom()接口输入参数	34
表 52	TCM2_StirRandom()接口输出参数	34
表 53	TCM2_Hash()接口输入参数	35
表 54	TCM2_Hash()接口输出参数	35
表 55	TCM2_HMAC()接口输入参数	36
表 56	TCM2_HMAC()接口输出参数	36
表 57	TCM2_HMAC_Start()接口输入参数	36
表 58	TCM2_HMAC_Start()接口输出参数	37
表 59	TCM2_HashSequenceStart()接口输入参数	37
表 60	TCM2_HashSequenceStart()接口输出参数	38

表 61	TCM2_SequenceUpdate()接口输入参数	38
表 62	TCM2_SequenceUpdate()接口输出参数	38
表 63	TCM2_SequenceComplete()接口输入参数	39
表 64	TCM2_SequenceComplete()接口输出参数	39
表 65	TCM2_EventSequenceComplete()接口输入参数	40
表 66	TCM2_EventSequenceComplete()接口输出参数	40
表 67	TCM2_Certify()接口输入参数	41
表 68	TCM2_Certify()接口输出参数	41
表 69	TCM2_CertifyCreation()接口输入参数	42
表 70	TCM2_CertifyCreation()接口输出参数	42
表 71	TCM2_Quote()接口输入参数	43
表 72	TCM2_Quote()接口输出参数	43
表 73	TCM2_GetTime()接口输入参数	44
表 74	TCM2_GetTime()接口输出参数	44
表 75	TCM2_EC_Ephemeral()接口输入参数	45
表 76	TCM2_EC_Ephemeral()接口输出参数	45
表 77	TCM2_Commit()接口输入参数	45
表 78	TCM2_Commit()接口输出参数	46
表 79	TCM2_VerifySignature()接口输入参数	46
表 80	TCM2_VerifySignature()接口输出参数	47
表 81	TCM2_Sign()接口输入参数	47
表 82	TCM2_Sign()接口输出参数	48
表 83	TCM2_PCR_Extend()接口输入参数	48
表 84	TCM2_PCR_Extend()接口输出参数	49
表 85	TCM2_PCR_Read()接口输入参数	49
表 86	TCM2_PCR_Read()接口输出参数	49
表 87	TCM2_PCR_Reset()接口输入参数	50
表 88	TCM2_PCR_Reset()接口输出参数	50
表 89	TCM2_PolicySigned()接口输入参数	51
表 90	TCM2_PolicySigned()接口输出参数	51
表 91	TCM2_PolicySecret()接口输入参数	52
表 92	TCM2_PolicySecret()接口输出参数	52
表 93	TCM2_PolicyTicket()接口输入参数	53
表 94	TCM2_PolicyTicket()接口输出参数	54
表 95	TCM2_PolicyOR()接口输入参数	54
表 96	TCM2_PolicyOR()接口输出参数	55
表 97	TCM2_PolicyPCR()接口输入参数	55



表 98	TCM2_PolicyPCR()接口输出参数	56
表 99	TCM2_PolicyLCommandCode()接口输入参数	56
表 100	TCM2_PolicyLCommandCode()接口输出参数	56
表 101	TCM2_PolicyPhysicalPresence()接口输入参数	57
表 102	TCM2_PolicyPhysicalPresence()接口输出参数	57
表 103	TCM2_PloicyHash()接口输入参数	57
表 104	TCM2_PloicyHash()接口输出参数	58
表 105	TCM2_PolicyAuthValue()接口输入参数	58
表 106	TCM2_PolicyAuthValue()接口输出参数	59
表 107	TCM2_PloicyPassword()接口输入参数	59
表 108	TCM2_PloicyPassword()接口输出参数	59
表 109	TCM2_PloicyGetDigest()接口输入参数	60
表 110	TCM2_PloicyGetDigest()接口输出参数	60
表 111	TCM2_CreatePrimary()接口输入参数	60
表 112	TCM2_CreatePrimary()接口输出参数	61
表 113	TCM2_HierarchyControl()接口输入参数	62
表 114	TCM2_HierarchyControl()接口输出参数	62
表 115	TCM2_SetPrimaryPolicy()接口输入参数	62
表 116	TCM2_SetPrimaryPolicy()接口输出参数	63
表 117	TCM2_Clear()接口输入参数	63
表 118	TCM2_Clear()接口输出参数	64
表 119	TCM2_ClearControl()接口输入参数	64
表 120	TCM2_ClearControl()接口输出参数	65
表 121	TCM2_HierachyChangeAuth()接口输入参数	65
表 122	TCM2_HierachyChangeAuth()接口输出参数	65
表 123	TCM2_DictionaryAttackLockReset()接口输入参数	66
表 124	TCM2_DictionaryAttackLockReset()接口输出参数	66
表 125	TCM2_DictionaryAttackParameters()接口输入参数	66
表 126	TCM2_DictionaryAttackParameters()接口输出参数	67
表 127	TCM2_PP_Commands()接口输入参数	67
表 128	TCM2_PP_Commands()接口输出参数	68
表 129	TCM2_ContextSave()接口输入参数	68
表 130	TCM2_ContextSave()接口输出参数	69
表 131	TCM2_ContextLoad()接口输入参数	69
表 132	TCM2_ContextLoad()接口输出参数	69
表 133	TCM2_FlushContext()接口输入参数	70
表 134	TCM2_FlushContext()接口输出参数	70

表 135	TCM2_EvictControl()接口输入参数	70
表 136	TCM2_EvictControl()接口输出参数	71
表 137	TCM2_GetCapability()接口输入参数	71
表 138	TCM2_GetCapability()接口输出参数	71
表 139	TCM2_TestParms()接口输入参数	72
表 140	TCM2_TestParms()接口输出参数	72
表 141	TCM2_NV_DefineSpace()接口输入参数	73
表 142	TCM2_NV_DefineSpace()接口输出参数	73
表 143	TCM2_UndefineSpace()接口输入参数	73
表 144	TCM2_UndefineSpace()接口输出参数	74
表 145	TCM2_NV_ReadPublic()接口输入参数	74
表 146	TCM2_NV_ReadPublic()接口输出参数	74
表 147	TCM2_NV_Write()接口输入参数	75
表 148	TCM2_NV_Write()接口输出参数	75
表 149	TCM2_NV_Increment()接口输入参数	76
表 150	TCM2_NV_Increment()接口输出参数	76
表 151	TCM2_NV_Extend()接口输入参数	77
表 152	TCM2_NV_Extend()接口输出参数	77
表 153	TCM2_NV_SetBits()接口输入参数	77
表 154	TCM2_NV_SetBits()接口输出参数	78
表 155	TCM2_WriteLock()接口输入参数	78
表 156	TCM2_WriteLock()接口输出参数	79
表 157	TCM2_NV_GlobalWriteLock()接口输入参数	79
表 158	TCM2_NV_GlobalWriteLock()接口输出参数	79
表 159	TCM2_NV_Read()接口输入参数	80
表 160	TCM2_NV_Read()接口输出参数	80
表 161	TCM2_NV_ReadLock()接口输入参数	81
表 162	TCM2_NV_ReadLock()接口输出参数	81
表 163	TCM2_ChangAuth()接口输入参数	82
表 164	TCM2_ChangAuth()接口输出参数	82
表 165	TCM2_Startup()接口输入参数	83
表 166	TCM2_Startup()接口输出参数	83
表 167	TCM2_PCR_Extend()接口输入参数	83
表 168	TCM2_PCR_Extend()接口输出参数	84
表 169	TCM2_PCR_Read()接口输入参数	84
表 170	TCM2_PCR_Read()接口输出参数	84
表 A.1	命令码	86

表 A.2	返回码	90
表 A.3	基本类型定义	95
表 A.4	逻辑数值定义	95
表 A.5	其他类型定义	95
表 A.6	TCM2_SPEC 常量定义	96
表 A.7	TCM2_ALG_ID 表图例	96
表 A.8	TCM2_ALG_ID(UINT16)定义	97
表 A.9	TCM2_ECC_CURVE(UINT16)定义	98
表 A.10	TCM 命令 32 位结构	98
表 A.11	TCM 命令格式字段描述	99
表 A.12	TCM2_ST(UINT16)定义	99
表 A.13	TCM2_Cap 值	100
表 A.14	TCM2_PT 值	101
表 A.15	TCM2_PT_PCR(UINT32)定义	103
表 A.16	句柄定义	105
表 A.17	TCM2_HT(UINT8)常量定义	105
表 A.18	TCM2_RH(TCM2_HANDLE)定义	106
表 A.19	TCM2_HC(TCM2_HANDLE)类型定义	107
表 A.20	TCMI_YES_NO(BYTE)类型定义	108
表 A.21	TCMI_DH_OBJECT 定义	108
表 A.22	TCMI_DH_PARENT 定义	109
表 A.23	TCMI_DH_PERSISTENT 定义	109
表 A.24	TCMI_DH_ENTITY 定义	109
表 A.25	TCMI_DH_PCR 定义	110
表 A.26	TCMI_SH_AUTH_SESSION 定义	110
表 A.27	TCMI_SH_HMAC 定义	110
表 A.28	TCMI_SH_POLICY 定义	111
表 A.29	TCMI_DH_CONTEXT 定义	111
表 A.30	TCMI_RH_HIERARCH 定义	111
表 A.31	TCMI_SH_ENABLES 定义	112
表 A.32	TCMI_HIERARCHY_AUTH 定义	112
表 A.33	TCMI_RH_PLATFORM 定义	112
表 A.34	TCM2_RH_OWNER 定义	113
表 A.35	TCM2_RH_ENDORSEMENT(TCM2_HANDLE)定义	113
表 A.36	TCMI_RH_PROVISION(TCM2_HANDLE)类型定义	113
表 A.37	TCMI_RH_CLEAR(TCM2_HANDLE)定义	113
表 A.38	TCMI_RH_NV_AUTH(TCM2_HANDLE)定义	114

表 A.39	TCMI_RH_LOCKOUT(TCM2_HANDLE)定义	114
表 A.40	TCMI_RH_NV_INDEX(TCM2_HANDLE)定义	114
表 A.41	TCMI_ALG_HASH(TCM2_ALG_ID)定义	114
表 A.42	TCMI_ALG_ASYM (TCM2_ALG_ID)定义	115
表 A.43	TCMI_ALG_SYM (TCM2_ALG_ID)定义	115
表 A.44	TCMI_ALG_SYM_OBJECT(TCM2_ALG_ID)定义	115
表 A.45	TCMI_ALG_SYM_MODE(TCM2_ALG_ID)定义	116
表 A.46	TCMI_ALG_SIG_SCHEME(TCM2_ALG_ID)定义	116
表 A.47	TCMI_ECC_KEY_EXCHANGE(TCM2_ALG_ID)定义	116
表 A.48	TCMI_ST_COMMAND_TAG(TCM2_ST)定义	116
表 A.49	TCMS_ALGORITHM_DESCRIPTION 结构体定义	117
表 A.50	TCMU_HA 结构体定义	117
表 A.51	TCMT_HA 结构体定义	117
表 A.52	TCM2B_DIGEST 结构体定义	118
表 A.53	TCM2B_DATA 结构体定义	118
表 A.54	TCM2B_NONCE 结构体定义	118
表 A.55	TCM2B_AUTH 结构体定义	118
表 A.56	TCM2B_OPERAND 结构体定义	119
表 A.57	TCM2B_EVENT 结构体定义	119
表 A.58	TCM2B_MAX_BUFFER 结构体定义	119
表 A.59	TCM2B_MAX_NV_BUFFER 结构体定义	119
表 A.60	TCM2B_TIMEOUT 结构体定义	120
表 A.61	TCM2B_IV 结构体定义	120
表 A.62	TCMU_NAME 结构体定义	120
表 A.63	TCM2B_NAME 结构体定义	120
表 A.64	TCMS_PCR_SELECT 结构体定义	121
表 A.65	TCMS_PCR_SELECTION 结构体定义	121
表 A.66	Tickets 中 Proof 的值	122
表 A.67	TCMS_TK_CREATION 结构体定义	122
表 A.68	TCMS_TK_VERIFIED 结构体定义	122
表 A.69	TCMS_TK_AUTH 结构体定义	123
表 A.70	TCMS_TK_HASHCHECK 结构体定义	123
表 A.71	TCMS_ALG_PROPERTY 结构体定义	123
表 A.72	TCMS_TAGGED_PROPERTY 结构体定义	124
表 A.73	TCMS_TAGGED_PCR_SELECT 结构体定义	124
表 A.74	TCMS_TAGGED_POLICY 结构体定义	124
表 A.75	TCMA_MODES 结构体定义	124

表 A.76	TCML_CC 结构体定义	125
表 A.77	TCML_CCA 结构体定义	125
表 A.78	TCML_ALG 结构体定义	125
表 A.79	TCML_HANDLE 结构体定义	126
表 A.80	TCML_DIGEST 结构体定义	126
表 A.81	TCML_DIGEST_VALUES 结构体定义	126
表 A.82	TCM2B_DIGEST_VALUES 结构体定义	127
表 A.83	TCML_PCR_SELECTION 结构体定义	127
表 A.84	TCML_ALG_PROPERTY 结构体定义	127
表 A.85	TCML_TAGGED_TCM2_PROPERTY 结构体定义	127
表 A.86	TCML_TAGGED_PCR_PROPERTY 结构体定义	128
表 A.87	TCML_ECC_CURVE 结构体定义	128
表 A.88	TCMU_CAPABILITIES 结构体定义	128
表 A.89	TCMS_CAPABILITY_DATA 结构体定义	129
表 A.90	TCMS_CLOCK_INFO 结构体定义	129
表 A.91	TCMS_TIME_INFO 结构体定义	130
表 A.92	TCMS_TIME_ATTEST_INFO 结构体定义	130
表 A.93	TCMS_CERTIFY_INFO 结构体定义	130
表 A.94	TCMS_QUOTE_INFO 结构体定义	130
表 A.95	TCMS_CREATION_INFO 结构体定义	131
表 A.96	TCMI_ST_ATTEST 结构体定义	131
表 A.97	TCMU_ATTEST 结构体定义	131
表 A.98	TCMS_ATTEST 结构体定义	132
表 A.99	TCM2B_ATTEST 结构体定义	132
表 A.100	TCMS_AUTH_COMMAND 结构体定义	132
表 A.101	TCMS_AUTH_RESPONSE 结构体定义	133
表 A.102	TCMI_! ALG.S_KEY_BITS 类型定义	133
表 A.103	TCMU_SYSM_KEY_BITS 联合体定义	133
表 A.104	TCMU_SYM_MODE 联合体定义	134
表 A.105	TCMT_SYM_DEF_OBJECT 结构体定义	134
表 A.106	TCMU_SYM_DETAILS 联合体定义	134
表 A.107	TCM2B_SYM_KEY 结构体定义	135
表 A.108	TCM2B_DERIVE 结构体定义	135
表 A.109	TCM2B_SENSITIVE_CREATE 结构体定义	135
表 A.110	TCM2B_SENSITIVE_DATA 结构体定义	136
表 A.111	TCM2B_ECC_PARAMETER 结构体定义	136
表 A.112	TCMS_ECC_POINT 结构体定义	136

表 A.113	TCM2B_ECC_POINT 结构体定义	136
表 A.114	TCMU_SIGNATURE 结构体定义	137
表 A.115	TCMT_SIGNATURE 结构体定义	137
表 A.116	TCMU_ENCRYPTED_SECRET 联合体定义	137
表 A.117	TCM2B_ENCRYPTED_SECRET 结构体定义	138
表 A.118	TCMI_ALG_PUBLIC 结构体定义	138
表 A.119	TCMU_PUBLIC_ID 结构体定义	138
表 A.120	TCMS_ASYM_PARMS 结构体定义	139
表 A.121	TCMS_ECC_PARMS 结构体定义	139
表 A.122	TCMU_PUBLIC_PARMS 结构体定义	140
表 A.123	TCMT_PUBLIC 结构体定义	140
表 A.124	TCM2B_PUBLIC 结构体定义	140
表 A.125	TCM2B_TEMPLATE 结构体定义	141
表 A.126	TCMU_SENSITIVE_COMPOSITE 结构体定义	141
表 A.127	TCMT_SENSITIVE 结构体定义	142
表 A.128	TCM2B_SENSITIVE 结构体定义	142
表 A.129	TCM2B_PRIVATE 结构体定义	142
表 A.130	TCMS_ID_OBJECT 结构体定义	143
表 A.131	TCM2B_ID_OBJECT 结构体定义	143
表 A.132	TCM_NV_INDEX 结构体定义	143
表 A.133	TCMA_NV 结构体定义	144
表 A.134	TCMS_NV_PUBLIC 结构体定义	146
表 A.135	TCM2B_NV_PUBLIC 结构体定义	146
表 A.136	TCM2B_CONTEXT_SENSITIVE 结构体定义	147
表 A.137	TCMS_CONTEXT_DATA 结构体定义	147
表 A.138	TCM2B_CONTEXT_DATA 结构体定义	147
表 A.139	TCMS_CONTEXT 结构体定义	147
表 A.140	Context Handle 值	148
表 A.141	TCMT_TK_CREATION 结构体定义	148
表 A.142	TCMT_TK_VERIFIED 结构体定义	149
表 A.143	TCMT_TK_AUTH 结构体定义	149
表 A.144	TCMT_TK_HASHCHECK 结构体定义	149
表 A.145	TCMI_ALG_PUBLIC(TCM2_ALG_ID)类型定义	150
表 A.146	TCMT_PUBLIC 结构体定义	150
表 A.147	TCM2B_PUBLIC 结构体定义	150
表 C.1	层级控制的配置组合	179
表 C.2	标记值	185

表 C.3	授权/会话块的使用 .....	186
表 C.4	sessionAttributes 描述 .....	188
表 C.5	命令的口令授权 .....	190
表 C.6	回应密码确认 .....	190
表 C.7	基于会话的命令授权 .....	191
表 C.8	基于会话的应答 .....	192
表 C.9	XOR 参数 .....	205
表 C.10	KDPa 参数 .....	205
表 C.11	层次结构属性的映射 .....	212
表 C.12	允许的层次结构设置 .....	213
表 C.13	公共区域参数 .....	216
表 C.14	敏感区域参数 .....	216
表 C.15	标准证明结构 .....	226
表 C.16	ORDERLY_DATA 结构的内容 .....	232
表 C.17	STATE_CLEAR_DATA 结构的内容 .....	232
表 C.18	STATE_RESET_DATA 结构的内容 .....	233
表 C.19	PERSISTENT_DATA 结构的内容 .....	233
表 D.1	第 5 章和附录 C 与 ISO/IEC 11889-1:2015 章条编号对照情况 .....	236
表 D.2	第 7 章与 ISO/IEC 11889-3:2015 章条编号对照情况 .....	237
表 D.3	附录 A 与 ISO/IEC 11889-2:2015 章条编号对照情况 .....	238

## 前 言

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。

本文件代替 GB/T 29829—2013《信息安全技术 可信计算密码支撑平台功能与接口规范》，与 GB/T 29829—2013 相比，除结构调整和编辑性改动外，主要技术内容变化如下：

- a) 更改了“术语、定义和缩略语”，且增加和更改了术语和定义的内容（见第 3 章，2013 年版的 3.1）；
- b) 增加了第 4 章“缩略语”且增加和更改了部分内容（见第 4 章，2013 年版的 3.2）；
- c) 更改了“平台体系架构”和“功能原理”的内容，并将其调整为 6.1 和 6.2，对部分内容进行了更改（见 6.1 和 6.2，2013 年版的 4.1 和 4.3）；
- d) 删除了“密码算法要求”的内容（见 2013 年版的 4.2）；
- e) 增加了“可信计算密码支撑平台概述”的内容（见第 5 章）；
- f) 删除了“可信计算密码支撑平台功能服务接口”的内容（2013 年版的第 5 章）；
- g) 增加了“可信密码模块接口”的内容（见第 7 章）；
- h) 增加了关于 SM2 非对称加解密的指令的实现要求（见 7.7）；
- i) 增加了“证实方法”的内容（见第 8 章）；
- j) 更改了附录 A（规范性）“数据结构”（见附录 A）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：联想（北京）有限公司、国民技术股份有限公司、中国科学院软件研究所、北京信息科技大学、中国电子技术标准化研究院、武汉大学、北京大学、北京奇虎科技有限公司、大唐高鸿信安（浙江）信息科技有限公司、中电科技（北京）股份有限公司、神州网信技术有限公司、浪潮电子信息产业股份有限公司、兴唐通信科技有限公司、阿里云计算有限公司、深圳数字电视国家工程实验室股份有限公司、国家计算机网络与信息安全管理中心、公安部第三研究所、国民认证科技（北京）有限公司、北京蚂蚁云金融信息服务有限公司、华为技术有限公司、北京卓识网安技术股份有限公司、同方股份有限公司、山谷网安科技股份有限公司、联想（北京）信息技术有限公司、全球能源互联网研究院有限公司、深圳市腾讯计算机系统有限公司、新华三技术有限公司。

本文件主要起草人：韦卫、李汝鑫、秦宇、刘鑫、宁晓魁、付月朋、柴海新、吴秋新、张屹、王惠莅、张严、孙彦、王鹏、严飞、沈晴霓、张晓磊、郑驰、张佳建、陈小春、孙亮、王强、杨尚欣、吴保锡、白欣璐、王悦、付颖芳、肖鹏、李新国、王晖、陶源、李俊、初晓博、张小虎、张梦良、许东阳、刘韧、刘锋、姚金龙、吴会军、杜克宏、卢卫疆、赵保华、刘大迢、黄超、蒋增增、万晓兰、冯伟、李为、张立强、余发江、赵波、李业旺、秦文杰、罗武。

本文件及其所代替文件的历次版本发布情况为：

——2013 年首次发布为 GB/T 29829—2013；

——本次为第一次修订。



## 引 言

为满足可信计算产业不断发展的新需求。本文件以商用密码算法应用为核心,以可信计算技术应用需求为基础,描述了可信计算密码支撑平台的功能;参考了我国商用密码算法、可信计算技术在 ISO 国际标准中采纳和应用的成果,定义了可信计算密码支撑平台接口形式。本文件符合不同应用场景下可信计算密码支撑平台设计需求,兼容各种硬件平台、宿主机软件系统、应用系统,确保产业界产品的统一性和兼容性,用于指导我国可信计算相关产品开发和应用。

# 信息安全技术 可信计算 密码支撑平台功能与接口规范

## 1 范围

本文件给出可信计算密码支撑平台的体系框架和功能原理,规定了可信密码模块的接口规范,描述了对应的证实方法。

本文件适用于可信计算密码支撑平台相关产品的研制、生产、测评与应用开发。

## 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 20518	信息安全技术	公钥基础设施	数字证书格式
GB/T 25069	信息安全技术	术语	
GB/T 32905	信息安全技术	SM3	密码杂凑算法
GB/T 32907	信息安全技术	SM4	分组密码算法
GB/T 32915	信息安全技术	二元序列随机性检测方法	
GB/T 32918.2	信息安全技术	SM2 椭圆曲线公钥密码算法	第2部分:数字签名算法
GB/T 32918.3	信息安全技术	SM2 椭圆曲线公钥密码算法	第3部分:密钥交换协议
GB/T 32918.4	信息安全技术	SM2 椭圆曲线公钥密码算法	第4部分:公钥加密算法
GB/T 35276	信息安全技术	SM2	密码算法使用规范

## 3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

### 3.1

**存储主密钥** storage master key

用于保护操作系统密钥和用户密钥的主密钥。

### 3.2

**可信计算平台** trusted computing platform

构建在计算系统中,用于实现可信计算功能的支撑系统。

### 3.3

**可信计算密码支撑平台** cryptographic support platform for trusted computing

可信计算平台的重要组成部分,包括密码算法、密钥管理、证书管理、密码协议、密码服务等内容,为可信计算平台自身的完整性、身份真实性和数据保密性提供密码支持。