



炼石
CipherGateway

2021 密码应用技术白皮书

北京炼石网络技术有限公司

V1.0.4

北京炼石网络技术有限公司对密码应用技术白皮书(以下简称本技术报告或本白皮书)的内容及相关产品信息拥有受法律保护的著作权, 未经授权许可, 任何人不得将报告的全部或部分内容以转让、出售等方式用于商业目的使用。转载、摘编使用本报告文字或者观点的应注明来源。报告中所载的材料和信息, 包括但不限于文本、图片、数据、观点、建议等各种形式, 不能替代律师出具的法律意见。违反上述声明者, 本公司将追究其相关法律责任。报告撰写过程中, 为便于技术说明和涵义解释, 引用了一系列的参考文献, 内容如有侵权, 请联系本公司修改或删除。

北京炼石网络技术有限公司

联系电话: 4008190181

邮箱: support@ciphergateway.com

前言

2022年1月，国务院印发《“十四五”数字经济发展规划》（以下简称“规划”），明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。规划指出，数字经济是继农业经济、工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。

业务伴生风险。数据要素是数字经济深化发展的核心引擎，数据对提高生产效率的乘数作用不断凸显，成为最具时代特征的生产要素，数据的爆发增长、海量集聚蕴藏了巨大价值，数据的开发利用为经济社会发展提供了强大动力。安全是发展的前提，传统业务需求侧重于“希望发生什么”，而安全需求侧重于“不希望发生什么”，从而“确保发生什么”。因此，凡是有数据开发利用的场景，总会伴生着数据安全风险，都会产生数据安全需求。

风险驱动密码。数字时代呼唤安全创新，密码是国之重器，是数字技术发展的安全基因，是保障网络与数据安全的核心技术，也是推动我国数字经济高质量发展、构建网络强国的基础支撑。从实战需求看，日趋严峻的网络与数据安全威胁使得数字经济迫切需要密码技术这个“压舱石”，以有效抵御外部黑客攻击、防止内部人员泄露。从合规需求看，以密码应用安全性评估为抓手落实《密码法》，并结合《网络安全法》《数据安全法》《个人信息保护法》等法律法规，也在持

续拉动密码应用新需求。实战与合规叠加的需求成为安全产业发展的关键动力，推动新密码市场加速形成。

密码融入业务。密码作为直接作用于数据的安全技术，只有融入数据处理流程才能有效防范业务风险。从技术路线上，传统“外挂式”密码产品采用开发改造应用的模式门槛高、周期长、风险大，用户面临“难用、难管”等挑战。“面向切面安全”等新模式提出“内嵌式”密码技术创新，将安全与业务在技术上解耦、但又在能力上融合交织，提供轻量级改造应用的实施模式，有效防护企业应用与数据，让密码“好用、好管”。

本白皮书以“用密”为主线展开介绍密码技术、产品、服务、集成、合规等密码相关知识，希望为需求和供给两侧从业者提供密码应用参考手册。作为重点部分，从业务视角归纳了 20 种密码应用模式，尝试在保密性、完整性、真实性、不可否认性等的基础上，从数据开发利用场景提炼更直观的密码使用方案。进一步的，对全面开展中的密评工作，梳理了典型的密评改造技术方案，为密评工作者提供参考。

由于编者水平有限，时间仓促，白皮书中不妥和错漏之处在所难免，敬请各位读者批评指正和提出宝贵意见。在此也欢迎业界专家和同仁拨冗参与本白皮书下一版本改进完善，共同为密码技术应用推广贡献力量！

本白皮书编写过程中获得了腾讯云鼎实验室等众多专家和机构的指导与帮助，在此特别致谢。

目录

声 明	1
前 言	3
1. 数字经济伴生安全风险	15
1.1. 数字经济定位为主要经济形态	15
1.2. 数据资源已成为关键生产要素	15
1.3. 数据处理伴生着安全威胁风险	17
1.3.1. 数据收集风险	17
1.3.2. 数据存储风险	20
1.3.3. 数据使用风险	24
1.3.4. 数据加工风险	27
1.3.5. 数据传输风险	28
1.3.6. 数据提供风险	29
1.3.7. 数据公开风险	32
2. 密码产业护航数字经济	34
2.1. 数字经济呼唤创新密码应用	34
2.1.1. 密码技术是数字安全压舱石	34
2.1.2. 实战合规是密码建设指南针	36
2.1.3. 密码创新是数字安全领头雁	38
2.2. 密码产业进入黄金发展时代	40
2.2.1. 顶层战略引导数字经济安全建设	41
2.2.2. 国家法律加速密码应用推广普及	45
2.2.3. 行业地区出台密码技术应用要求	51
2.3. 密码技术筑牢数字安全屏障	81
2.3.1. 密码技术进步促进应用融合	81
2.3.2. 信息技术升级促进产品演进	82
2.3.3. 攻防演练对抗促进实战发展	83
2.3.4. 数据要素市场促进密码创新	83
2.4. 业务视角归纳密码应用模式	85
(一) 身份鉴别及密钥管理	87
2.4.1. PKI 信任体系	87

2.4.2. IBC 信任体系.....	92
2.4.3. 预共享密钥的身份鉴别.....	95
2.4.4. 基于数字签名的身份鉴别.....	98
(二) 数据传输 (通信安全)	105
2.4.5. 离线通信消息加密.....	105
2.4.6. 代理重加密受控分发消息.....	108
2.4.7. 在线通信消息加密.....	111
2.4.8. 可感知窃听的专线通信.....	118
(三) 数据存储 (数据资产安全)	121
2.4.9. 应用内数据加密.....	121
2.4.10. 数据库存储加密.....	126
2.4.11. 文件存储加密.....	132
(四) 数据使用 (数据共享与安全兼得)	135
2.4.12. 基于差分隐私的数据匿名化.....	135
2.4.13. 基于属性加密的访问控制.....	138
2.4.14. 锚点解密的防绕过数据安全.....	143
2.4.15. 不可信环境中的数据运算.....	146
2.4.16. 可验证结果的计算外包.....	157
2.4.17. 封装业务逻辑的可信运算环境.....	160
2.4.18. 基于密码的数字水印追溯.....	164
2.4.19. 基于密码校验的防篡改.....	170
2.4.20. 基于私钥签名的责任认定.....	175
3. 密码技术集聚创新原力.....	179
3.1. 基础算力类.....	179
3.1.1. 密码卡.....	179
3.1.2. 密码套件.....	182
3.1.3. 智能密码钥匙.....	185
3.1.4. 服务器密码机.....	188
3.1.5. 签名验签服务器.....	191
3.2. 应用场景类.....	194
3.2.1. 数字证书认证系统.....	194
3.2.2. CASB 数据加密平台.....	197
3.2.3. 金融数据密码机.....	201

3.2.4. VPN 虚拟专用网络.....	202
3.2.5. 电子签章系统.....	204
3.2.6. 身份鉴别系统.....	206
3.3. 管理支撑类.....	209
3.3.1. 密钥管理系统.....	209
4. 密码能力融入业务流程.....	216
4.1. 数据安全本质是对数据重建访问规则.....	216
4.2. 安全技术从基础设施演进到业务应用.....	219
4.3. 密码安全融合打造面向业务实战防护.....	220
5. 密评合规重构安全防护.....	225
5.1. 密码应用典型性问题分析.....	225
5.1.1. 密码应用不广泛.....	225
5.1.2. 密码应用不规范.....	226
5.1.3. 密码应用不安全.....	226
5.2. 密评为密码合规提供基线.....	227
5.2.1. 密评发展历程.....	227
5.2.2. 密评开展依据.....	229
5.2.3. 密评适用对象.....	231
5.2.4. 密评政策法规.....	235
5.2.5. 密评遵循标准.....	242
5.2.6. 密评核心内容.....	257
5.2.7. 密评等保关系.....	258
5.2.8. 密评机构名单.....	261
5.3. 密码应用安全性评估标准.....	265
5.3.1. 密评测评要求.....	265
5.3.2. 密评测评过程.....	278
5.3.3. 密评高风险项.....	287
5.3.4. 密评评分规则.....	297
5.3.5. 密评测评结论.....	308
5.4. 密评改造专业化技术方案.....	309
5.4.1. 密改总体框架.....	309
5.4.2. 密改技术方案.....	311
5.4.3. 密钥管理方案.....	333

5.4.4. 安全管理方案.....	342
5.4.5. 安全合规分析.....	354
5.4.6. 密改方案效果.....	357
5.4.7. 密改设备清单.....	360
6. 附录.....	363
6.1. 密码基本知识.....	363
6.1.1. 密码算法.....	363
6.1.2. 密码协议.....	385
6.1.3. 密码认证.....	389
6.1.4. 密钥管理.....	400
6.1.5. 密码价值.....	408
6.2. 密码相关标准.....	414
6.2.1. 国家标准.....	414
6.2.2. 行业标准.....	447
参考文献.....	456
作者介绍.....	461

图目录

图 1	企业信息化技术演进示意图.....	39
图 2	政务信息系统密码应用与安全性评估实施过程示意图.....	63
图 3	密码产业组成示意图.....	85
图 4	信任体系威胁示意图.....	87
图 5	信任体系 PKI 防护模型示意图.....	88
图 6	用户申请证书过程示意图.....	90
图 7	用户使用证书过程示意图.....	91
图 8	信任体系 IBC 防护模型示意图.....	92
图 9	基于 IBC 的安全邮件示意图.....	94
图 10	身份认证威胁示意图.....	95
图 11	预共享密钥防护模型示意图.....	96
图 12	Windows 中基于 L2TP/IPSec 的 VPN.....	97
图 13	基于单一设备签名的身份鉴别威胁示意图.....	98
图 14	基于单一设备签名的身份鉴别防护模型示意图.....	99
图 15	银行 U 盾使用过程示意图.....	100
图 16	基于协同签名的身份鉴别威胁示意图.....	102
图 17	基于协同签名的身份鉴别防护模型示意图.....	103
图 18	手机盾认证系统架构示意图.....	104
图 19	离线通信威胁示意图.....	105
图 20	离线通信防护模型示意图.....	106
图 21	PGP 邮件加密发送示意图.....	107
图 22	PGP 邮件接收解密示意图.....	107
图 23	代理重加密威胁示意图.....	108
图 24	代理重加密防护模型示意图.....	109
图 25	云上密文共享示意图.....	110
图 26	在线通信攻击模型.....	111
图 27	在线通信防护模型.....	112
图 28	HTTPS 传输加密示意图.....	114
图 29	两类常见 VPN 产品.....	115
图 30	同步链路密码机应用模式.....	117
图 31	通信传输攻击模型.....	118

图 32	通信传输防护模型.....	118
图 33	基于 BB84 协议的量子密钥分发.....	120
图 34	明文数据在各个阶段都面临被窃取的风险.....	122
图 35	使用密码技术防止应用内威胁.....	123
图 36	应用内加密（集成密码 SDK）技术原理.....	124
图 37	CASB 代理网关技术原理.....	124
图 38	应用内加密（AOE 面向切面加密）技术原理.....	125
图 39	存储的数据面临被窃取的威胁.....	127
图 40	使用密码技术保护存储的数据.....	127
图 41	数据库外挂加密技术原理.....	129
图 42	透明数据加密技术原理.....	130
图 43	数据库加密网关技术原理.....	131
图 44	透明文件加密技术原理.....	133
图 45	FDE 磁盘加密系统组成.....	134
图 46	基于隐私的数据匿名化示意图.....	138
图 47	隐私数据泄露威胁.....	139
图 48	细粒度访问控制防护模型.....	140
图 49	ABAC 机制框架示意图.....	142
图 50	ABE 机制框架示意图.....	143
图 51	数据访问控制机制被绕过.....	144
图 52	基于密码控审一体化的防绕过机制.....	144
图 53	密码控审一体化.....	146
图 54	不可信服务端对明文进行计算示意图.....	146
图 55	不可信服务端环境运算示意图.....	147
图 56	全同态加密的一般性应用框架.....	149
图 57	基于全同态的数据检索过程.....	151
图 58	传统数字水印与基于全同态加密的数字水印的区别.....	153
图 59	外包计算威胁.....	157
图 60	可验证外包计算流程.....	158
图 61	外包计算模型.....	159
图 62	应用运行环境存在风险.....	160
图 63	TPM 硬件构成.....	161
图 64	TEE 系统架构.....	162

图 65	数据违规外发.....	165
图 66	基于时间戳实现可追溯数字水印.....	166
图 67	数字水印处理系统基本框架.....	166
图 68	数字水印嵌入模型.....	167
图 69	数字水印恢复模型.....	168
图 70	电子签章系统的组织架构.....	170
图 71	数据获取过程中存在被篡改威胁.....	170
图 72	基于密码校验的防篡改.....	171
图 73	文件完整性验证过程.....	174
图 74	否认导致责任难认定.....	175
图 75	基于私钥签名责任认定防护模型.....	176
图 76	数字签名方案的基本组成.....	177
图 77	PCI-E 密码卡.....	179
图 78	智能密码钥匙应用逻辑结构图.....	186
图 79	典型的服务器密码机软/硬件架构.....	188
图 80	服务器密码机密钥体系结构.....	189
图 81	数字证书认证系统的逻辑结构图.....	194
图 82	数字证书认证系统在电子商务中的应用.....	195
图 83	数据动态脱敏.....	200
图 84	电子签章系统在电子公文领域的应用.....	205
图 85	身份鉴别系统密码应用部署图.....	208
图 86	密钥管理系统密码应用部署图.....	211
图 87	密钥管理系统的密码应用工作流程.....	214
图 88	网络/主机和数据分别是两个正交的维度.....	217
图 89	网络与数据并重的新安全建设体系.....	218
图 90	数据安全从以基础设施为抓手，演进到以应用为抓手.....	219
图 91	数据安全密码防护体系.....	221
图 92	CASB 的三种交付模式部署对比.....	223
图 93	GM/T 0054 标准基本要求架构图.....	243
图 94	GB/T 39786 标准基本要求架构图.....	245
图 95	等保和密评评估对象以及关基三者之间的关系.....	259
图 96	测评实施过程.....	278
图 97	测评准备活动的工作流程.....	280

图 98	方案编制活动的工作流程.....	281
图 99	现场测评活动的工作流程.....	283
图 100	分析和报告编制活动的工作流程.....	285
图 101	国标 GB/T39786 密码应用基本要求.....	310
图 102	国密改造整体密码应用技术框架.....	311
图 103	物理和环境改造图.....	316
图 104	网络和通信改造图.....	319
图 105	设备和计算改造图.....	324
图 106	应用和安全改造图.....	331
图 107	三层密钥体系图.....	341
图 108	方案效果图.....	357
图 109	对称密码加密和解密基本流程.....	363
图 110	序列密码和分组密码的加密流程.....	364
图 111	ECB 模式的加密和解密流程.....	365
图 112	CBC 模式的加密和解密流程.....	367
图 113	CTR 模式的加密和解密流程.....	368
图 114	GCM 模式的加密流程.....	369
图 115	ZUC 算法结构.....	370
图 116	迭代加密算法的基本结构.....	372
图 117	SM4 算法结构图.....	373
图 118	M-D 结构.....	382
图 119	经典 Diffie-Hellman 密钥交换协议.....	386
图 120	单向散列函数.....	389
图 121	使用单向散列函数检测软件是否被篡改.....	390
图 122	消息认证码.....	394
图 123	基于 MAC 的消息完整性保护过程.....	409
图 124	基于数字签名的消息完整性保护流程.....	410
图 125	基于密码的鉴别方案的基本框架.....	411

表目录

表 1	企业需遵循的密码相关法律法规.....	36
表 2	2016-2020 年商用密码产业总体规模及同比增长率.....	41
表 3	定级要素与安全保护等级的关系.....	60
表 4	20 种密码应用实战模式汇总.....	85
表 5	不同类型的密码机所要遵循的技术和检测规范.....	201
表 6	密钥管理系统对称密钥列表.....	212
表 7	密钥管理系统非对称密钥列表.....	213
表 8	CASB 的三种交付模式技术对比.....	223
表 9	等级测评和密评的主要参考标准和评估内容.....	260
表 10	商用密码应用安全性评估试点机构目录.....	262
表 11	物理和环境密评测评要求.....	267
表 12	网络和通信密评测评要求.....	267
表 13	设备和计算密评测评要求.....	268
表 14	应用和数据密评测评要求.....	269
表 15	信息系统等级保护 1 级到 4 级的密码要求强度.....	275
表 16	测评实施流程的各环节.....	279
表 17	密码算法、密码技术、密码产品和服务的高风险项.....	288
表 18	物理和环境安全的高风险项.....	290
表 19	网络和通信安全的高风险项.....	290
表 20	设备和计算安全的高风险项.....	292
表 21	应用和数据安全的高风险项.....	294
表 22	密码应用管理要求的高风险项.....	296
表 23	测评对象评分量化规则.....	297
表 24	测评单元的权重.....	300
表 25	安全层面相应的权重.....	303
表 26	身份鉴别单元测评对象得分情况.....	306
表 27	物理和环境测评单元得分情况.....	306
表 28	各安全层面得分.....	307
表 29	物理和环境安全风险.....	312

表 30	物理和环境应用测评指标.....	313
表 31	网络和通讯安全风险.....	317
表 32	设备和计算安全风险.....	321
表 33	设备和计算测评指标.....	323
表 34	应用和数据安全风险.....	326
表 35	应用和数据测评指标.....	328
表 36	密钥管理机制.....	336
表 37	IPsec/SSL VPN 安全网关密钥管理机制.....	337
表 38	堡垒机设备密钥管理机制.....	337
表 39	业务系统密钥管理机制.....	338
表 40	工作密钥管理机制.....	339
表 41	密码应用合规对照表.....	354
表 42	密改软硬件设备建设清单.....	360
表 43	AES 基本特性.....	374
表 44	6 种版本的 SHA-2.....	392

1. 数字经济伴生安全风险

1.1. 数字经济定位为主要经济形态

2022年1月12日，国务院印发的《“十四五”数字经济发展规划》中明确指出：数字经济是继农业经济、工业经济之后的主要经济形态，是以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。^[1]

数据作为一种新型生产要素较早被写入到国家顶层规划中，体现了互联网大数据时代的新特征。当前数字经济正在引领新经济发展，数字经济覆盖面广且渗透力强，与各行业融合发展，并在社会治理中如城市交通、老年服务、城市安全等方面发挥重要作用。而数据作为基础性资源和战略性资源，是数字经济高速发展的基石，也将成为“新基建”最重要的生产资料。数据要素的高效配置，是推动数字经济发展的关键一环。加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护，使大数据成为推动经济高质量发展的新动能，对全面释放数字红利、构建以数据为关键要素的数字经济具有战略意义。

1.2. 数据资源已成为关键生产要素

在数据时代，以大数据为代表的信息资源向生产要素形态演进，数据已同其他要素一起融入经济价值创造过程。与其他资源要素相比，数据资源要素具有如

下特征：一是数据体量巨大。且历史数据量不断累积增加，通过流转和共享对社会发展产生重要价值，基于数据创新的商业模式或应用不断演进。二是数据类型复杂。不仅包含各种复杂的结构化数据，而且图片、指纹、声纹等非结构化数据日益增多；三是数据处理快，时效性要求高。通过算法对数据的逻辑处理速度非常快，区别于传统数据挖掘，大数据处理技术遵循“一秒定律”，可以从各种类型的数据中快速获得高价值的信息。四是数据价值密度低。数据价值的高度与精确性、信噪比有关，在海量数据面前有价值的数据所占比例很小。在获取高价值数据的过程中，往往需要借助数据挖掘等方法深度分析海量数据，从中提取出对未来趋势与模式预测分析有价值的数据。

基于以上四个特性分析，数据在参与经济建设、社会治理、生活服务时，具有重要意义。一是数据作为一种生产性投入方式，可以大大提高生产效率，是新时期我国经济增长的重要源泉之一。二是推动数据发展和应用，可以鼓励产业创新发展，推动数据与科研创新的有机结合，推进基础研究和核心技术攻关，形成数据产业体系，完善数据产业链，使得大数据更好地服务国家发展战略。三是数据安全是数据应用的基础。保护个人隐私、企业商业秘密、国家秘密等。在加强安全管理的同时，又鼓励合规应用，促进创新和数字经济发展，实现公共利益最大化。从合规要求看，数据安全成为国家顶层设计，相关法律政策明确提出加强网络安全、数据安全和个人信息保护，数据安全产业迎来前所未有的历史发展机遇。最终用户对于主动化、自动化、智能化、服务化、实战化的安全需求进一步提升，在此需求推动下，数据安全市场未来五年将继续维持高增速发展。根据赛迪咨询数据测算，2021 年我国数据安全市场规模为 69.7 亿元，预测在 2023 年我国数据安全市场规模将达到 127 亿元。从实战需求看，日趋严峻的网络安全威胁

让企业面临业务风险，数字产业化迫切需要数据安全能力，而产业数字化转型带来数据安全新需求。当前，我国数据安全产业处于起步期，相比于西方发达国家，我国尚有很大增长潜力，这既是短板也是市场机会。随着实战化和新合规的要求逐步深入，数据安全将迎来广阔的市场空间。

1.3. 数据处理伴生着安全威胁风险

数据这种新型生产要素，是实现业务价值的主要载体，数据处理必然要求数据在应用系统中流动，而流动的数据必然伴随风险。可以说，数据安全威胁时刻伴随业务生产。结合到企业或机构的信息系统中，数据安全则来自于业务处理中的风险映射。从时间维度看，数据在流转的全生命周期中的各个环节都会有相应的安全需求。从空间维度看，数据在基础设施层、平台层以及应用层之间流转，不同层次会有不同颗粒度的防护需求。《数据安全法》提出“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等”，为数据生命周期的各环节提供了明确定义，数据在各环节均面临诸多泄露威胁与安全挑战。

1.3.1. 数据收集风险

在数据收集环节，风险威胁涵盖保密性威胁、完整性威胁等，以及超范围采集用户信息等。保密性威胁指攻击者通过建立隐蔽隧道，对信息流向、流量、通信频度和长度等参数的分析，窃取敏感的、有价值的信息；完整性威胁指数据伪造、刻意篡改、数据与元数据的错位、源数据存在破坏完整性的恶意代码。

(1)国内

1) 某程集团因涉嫌违规采集个人信息被诉至法院

司法机关：浙江省绍兴市柯桥区人民法院

案例描述：2021 年 7 月，浙江省绍兴市柯桥区人民法院开庭审理了胡某诉上海某程集团侵权纠纷案件。胡某以上海某程集团采集其个人非必要信息，进行“大数据杀熟”等为由诉至法院，要求某程集团 APP 为其增加不同意“服务协议”和“隐私政策”时仍可继续使用的选项。法院审理后认为，某程集团的“服务协议”和“隐私政策”以拒绝提供服务形成对用户的强制。其中，“服务协议”和“隐私政策”要求用户特别授权某程集团及其关联公司、业务合作伙伴共享用户的注册信息、交易、支付数据并允许某程集团及其关联公司、业务合作伙伴对其信息进行数据分析等内容属于非必要信息的采集和使用，无限加重了用户个人信息使用风险。据此，法院判决某程集团应为原告增加不同意其现有“服务协议”和“隐私政策”仍可继续使用的选项，或者为原告修订“服务协议”和“隐私政策”，去除对用户非必要信息采集和使用的相关内容，修订版本须经法院审定同意。^[2]

2) 北京某借网络贩卖个人信息被罚

执法机构：江苏省仪征市人民法院

法律依据：《中华人民共和国刑法》第二百五十三条之一第一、四款，第二十五条第一款，第二十六条第一、四款，第二十七条，第六十七条第一、三款，第四十五条，第七十二条第一、三款，第七十三条第二、三款，第五十二条，第五十三条第一款，第六十四条和《中华人民共和国刑事诉讼法》第十五条

案例描述：2016 年，贤某成立北京某借网络科技有限公司（简称“某借网络”），并担任法定代表人，从事贷款超市等业务。2018 年 1 月至 2019 年 7 月间，贤某

与公司技术部负责人赵某等人共同商议孵化“一键贷”项目。在明知公司没有贷款资质的情况下，贤某及相关负责人仍开发“一键贷”贷款申请页面投放网络，诱骗他人申请注册，收集个人信息，在未取得受害人同意的情况下，向下游多家不特定信息服务公司出售包含姓名、身份证号、手机号等个人信息，非法盈利共计 316.96 余万元。买方涉及多家知名公司，如某普惠、某拍贷、某我贷等。最终法院判决某借网络犯侵犯公民个人信息罪，并处罚金 320 万元。主犯贤某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金 30 万元。^{[3][4]}

(2) 国外

1) ZOOM 因涉嫌非法泄漏个人数据而被起诉

法律依据：《加州消费者隐私法》

案例描述：根据 2020 年 4 月在加利福尼亚州圣何塞市联邦法院提起的诉讼，用户安装或打开 Zoom 应用程序时收集信息，并在没有适当通知的情况下将其分享给包括 Facebook 在内的第三方。Zoom 的隐私权政策并未向用户说明其应用程序包含向 Facebook 和潜在的其他第三方披露信息的代码。投诉称，该公司的“程序设计和安全措施完全不足，并将继续导致未经授权而泄露其用户个人信息”。根据《加州消费者隐私法》规定，任何消费者如其在第 1798.81.5 节（d）条（1）款（A）项下所定义的未加密和未经处理的个人信息，由于企业违反义务而未实施和维护合理安全程序以及采取与信息性质相符的做法来保护个人信息，从而遭受了未经授权的访问和泄露、盗窃或披露，则消费者可提起民事诉讼并请求。为每个消费者每次事件赔偿不少于一百美元（100 美元）且不超过七百五十美元（750 美元）的损害赔偿金或实际损害赔偿金，以数额较大者为准。

1.3.2. 数据存储风险

在数据存储环节，风险威胁来自外部因素、内部因素、数据库系统安全等。

外部因素包括黑客脱库、数据库后门、挖矿木马、数据库勒索、恶意篡改等，内部因素包括内部人员窃取、不同利益方对数据的超权限使用、弱口令配置、离线暴力破解、错误配置等；数据库系统安全包括数据库软件漏洞和应用程序逻辑漏洞，如：SQL 注入、提权、缓冲区溢出；存储设备丢失等其他情况。

(1)国内

1) 某东电商平台确认 12G 用户数据泄漏

案例描述：2016 年 2 月，国内媒体一本财经报道称一个超过 12G 的数据包正在黑市流通，数据包信息包括用户名、密码、真实姓名、身份证号、电话号码、QQ 号、邮箱等多类个人用户信息。这个数据包已在黑市上明码交易，价格在 10 万-70 万不等，黑市买卖双方表示该数据包来源为某电商平台。某东电商平台表示，黑客利用了 Struts 2 的漏洞对某电商平台数据库进行了拖库。^[5]

2) 济南 20 万孩童信息以每条一两毛被打包出售

案例描述：2016 年，济南 20 万名孩童信息被打包出售，每条信息价格一两毛。泄漏信息包括孩子的姓名、年龄、性别、父亲姓名以及父母联系电话、家庭住址（全部精确到户）等。济南警方侦破案件，系黑客入侵免疫规划系统网络，4 名嫌犯被抓获。^[6]

3) 某论坛 2300 万用户信息泄露

案例描述：2015 年 1 月，名为“蓝猫超人”的白帽子向“漏洞盒子”提供编号为“vulbox-2015-01928”的漏洞数据验证，直指某论坛的 2300 万用户的信息遭到泄露，包含用户名、邮箱、加密密码等。论坛称这些被指泄露的数据属于 2013 年泄露的老数据，同时建议用户升级密码。“蓝猫超人”表示，虽然无法确认用户数据由该论坛直接泄露，但验证过程表明数据属实。某论坛掌握众多用户个人信息和敏感个人信息，应采取相关技术保护个人信息安全，防止用户信息泄漏。^[7]

4) 乌云漏洞报告某易用户数据库疑似泄露（亿级）

执法机构：北京市第一中级人民法院

法律依据：《网络安全法》第 42 条

案例描述：2015 年 10 月，国内安全网络反馈平台 WooYun(乌云)发布消息称，某易的用户数据库疑似泄露，影响数量共计数亿条，泄露信息包括用户名、MD5 密码、密码提示问题/答案(hash)、注册 IP、生日等。某易邮箱过亿数据泄漏(涉及邮箱账号/密码/用户密保等)。根据《网络安全法》第 42 条相关规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。某易产品收集大量用户信息和重要数据，应该采取相关措施保护数据安全，防止数据泄露事件发生。^[8]

5) 某物流公司 10 亿条用户信息数据被出售

案例描述：2019 年，暗网一位 ID “f666666” 的用户开始兜售某物流公司 10 亿条快递数据，该用户表示售卖的数据为 2014 年下旬的数据，包括寄（收）件人姓名、电话、地址等信息，10 亿条数据已经过去重处理，数据重复率低于 20%，数据被该用户以 1 比特币打包出售。^[9]

(2) 国外

1) Facebook 证实 4.19 亿用户的电话信息被泄露

案例描述：2019 年 9 月 Facebook 证实，存储了超 4 亿条与 Facebook 账户关联的电话号码数据库被曝光，每条记录都包含一个用户的 Facebook ID 和连接到他们账户的电话号码。同样，2018 年 3 月“剑桥分析丑闻”首次被曝光——Facebook 8700 万用户数据泄露，一家名为剑桥分析的公司通过这些数据影响了美国选举。最终，美国联邦贸易委员会（FTC）宣布与 Facebook 就该事件达成一项 50 亿美元的和解协议。

2) 微软泄露 2.5 亿条客户支持记录和 PII（个人验证信息）

案例描述：2020 年 1 月，微软意外地在网上曝光了 2.5 亿条客户服务和支持记录。泄漏的数据包含客户电子邮件地址，IP 地址，地点，CSS 声明和案例的描述，案例编号，解决方案和备注等。微软确认此数据泄漏，并揭示此问题是由微软内部案例分析数据库的配置错误而导致。

3) 5700 万名优步司机信息遭泄露

执法机构：美国伊利诺伊州司法部

法律依据：《国家消费者保护法》

案例描述：据环球网科技综合 2018 年 9 月报道，美国科技公司优步 2016 年泄漏约 5700 万名乘客与司机个人资料，在长达一年的时间里，优步未能通知司机该平台遭受黑客袭击导致司机们个人信息被泄漏一事，而且隐瞒盗窃证据，并向黑客支付赎金以确保数据不会被滥用。美国 50 州及华盛顿特区官员向该公司提起集体诉讼，之后优步与各州达成和解协议。2018 年 9 月优步宣布：将支付 1.48 亿美元罚金，并承诺加强数据安全。和解要求优步遵守维护个人信息的国家消费者保护法，并在发生信息泄漏情况下立即通知相关部门，保护第三方平台用户数据，并制定强有力的密码保护政策。优步还将聘请一家外部公司对优步的数据安全进行评估，并按照其建议进一步加固数据安全。

4) 美国第二大医疗保险公司 Anthem 泄露 8000 万个人信息

法律依据：《国家消费者保护法》

案例描述：人民网旧金山 2015 年 2 月 5 日报道，美国第二大医疗保险公司 Anthem (安塞姆) 2 月 5 日向客户发邮件称，公司数据库遭黑客入侵，包括姓名、出生日期、社会安全号、家庭地址以及受雇公司信息等 8000 名用户个人信息受到影响。这已经不是 Anthem 第一次遭遇黑客攻击。另据 Threatpost 网站 2017 年 8 月 1 日报道，2017 年 7 月，Anthem 就此次信息泄露事件达成了 1.15 亿美元的和解。

5) 雅虎曝史上最大规模信息泄露 5 亿用户资料被窃

案例描述：2016 年 9 月，美国互联网公司雅虎证实，至少 5 亿用户的账户信息在 2014 年遭黑客盗取，创造了史上最大单一网站信息遭窃的纪录，泄漏信

息包括：受影响用户的姓名、邮箱地址、电话号码、出生日期、密码以及部分取回密码时的安全问题。受事件影响，雅虎股票午盘下跌 0.3%至 44.02 美元，Verizon 股价反而上升 1%至 52.39 美元。

6) 英国电信运营商 CarphoneWarehouse 240 万用户个人信息泄露

法律依据：《数据保护法案》

案例描述：据《华尔街日报》杂志版 2015 年 8 月报道，英国电信运营商 Carphone Warehouse 表示，在近来备受外界关注的黑客入侵事件中，约有 240 万在线用户的个人信息遭到黑客入侵，包含姓名、地址、出生日期和加密的信用卡数据。根据《数据保护法案》规定：处理过程中应确保个人数据的安全采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失（“数据的完整性与保密性”）。控制者有责任遵守以上第 1 段，并且有责任对此提供证明。（“可问责性”）违反相关规定，英国信息专员办公室有权对违反该项数据法的公司施以高达 1700 万英镑(约合人民币 1.49 亿元)的罚款，或者征收该公司 4%的全球营业额。

1.3.3. 数据使用风险

在数据使用环节，风险威胁来自于外部因素、内部因素、系统安全等。外部因素包括账户劫持、APT 攻击、身份伪装、认证失效、密钥丢失、漏洞攻击、木马注入等；内部因素包括内部人员、DBA 违规操作窃取、滥用、泄露数据等，如：非授权访问敏感数据、非工作时间、工作场所访问核心业务表、高危指令操作；系统安全包括不严格的权限访问、多源异构数据集成中隐私泄露等。

(1)国内

1) 湖南某银行 257 万条公民银行个人信息被泄露

执法机构：绵阳市公安局网络安全保卫支队

法律依据：《刑法》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

案例描述：湖南某银行支行行长，出售自己的查询账号给中间商，再由中间商将账号卖给有银行关系的“出单渠道”团伙，再由另外一家银行的员工进入内网系统，大肆窃取个人信息，泄漏的个人信息包括征信报告、账户明细、余额等。2016 年 10 月，绵阳警方破获公安部挂牌督办的“5·26 侵犯公民个人信息案”，抓获包括银行管理层在内的犯罪团伙骨干分子 15 人、查获公民银行个人信息 257 万条、涉案资金 230 万元。根据最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》中规定，未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法规定的“提供公民个人信息”；第四条规定，违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法规定的“以其他方法非法获取公民个人信息”。根据《刑法》的相关规定：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。^[10]

(2) 国外

1) 伟易达被曝 480 万家长及儿童信息泄露来源

法律依据：《美国儿童网络隐私保护法 COPPA》

案例描述：2015 年，全球最大的婴幼儿及学前电子学习产品企业伟易达，被曝出其存在安全漏洞，致使数百万家长 and 儿童的数据曝光，包括家长注册账号使用的姓名、住址、邮件、密码等。2018 年，美国联邦贸易委员会(FTC)宣布对伟易达(VTech)2015 年因安全漏洞导致数百万家长及孩子的数据泄露事件进行处罚，宣布处以 65 万美元的罚款。《美国儿童网络隐私保护法 COPPA》规定，运营者需建立并维护合理的措施以保护儿童个人信息的保密、安全和完整性。采取合作的措施保证仅向有能力保护儿童个人信息的保密、安全和完整性并为其提供保障的服务提供商和第三方披露儿童个人信息。

作为对照，我国《个人信息保护法》规定，个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

2) Zoom 超 50 万个 Zoom 账户泄露并在 Dark Web 出售

案例描述：2020 年 4 月，Zoom 被爆出漏洞，黑客通过凭据注入攻击收集，在 Dark Web 和黑客论坛上，出售超过 50 万个 Zoom 帐户，1 块钱可以买 7000 个。泄漏数据包括邮箱、密码以及个人会议链接和密钥，甚至许多还被免费赠送。另外，2020 年 11 月据美国联邦贸易委员会(FTC)，Zoom 将制定一项全面的安全计划，以解决该公司涉嫌欺诈和不公平行为的指控。FTC 的指控可以追溯到 2018

年 Zoom 的 Mac 桌面应用程序的更新，该程序秘密安装了 ZoomOpener 网络服务器，绕过 Safari 浏览器的安全措施，在没有提醒的情况下启动该应用程序。根据协议，Zoom 将在以后的每次违规行为中面临高达 43280 美元的罚款。

1.3.4. 数据加工风险

在数据加工环节，泄露风险主要是由分类分级不当、数据脱敏质量较低、恶意篡改/误操作等情况所导致。

(1)国内

1) 某集团 80 万用户数据被删除

案例描述：2017 年，因某为公司误操作导致某集团 80 万用户数据丢失，此次故障影响面非常大，涉及到钦州、北海、防城港、桂林、梧州、贺州等地用户，属于重大通信事故。事故发生后，某集团已经发布声明承认故障影响，技术人员也已经展开紧急维修。有消息称因为此次事故，某为公司已经被某集团处以 5 亿罚款，同时某集团已经展开全国范围的系统大排查，主要针对某技术公司第三方代维隐患问题。^[11]

(2)国外

1) 代码资源托管网站运维人员误删 300G 数据

案例描述：2017 年，著名代码资源托管网站 Gitlab.com 的一位工程师在维护数据时不慎删除约 300GB 的数据。本次事故也影响到了约 5000 个项目，5000 个评论和 700 个新用户账户。

1.3.5. 数据传输风险

在数据传输环节，数据泄露主要包括网络攻击、传输泄露等风险。网络攻击包括 DDoS 攻击、APT 攻击、通信流量劫持、中间人攻击、DNS 欺骗和 IP 欺骗、泛洪攻击威胁等；传输泄露包括电磁泄漏或搭线窃听、传输协议漏洞、未授权身份人员登录系统、无线网安全薄弱等。

(1)国内

1) “某智华胜”涉嫌非法窃取用户信息 30 亿条

案号：（2019）浙 0602 刑初 1143 号

法律依据：《中华人民共和国刑法》第二百八十五条、第二十五条第一款、第二十七条、第六十七条第三款、第七十二条第一、三款；《中华人民共和国刑事诉讼法》第十五条、第二百零一条

司法机关：浙江省绍兴市越城区人民法院

案例描述：邢某于 2013 年 5 月在北京成立某智华胜。某智华胜通过邢某成立的其他关联公司与运营商签订精准广告营销协议，获取运营商服务器登录许可，并通过部署 SD 程序，从运营商服务器抓取采集网络用户的登录 cookie 数据，并将上述数据保存在运营商 redis 数据库中，利用研发的爬虫软件、加粉软件，远程访问 redis 数据库中的数据，非法登录网络用户的淘宝、某博等账号，进行强制加粉、订单爬取等行为，从中牟利。案发前，某智华胜发现淘宝网在调查订单被爬的情况，遂将服务器数据删除。经查，2018 年 4 月 17-18 日期间，某智华胜爬取淘宝订单共计 22 万余条（浙江淘宝网络有限公司实际输出 1 万条），

向指定加粉淘宝账号恶意加淘好友共计 13.7 万余个（浙江淘宝网络有限公司实际输出 2 万个）。最终判决被告人王某犯非法获取计算机信息系统数据罪，判处有期徒刑二年，缓刑二年六个月，并处罚金人民币六万元。^[12]

(2) 国外

1) 南非大规模数据泄露事件 3160 万份南非公民数据被泄漏

案例描述：2017 年，南非史上规模最大的数据泄露事件——共有 3160 万份用户的个人资料被公之于众，连总统祖马和多位部长都未能幸免。泄漏信息包括身份号码、个人收入、年龄，甚至就业历史、公司董事身份、种族群体、婚姻状况、职业、雇主和家庭地址等敏感信息。此次被黑客公布的数据来源于 Dracore Data Sciences 企业的 GoVault 平台，其公司客户包括南非最大的金融信贷机构——TransUnion。

1.3.6. 数据提供风险

在数据提供环节，风险威胁来自于政策因素、外部因素、内部因素等。政策因素主要指不合规地提供和共享；内部因素指缺乏数据拷贝的使用管控和终端审计、行为抵赖、数据发送错误、非授权隐私泄露/修改、第三方过失而造成数据泄露；外部因素指恶意程序入侵、病毒侵扰、网络宽带被盗用等情况。

(1) 国内

1) 脱口秀演员交易流水遭泄露，某银行被罚 450 万元

执法机构：中国银行保险监督管理委员会

法律依据：《中华人民共和国银行业监督管理法》第二十一条、第四十六条和相关审慎经营规则《中华人民共和国商业银行法》第七十三条

案例描述：2020年5月6日，脱口秀演员池子（本名王越池）通过新浪微博控诉某银行上海虹口支行在未经其授权的情况下，私自将其个人账户流水提供给上海笑果文化传媒有限公司。王越池认为，某银行的这一行为侵犯了其合法权益，要求某银行赔偿损失，并公开道歉。同时，王越池还表示，某银行方面对此作出的回应为“配合大客户的要求”。对于举报，某银行也曾在官方微博公开发布致歉信称，该行员工未严格按规定办理，向笑果文化提供收款记录；某银行已按制度规定对相关员工予以处分，并对支行行长予以撤职。2021年3月19日，银保监会消保局公布的罚单信息显示，某银行因涉及客户信息保护体制机制不健全、客户信息收集环节管理不规范等四项违法违规行为，被处罚款450万元。^[13]

2) 掉进短信链接“陷阱”被骗3.6万余元

法律依据：[2014]10号《关于加强商业银行与第三方支付机构合作业务管理的通知》第三条规定，银发(2009)142号《中国人民银行、中国银行业监督管理委员会、公安部、国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》第二条第（六）项，《中华人民共和国合同法》第一百零七条

执法机构：河南省高级人民法院

案号：（2019）豫民申6252号、（2018）豫0326民初2446号

案例描述：2017年3月18-19日，顾某收到“车辆违规未处理”短信，在点击链接后，其银行账户被开通天翼电子商务、易宝支付、苏宁易付宝、北京百付宝、快钱支付、美团大众点评、支付宝、财付通、电e宝、拉卡拉、上海盛付

通、某易宝等十余个第三方快捷支付服务，并通过其中部分第三方支付平台连续扣款 52 笔，每笔金额从 1 元至 2500 元不等，共计 36960.79 元。顾某报警后，在公安机关和银行等机构的协作下，部分款项被追回并转入原告银行卡中，剩余 17728.94 元未能追回。法院认为，被告某行汝阳支行在为原告顾三斗办理银行卡时提供的相关格式文件条款中，未能反映出原告顾三斗主动申请并书面确认开通网上银行或电子银行等业务，原告因点击手机不明链接导致账户资金被盗取，较大可能系不法分子通过网上银行或电子银行操作，被告未能严格按照上述通知要求执行，对此应承担相应的责任。^{[14][15]}

3) 侵犯公民的电话信息 10 万多条

案号：（2020）冀 0681 刑初 507 号、（2021）冀 06 刑终 180 号

法律依据：《中华人民共和国刑法》第二百五十三条之一、第六十七条第三款、第六十四条、第七十二条第一款，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第三条第二款、第五条，《中华人民共和国刑事诉讼法》第二百零一条，《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第三百六十五条，《中华人民共和国网络安全法》第七十六条第五项，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条

司法机关：河北省保定市中级人民法院

案例描述：2020 年 5 月份至 8 月份，被告人刘某花 8000 元在网上购买“北斗创客”软件，通过该软件非法获取公民的电话信息 10 万多条。2020 年 7 月份，刘某通过 QQ 联系被告人高某欲购买公民个人信息数据，后被告人高某分两次以

1000 元的价格出售给被告人刘某公民个人信息数据 6 万多条。判决如下：判决如下：被告人刘某犯侵犯公民个人信息罪，判处有期徒刑三年，并处罚金人民币五千元；被告人高某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑五年，并处罚金人民币五千元。^[16]

1.3.7. 数据公开风险

在数据公开环节，泄露风险主要是很多数据在未经过严格保密审查、未进行泄密隐患风险评估，或者未意识到数据情报价值或涉及公民隐私的情况下随意发布的情况。

(1)国内

1) 微信朋友圈中流传着某医院数千人名单

执法机构：胶州市公安局

法律依据：《中华人民共和国治安管理处罚法》第二十九条

案例描述：2020 年 4 月 13 日，微信群里出现某医院出入人员名单信息，内容涉及 6000 余人的姓名、住址、联系方式、身份证号码等个人身份信息，造成了不良社会影响。依据《中华人民共和国治安管理处罚法》第二十九条规定，有下列行为之一的，处 5 日以下拘留；情节较重的，处 5 日以上 10 日以下拘留：违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的。公安机关依法对叶某、姜某、张某给予行政拘留的处罚。^[17]

2) 某市区政府泄露特困人员隐私法律

执法机构：某区政府办公室

法律依据：《网络安全法》第 42 条、第 72 条

案例描述：2020 年 8 月 24 日，河北省某市区人民政府信息公开网站发布了一份《某区 2020 年 8 月份农村特困供养金发放明细》，公示了多个乡镇 129 位村民的信息，公示名单中除了所属乡镇、姓名、发放款数、备注等信息之外，还悉数公开了村民的身份证号和银行卡号。经核实，发布机构某区民政局确实存在泄露隐私的问题，随后删除了该名单，并受到了内部公开群内通报批评，书面反馈整改内容的处罚。^[18]

2. 密码产业护航数字经济

2.1. 数字经济呼唤创新密码应用

2.1.1. 密码技术是数字安全压舱石

企业信息化高速发展，伴随着数字化资产爆发式增长，数据作为最重要的生产要素，在企业应用系统内部高速流转、共享、协同，驱动业务效率提升，带来了巨大效益。与此同时，数据的高价值使之成为被觊觎的目标，数据安全威胁已经成为关乎企业命运的关键业务风险，这也对企业数据安全防护体系提出新需求。

近年来，企业纷纷加强网络安全建设，部署了防火墙、反病毒网关、漏洞扫描系统、入侵检测系统、数据防泄漏等传统的安全设备，但数据泄漏事件依然频发。企业外部黑客攻击、内部人员窃取数据非法销售的事情层出不穷，数据泄漏频发的背后，归根到底是针对敏感数据本身保护不够。

目前来看，企业信息系统普遍缺失内建数据安全能力，同时随着企业内部各类信息系统之间打通共享，成倍放大了数据安全复杂度，面临着更为严峻的安全挑战。数据在不同系统之间流转，导致数据的所有者、控制者和处理者难以有效控制，数据可能被非法访问和处理，造成数据保密性和完整性等方面的巨大安全威胁。

造成应用缺失安全能力的原因有多个方面：

1.应用软件开发商或者集成商重点关注的是针对业务方面问题的解决，而缺乏在软件安全设计方面的投入，软件研发在安全方面的人员在研发人员中占比极低，甚至没有进行架构安全方面的设计，使得应用软件内普遍存在安全功能不足。

2.应用软件针对多个行业都有具体的解决方案，而每个行业针对业务安全方面的需求也不尽相同，从而使应用软件需要针对不同行业或企业的安全需求进行分别定制，因此，软件开发商也不会软件研发过程中加大对安全方面的投入。

3.不管是甲方还是应用集成商，能把应用开发能力和安全能力结合起来的人才非常匮乏，造成对应用的安全改造能力比较薄弱。

信息系统不可避免的存在安全缺陷，利用缺陷进行漏洞攻击或是网络安全永远的命题，攻防对抗视角的网络安全防护是过去主要的安全防护手段。当然，所有网络安全防护最终还是为了保护数据，防止“偷数据、改数据”，但是网络漏洞始终在所难免，所以需要从“防漏洞、补漏洞”的应对式防护，转化到“为数据访问重建安全规则”的主动式防护，也即“以数据为中心的安全”，这也是安全技术不断进化的必然产物。将密码技术等安全手段直接作用于数据，是最直接有效的主动防护措施，密码技术可以直接保障数据的机密性和完整性，同时也可以保障信息传递中的真实性和不可否认性。

密码技术在数据安全保护中起到“重构数据边界”的作用。如果缺失加密，数据在数据库或备份的过程中会有被盗取风险，此时的访问控制容易被绕过、形同虚设。数据安全保护方案可以在数据加密基础上，将“主体到应用内用户，客体到字段级”的访问控制、审计等技术相结合，打造防绕过的数据防护机制，并支持可独立部署的数据访问审计，每条日志支持主体追溯到应用业务用户，并为

审计日志进行完整性保护，保障信息泄漏后可追溯源头，最终打造“以密码技术为核心，多种安全技术相互融合”的数据安全防护体系。

2.1.2. 实战合规是密码建设指南针

近年来，国家十分重视数据安全，并提出使用国产商用密码技术来保护重要敏感数据，这些法律法规包括：

表 1 企业需遵循的密码相关法律法规

层级	名称	条例
数据安全政策法规	《网络安全法》	第二十一条：国家实行网络安全等级保护制度。其安全保护义务第 4 条明确采取数据分类、重要数据备份和加密等措施。
	《数据安全法》	第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。
	《个人信息保护法》	第五十一条第三款：采取相应的加密、去标识化等安全技术措施；

		第六十六条：情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款……
密码产业政策法规	《密码法》	二十七条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护。关键信息基础设施运营者，应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。
	《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）	第四章第三十条：各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
	《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2015〕116号）	第二部分第六点：落实密码安全防护要求。 网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。 第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码

	020]1960 号)	产品和服务。
	《关键信息基础设施安全保护条例》	规定履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度。关键信息基础设施中的密码使用和管理，应当遵守相关法律、行政法规。
	《商用密码管理条例(修订草案征求意见稿)》	提出非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，其运营者应当使用商用密码进行保护。

同时，国家也陆续出台相关法律法规，要求定期开展密码应用与安全性评估、等保测评等。

在多重法律、法规、行业指导的叠加驱动下，企业数据安全保护体系的建设工作，迎来了更高的、全新的合规性要求。如何有效满足多重的合规要求，对国产密码保护系统建设的规划、设计、实施能力提出了更高挑战。

2.1.3. 密码创新是数字安全领头雁

目前，企业在应用商用密码技术以及相关密码产品的过程中，一方面，具有自身保护数据资产的需要，以及相关法律法规的合规要求，另一方面，存在着密码产品“不能用”、“不好用”以及“用不好”的情况，因此，企业处于了“两难”的境地，急需高质量密码产品的供给。

密码高质量创新需要解决以下三方面的问题：

1. 能用

IT 技术快速发展，企业信息化水平也达到较高水平，数据在各种信息系统中高速流转。信息系统加入密码技术保护数据安全，需要不影响业务效率，保证数据的流转效率，从而为企业创造价值。然而，目前商用密码产品中算法的实现性能无法满足数据高速流转的场景需求，造成了企业不用密码，或者使用国外 AES 密码算法的情况（AES 算法的实现性能远远优于目前商用密码算法 SM4 的实现性能）。因此，商用密码 SM 系列算法亟待实现性能优化。

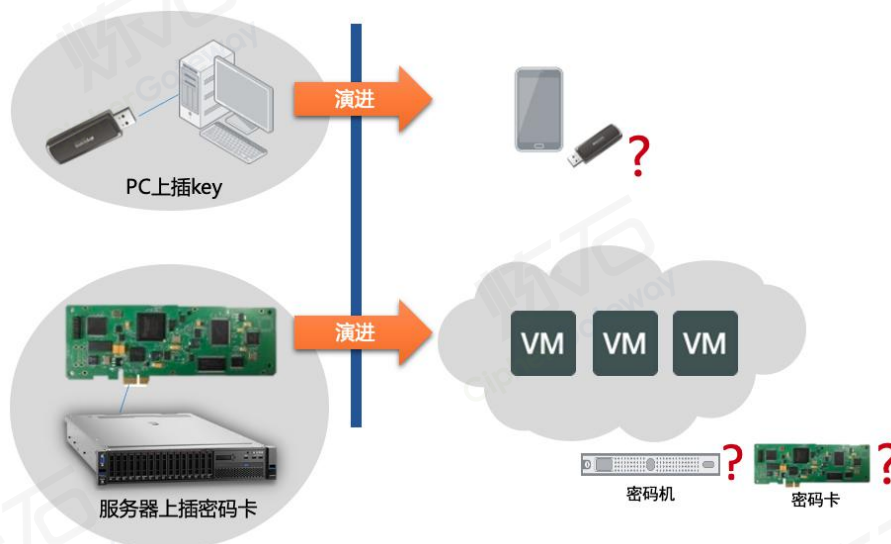


图 1 企业信息化技术演进示意图

另外，企业信息化建设向移动化和云化方向发展，之前在桌面端可以使用的鉴别用户身份的硬件智能密码钥匙（USBKey），无法插入移动终端；之前可以插入服务器中的密码卡，或者直接使用的硬件服务器密码机，无法在云场景的虚拟机中使用。因此，商用密码产品能够全面覆盖服务器、云端、桌面端、移动端、物联网等多种场景，从而适应企业信息化技术的发展和建设的需要。

2. 好用

企业的信息数据都是在各种信息系统中生成、流转和存储，而且这些信息系统经过长期的信息化建设，已经形成了集成化、规模化的特点，在这些已经稳定运行的信息系统中加入密码能力，需要避免对原系统进行开发改造，避免“开发周期长、投入成本高、实施风险大”的局面产生。

供给的密码产品要易用，消除用户的使用门槛。企业的使用人员一般都缺乏密码学知识，更不知道如何安全、有效的使用密码技术，提供的密码产品要能够实现对密码接口的业务级封装，比如提炼出密码中间件产品，让一般程序员通过调用 API 接口的方式，就能实现密码功能。

3. 好管

密码产品的引入，也属于企业信息化建设的一部分，企业当前的安全管理制度难以匹配密钥、加密策略、实施运维、合规等管理要求，毕竟密码自身的管理要求要高于一般信息系统的管理要求，需要密码产品的供应方考虑将管理融入到产品功能中，提供“好管”的密码产品。

密码的目的是为了保护数据安全，而数据是企业业务运转的“血液”，密码作用于数据，也就与业务进行了结合，成为“密码及安全和业务流程扭结缠绕”的新状态，需要密码产品在供给时考虑降低系统规划、建设、运维的复杂度。

2.2. 密码产业进入黄金发展时代

据《2020-2021 中国商用密码产业发展报告》显示，2016 年至 2020 年，我国商用密码产业总体规模持续增长，2020 年我国商用密码产业规模突破 466 亿，同比增速超 33%，详见下表所示^[19]。

表 2 2016-2020 年商用密码产业总体规模及同比增长率

年份（年）	2016	2017	2018	2019	2020
产业规模（亿元）	151.64	239.41	283	350	466
同比增速（%）	19.05	57.88	18.21	23.67	33.14

在内在市场需求和外部法律法规共同驱动下，密码产业已经进入到前所未有的黄金发展时代。

2.2.1. 顶层战略引导数字经济安全建设

2.2.1.1. 国家信息化发展战略纲要

2016 年 7 月实施的《国家信息化发展战略纲要》提到当今世界信息技术创新日新月异，以数字化、网络化、智能化为特征的信息化浪潮蓬勃兴起。没有信息化就没有现代化。以信息化驱动现代化，建设网络强国，是实现“两个一百年”奋斗目标和中华民族伟大复兴中国梦的必然选择，因此需要采取强有力的措施，持续不断的优化信息化发展环境。

1. 推进信息化法治建设

有序推进信息化立法进程。强化网络基础设施保护，加快制定网络安全法、电信法、电子商务法，研究制定密码法。加强网络用户权利保护，研究制定个人信息保护法、未成年人网络保护条例。

2. 加强网络生态治理

强化互联网管理。全面规范企业和个人信息采集、存储、使用等行为，防范信息滥用。加强个人数据保护，依法打击网络违法犯罪。

3.加快构建关键信息基础设施安全保障体系

维护网络空间安全，提升全天候全方位感知网络安全态势能力，做好等级保护、风险评估、漏洞发现等基础性工作，完善网络安全监测预警和网络安全重大事件应急处置机制。

4.实施网络安全人才工程

通过加强信息安全学科、专业建设和人才培养工作，开展全民网络安全教育，提升网络媒介素养，促进我国网络安全人才队伍建设，进一步增强全社会网络安全意识和防护技能。

2.2.1.2. 国家网络空间安全战略

2016年12月27日，国家互联网信息办公室发布了《国家网络空间安全战略》。贯彻落实习近平总书记网络强国战略思想，阐明了中国关于网络空间发展和安全的重要性。

《战略》指出，随着信息技术深入发展，网络安全形势日益严峻，必须坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及13亿多中国人民，造福全人类，坚定维护世界和平。

《战略》要求，要以总体国家安全观为指导，增强风险意识和危机意识，统筹发展安全两件大事，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

《战略》明确，国家网络空间安全工作的战略任务是坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力等 9 个方面。

2.2.1.3. 十四五国家信息化规划

2021 年 3 月 11 日，十三届全国人大四次会议通过《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》。在经济社会发展主要指标中，“安全保障”成为和经济发展、创新驱动、民生福祉和绿色生态并齐的国家五大发展核心指标之一，首次提高到关乎国家发展和国计民生的经济、创新、民生和绿色生态同等的核心地位，体现了国家对安全产业的高度重视。

国家十四五规划中，国家提出了加快构建全国一体化大数据中心体系，提升大数据安全水平，强化对算力和数据资源的安全防护，形成“数盾”体系。

国家十四五规划中，营造良好数字生态，强调建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。完善监测预警与应急平台，加强网络安全风险评估和审查。提出了网络安全保护“三化六防”的实施目标，全面提升国家关键信息基础设施综合防御能力。

2.2.1.4. 十四五推进国家政务信息化规划

2021 年 12 月，国家发展改革委印发了《“十四五”推进国家政务信息化规划》。本规划是根据《中华人民共和国国民经济和社会发展第十四个五年规划和

2035 年远景目标纲要》而制定，作为“十四五”期间统筹推进国家政务信息化工作，指导各地方有序开展政务信息化建设的重要依据。

《规划》总体要求里提出了主要规划目标。到 2025 年，推进政务信息化工作迈入以数据赋能、协同治理、智慧决策、优质服务为主要特征的“融慧治理”新阶段。其中目标之一是安全保障要达到新水平。全面落实信息安全和信息系统等级分级保护制度，基本实现政务信息化安全可靠应用，确保政务信息化建设和应用全流程安全可靠，实现政务数据资源全生命周期安全保护。

《规划》提出了三大任务 11 项具体工程。其中任务之一是加强网络安全保障。加强数字政府网络安全体系顶层设计，推进国产密码应用，严格落实等级保护和分级保护制度。强化政务数据安全，建立健全政务信息化工程全过程安全监督机制，落实网络安全工作责任制，形成跨部门、跨地区条块融合的安全保障工作联动机制。健全完善政务云服务评估制度，强化政务数据安全保障。

2.2.1.5. 国家创新驱动发展战略纲要

2016 年 5 月，《国家创新驱动发展战略纲要》由中共中央、国务院发布，自 2016 年 5 月实施。

为加快实施党的十八大提出的实施创新驱动发展战略，强调科技创新是提高社会生产力和综合国力的战略支撑，必须摆在国家发展全局的核心位置这一重大发展战略，制定本纲要。

战略任务之一是紧紧围绕国家安全等重大挑战，发展新一代信息技术，增强经济社会发展的信息化基础。加大自主软硬件产品和网络安全技术攻关和推

广力度，为我国经济转型升级和维护国家网络安全提供保障。加强面向国家战略需求的技术研发，支撑产业变革和保障国家安全。围绕涉及长远发展和国家安全的“卡脖子”问题，加大对空间、海洋、网络、核、材料、能源、信息、生命等领域关键核心技术安全、自主、可控。

2.2.1.6. 政府网站发展指引

2017 年，《政府网站发展指引》发布，明确要求对重要数据、敏感数据进行分类管理，做好加密存储和传输。《政府网站发展指引》要求“使用符合国家密码管理政策和标准规范的密码算法和密码产品，逐步建立基于密码的网络信任、安全支撑和运行监管机制”。政府网站汇聚了大量政务服务数据和公民个人信息，数据一旦遭到泄露,将造成严重后果。因此，文件对政府网站提出了使用密码进行数据保护的要求，其核心目标就是建立合规、安全、有效的密码保障体系，为政府网站安全保驾护航。

2.2.2. 国家法律加速密码应用推广普及

2.2.2.1. 网络安全法

2017 年 6 月 1 日实施的《网络安全法》，规定了网络运营者应该按照网络安全等级保护制度的要求履行安全保护义务。保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改，采取数据分类、重要数据备份和加密等措施，维护网络数据的完整性、保密性、真实性及不可否认性。加大

投入扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务。

2.2.2.2. 密码法

2020 年 1 月 1 日施行的《密码法》填补了密码领域的法律空白，推动密码在网络安全与信息化发展中发挥更大作用。

《密码法》按照中央确定的密码管理原则和应用政策，规定了密码应用主要制度和要求，明确了密码的定义和分类。强调国家积极规范和促进密码应用；建立商用密码检测认证体系，鼓励从业单位自愿接受商用密码检测认证；明确关键信息基础设施使用密码和进行密码应用安全性评估的要求；建立安全审查机制；对采用商用密码技术从事电子政务电子认证服务的机构进行认定。密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。密码分为核心密码、普通密码和商用密码。商用密码用于保护不属于国家秘密的信息。

2.2.2.3. 数据安全法

2021 年 9 月 1 日施行的《数据安全法》，是为了规范数据处理活动，为维护国家、组织、个人的合法权益。该法对数据和数据处理的范围进行了定义，数据是指任何以电子或者其他方式对信息的记录。数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。并且提出要建立数据分类分级保护制度，数据安全应急处置机制，数据安全审查制度和数据安全管理制度等数据安全保护措施，组织开展数据安全教育培训，加强风险监测和风险评估。以及明确了违法数据安全需承担的责任。

2.2.2.4. 个人信息保护法

2021 年 11 月 1 日施行的《个人信息保护法》明确了个人信息处理和跨境时提供个人信息的规则，以及明确了个人信息处理的范围，以及信息处理者的权利和义务。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

其中第五十一条指出，个人信息处理者应当对个人信息实行分类管理、加密、去标识化等安全技术措施，制定安全管理制度，合理确定操作权限，安全教育和培训，制定应急预案等措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。

处理个人信息原则上应当取得个人同意，除法律、行政法规另有规定外。侵害个人信息权益造成损害的，应当依法承担相应责任。

2.2.2.5. 关键信息基础设施安全保护条例（国令第 745 号）

2021 年 9 月 1 日施行的《关键信息基础设施安全保护条例》，明确了关键信息基础设施的密码应用要求，保障关键信息基础设施安全，维护网络安全。

本条例规定了在关键信息基础设施保护工作中，开展有关密码管理工作的责任义务和相关法律责任。指出安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。开展网络安全监测、检测、风险评估和安全审查；制定网络安全应急预案；组织网络安全教育、培训、考核。

2.2.2.6. 网络安全等级保护条例（征求意见稿）

2018年6月27日，公安部发布了《网络安全等级保护条例（征求意见稿）》。其中设置了密码管理专章，明确了网络安全等级保护密码管理的主要思路、方式和手段，强调网络安全等级保护第三级及以上系统应使用密码进行保护，强化密码管理部门在等级保护技术标准制定、监督检查、密码应用安全性评估等方面的职权，还从网络安全等级保护的事前备案审核、事中应用要求，及事中事后监管和法律责任各环节对密码管理和应用进行了规定。

在网络建设过程中，网络运营者应当同步规划、同步建设、同步运行网络安全保护、保密和密码保护措施。保障网络和信息安全。建立网络安全等级保护制度；建立安全管理和技术保护制度；落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施；落实数据分类、重要数据备份和加密等措施。

2.2.2.7. 网络数据安全条例（征求意见稿）

2021年11月14日，国家互联网信息办公室发布了《网络数据安全条例（征求意见稿）》。主要是为规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。

该条例明确了境内和境外的适用范围。以及数据安全保护措施和管理制度。数据要采取分类分级、备份、加密、访问控制等保护措施。维护数据的完整性、保密性、可用性。

数据处理者应当建立数据分类分级保护制度，采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，维护数据

的完整性、保密性、可用性。处理重要数据或者赴境外上市的数据处理者，应当每年开展一次数据安全评估。

2.2.2.8. 商用密码管理条例（修订草案征求意见稿）

2019 年发布的《密码法》对商用密码管理制度进行了结构性重塑，为了落实党和国家要求，贯彻《密码法》精神，适应新时代商用密码事业发展需求，亟需对《商用密码管理条例》（简称《条例》，1999 年发布）进行修订。

修订草案征求意见稿中明确提出，非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，其运营者应当使用商用密码进行保护。

2.2.2.9. 信息安全等级保护商用密码管理办法（国密局发 [2007]11 号）

2008 年 1 月 1 日施行的《信息安全等级保护商用密码管理办法》，为规范信息安全等级保护中使用商用密码的行为。

商用密码产品应当按照《商用密码产品目录》选用。对第二级及以上的信息系统，使用商用密码产品应当备案。对第三级以上信息系统，商用密码应用系统建设方案应当通过密码管理部门组织的评审后方可实施，商用密码应用系统要通过测评机构的密码测评后方可投入运行，密码测评包括资料审查、系统分析、现场测评、综合评估等。

2.2.2.10. 国家政务信息化项目建设管理办法（国办发〔2019〕57号）

2020年2月1日施行的《国家政务信息化项目建设管理办法》，是为了规范国家政务信息化建设管理。对国家政务信息系统的规划、审批、建设、共享和监管做出规定，其中明确规定了多项密码应用有关要求。包括备案及备案文件要求，安全监管与评估要求，以及不符合规定的系统需承担的后果等。

其中第九条，国家政务信息化项目需向国家发展改革委备案。备案文件应当包括应用系统、等级保护或者分级保护备案情况、密码应用方案和密码应用安全性评估报告等内容。第二十八条，对不符合密码应用和网络安全要求，或存在重大安全隐患的政务信息系统；不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。第三十条，加强国家政务信息系统的安全监管。按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。

2.2.2.11. 政务信息系统政府采购管理暂行办法（财库〔2017〕210号）

2017年12月26日施行的《政务信息系统政府采购管理暂行办法》，是为了推进政务信息系统政府采购工作能规范高效的开展，明确采购的需求范围、要求以及验收方案的内容。

政务信息系统采购需求里应包括数据共享、安全审查和保密、等级保护、分级保护等要求。采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。项目验收方案应当包括项目所有功能的实现情况、密码应用和安全审查情况等。

2.2.2.12. 电子认证服务密码管理办法

2009年12月1日施行的《电子认证服务密码管理办法》，规定面向社会公众提供电子认证服务应当使用商用密码，并规范其使用商用密码行为。

明确了申请电子认证服务使用密码许可应当具备的基本条件和程序，对电子认证服务系统的运行和技术改造等做出了规定。电子认证服务系统应由具有商用密码产品生产和密码服务能力的单位承建。系统建设和运行应当符合《证书认证系统密码及其相关安全技术规范》。并通过国家密码管理局组织的安全性审查。

国家密码管理局对电子认证服务系统进行安全性测试、监督、审查。检查发现存在不符合许可条件，需限期整改；情节严重的，吊销其《电子认证服务使用密码许可证》。

2.2.3. 行业地区出台密码技术应用要求

根据《密码法》的规定，国家对密码实行分类管理，商用密码用于保护不属于国家秘密的信息。在我国，商用密码已经广泛应用于国民经济发展和社会生产生活的方方面面，涵盖金融、能源、政务、电信、教育、公安、住建、交通、水利、医疗等众多领域。

随着《密码法》的施行，商用密码产业迎来重大发展机遇。依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，各行业也相继出台了行业密码应用要求。

2.2.3.1. 金融行业密码应用要求

1、金融行业的重要地位

习近平总书记指出，金融是国家重要的核心竞争力，是现代经济的核心。金融安全是国家安全的重要组成部分。金融业机构生产运行过程中产生的信息也逐步以不同形式转化为数字资产，在不同信息网络与系统之间流转。数据逐步转变为核心价值资产。随着互联网信息技术的广泛应用，极大地促进了金融业务的发展。

由于金融机构的特殊性质，其网络上传输的大部分数据为金融敏感信息（涉及用户个人属性、资金交易、合同等敏感信息），对金融信息安全带来了极大的威胁与风险。所有业务数据都要传送到数据中心进行集中处理，因此金融业务数据的安全处理和安全传输将成为关系到整个金融数据大集中系统战略成败的关键。如果不采取有效安全措施，这些数据的安全将可能受到危害和攻击，带来不可弥补的经济损失和社会影响。

密码作为保障信息安全的核心技术，在身份认证、信息完整性和保密性、电子合同不可抵赖性等方面发挥着关键性的作用。有效防止了敏感信息泄露、财产损失或业务中断，对维护金融信息安全具有重要的意义。

2、金融行业的重要标准规范

- 《中央办公厅-厅字[2018]36 号文 金融和重要领域密码应用与创新发展工作规划（2018-2022）》
- 《GB/T 36618-2018 信息安全技术金融信息服务安全规范》
- 《金融科技发展规划(2019-2021 年)》

- 《GM/T0065-2019 商用密码产品生产和保障能力建设规范》
- 《GM/T0066-2019 商用密码产品生产和保障能力建设实施指南》
- 《GM/T0067-2019 基于数字证书的身份鉴别接口规范》
- 《GM/T0068-2019 开放的第三方资源授权协议框架》
- 《GM/T0069-2019 开放的身份鉴别框架》
- 《GM/T0070-2019 电子保单密码应用技术要求》
- 《GM/T0071-2019 电子文件密码应用指南》
- 《GM/T0072-2019 远程移动支付密码应用技术要求》
- 《GM/T0073-2019 手机银行信息系统密码应用技术要求》
- 《GM/T0074-2019 网上银行密码应用技术要求》
- 《GM/T0075-2019 银行信贷信息系统密码应用技术要求》
- 《GM/T0076-2019 银行卡信息系统密码应用技术要求》
- 《GM/T0077-2019 银行核心信息系统密码应用技术要求》
- 《JR/T 0071-2020 金融行业网络安全等级保护实施指引》
- 《JR/T 0072-2020 金融行业网络安全等级保护测评指南》
- 《JR/T 0171- 2020 个人金融信息保护技术规范》
- 《JR/T 0197-2020 金融数据安全 数据安全分级指南》
- 《JR/T 0218-2020 金融业数据能力建设指引》
- 《JR/T 0060-2021 证券期货业网络安全等级保护基本要求》
- 《JR/T 0067-2021 证券期货业网络安全等级保护测评要求》
- 《JR/T 0222-2021 金融信息系统加密服务的技术能力评价模型》
- 《JR /T 0223-2021 金融数据安全 数据生命周期安全规范》

- 《JR/T 0224-2021 保险行业网络建设基本规范》
- 《JR/T 0225-2021 保险移动应用信息安全基本要求》

3、金融行业信息系统安全现状

中国金融行业信息化建设目前已完成金融电子化、金融数据集中化、金融信息系统业务综合化三阶段的规划发展。随着金融业对信息化依赖程度越来越大，大数据、云计算等新技术在金融领域的广泛应用，金融服务更加多样化，金融行业网络结构和网络应用日趋复杂，金融业信息安全迎来更大挑战。

金融行业目前存在的安全风险的原因：

- 机构内部人员操作不当、内部安全监管不到位；
- 核心安全设备和技术（包括操作系统、数据库、芯片等）依赖于国外厂商；
- 境内外网络黑客攻击；
- 大数据平台实现数据集中的同时，安全风险也相对集中。

Verizon 2021 数据泄露调查报告显示，今年金融服务领域 44% 的违规行为是由内部参与者造成的，占当年所有违规的 13%。金融行业的稳定可持续发展，亟待完善内部管理机制和提高安全治理能力，规避各类安全风险。

随着《密码法》及金融行业各项标准规范的出台，商用密码技术在金融行业也逐步落地开花，虽然银行业商用密码应用较为成熟，但体系化建设仍需增强。证券、保险行业商用密码应用相对较少，且证券交易对时延、稳定性要求高，对商用密码技术和产品的性能提出了巨大挑战。如何更好地应用商用密码技术保障金融安全，成为目前行业面临的严峻考验。

4、金融行业密码应用要求

1) 商用密码应用总体要求

依据《数据安全法》等相关法律，及《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》和《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》两部标准规范，并结合《JR/T 0197-2020 金融数据安全 数据安全分级指南》、《JR /T 0223-2021 金融数据安全 数据生命周期安全规范》、《金融行业密码应用基本要求》等金融行业密码应用的重要标准规范。金融行业商用密码应用总体要求需满足如下规定：

(1) 对系统数据实施分类分级管理

首先进行数据资产梳理，重要数据的识别，最后对数据进行分类分级。

根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到低划分为 5 级、4 级、3 级、2 级、1 级。

根据数据安全级别不同，有侧重地采取适当的安全防护措施，1 级数据为公开数据，2 级数据应优先考虑业务需求，4 级数据应优先考虑安全需求，5 级数据的保护按照国家及行业主管部门的有关要求执行。

根据《GM/T0077-2019 银行核心信息系统密码应用技术要求》，目前银行业核心系统安全级别为 3 级、4 级。

(2) 横向安全保护，从数据的流转方向实施安全保护

建立完善的金融数据生命周期保护。包括数据的收集、存储、使用、加工、传输、提供、公开等过程。

采集数据应采用摘要、消息认证码、数字签名等密码技术确保采集过程数据的完整性。对数据采集设备或系统的真实性进行验证。3 级及以上的数据传输和存储时，应采取商用密码技术、产品和服务来保障数据的机密性。数据在使用、

加工、提供、公开时，要使用访问控制技术、去标识化技术、记录日志等进行安全增强。

（3）纵向安全保护，从技术和管理两个维度实施商用密码应用

分别从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面提出了第一级到第四级的密码应用技术要求。并从管理制度、人员管理、建设运行和应急处置四个方向提出了第一级到第四级的密码应用管理要求。

2) 不同场景下商用密码应用要求

金融行业的商用密码应用场景包括传统的金融柜面系统，网上银行、证券交易、网上投保等各种网上系统，及金融机构间的横向信息系统。不同场景下商用密码要求如下：

（1）金融 IC 卡中的商用密码应用要求

金融 IC 卡是国际通用的基础支付方式，是整个支付产业的重要基础。用户通过 ATM 机、POS 机等终端完成交易。为保证线下交易的安全性，采用芯片技术、商用密码算法和多种密码安全认证技术保障持卡人用卡安全，有力地推进了金融行业商用密码技术的应用进程。

线下交易过程中，商用密码应用要求包括：

- 通过数据加密、消息验证、认证技术等，保证卡片密钥的装载安全。
- 通过对用户进行身份标识和身份鉴别，保证用户身份的真实性。
- 通过加密技术和认证技术，保证金融 IC 卡数据、持卡人数据、交易信息和日志等在传输和存储过程中的保密性和完整性。

- 基于商用密码算法进行加密，保证 PIN 在网络传输和验证时不以明文形式出现，保证工作密钥在应用系统交易中不以明文形式出现。

(2) 网上证券交易系统商用密码要求

网上证券交易系统一般提供交易下单、查询成交回报、资金划转、金融资讯、实时行情等一体化服务。与传统的交易渠道相比，网上证券交易系统能为更广泛的客户群体实时提供多样信息，使用户足不出户就能安全便捷地使用金融服务。

网上证券交易过程中，商用密码应用要求：

- 通过动态令牌或数字证书客户端工具实现用户和券商的身份认证，保证身份真实性、合法性；
- 客户端与交易系统之间建立基于商用密码算法的 SSL 加密传输通道，保证数据在互联网传输过程的保密性；
- 通过数字签名技术和散列函数保证交易信息不被篡改，保证了交易信息的完整性；
- 通过数字证书和数字签名技术保证了用户和券商的交易行为的不可否认性。

(3) 电子保单中商用密码应用要求

随着互联网和信息技术的发展，互联网线上交易逐渐在保险行业普及，客户购买保险不再依赖传统的保险办理方式，电子保单已成为重要途径。商用密码算法在电子保单的应用，保障了电子保单业务的安全，是网上保险发展的重要基石。

依据《GM/T0070-2019 电子保单密码应用技术要求》，电子保单管理过程商用密码应用要求：

- 通过身份认证技术，保证投保人与保险公司双方身份真实性。

- 基于数字签名和电子签章技术保证电子保单完整性和不可否认性，并为投保人提供电子保单真实性验证方式。
- 对电子保单办理过程中的相关信息（如身份证件、图像、签名）与电子保单结合进行数字签名和加密处理，并进行归档，保障电子保单具备法律效应，以便日后调阅或举证。

2.2.3.2. 电力行业密码应用要求

1、电力行业概述

电力属于国家能源资源之一，是国民经济的重要物质基础。电力行业信息化建设较早，涉及生产，运行，维护，销售等多个生产经营环节。但固定 PC 机前的操作局限使整个电力系统各自形成了信息孤岛，不便于沟通和资源共享。电力企业有向集团型发展的趋势。

电力行业属于国家关键基础设施，不仅关系到民众日常生活，同样对工控领域、甚至对国家安全都影响深远。因此，重点加强电力设施的安全建设及企业内部的安全防护显得尤为重要。

2、电力行业的重要标准规范

- 2005 年 5 月 1 日起施行的《电力监管条例》
- 《信息安全等级保护管理办法》（公通字[2007]43 号）
- 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
- 《电力二次系统安全防护规定》（电监会 5 号令）
- 《电力行业网络与信息安全监督管理暂行规定》（电监信息[2007]50 号）

- 国家电力监管委员会《关于开展电力行业信息系统安全等级保护顶级工作的通知》（电监信息[2007]34号）
- 2007年11月，出台《电力行业信息系统安全等级保护定级工作指导意见》（电监信息[2007]44号）
- 2014年7月2日，国家能源局发布《电力行业网络与信息安全管理办法》
- 2018年9月13日，国家能源局发布《关于加强电力行业网络安全工作的指导意见》对关键信息基础设施安全保护、加强电力企业数据安全保护等提出了更高要求。
- 《电力行业信息系统安全等级保护基本要求》（征求意见稿）

3、电力行业信息系统安全现状

电力行业的快速发展，使人们对电力行业安全要求越来越高，现有电力系统网络安全防护方案，包括内外网隔离、分区隔离、网络专用等措施，很好地隔离了外网、管理信息区、生产控制区之间的非法访问。随着密码技术的推广，在能源领域，基于密码技术的电力调度安全防护体系在国家电网等企业实现全覆盖，使用密码模块生产的智能电表超5亿只，发放用户卡超1亿张。

但在管理信息区中，积累了大量的电力敏感数据，例如财务数据、营销数据、人资数据、市场信息、生产管理信息等，来自于不同应用系统的数据集中存储在数据库中。内部人员、第三方运维人员、数据库系统DBA、开发人员对数据库中的数据都需要频繁地访问，诸多的人群和过高的权限造成电力敏感数据集中泄露、篡改的风险。

4、电力行业密码应用要求

依据国家针对信息系统密码应用的法律法规及电力行业密码应用相关标准。

对电力行业信息系统密码应用要求，主要包括几下几方面：

1) 电力信息系统安全等级划分

根据《电力行业信息系统安全等级保护定级工作指导意见》等级保护相关管理文件，按照信息系统破坏后，对公民、法人、和其他组织的合法权益，对社会秩序和公共利益，对国家安全，三个不同客体造成的不同损害程度（一般、严重、特别严重），将电力行业信息系统安全保护等级分为五级。如下表：

表 3 定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

电力行业信息系统分为生产控制系统、生产管理系统、网站系统、管理信息系统、信息网络五大类。按照不同系统业务数据重要类别，将电力行业重要信息系统进行等级保护定级。

2) 电力信息系统不同的安全等级保护

针对电力行业，除去满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》对通用信息系统的密码应用要求标准外，还需满足电力行业信息系统等级保护要求。除了选择合适的商用密码技术、产品及服务外，同时从云数

据及互联网大数据角度出发，加密商用密码技术在电力行业中的应用，提高电力行业的密码服务体系。

根据《电力行业信息系统安全等级保护基本要求》，依据系统抵抗不同程度的攻击、危害程度、恢复能力等，将信息系统安全保护能力分为五级。

从技术和管理两个维度，对电力行业不同安全保护等级信息系统进行安全建设和监督管理。基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出保护；基本管理要求从制度、机构、人员、建设和运维等几个方面提出安全管理。

2.2.3.3. 政务行业密码应用要求

1、政务行业概述

随着信息社会的发展，电子政务成为实现政府信息化的重要方式。电子政务信息安全，关系到国家政治、军事等重要情报，一旦信息被泄密，就可能会影响国家的安全，带来不可弥补的损失。

我国政府信息化建设经历了从政务信息电子化、计算机化、网络化的渐变过程。目前电子政务大数据是政务信息发展的新阶段，这一阶段的特点是开放、共享、动态、实时、智能。同时也迎来了技术、管理和安全等方面的新挑战。

2、政务行业的重要标准规范

- 《政务信息资源共享管理暂行办法》（国发〔2016〕51号）
- 《政务信息系统整合共享实施方案》（国办发〔2017〕39号）
- 《密码标准应用指南》（密标会 2018 版本）
- 《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）

- 《政务信息系统密码应用与安全性评估工作指南》（2020 版）
- 《“互联网+政务服务”技术体系建设指南》
- 《政府网站发展指引》

3、政务行业信息安全现状

电子政务系统一般包括：电子政务网络平台、政府门户网站、办公自动化系统等。相比于传统信息系统，政务大数据或政务云系统在安全方面面临新的挑战。一方面，政务云系统中主机边界、网络边界模糊，风险不但来自南北流量（外部用户与内部服务器间的流量），同时也来自东西流量（内部服务器间的流量）；另一方面，云系统承载多个单位的业务系统，各单位的业务系统需要密码技术来支撑自身的业务服务。因此，政务云系统需要将密码作为一种服务，为这些系统提供支撑。

4、政务行业密码应用要求

根据《政务信息系统密码应用与安全性评估工作指南》(2020 版)，政务行业信息系统密码应用要求主要包括以下三个方面：

1) 政务信息系统中的密码保障系统应做到 “三同步一评估”

项目建设单位应落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估”。政务信息系统的密码应用与安全性评估贯穿于系统的规划、建设和运行阶段，其实施过程如下图所示。

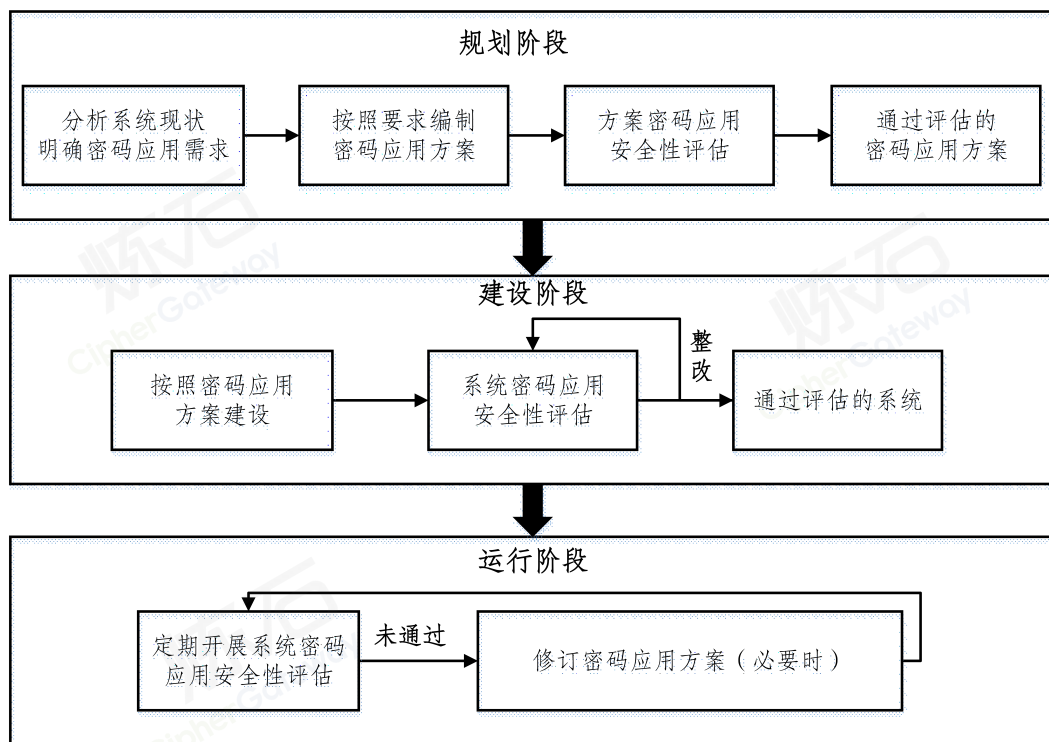


图 2 政务信息系统密码应用与安全性评估实施过程示意图

2) 政务信息系统密码应用措施

项目建设单位需从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面采用密码技术措施，建立安全的密钥管理方案，并采取有效的安全管理措施，对政务信息系统进行保护。

政务信息系统需使用经检测认证合格的商用密码产品或服务，使用的商用密码算法、技术应遵循密码相关国家标准和行业标准，项目建设单位选择具有电子政务电子认证服务资质的机构。

3. 政务信息系统密码应用与安全性评估

根据《政务信息系统密码应用与安全性评估工作指南》，针对政务行业信息系统的不同建设阶段，对建设、使用及集成单位、密评机构等提出了不同的要求。

项目规划阶段，建设单位根据系统网络安全保护等级，编制政务信息系统密码应用方案。项目建设阶段，系统集成单位应严格按照通过密评的密码应用方案开展工程实施、建设密码保障系统。项目建设完成后，密评机构对系统密码应用情况开展密评。

2.2.3.4. 电信行业密码应用要求

1、电信行业概述

电信和互联网行业是全球数字化进程的先驱，在现代社会中占有重要地位。《中国互联网络发展状况统计报告》显示，截至 2020 年 12 月，我国网民规模达 9.89 亿，互联网普及率达 70.4%。电信行业的发展大大加速了信息的流动，缩短空间距离，提高社会经济的运行效率，从而创造巨大的社会效益。电信行业具有服务性、网络性、技术密集型等特点。

伴随数字经济的持续发展，电信行业信息化程度不断加深，系统的复杂度与开放度随之提升。对拥有海量用户敏感信息的电信企业而言，保护用户的数据安全至关重要。根据工信部日前发布的《网络安全产业高质量发展三年行动计划(2021-2023 年)(征求意见稿)》，2023 年，网络安全产业规模将超过 2500 亿元，年复合增长率超过 15%，电信等重点行业网络安全投入占信息化投入比例要达 10%。

2、电信行业的重要标准规范

- 《电信和互联网用户个人信息保护规定》
- 《电信和互联网行业数据安全治理白皮书（2020 年）》

- 《电信和互联网行业提升网络数据安全保护能力专项行动方案》（工信厅网安〔2019〕42号）
- 《电信和互联网行业网络数据安全标准体系建设指南》
- 《YD/T 3802-2020 电信网和互联网数据安全通用要求》

3、电信行业信息系统安全现状

随着中国电信行业信息化的发展，数据的产生和存储均在应用系统中发生，企业的业务已经离不开应用系统的支撑。已经建设的应用系统，大多都是网络侧的安全防护。普遍缺失数据安全保护的能力，需要补充和增强，这就面临着数据安全改造的挑战。

中国电信行业的信息化建设已经取得了较大成绩，已建设完成的应用系统众多，并且已经实现了系统集成、业务打通，已经改变了以前“各自为政、信息孤岛”的模式。在应用密码保护数据安全方面，也需要以全局化思维构建数据安全密码防护，建设可扩展、服务化的密码应用体系。

4、电信行业密码应用要求

结合《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》及《电信和互联网行业网络数据安全标准体系建设指南》等电信和互联网行业相关标准，针对电信行业密码应用要求，主要包括：

1) 行业数据安全治理

对数据资产梳理，行业数据分类分级保护，维护数据安全与促进数据开发利用。

2) 行业数据安全等级保护

从数据采集、传输、存储、处理、交换、销毁等数据全生命周期流转过程，及物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面，采用密码技术措施对数据进行立体维度的安全技术保护。

从数据安全规范、评估、监控预警与处置、应急响应与灾难备份、安全能力认证等视角进行安全管理增强。

3) 行业网络数据安全监管

通过集中开展数据安全专项治理和监督检查，督促基础电信企业强化网络数据安全全流程管理，及时整改消除重大数据泄露、滥用等安全隐患。基本建立行业网络数据安全保障和标准体系。加强行业网络数据安全应急管理，开展网络数据安全风险评估。

2.2.3.5. 教育行业密码应用要求

1、教育行业概述

教育事业是民族振兴和社会进步的基石，2010 年以来我国大力开展教育信息化建设，为贯彻落实党的十九大精神，推进“互联网+教育”发展，加快教育现代化和教育强国建设。2018 年教育部制定了《教育信息化 2.0 行动计划》。目前我国教育行业信息化工程取得良好成效。2020 年初新冠疫情对传统教育模式带来冲击，互联网在线教育再次发挥重要作用。

到 2022 年基本实现“三全两高一大”的发展目标。覆盖全体适龄学生、数字校园建设覆盖全体学校，信息化应用水平和师生信息素养普遍提高，建成“互联网+教育”大平台，推动从教育专用资源向教育大资源转变，努力构建“互联

网+”条件下的人才培养新模式、发展基于互联网的教育服务新模式、探索信息时代教育治理新模式。

2、教育行业的重要标准规范

- 《国家中长期教育改革和发展规划纲要（2010—2020 年）》
- 《教育信息化十年发展规划（2011-2020 年）》
- 《国家教育事业发展规划“十三五”规划》
- 《教育信息化“十三五”规划》
- 《关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4 号）
- 《教育部办公厅关于印发〈教育行业信息系统安全等级保护定级工作指南（试行）〉的通知》（教技厅函〔2014〕74 号）
- 《关于推进“互联网+教育”发展的指导意见（征求意见稿）》
- 《关于引导规范教育移动互联网应用有序健康发展的意见》
- 《教育信息化 2.0 行动计划（2018 年）》
- 《教育行业密码应用与创新发展实施方案》（2019）
- 《2020 年教育信息化和网络安全工作要点》
- 《教育行业网络安全白皮书（2020 年）》

3、教育行业信息系统安全现状

教育行业信息系统包括校园管理信息化平台、数字校园等平台、网上办事大厅平台等。信息系统中用户多、数量大，承载的数据与信息也极其庞大，包含师生个人隐私数据，学校教学科研核心数据等。

教育信息安全所涉及的领域非常广泛，有网络、终端、交换设备等信息化硬件设备，有教学管理系统、学习资源系统等信息化软件系统，还有安全服务、安全管理和安全监控等信息化管理平台。

近年来，各大高校信息化建设不断发展和完善，通过云计算技术构建覆盖全国互联互通的“教育资源公共服务平台”。随着信息技术在教育行业的广泛应用和深度融合，网络信息安全风险随之而来，亟需提升教育行业的网络与信息安全意识及整体安全防护水平。《教育信息化 2.0 行动计划》强调建立网络安全和信息化统筹协调的领导体制，做到网络安全和信息化统一谋划、统筹推进。完善网络安全监督考核机制。以《网络安全法》等为纲，全面提高教育系统网络安全防护能力。

教育信息化“十三五”期间，高校基本已完成校园信息化建设，已建立了学生、人事、财务、科研等重要信息系统，支撑了校内各类型教育教学管理业务的开展。部分学校建立信息门户网站、移动校园平台等，为校内教职工、学生的生活、工作提供了便捷的信息化服务。但高校的密码应用服务薄弱，一直没有形成统一的建设标准规范，《教育行业密码应用与创新发展实施方案》为高校的密码应用与改造提供了建设思路。

4、教育行业密码应用要求

为推进“互联网+教育”发展，落实教育领域网络安全和信息化的战略部署。教育部 2020 年 3 月份印发《2020 年教育信息化和网络安全工作要点》。其中第 15 章指出，加强教育系统密码应用与管理，落实《教育行业密码与应用创新发展实施方案》，推进密码基础设施和支撑体系建设，推动教育重要业务信息系统开展密码应用安全性评估，完善教育数字认证（CA）基础支撑体系建设，推动

国家教育管理信息系统密码普遍应用，提升系统安全和数据安全。第 32 章指出，加强网络安全防护和保障能力。落实教育系统关键信息基础设施安全防护，组织开展应急演练。建立覆盖数据全生命周期的安全管理机制。

根据教育部办公厅于 2019 年 10 月份印发的《教育行业密码应用与创新发展实施方案》，包括构建教育行业密码支撑体系、推进教育行业密码普及应用、推进教育密码工作落实和创新发展等。通过对《教育行业密码应用与创新发展实施方案》分析，在教育行业密码应用建设过程中，可提供：

1) 完成共享服务平台本地化服务系统建设

面向业务系统提供标准化、统一化的密码服务接口，减少集成复杂度，方便本地应用系统的密码服务调用。

2) 完成教育密码在校园管理信息化、数字校园应用建设

基于教育部教育行业密码基础设施和支撑平台的基础数字证书服务、电子证照、可信身份等服务对接，建设一套可以为个学校各类信息系统提供安全、可信的密码应用平台，密码应用具体包括：

- 实现各类校园信息化业务关键节点的可信时间的留存和业务关键节点的时间签署留存，将业务产生或者操作的时间进行固化，并留存到业务数据库或者相关凭证文档中；
- 实现各类校园信息化业务操作行为的数据完整性、数据机密性、数据防篡改和行为防抵赖；
- 实现移动校园改造；
- 实现各类校园信息化业务产生的凭据的合法可信，具备防篡改、防伪、可验证性。

3) 完成教育密码认证应用系统建设

各高校根据自身情况,完成教育密码应用基础支撑与共享服务平台的高校本地化服务子系统建设,包括:教育数字认证子系统、教育可信身份认证服务子系统、将可信密码服务平台作为校级服务平台。

4) 完成校园密码应用改造

各高校根据自身情况,完成学生、教职工基于密码技术的可信电子身份证件;OA等业务系统无纸化应用建设,并集成移动签名网关系统,完成个人电子签名。

2.2.3.6. 公安行业密码应用要求

1、公安行业概述

公安隶属政法部门,公安系统的网络信息系统,主要为相关公安系统工作人员,提供对内管理及对外办公服务,均涉及人民群众的切身利益和国家安全问题。

其各类信息系统众多,且存储着大量的重要数据和个人敏感信息,包括公民身份档案信息、旅馆管理信息、警员信息,罪犯犯罪记录等重要敏感数据,容易成为网络攻击者觊觎的目标,敏感数据一旦遭到泄露,不仅会使个人利益受损,也会影响到政法部门公众形象,甚至关系到国家安全。

密码技术是保护数据最经济有效的手段,国家也十分重视国产密码技术的发展,明确规定了涉及国计民生的各行各业要应用密码保护网络信息安全。

2、公安行业的重要标准规范

- 《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安[2007]861号)
- 《信息安全等级保护管理办法》(公通字[2007]43号)

- 《商用密码管理条例》
- 《信息安全等级保护商用密码技术要求》
- 《指纹信息采集系统技术规范 2008》
- 《指纹信息采集系统数据规范 2008》
- 《公共安全视频图像信息系统管理条例》
- 《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》

3、公安行业信息系统安全现状

随着公安行业信息化的发展，由于信息系统普遍缺失数据安全保护的能力，数据在信息系统中不停流转时容易面临安全威胁：

- 大量的数据集中存储面临着被拖库的风险；
- 数据在交互、共享、流转中，由于政法及涉密工作人员等都会接触到敏感信息，容易造成数据泄露。

因此，必须采用密码等新技术实现对信息系统数据全生命周期的安全保护，同时建立健全的网络管理制度，提升公安网络系统的管理水平。

4、公安行业密码应用要求

《信息安全等级保护管理办法》提出对信息系统安全保护分五个等级实行安全保护、监督、管理。

依据《信息安全等级保护商用密码技术要求》和《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，从管理和技术两个方面来规范和促进信息安全等级保护制度的全面落实。分别对一级至四级信息系统安全保护的从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出

基本技术要求。依靠密码技术的支撑来实现身份的真实性、行为的抗抵赖、内容的机密性和完整性。

2.2.3.7. 住建行业密码应用要求

1、住建行业系统概述

2016 年国家重点推进“互联网+政务服务”、政府资源信息共享和政务信息公开，强调政府工作由管理向服务转型，不断提高政府效能。有效落实“让数据多跑路，让群众少跑腿”的主动服务思想，最大限度的方便广大房地产相关企业和公众办理房地产交易各项业务。

各地市住建局为加强对房地产市场的监管，借助先进的信息化技术，建立全市统一的智慧房产平台，加强对房地产市场实时监测、分析预警功能，同时预留与其他部门系统间的数据交换接口，满足市级政府资源共享和大数据应用的要求。提高全市房地产行业的管理效率和社会服务水平。

2、住建行业的重要标准规范

- 《CJJT115-2007-房地产市场信息系统技术规范》
- 《建筑及居住小区门禁系统应用方案》
- 住房和城乡建设部《2011-2015 年建筑业信息化发展纲要》(建质〔2011〕67 号)
- 《2016-2020 年建筑业信息化发展纲要》
- 《促进建筑业业务可持续健康发展的意见》（2017）
- 《基于国产密码算法的城市物联网密钥管理系统规划方案》
- 《基于窄带物联网（NB-IoT）的道路照明智能控制系统技术规范》

- 《建筑智能化系统运行维护技术规范》
- 《住房和城乡建设部等部门关于加快发展数字家庭 提高居住品质的指导意见》（建标[2021]28号）
- 《中华人民共和国住房和城乡建设部文告》2021年第4、5期

3、住建行业信息系统安全现状

随着物联网和大数据技术与住建行业的深度融合，不断催生了智慧社区、智能汽车、智能家居等领域的发展。2018年，住房和城乡建设部信息中心组织开展了基于国密算法的城市物联网密钥管理系统的升级工作。推动了城市物联网安全体系应用到智能门锁、民用三表管理等领域的发展。

为了保障住建行业信息化安全建设和发展，在城市基础设施信息系统、面向社会服务的政务信息系统、行业性业务系统和办公系统中应加强密码应用。

4、住建行业密码应用要求

住建行业信息系统的规划、建设实施和验收除应符合本行业相关规范外，尚应符合国家现行有关标准的规定。要求使用符合国家密码法律法规和标准规范的密码算法和密码产品，实现密码在本领域的全面应用。

根据《中华人民共和国住房和城乡建设部文告》，在完善数字家庭系统建设中强化网络和数字安全保障。数字家庭系统应同步规划、同步建设、同步使用网络安全技术。采取密码技术等必要措施，保障数字家庭系统安全稳定运行，防止信息泄露、损毁、丢失，确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可控完整的产业生态系统。

在智慧社区建设方面，根据《基于国产密码算法的城市物联网密钥管理系统规划方案》，在家居、建筑、门锁、门禁、三表等多场景应用加装行业级国密安

全模块，实现智能终端间互联互通。保障设备与平台、平台与平台间的身份认证和加密传输，保障数据安全。

2.2.3.8. 交通行业密码应用要求

1、交通行业概述

交通运输行业作为国民经济的基础产业，大力推动信息化建设对于促进交通运输又好又快发展具有重要的意义。交通运输行业信息化涉及综合运输、公路交通、水路交通、民用航空、邮政服务及城市客运管理等各个方面。

随着交通信息化、便捷化的不断推进，精准感知、精确分析、精心服务的交通功能体系和网络安全体系将被打造。建设交通运输领域新型基础设施过程中，ETC、城市交通一卡通、电子证照等系统将与商用密码技术不断融合，商用密码应用在交通运输领域正在迎来前所未有的发展机遇。

2、交通行业的重要标准规范

- 欧盟 EDPB《车联网个人数据保护指南》
- 《汽车数据安全若干规定（试行）》
- 交通运输部《关于进一步开展交通运输行业信息安全等级保护工作的通知》（厅科技字[2012]120号）
- 《GB T 37378-2019 交通运输 信息安全规范》
- 《交通运输行业信息系统安全等级保护基本要求》（征求意见稿）

3、交通行业信息安全现状

回顾交通运输行业“十三五”信息化发展建设历程，公路水路交通基础设施运行管理系统建设使得通行效率明显提高；行业公共信息服务平台建设使得信息

服务水平明显提升；交通安全监管和应急系统建设使得保障能力明显提高；信息化发展条件建设使得发展环境明显改善。

但信息化的安全保障建设方面暴露了一定的不足：

- 已有系统的安全机制由于技术不断进步变得不再安全；
- 各业务系统的信息安全建设相互独立，只能“一卡单能”，导致重复建设，缺乏行业统一规划。
- 物联网等新技术也对行业信息安全带来了新挑战，主要是用于信息数据的获取的感知节点的安全问题。

4、交通行业密码应用要求

根据《交通运输行业信息系统安全等级保护基本要求》，交通行业三级系统密码应用需满足以下要求：

1) 构建统一身份认证体系

应采用密码技术对信息系统配套的各种户外感知节点、数据采集终端、室外无线接入设备进行接入认证，确保非法节点不能接入。

登陆系统的用户，采用鉴别技术进行身份标识和鉴别、访问控制等功能。使用口令时，口令在存储和传输时加密保护。

2) 网络通信安全

通过互联网、信息专网、无线短程通信网、GPRS 网和卫星网等网络通信时，应采用密码技术或可靠的身份认证技术保证通信过程中数据的完整性。应对通信过程中的整个报文、会话过程或关键报文进行加密。实现通信过程中的完整性和保密性保护。

3) 数据传输和存储安全

通过互联网、信息专网、无线短程通信网、GPRS 网和卫星网等网络传递数据，应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。

与客运票务、资金收取与使用、调查与统计和行政与执法相关的业务数据信息，在存储时应加密。

4) 密码安全管理

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

5) 设备安全技术要求

载运装备单元等设备应具有唯一性标识，进行自身身份标识。与其他系统、终端或智能 IC 卡进行传输和通信时，应确保数据的保密性、完整性和可用性。

2.2.3.9. 水利行业密码应用要求

1、水利行业概述

水利是国民经济和社会发展的基础设施和基础产业。近年来可持续发展水利思路指明了以水利信息化带动水利现代化发展。水利信息网络的建设可为各种水利应用系统提供统一的数据传输平台。

水利十大重点业务系统包括国家防汛抗旱指挥系统、水利电子政务信息系统、水资源管理决策支持系统、水土保持检测与管理信息系统、水质监测与评价信息系统、全国水利工程管理信息系统、全国农村水利水电及电气化管理信息系统、水利信息公众服务系统、全国水利规划设计管理信息系统和数字化图书馆。

2、水利行业的重要标准规范

- 《全国水利信息化发展"十二五"规划》

- 《第一次全国水利普查数据处理实施方案》
- 《水利网络安全管理办法（试行）》
- 《水利网络安全事件应急预案》
- 《SL/T 799—2020 水利数据目录服务规范》
- 《SL/T 797—2020 水利空间数据交换协议》
- 《SL/T 801—2020 水利一张图空间信息服务规范》
- 《水利信息化资源整合共享顶层设计》
- 《水利信息化资源整合实施方案》
- 《数据存储类 | 水利工程建设与管理数据库表结构及标识符
SL700-2015》
- 《数据存储类 | 水利空间要素数据字典 SL729-2016》
- 《运行维护类 | 水利信息网网络管理规程 SL444-2009》
- 《运行维护类 | 水利数据中心管理规程 SL604-2012》
- 《建设管理类 | 水利信息网建设指南 SL434-2008》
- 《水利信息资源共享管理办法（试行）》
- 《水利关键信息基础设施认定规则》
- 《"十四五"水利网信建设实施方案》
- 《2019 年全国水利网信发展报告》
- 《水利关键信息基础设施网络安全建设指导意见》
- 《水利部密码应用与创新发展实施方案（2018-2022 年）》
- 《2020 年水利网信工作要点》(办信息〔2020〕22 号)

3、水利行业信息系统安全现状

随着数字化、网络化的快速发展，数字水利及水资源管理体系等信息化水利建设过程中，网络安全和数据安全问题也逐渐增多，水利信息体系所称承受的安全风险也随之增加。需要采用先进的密码等安全技术，加强对水利信息化安全体系的建设、运维和管理工作的。

4、水利行业密码应用要求

2020年2月14日，国家水利部印发《2020年水利网信工作要点》(办信息〔2020〕22号)，明确了2020年水利网信工作的26项重点工作。重点做好水利信息系统等保达标、应用系统安全防护、关键信息基础设施保护等工作。

针对水利行业信息系统商用密码的应用提出：组织宣贯《密码法》，开展水利行业密码应用专题调研，出台推进商用密码应用具体措施。落实《水利部密码应用与创新发展实施方案》，持续推进三峡水利枢纽、南水北调工程等重要水利基础设施和国家水资源管理系统等重要信息系统的密码应用。开展水利行业重要信息系统等保定级、备案和测评工作。完成水利部机关政务内网分级保护风险评估工作。

2.2.3.10. 医疗行业密码应用要求

1、医疗行业概述

近年来，医疗行业信息化得到全面快速发展，互联网、大数据、云计算等新兴技术与传统医疗不断深化融合，促进了医疗服务水平提升。在今年新型冠状病毒肺炎疫情防控期间，许多医院、基层医疗卫生机构、专业公共卫生机构等通过互联网提供在线问诊、智能问药、药品快递到家等服务，减少了接触传染的风险，增强了就医的便捷性，提高了优质医疗资源的利用效率。与此同时，医疗行业面

临的网络安全风险也逐渐增多。虽各方高度重视，但我国医疗行业网络安全仍处于工作起步较晚、整体风险较高、防护水平相对落后的局面，网络安全形势不容乐观。

2、医疗行业的重要标准规范

- 《GB / T 39725-2020 信息安全技术 健康医疗数据安全指南》
- 《医疗行业网络安全白皮书（2020 年）》
- 《移动互联网医疗安全风控白皮书（2020 年）》
- 《关于印发全国医院信息化建设标准与规范（试行）的通知》
- 《关于印发全国基层医疗卫生机构信息化建设标准与规范（试行）的通知》

3、医疗行业信息系统安全现状

医疗行业网络安全是我国网络安全的重要组成部分，受到国家高度重视。随着医疗行业信息网络技术的深入应用和“互联网+医疗健康”的不断推进，党中央、国务院及医疗监管部门陆续出台了一系列信息化安全建设与管理的政策法规，逐步完善医疗行业网络安全体系。

4、医疗行业密码应用要求

根据 2018 年 4 月，国家卫生健康委发布的，针对二级及以上医院的数据中心安全、终端安全、网络安全及容灾备份提出要求。《关于印发全国医院信息化建设标准与规范（试行）的通知》

根据 2019 年 4 月，国家卫生健康委发布《关于印发全国基层医疗卫生机构信息化建设标准与规范（试行）的通知》，明确了基层医疗卫生机构未来 5-10 年信息化建设的基本内容和要求。其中信息安全部分包括身份认证、桌面终端安全、

移动终端安全、计算安全、通信安全、数据防泄露、可信组网、数据备份与恢复、应用容灾、安全运维等 10 个方面。

2.2.3.11. 各地区密码应用政策要求

各地区各部门按照《密码法》要求，不断加大密码应用推进力度。基础信息网络、重要信息系统、重要工业控制系统和政务信息系统等重要领域密码应用持续深化，密码技术积极护航 5G、云计算、物联网等新基建安全发展，为网络空间安全秩序提供了高质量的密码技术和服 务。同时各地区也推出了密码应用相关政策，列举如下：

- 2004 年 7 月 30 日，《湖南省信息化条例》作为全国第一部信息化的地方性法规，在湖南省正式实施。
- 《珠海市市级政务信息化项目商用密码应用工作指引》，以此开展商用密码应用安全性评估工作。
- 2016 年 11 月 2 日，江苏省商用密码产业协会会员大会在无锡召开，会议就重要领域密码应用工作相关情况进行了介绍。
- 2017 年，国家密码管理局要求对广东、四川、云南等 7 个省市推进政务云密码应用示范，期望形成密码应用的范例。对以政务云为基础的智慧城市实施全面的网络和数据安全保护。
- 2019 年 7 月 18 日，深圳举办“基于国密算法的物联网密钥管理系统在智能门锁应用技术交流会”。提升智能门锁行业信息安全，推动国密算法在智能门锁行业的应用。

- 2019 年 10 月 23 日，北京市密码管理局组织编写《北京商用密码发展报告》，为推动北京商用密码事业发展，全面系统梳理北京商用密码产业情况。
- 2021 年 3 月 17 日，海南省国家密码管理局等 6 部门联合发布《关于进一步明确省政务信息化项目密码应用有关要求的通知》。

2.3. 密码技术筑牢数字安全屏障

针对需求侧产生的供给高质量密码产品的需求，同时，信息技术、监管侧也发生了强烈变化，这些推动了密码产品供给侧的演进与升级，而信创又给国产密码发展带来了新契机。密码产品供给侧应当抓住这个窗口期，做强做优商用密码产业，夯实筑牢网络安全基石，保驾护航数字经济发展。

2.3.1. 密码技术进步促进应用融合

一是密码和业务应用融合。传统密码产品开发改造应用的密码集成模式门槛高、周期长、风险大，用户面临“难用、难管”，很难将密码能力深度融合到信息系统，而业务应用改造也正是密码防护和密评整改的难点，与金融、交通、医疗等行业应用场景紧密结合的密码需求也会更加细化。业内提出基于“面向切面安全”的密码中间件模式，将安全与业务在技术上解耦、但又在能力上融合交织，提供轻量级改造应用的密码应用实施模式，有效防护企业应用与数据，让密码“好用、好管”。

二是一体化的密码平台集约建设。企业业务需求持续变化决定了企业应用系统复杂多样，而在密码全方位应用要求背景下，针对每个应用分别实施密码防护会面临技术、管理等挑战，因此，亟待结合企业数字化现状和具体问题，遵循统一标准体系，建设统一密码平台，实施统一安全防护，落实统一运维监管，打造一体化的密码支撑体系。

2.3.2. 信息技术升级促进产品演进

一是新一代信息技术加速促使密码产品演进。例如云模式交付拉动密码产品向“云原生”发展，从传统密码产品以硬件为主，转向侧重软件形态的软硬均衡，而新发布的密评国标 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》也规范了密码软件合规要求，属于政策对密码软件形态的引导鼓励。类似的，大数据对加解密性能提出更高要求，物联网对密码产品形态要求更灵活等。

二是信创带来历史机遇，国产密码本身就是信创产业的核心部分，密码又能为蓬勃发展的信创产业保驾护航，所以，适配优化信创平台、在信创安全体系中全面应用密码等新需求对密码产品形态会产生深刻影响。

三是兼容新的国际技术标准。当前，国密算法已逐步进入国际标准，展望未来，从上游的网络协议及规范，到中游的网络协议栈实现、软件开发工具链，硬件密码模块，再到下游的基础软件和应用软件，国密将逐步融入这些标准。随着中国科技企业进入海外市场，中国密码技术也将“走出去”。

2.3.3. 攻防演练对抗促进实战发展

一是密码安全一体化。数据加密只是把明文安全问题转移到密钥安全问题，但是如果没有结合业务的密钥访问控制，防护价值非常有限。过去，由于市场准入等因素，密码和安全技术在建设落地时相对分离，但是，随着密码“放管服”落实以及监管侧改革，“以密码技术为核心、多种安全技术相互融合”将成为主流思路，并统筹实施等保与密评。通过加密技术，为流转的数据重新定义了虚拟防护边界，在边界上施加访问控制、审计等技术，实现“防绕过的访问控制”以及“高置信度审计”，进一步集成企业 IAM 身份认证管理，打造同时满足传统场景和零信任场景的有效数据保护。

二是加强密码产品自身安全保护。这是威胁对抗常态化带来的必然要求，密码厂商会更加重视密码产品研发和生产等全生命周期中的安全，同时，监管机构也提高了密码产品的安全性检测认证要求，用“安全的密码产品”有效保护企业数字化安全。

三是多重需求拉动密码服务蓬勃发展。过去，合规主导的密码市场侧重产品本身，而当下企业更注重有效防护，要将安全产品转化为有效防护能力，需要提供服务，尤其是结合安全运维，所以，密码交付形态正在从“以产品为主”演进为“产品与服务相结合”。

2.3.4. 数据要素市场促进密码创新

数据作为新的生产要素，对全面释放数字红利、占领数字经济全球竞争制高点具有战略意义。与此同时，数据生产要素具备自身特性，例如难以从技术上分

割使用权和所有权,而通过创新的密码技术和方案可实现多个企业或机构间的数据共享互联,具有广阔发展空间。

一是“软硬兼备”的密码产品形态将成未来的主流。从目前国际密码产品的发展情况来看,国内密码产品的走向也将会朝着“软硬结合,以软为主”的方向发展,从机卡 Key 等强调安全合规性,到“识别和防护”的实战化安全产品将百花齐放,内嵌式密码产品或将成为市场主流。

二是隐私增强计算技术,例如联邦学习、安全多方计算、机密计算、差分隐私、同态加密等,实现“数据可用不可见”。

三是基于密码的新兴信息技术,例如区块链,就是加密技术、分布式网络、智能合约等多种技术集成的新型数据库软件,通过数据透明、不易篡改、可追溯,有望解决数据生产要素化的信任和安全问题。

四是结合传统密码技术和多种安全保密技术,使数据在共享时实现“最少可用原则”和“最小权限原则”,让数据在业务系统中实现共享与安全兼得。

2.4. 业务视角归纳密码应用模式

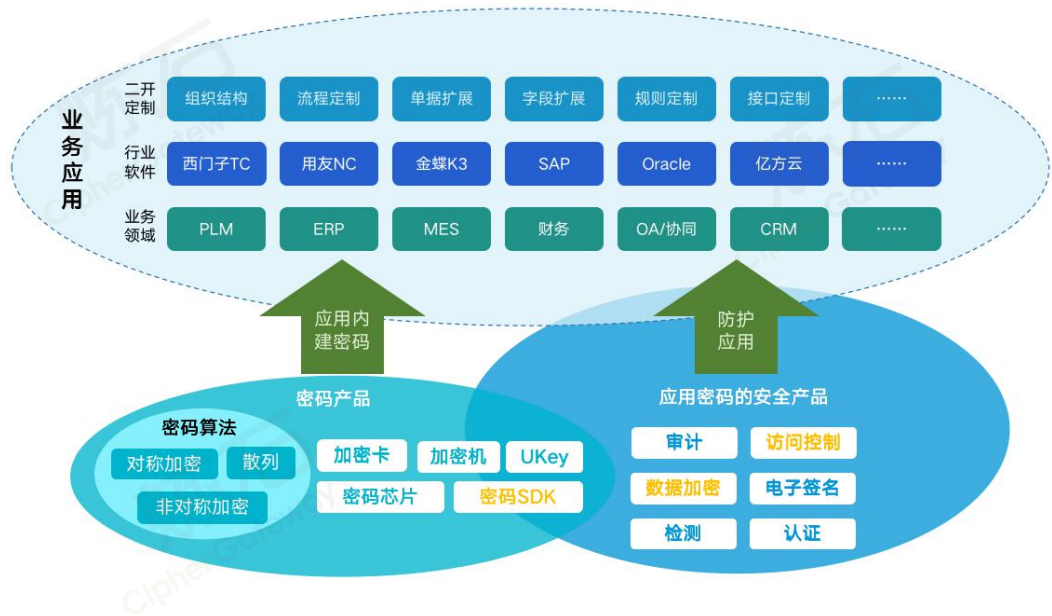


图 3 密码产业组成示意图

如上图所示，商用密码产业由密码算法（研究机构）、密码产品（密码厂商）、含密安全产品（安全厂商）以及密码应用产品（各种使用密码功能的业务应用系统开发商）组成。从密码算法到最终的密码应用，各个环节都将密码技术进行“叠加封装”，最终形成丰富的密码产品。

采用密码产品的目的就是将在各种应用场景中发挥密码的作用，达到安全防护的目标。而在密码应用的实战过程中，不同的使用场景中类似的密码应用模式会反复出现，本白皮书将这些反复出现的密码应用模式进行了提炼总结，针对每种模式进行了威胁分析、模式说明以及典型应用的示例说明，使密码技术使用者能够在密码应用中快速定位要采用的密码解决方案。

表 4 20 种密码应用实战模式汇总

	身份鉴别及密钥管理	数据传输(通信安全)	数据存储(数据资产安全)	数据使用(数据共享与安全兼得)
应用层	③ 预共享密钥的身份鉴别 ④ 基于数字签名的身份鉴别 <ul style="list-style-type: none"> - 基于单一设备签名的身份鉴别 - 协同签名 - 阈值签名 	⑤ 离线通信消息加密 <ul style="list-style-type: none"> - PGP邮件加密 - S/MIME邮件加密 - Signal/OTR聊天加密 ⑥ 代理重加密受控分发消息	⑨ 应用内数据加密 <ul style="list-style-type: none"> - 应用内开发集成加密 - CASB代理网关加密 - AOE面向切面加密 	⑫ 基于差分隐私的数据匿名化 ⑬ 基于属性加密的访问控制 ⑭ 锚点解密的防绕过数据安全 <ul style="list-style-type: none"> - TDF可控分享秘密信息 ⑮ 不可信环境中的数据运算 <ul style="list-style-type: none"> - FHE全同态加密 - MPC多方安全计算 - ZKP零知识证明、区块链隐私保护 ⑯ 可验证结果的计算外包 ⑰ 封装业务逻辑的可信运算环境 <ul style="list-style-type: none"> - 金融数据密码机
终端与基础设施层		⑦ 在线通信消息加密 <ul style="list-style-type: none"> - 基于SSL/TLS的HTTPS - VPN虚拟专用网络 - 链路密码机/网络密码机 ⑧ 可感知窃听的专线通信 <ul style="list-style-type: none"> - BB84量子密钥分发 	⑩ 数据库存储加密 <ul style="list-style-type: none"> - DB-Proxy数据库代理加密 - 数据库UDF开发集成加密 - 数据库外挂加密 - TDE透明数据加密 ⑪ 文件存储加密 <ul style="list-style-type: none"> - TFE透明文件加密 - FDE全磁盘加密 	⑱ 基于密码的数字水印追溯
基础密码产品	① PKI信任体系 <ul style="list-style-type: none"> - CA证书认证系统 - 安全认证网关 ② IBC信任体系			⑲ 基于密码校验的防篡改 <ul style="list-style-type: none"> - 电子签章 ⑳ 基于私钥签名的责任认定 <ul style="list-style-type: none"> - 签名验签服务器

如上表中所述，在身份鉴别及密钥管理、数据传输、数据存储以及数据使用的阶段，提炼总结出 20 种密码应用模式，密码技术主要用于身份鉴别、传输安全、存储安全、使用安全等场景，本章节将进行详细说明。

（一）身份鉴别及密钥管理

2.4.1. PKI 信任体系

2.4.1.1. 模式说明

2.4.1.1.1. 威胁分析

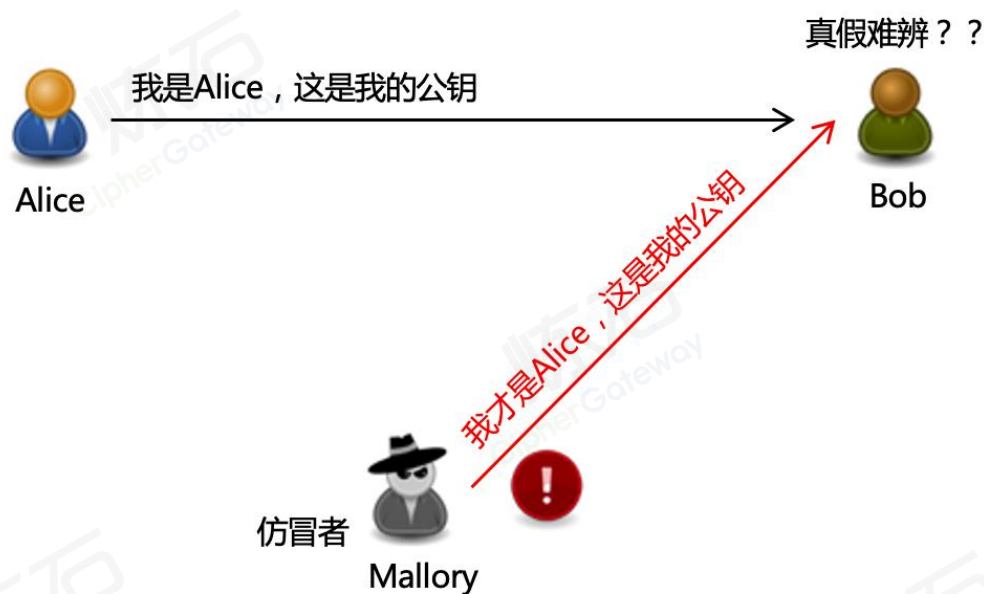


图 4 信任体系威胁示意图

Alice 与 Bob 预先交换公钥，但 Mallory 仿冒 Alice 也可以与 Bob 交换公钥，而 Bob 并不能辨认出 Mallory 是仿冒的。也就是说，网络用户之间无法识别对方的身份，容易被攻击者仿冒，这种线下预先交换公钥的方式，具有很大局限性。在缺少权威证书颁发机构的情况下，身份容易被攻击者仿冒。

2.4.1.1.2. 防护模型

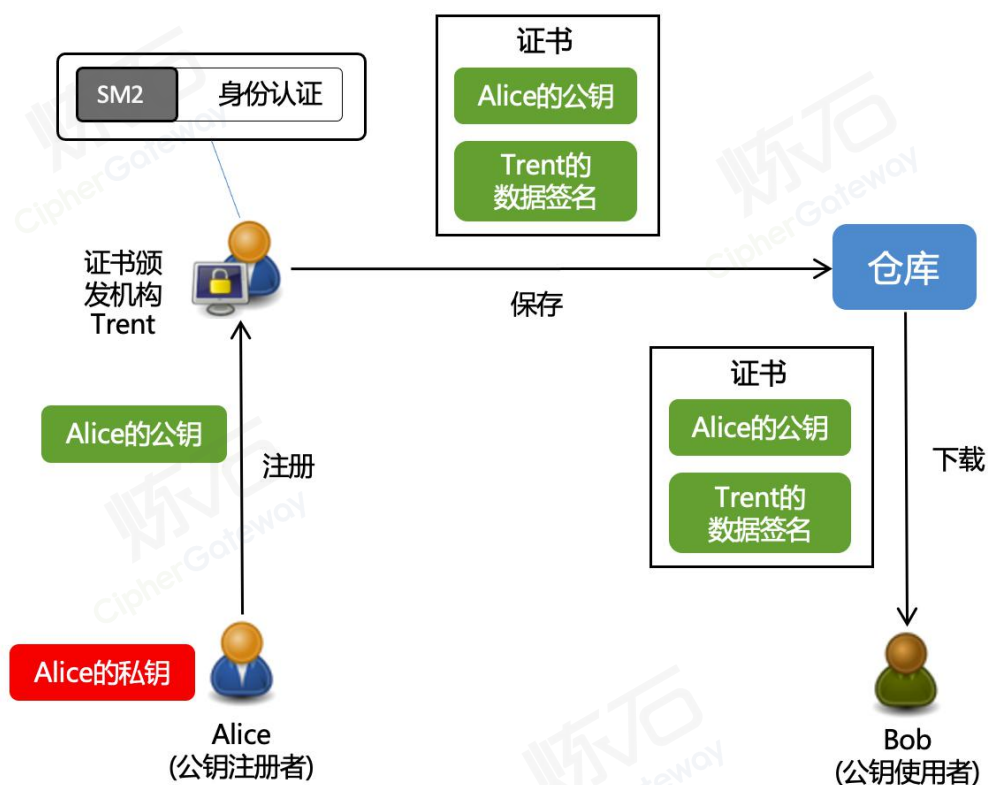


图 5 信任体系 PKI 防护模型示意图

标准的 PKI 组成要素包括^[57]:

1. 用户——使用 PKI 服务的人;
2. 认证机构——颁发证书的人;
3. 仓库 (Repository) ——存储证书的数据库。

如图中所示, Alice 和 Bob 是 PKI 服务的使用者, Alice 是公钥注册者, Bob 是公钥使用者:

【Alice 要做】

- 生成密钥对

- 在认证机构注册公钥
- 向认证机构申请证书
- 根据需要申请作废已注册的公钥
- 解密接收到的密文
- 对消息进行数字签名

【Bob 要做】

- 将消息加密后发送给接收者
- 验证数字签名

Trent 是认证机构，对证书进行管理，要做的操作：

- 生成密钥对
- 在注册公钥时对本人身份进行认证
- 生成并颁发证书
- 作废证书

仓库（Repository）是保存证书的数据库，PKI 用户在需要的时候可以从其中获取证书，Bob 获取 Alice 的证书就可以从仓库中下载。

在政策的指引下，目前 PKI 的供应商均能够提供基于国密 SM2、SM3、SM4 算法实现的产品，用户可以选择该类产品满足合规要求。

2.4.1.2. 典型应用示例

PKI 信任体系的典型应用是基于 PKI 的身份认证系统。

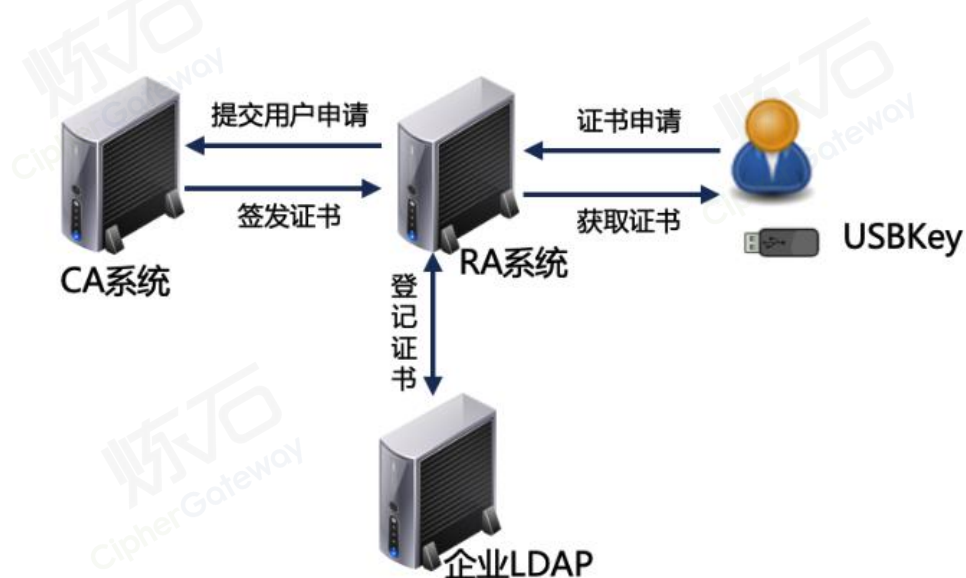


图 6 用户申请证书过程示意图

在身份认证系统中，用户需要先申请证书。过程为：

- (1) 用户向注册中心（RA）提交证书申请；
- (2) 注册中心对用户身份进行审核；
- (3) 注册中心将审核后的用户证书申请请求提交认证机构（CA）；
- (4) 认证机构签署证书并且颁发用户证书，并将证书存储到企业 LDAP 目录服务器中，并存入证书数据库中，以供用户查询；
- (5) 用户会得到存储了个人证书的 USBKey，同时存储的还有用户的私钥。

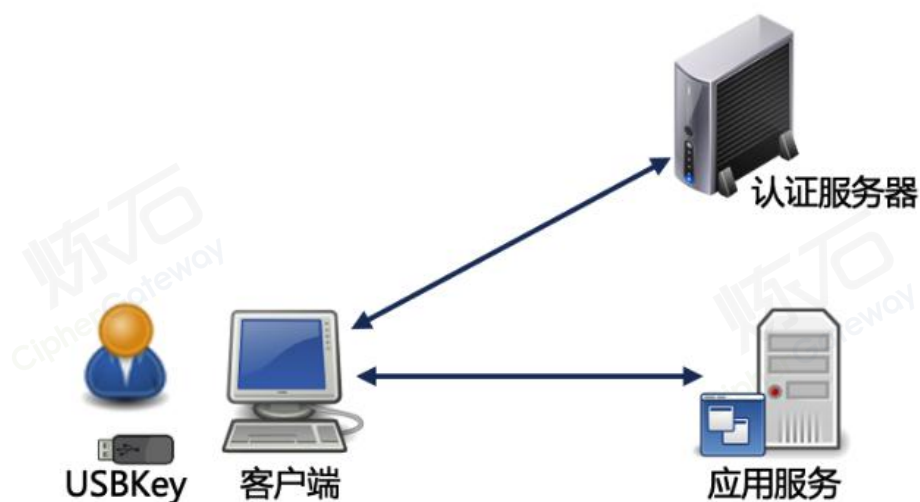


图 7 用户使用证书过程示意图

用户使用 USBKey 进行身份认证登录应用系统的过程如下：

- (1) 用户在客户端插入 USBKey，输入用户名、PIN 码以及动态验证码（服务端随机生成，一次性有效，防范重放攻击）；
- (2) 对服务端随机生成的验证码进行签名，并将验证码、签名数据、用户名一起提交服务端认证；
- (3) 服务端接收到数据后，通过用户名定位到用户证书；
- (4) 服务端使用用户证书对签名数据进行验签，如果验证通过，则证明是合法用户，通过了身份认证，同时对随机验证码进行重置，防止重复使用；
- (5) 用户可成功登录应用系统。

2.4.2. IBC 信任体系

2.4.2.1. 模式说明

2.4.2.1.1. 威胁分析

威胁同 PKI 信任体系，需要防范身份仿冒问题。

2.4.2.1.2. 防护模型

虽然 PKI 是一种构建网络信任体系和提供公钥信息安全服务的主流解决方案，拥有技术成熟、适用于大规模部署等诸多优点，但也存在困扰其发展的问题：PKI 用户之间需要交换数字证书，为了减少数字证书的管理开销，IBC 信任体系被提出^[20]。

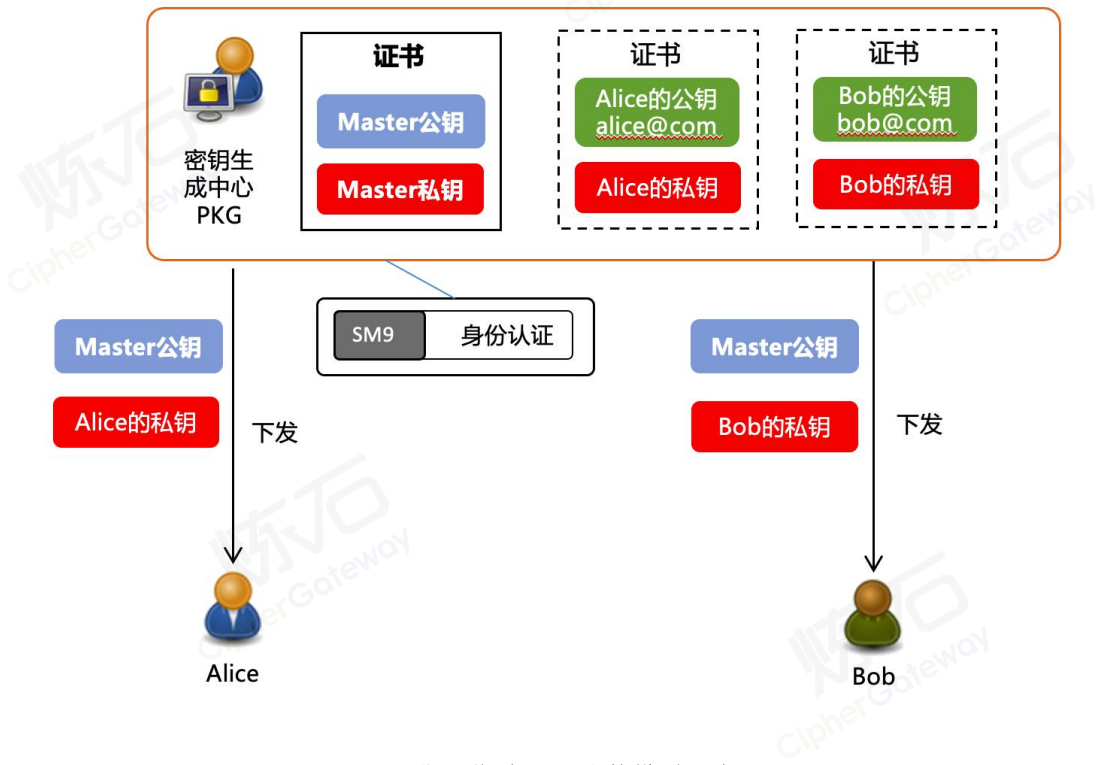


图 8 信任体系 IBC 防护模型示意图

在 IBC 信任体系中，可以将用户的公开信息，如 Email 地址、姓名、手机号码等直接作为公钥，从而避免了 PKI 中与证书相关的复杂操作，用户私钥有私钥中心（Private Key Generator，PKG）根据公钥集中产生并分发，管理与维护相对简单。

在 IBC 信任体系中，Alice 和 Bob 各自可向 PKG 申请私钥并妥善保管，Alice 和 Bob 可以将对方的公开信息，如 Email 地址等作为对方的公钥，无需再向“仓库”申请。双方可以直接使用“挑战——应答机制”确认对方的身份，认证过程为：

- （1）Alice 与 Bob 建立连接；
- （2）Alice 向 Bob 发送请求，并发送 Email 地址（Alice 公钥）；
- （3）Bob 生成随机数作为挑战报文返回给 Alice 进行挑战；
- （4）Alice 使用自身私钥对挑战报文进行签名，返回给 Bob；
- （5）Bob 使用 PKG 的主公钥和 Alice 的公钥（Email）进行签名验证；
- （6）验签通过，则可确认 Alice 身份，可以进行通信；
- （7）验签不通过，则 Alice 身份未通过确认，立即终止连接。

IBC 需要构建安全通道为用户传递私钥，因而使用环境受到一定限制，此外，存在着集中产生私钥带来的密钥托管问题，由于用户自己无法产生私钥，难以实现不可否认性业务^[21]。

2.4.2.2. 典型应用示例

IBC 信任体系的典型应用是基于 IBC 的安全邮件。

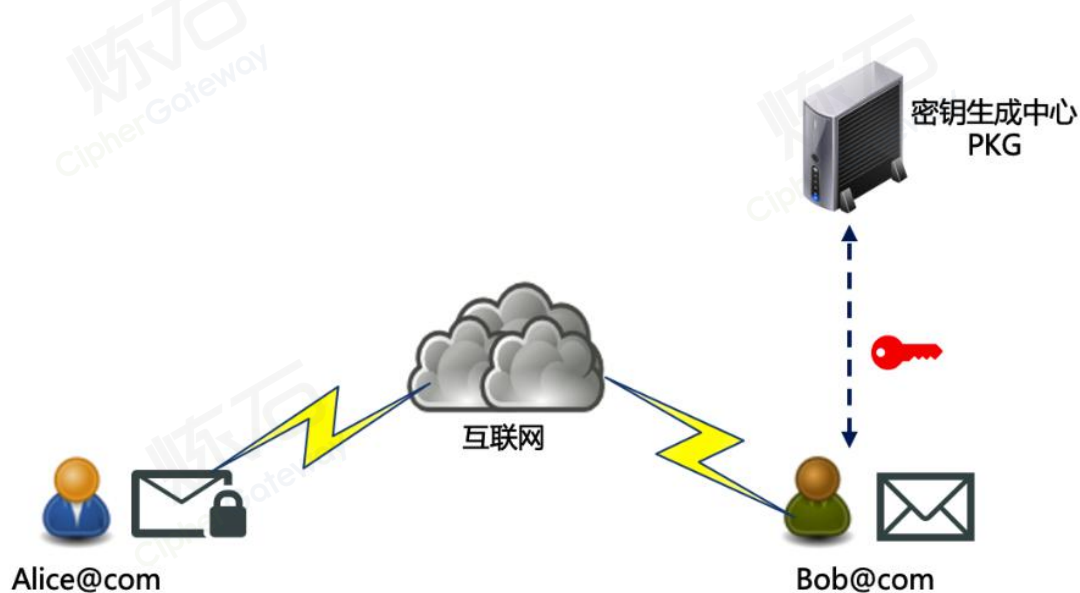


图 9 基于 IBC 的安全邮件示意图

Alice 通过 IBC 安全邮件方式向 Bob 发送邮件的过程为：

- (1) Bob 先从密钥生成中心 PKG 中，认证并申请 bob@com 对应的私钥；
- (2) Alice 直接使用 Bob 的邮件地址 bob@com, 作为 Bob 的公钥对邮件内容进行加密；
- (3) Alice 将密文邮件发出；
- (4) Bob 接收到密文邮件；
- (5) Bob 使用私钥对密文邮件进行解密，得到明文内容。

2.4.3. 预共享密钥的身份鉴别

2.4.3.1. 模式说明

2.4.3.1.1. 威胁分析

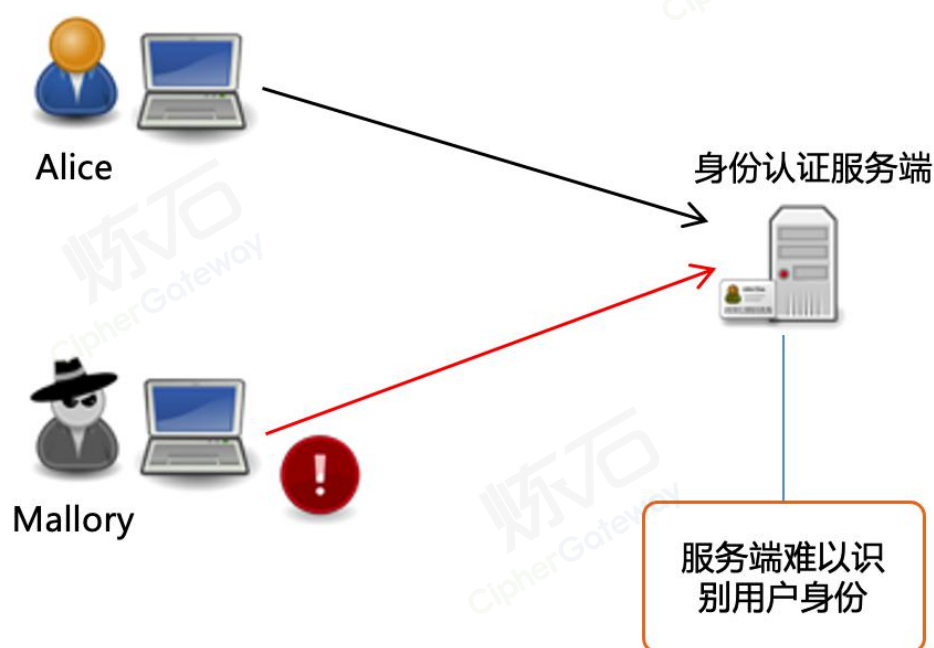


图 10 身份认证威胁示意图

合法使用者 Alice 在使用服务之前，需要先进行身份认证，通过后才可以使用服务。攻击者 Mallory 可以伪装成 Alice 向服务端发起请求；或者 Mallory 伪装成服务端，来应答 Alice 的请求。如果远程访问服务器上的预共享密钥发生更改，则手工配置预共享密钥的客户端将无法连接到该服务器上，需要重新配置。而在身份认证过程时，一般需要用户手动输入预共享密钥，安全性较差。

2.4.3.1.2. 防护模型



图 11 预共享密钥防护模型示意图

Alice 和服务端预先共享密钥（PSK），并通过“挑战——应答机制”实现双方的身份认证。认证过程为：

- （1）Alice 向服务端发送身份标识；
- （2）服务端返回一个随机数作为挑战；
- （3）客户端用 PSK 加密随机数，并将密文作为应答返回给服务端；
- （4）服务端接收到应答消息并解密验证，可确认 Alice 的身份。

预共享密钥的身份鉴别机制需要保证预共享密钥的安全，可以使用国密 SM3、SM4 算法进行实现，通过通信双方预共享密钥，实现双方的身份鉴别，最终完成安全通信。

2.4.3.2. 典型应用示例

预共享密钥的身份鉴别模式的典型应用是，Windows Server 的远程访问。

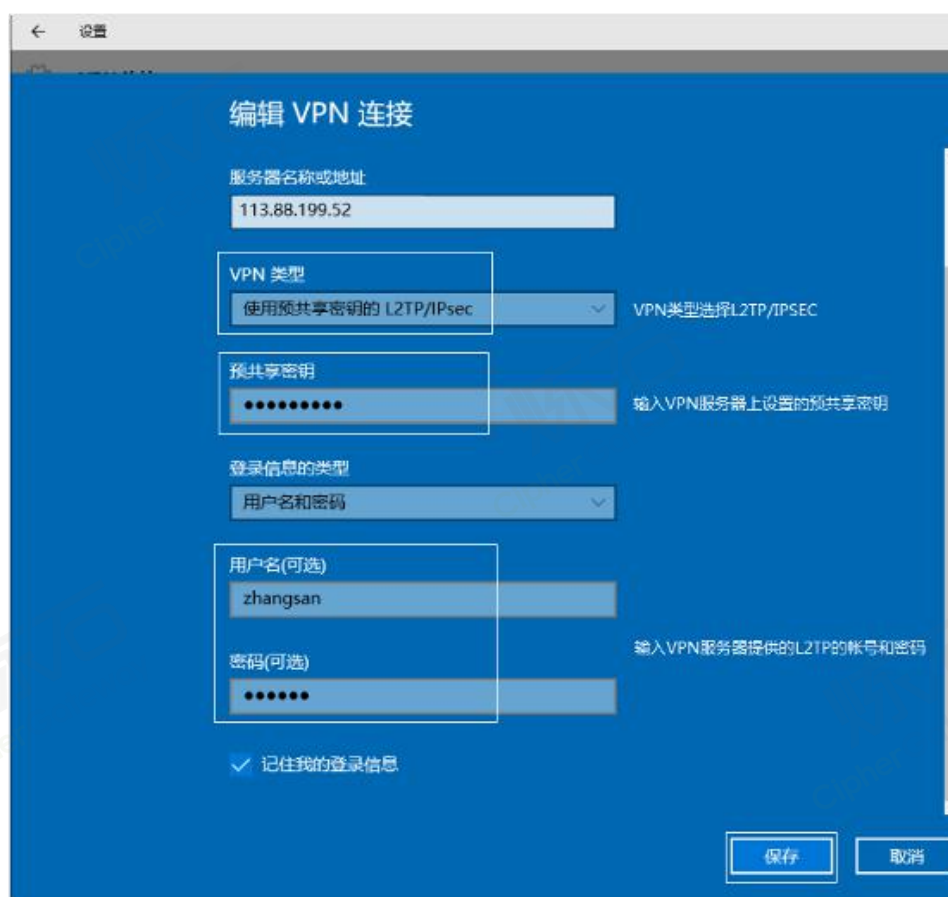


图 12 Windows 中基于 L2TP/IPSec 的 VPN

Windows 中基于 L2TP/IPSec 的 VPN 即采用了预共享密钥的认证机制，可以通过配置“路由和远程访问”来验证支持预共享密钥的 VPN 连接。许多操作系统都支持使用预共享密钥，包括 Windows Server 2003 家族和 Windows XP 等。也可以

配置运行 Windows Server “路由和远程访问”的服务器，使用预共享密钥验证来自其他路由器的连接。

2.4.4. 基于数字签名的身份鉴别

2.4.4.1. 基于单一设备签名的身份鉴别

2.4.4.1.1. 模式说明

1. 威胁分析

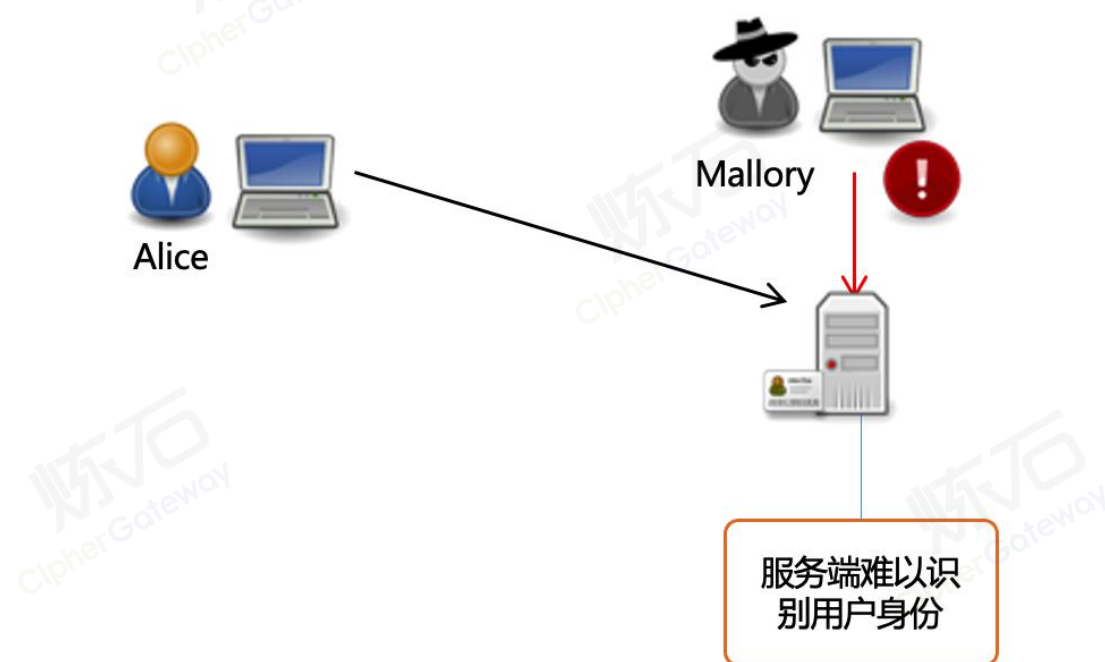


图 13 基于单一设备签名的身份鉴别威胁示意图

攻击者 Mallory 可以伪装成 Alice 向服务端发起数据访问请求，而服务端难以识别伪装的用户身份。Alice 存在较高的身份凭证丢失的风险，如果 Alice 使用了弱口令，也很容易被 Mallory 破解并仿冒。

2. 防护模型

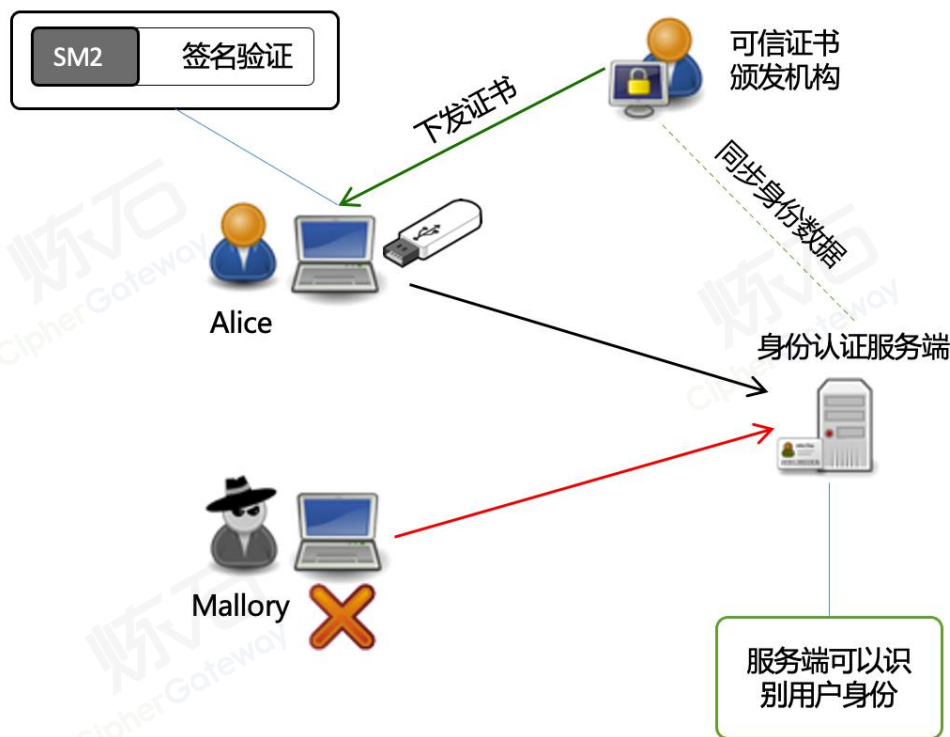


图 14 基于单一设备签名的身份鉴别防护模型示意图

基于 PKI 体系由可信证书颁发机构，向 Alice 下发证书（以 USBKey 形式），并向身份认证服务器同步 Alice 的身份数据。Alice 使用 USBKey 进行身份认证过程为：

- （1）Alice 插入 USBKey，并输入用户名和 PIN 码；
- （2）USBKey 中含有用户私钥，对服务端随机生成的验证码进行签名得到签名数据，并将用户名、验证码和签名数据一起发送给服务端；
- （3）服务端根据用户名获取用户签名证书；
- （4）服务端对验证码进行验签，如果验证通过，则证明 Alice 是合法用户，身份认证通过。

基于单一设备签名的身份鉴别可采用以 SM2 为主的国密算法进行实现，可保证用户与服务端之间的通信安全。

2.4.4.1.2. 典型应用示例

基于单一设备签名的身份鉴别的典型应用是银行 U 盾的使用。

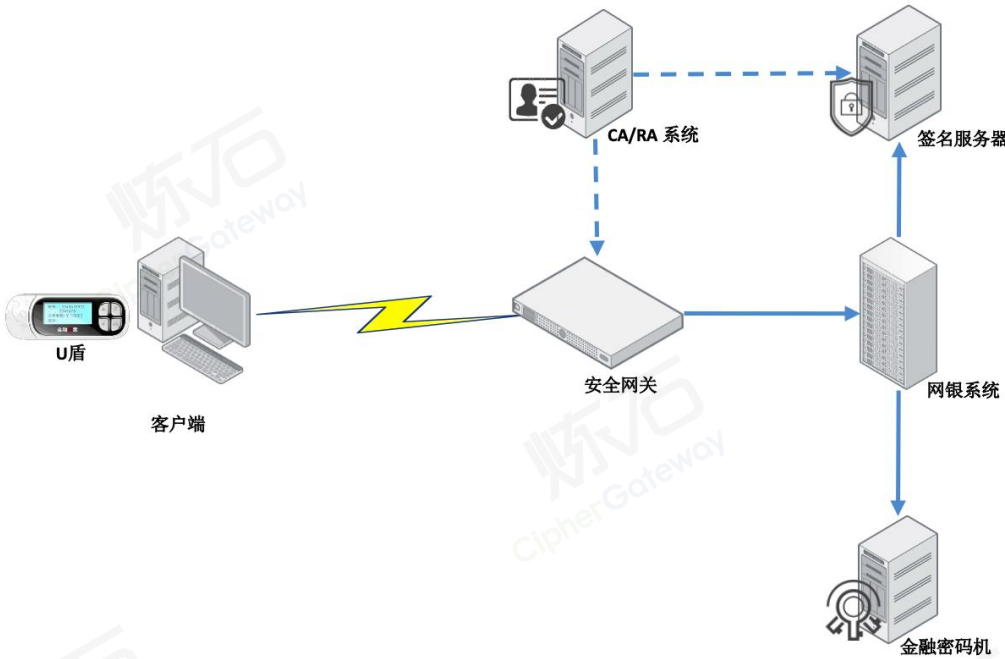


图 15 银行 U 盾使用过程示意图

在银行给客户分发的 U 盾中，存储有客户个人的数字证书和私钥，U 盾的控制芯片被设计为私钥不能被明文读出，并且所有利用证书或私钥进行的运算都在 U 盾中进行。在银行端也存储有该客户的数字证书。当客户进行转账时，过程如下：

- (1) 客户通过 U 盾的按钮，将用户名和口令发送给银行；

(2) 银行向客户发送由时间、交易信息、随机数（防重放攻击字符串）、以及银行对随机数的签名值组合在一起形成数据 1，由客户公钥进行加密后得到的数据 2；

(3) 客户收到数据 2 后，使用 U 盾中客户的私钥对数据 2 进行解密，并对随机数的签名进行验签，验签通过后，可确认银行身份；

(4) 在客户端对随机数进行签名，将时间、交易信息、随机数、以及客户对随机数的签名值组合在一起，并用银行公钥进行加密，得到数据 3，并将数据 3 发送给银行；

(5) 银行端收到数据 3 后，用银行私钥解密，与数据 1 进行比对，并对签名值进行验签，若一致和通过验签，则客户通过银行的身份认证。

2.4.4.2. 基于协同签名的身份鉴别

2.4.4.2.1. 模式说明

1. 威胁分析

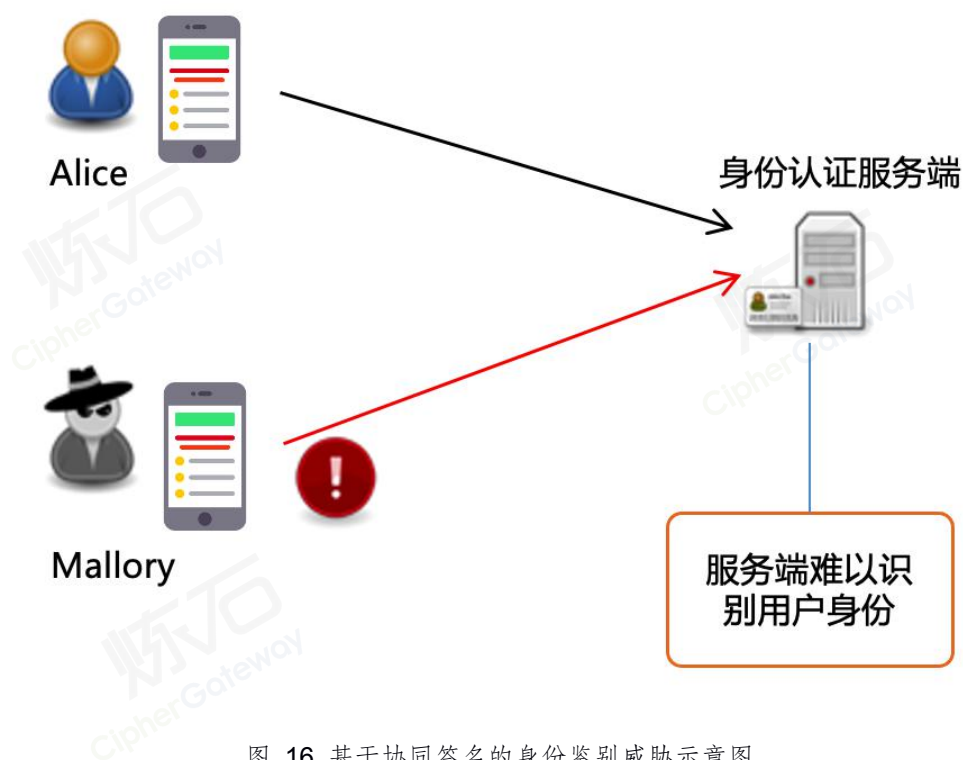


图 16 基于协同签名的身份鉴别威胁示意图

在移动场景中，攻击者 Mallory 可以伪装成 Alice 向服务端发起访问请求，而服务端难以识别伪装的用户身份。由于移动端无法支持 USBKey，只能使用软证书进行身份认证，而用户存在较高的身份凭证丢失的风险。攻击者 Mallory 可通过在手机中埋入木马，提权后窃取到 Alice 的软证书；如果 Alice 使用了弱口令，也很容易被 Mallory 破解并仿冒。

2. 防护模型

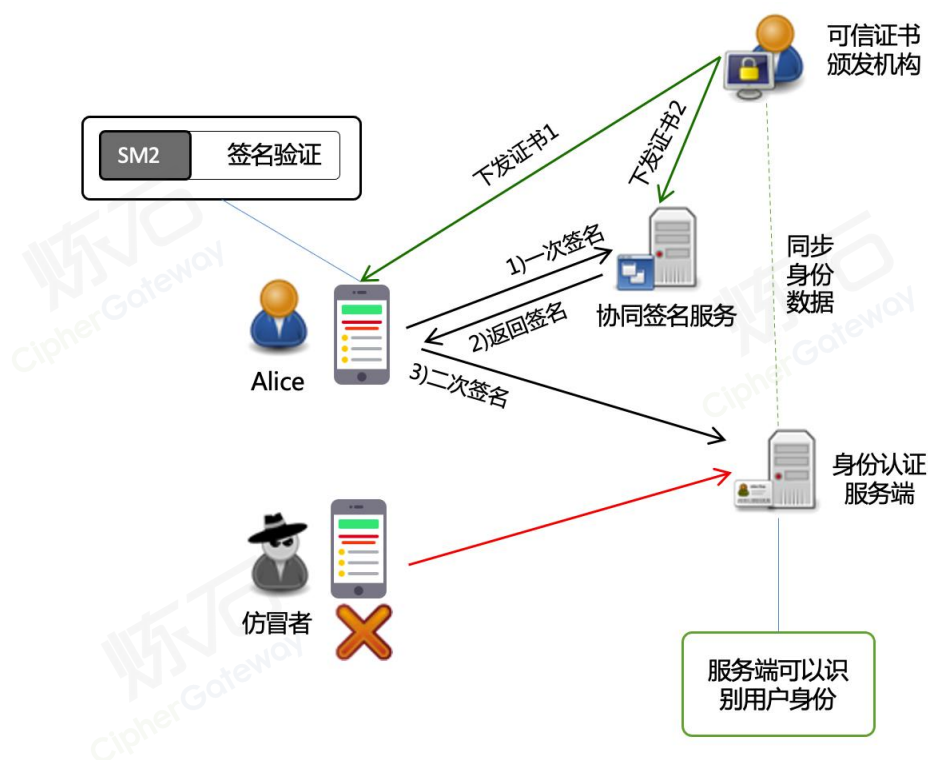


图 17 基于协同签名的身份鉴别防护模型示意图

可在通信双方 Alice 和服务端分别存储部分私钥，两方联合才能对消息进行签名或解密等操作，通信双方均无法获取到对方私钥的任何信息，因此攻击者在入侵其中任何一方的情况下，都不能伪造签名或解密密文，从而提高了移动场景中的私钥的安全性^[22]。协同签名的过程如下：

(1) Alice 生成自身的子私钥 D1，协同签名服务端生成自身的子私钥 D2；

(2) Alice 生成待签名消息 M 的消息摘要 e 和第一部分签名 Q1，并将 e 和 Q1 发送给协同签名服务端；

(3) 协同签名服务端根据 Q1 和 e 生成第二部分签名 r，并根据 D2 生成第三部分签名 s2 和第四部分签名 s3，将 r、s2 和 s3 发送给 Alice；

(4) Alice 根据 D1、r、s2 和 s3 生成完整签名并输出；

(5) 身份认证服务器使用公开的公钥进行验签，完成身份认证。

2.4.4.2.2. 典型应用示例

基于协同签名的身份鉴别的典型应用是手机盾认证系统。

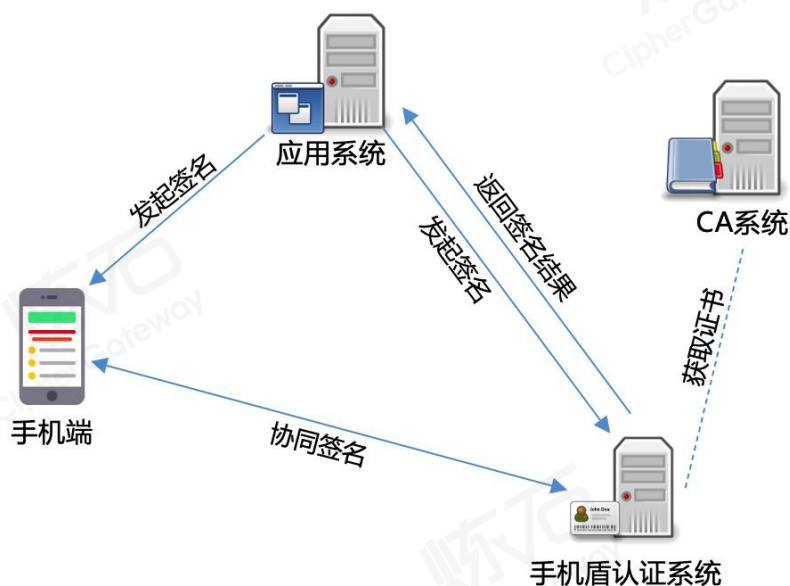


图 18 手机盾认证系统架构示意图

应用系统发起签名请求，同时将签名请求推送给手机端与认证服务端，手机端与服务端协同完成签名。

手机端与认证服务端协同合成用户公钥，并通过对接 CA 系统申请用户证书，当签名结果完成后，手机盾认证系统使用用户证书对完整签名进行正确性验证，从而确认手机端用户的身份。

（二）数据传输（通信安全）

2.4.5. 离线通信消息加密

2.4.5.1. 模式说明

2.4.5.1.1. 威胁分析

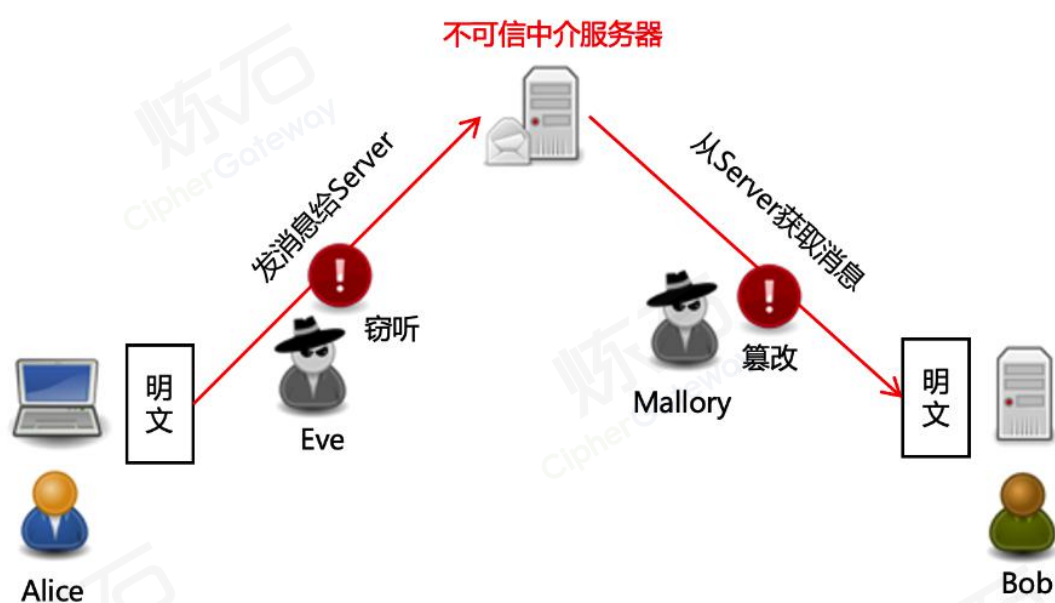


图 19 离线通信威胁示意图

Alice 和 Bob 通过中介服务器进行通信，先将消息发送给中介服务器，再由中介服务器转发给对方，而对方无需实时在线。对 Alice 来说，消息发出时 Bob 是离线状态，Alice 把消息发给中介服务器，Bob 定期从中介服务器更新消息。在此过程中会存在“窃听或篡改”的威胁。Eve 可在消息传递过程中进行窃听，Mallory 可在消息传递过程中进行篡改。

此种威胁多存在于邮件、短信以及 IM 聊天等场景中。

2.4.5.1.2. 防护模型

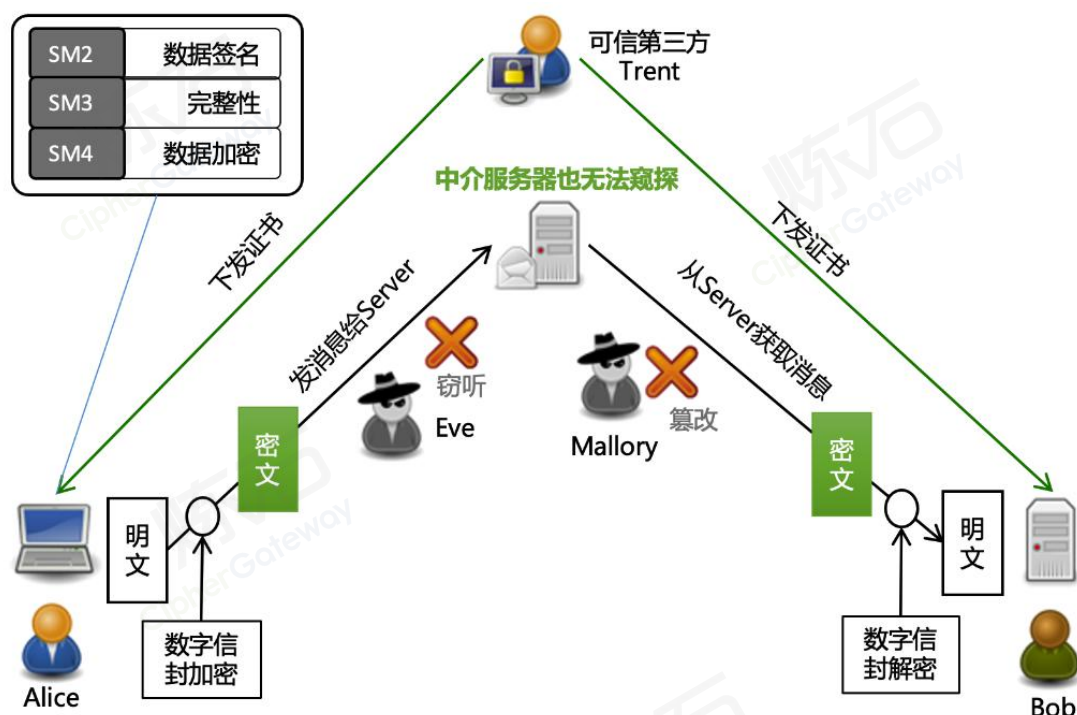


图 20 离线通信防护模型示意图

Alice 和 Bob 从可信第三方获取对方的证书（公钥），可采用“数字信封”的方式进行安全离线通信。过程为：

- (1) Alice 将消息使用 SM4 算法进行加密，生成密文消息；
- (2) Alice 使用 Bob 的公钥将加密密钥进行加密，并与密文消息一起封装成数字信封；
- (3) Alice 将数字信封通过中介服务器发送给 Bob；
- (4) Bob 接收到 Alice 的密文消息后，用自己的私钥解密数字信封，获取到加密密钥和密文信息，再对密文消息进行解密，从而获得明文消息。

2.4.5.2. 典型应用示例

离线通信消息加密的典型应用是 PGP 邮件。

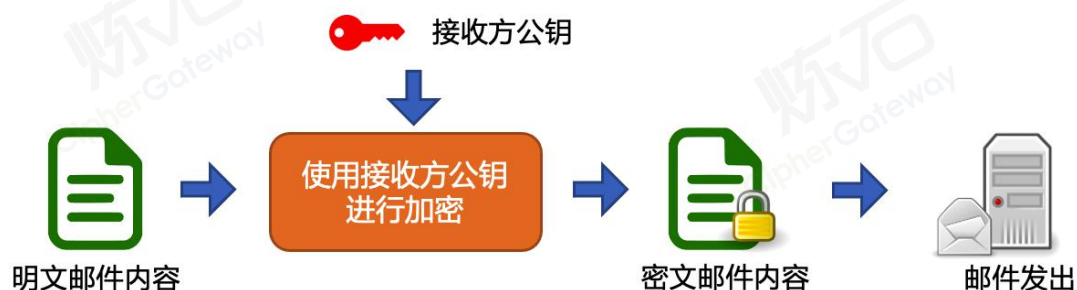


图 21 PGP 邮件加密发送示意图

PGP 邮件加密发送的过程如下：

- (1) 发送方获取到接收方的公钥；
- (2) 发送方将明文邮件内容，使用接收方公钥进行加密；
- (3) 发送方将加密后的密文邮件发出。

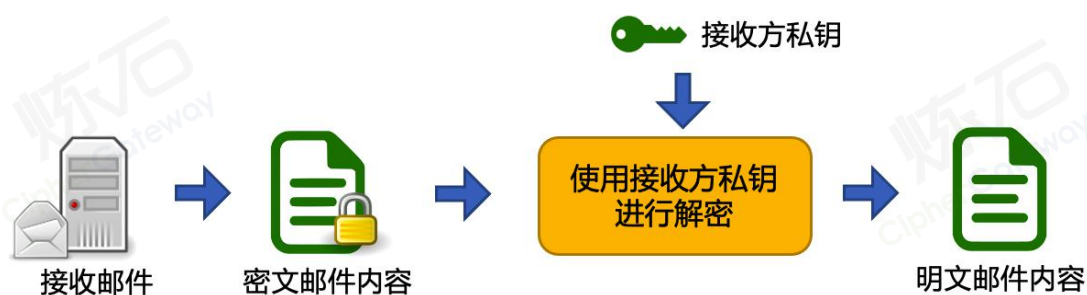


图 22 PGP 邮件接收解密示意图

PGP 邮件接收解密的过程如下：

- (1) 接收方获取密文邮件；
- (2) 接收方使用自己的私钥对密文邮件进行解密；

(3) 接收方获取到明文邮件。

2.4.6. 代理重加密受控分发消息

2.4.6.1. 模式说明

2.4.6.1.1. 威胁分析

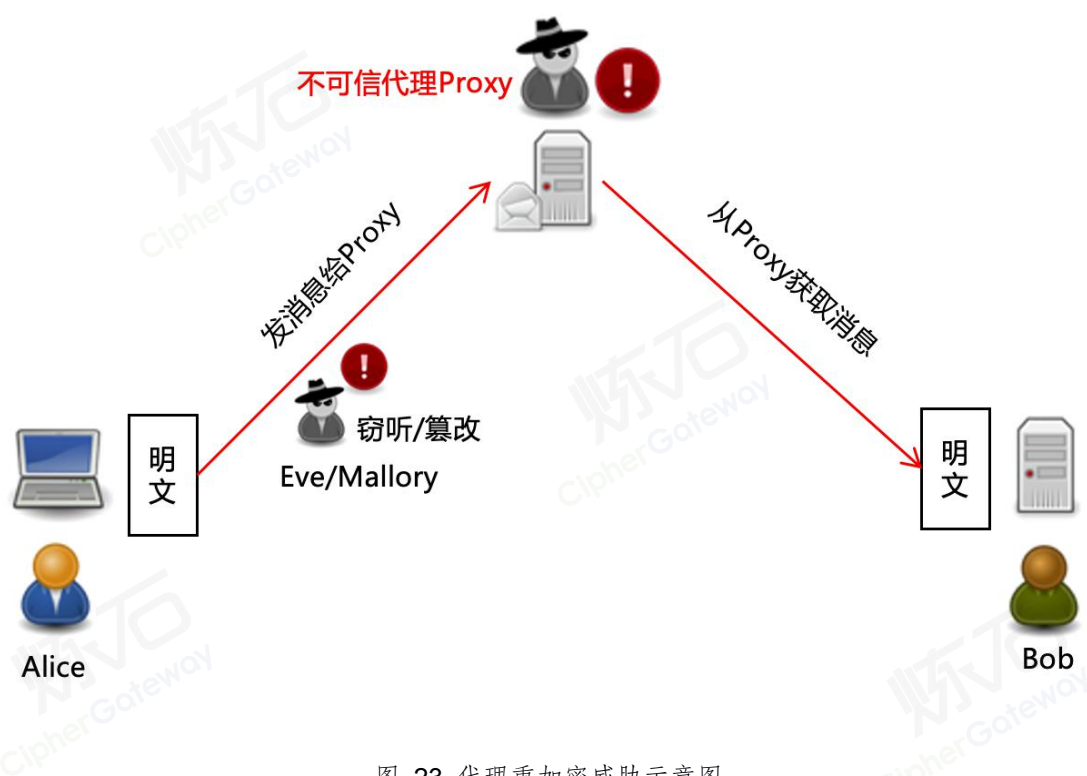


图 23 代理重加密威胁示意图

Alice 通过代理 Proxy 对外发送消息，先将消息发送给 Proxy，再委托 Proxy 将消息发出，Alice 并不确定消息要发给哪些接收者，或者 Alice 只有通过 Proxy 才能与 Bob 进行通信。在此过程中会存在“线路攻击者”和“恶意代理人”的威胁。Eve 可在消息传递过程中进行窃听，Mallory 可在消息传递过程中进行篡改；同样，Proxy 可在消息转发过程中进行窃听和篡改。

2.4.6.1.2. 防护模型

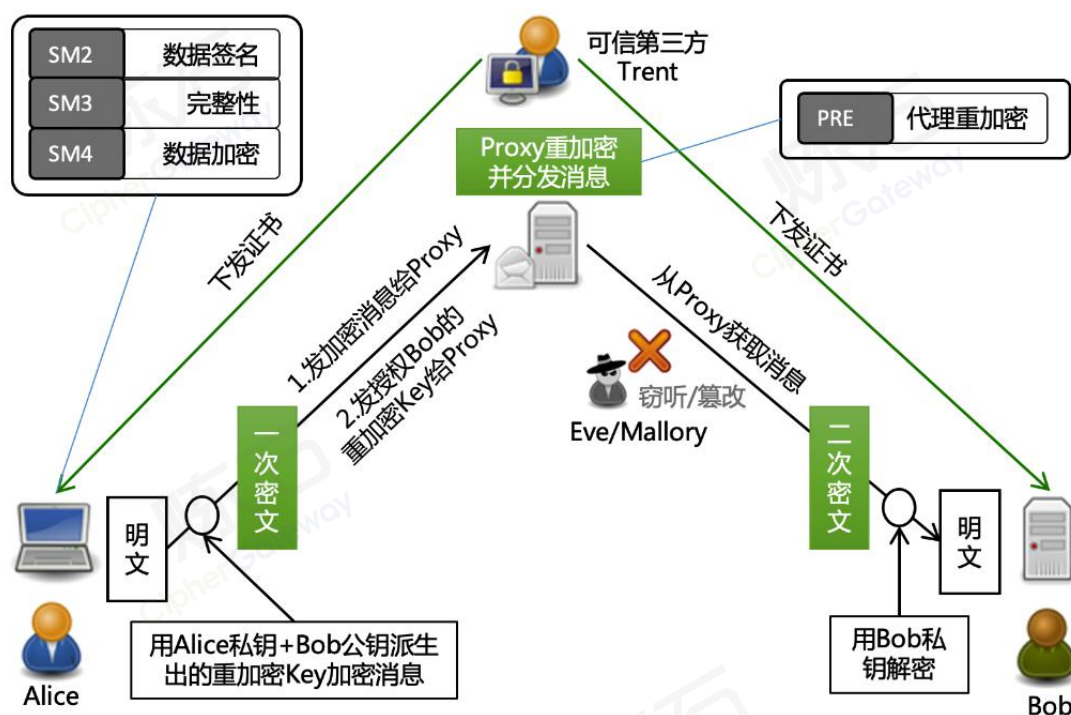


图 24 代理重加密防护模型示意图

Alice 从可信第三方获取 Bob 的证书（公钥），可采用“代理重加密”的方式将消息通过 Proxy 传递给 Bob。过程为：

- (1) Alice 将消息使用自己的公钥加密，得到密文消息 1；
- (2) Alice 计算或者获取 Bob 的代理重加密转换密钥 Key；
- (3) Alice 将密文消息 1 和密钥 key 发送给 Proxy；
- (4) Proxy 使用密钥 key 将密文消息 1 转化为 Bob 能够使用自己私钥解密的密文消息 2，并发送给 Bob；
- (5) Bob 接收到密文消息 2 后，使用自己的私钥进行解密，得到明文消息。

2.4.6.2. 典型应用示例

代理重加密的典型应用是云上密文共享。

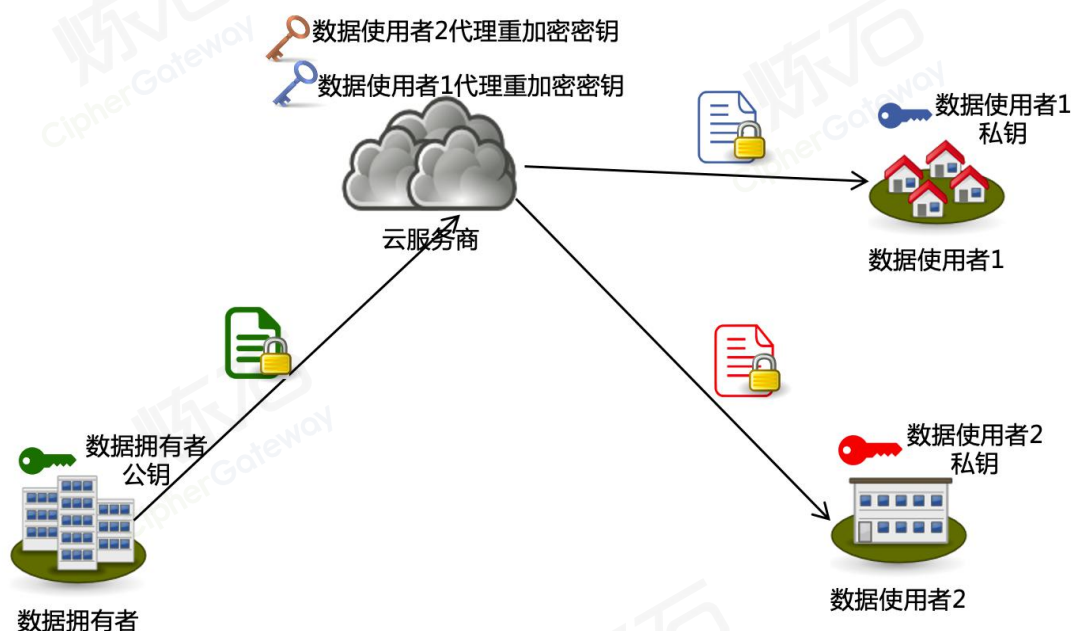


图 25 云上密文共享示意图

数据拥有者通过云盘将数据加密后进行共享，提供给数据使用者，云服务商承担 Proxy 的角色。过程如下：

(1) 数据拥有者将数据用自己的公钥进行加密后，上传至云盘，同时发送给云服务商的还有针对数据使用者的重加密密钥，重加密密钥是由数据拥有者的私钥和数据使用者的公钥派生而来，有多少个数据使用者就生成多少个重加密密钥；

(2) 云服务商拥有针对数据使用者相应的重加密密钥库；

(3) 云服务商使用重加密密钥将密文转化为数据使用者能够使用自己私钥解密的密文，并发送给数据使用者；

(4) 数据使用者接收到密文后，使用自己的私钥进行解密，得到明文。

2.4.7. 在线通信消息加密

2.4.7.1. 模式说明

2.4.7.1.1. 威胁分析

在线通信场景中主要是防止“线路攻击者”，重点从两个方面进行防护：防窃听和防篡改，用来保护传输内容的机密性、完整性和真实性。

典型的传输攻击模型如下图示，Bob 是在线服务提供者，当 Alice 向 Bob 发起请求，Bob 会实时响应，数据双向传递。在未做任何安全增强的通信网络中，潜伏在暗中的黑客（Eve 和 Mallory）就有可能通过技术手段窃听获得通信内容，或者通过伪造、篡改信息达到攻击的目的。



图 26 在线通信攻击模型

2.4.7.1.2. 防护模型

解决的手段是在通信时采用加密手段：对传输内容用对称加密算法加密，再结合公钥密码算法（非对称加密）、可信第三方的证书对双方身份进行认证。具体过程如下：

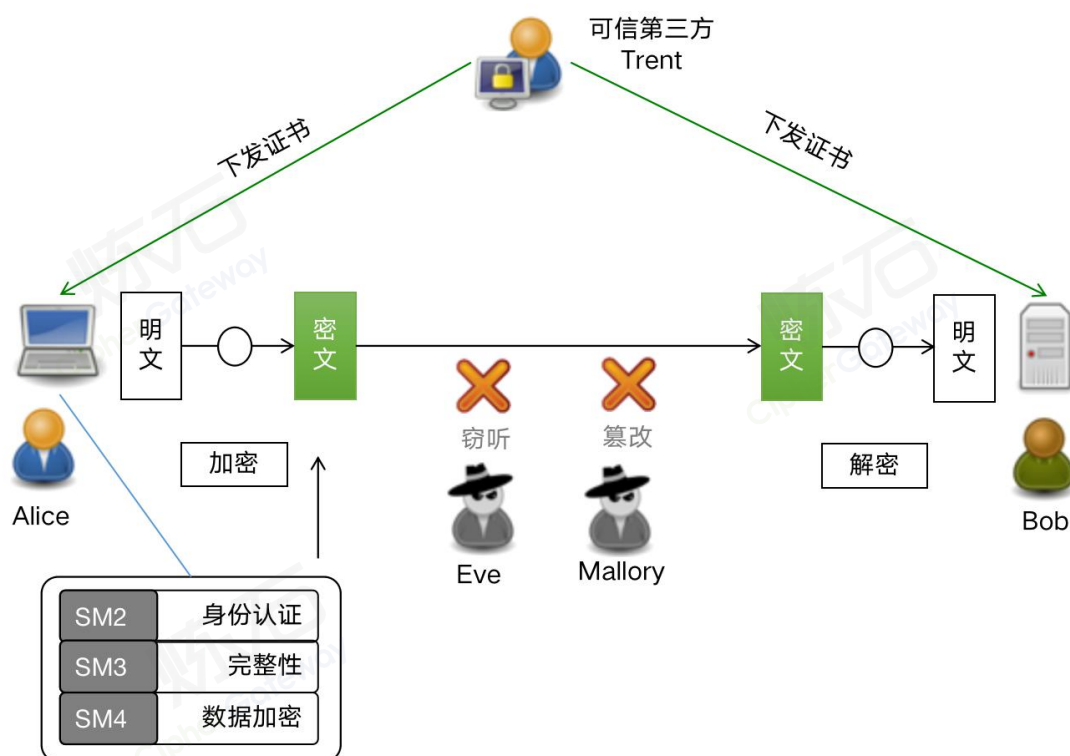


图 27 在线通信防护模型

1.可信的第三方 Trent（通常是数字证书签发机构 CA）分别给发送方和接收方颁发数字证书，数字证书里面包含证书拥有者的身份信息，第三方的签名（确保证书是真实的），证书拥有者的公钥（私钥由证书拥有者私密存储）。数字证书是面向公众开放的，即发送方和接收方都能很方便地获取到对方的真实数字证书，这是整个信任链的前提条件。

2.发送方（Alice）操作步骤：

（1）Alice 使用哈希算法（SM3 算法）对要发送的明文消息做哈希，并对哈希值计算签名（SM2 算法）。

（2）Alice 用对称密钥将明文、签名进行对称加密（SM4 算法），生成密文信息。

(3) Alice 用接收方 Bob 的公钥(从可信第三方的 Bob 数字证书获取)对上一步使用的对称密钥进行加密,并与密文消息一起封装成数字信封。

(4) Alice 将数字信封发送给 Bob。

3.接收方(Bob)操作步骤:

(1) Bob 接收到 Alice 的加密信息后,使用自己的私钥解密数字信封,获得对称密钥和密文信息。

(2) Bob 用上一步得到的对称密钥解密 Alice 发送过来的密文,获得最初的明文以及 Alice 的数字签名。

(3) Bob 使用 Alice 的公钥(从可信第三方的 Alice 的数字证书获取)对 Alice 的签名进行验签,如果确实是 Alice 的签名,则会验签成功,证明确实是 Alice 发的信息,而不是中间人伪造,确保信息传输的真实性和完整性。

(4) 当传输消息数量较多时,通常不直接使用数字签名来实现完整性,而是通过公钥密码算法协商 HMAC 密钥计算 HMAC 值,来实现完整性。

上述过程基于可信第三方的数字证书机制,再巧妙地组合三种加密算法(SM2、SM3、SM4),形成一种防窃听、防篡改、防伪造的通信机制,最终确保在线通信中信息的机密性、完整性和真实性。

2.4.7.2. 典型应用示例

2.4.7.2.1. 基于 SSL/TLS 的 HTTPS

基于数字证书的安全传输方案典型应用之一就是 HTTPS 协议，HTTPS 是叠加了数据加密技术的 HTTP 协议，主要是为了解决 HTTP 协议安全性不足的问题而设计。



图 28 HTTPS 传输加密示意图

如上图所示，HTTP 通过叠加利用 SSL（Secure Socket Layer）或者 TLS（Transport Layer Security）协议对通信内容进行加密，从而防止传输过程中的中间人攻击。

SSL/TLS 作为一种密码通信框架，其中包括对称密码、公钥密码、数字签名、单向散列函数等加密技术。也就是说，如果发现所使用的某个密码技术存在弱点，那么只要替换这一部分就可以。由于实际进行对话的客户端和服务端必须使用相同的密码技术才能进行通信，因此如果选择过于自由，就难以确保整体的兼容性。为此，SSL/TLS 就像事先搭配好的盒饭一样，规定了一些密码技术的“推荐套餐”，这种推荐套餐称为密码套件（cipher suite）^[57]。

目前已有国内厂家推出了集成支持国密算法的 TLS 协议的浏览器。

2.4.7.2.2. VPN 虚拟专用网络

VPN 即虚拟专用网络 (Virtual Private Network)，是以公用网络为基础通道，结合隧道封装技术、认证机制、加密技术、访问控制等多种网络和安全技术的安产品，借以实现跨境、跨区域的远程接入，是企业内部、分支机构和移动办公人员之间实现互联互通和资源共享的方法。

常见的 VPN 产品有 IPSec VPN 和 SSL VPN 两大类。如下图：

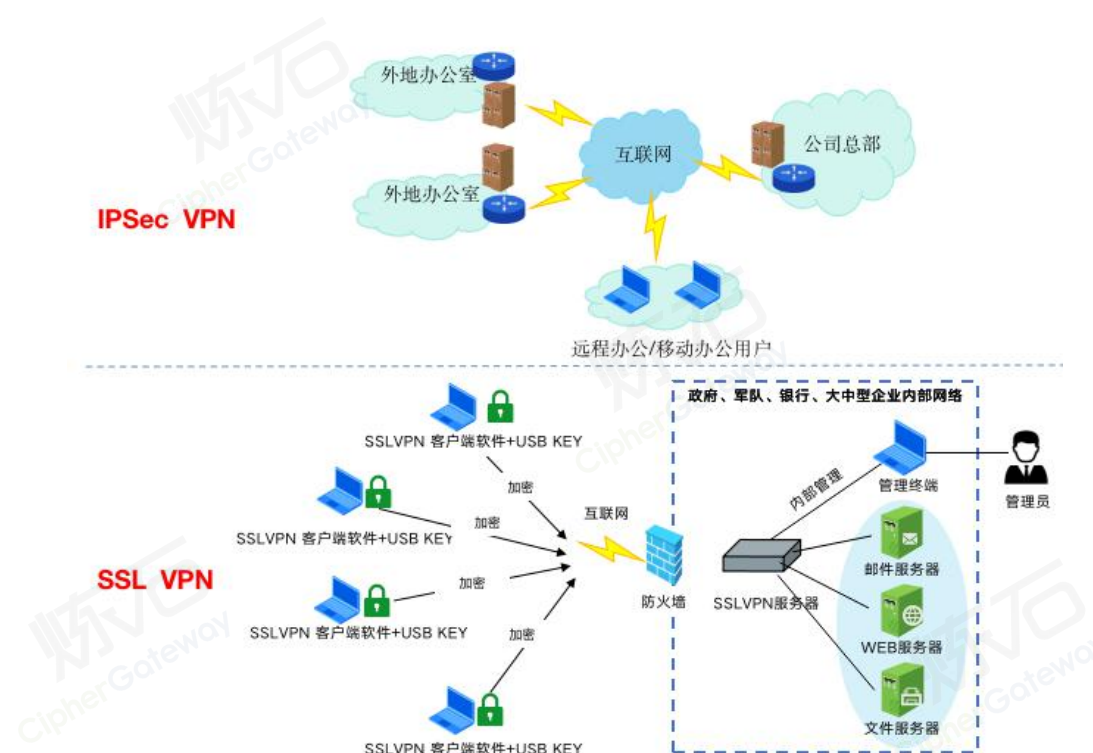


图 29 两类常见 VPN 产品

1. IPSec VPN

IPSec 是 IETF 在开发 IPv6 时研究制定一套用于保护 IP 数据包通信的 IP 安全协议，是 IPv6 协议的一个重要组成部分，也是 IPv4 可选的扩展协议。IPsec 提供较强的互操作性能力，具有完善的基于密码学的安全功能。在通信终端实体间的

IP 层通过加密与数据源验证等方式，来保证数据传输的保密性、完整性、可靠性和防重放攻击^[23]。

IPsec 不是单一的协议而是由一系列协议组成，IPSec 体系结构包括认证头 AH 协议和封装安全载荷 ESP 协议，安全关联 SA 协议，Internet 密钥交换协议及验证算法和加密算法等。

VPN 实体可以在网络中不同位置具有 IPsec 功能的网络设备(如防火墙、路由器、主机)上实现。IPsec 基于主机的实施可以实现端到端的安全服务。基于 IPsec 功能的路由器构建 VPN 实现网关间安全服务。将这两种解决方案有效地融合可以实现漫游接入(road warrior)的安全，为移动办公员工访问公司资源时提供安全服务^[24]。

2. SSL VPN

SSL VPN 是以 SSL 协议为安全基础的 VPN 远程接入技术，从硬件构成上看主要由远程客户端、SSL VPN 网关和企业内部网服务器等组成。远程客户端使用标准 WEB 浏览器，并利用浏览器内建的 SSL 封包处理功能，通过 Internet 连接到公司的 SSL VPN 网关服务器，SSL VPN 网关服务器通过身份认证技术对远程客户的进行身份认证后，授以相应的访问权限，然后利用内容重写和应用翻译等中间转换技术响应远程用户对内部资源的访问。

SSL VPN 用到的关键技术有：使用者与设备身份认证技术、隧道封装技术、加密技术、内容重写和应用翻译技术、精细可伸缩的访问控制技术以及终端端数据安全技术^[25]。

2.4.7.2.3. 链路密码机/网络密码机

同步链路密码机用于 DDN 专线网络环境,位于网络接入路由器和同步 Modem 之间,如下图所示。密码机通常采用对称加密算法对进出路由器的网络通信数据进行加/解密处理,为用户提供点对点的数据通信加密保护,确保敏感数据传输安全^[26]。

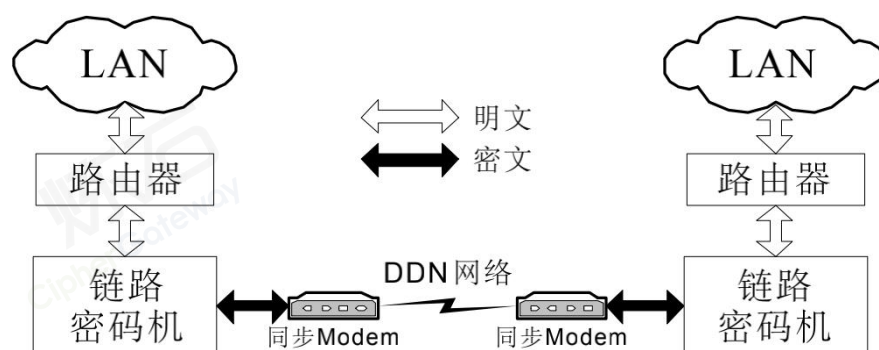


图 30 同步链路密码机应用模式

链路密码机是传输数据过程中在数据链路层进行加密的方案,接收方是传送路径上的各台节点机,信息在每台节点机内都要被解密和再加密,依次进行直至到达目的地。

密码机在链路层对所有数据进行处理,而不理会链路层上层复杂的通讯协议。因此,其应用范围非常广泛^[27]。

2.4.8. 可感知窃听的专线通信

2.4.8.1. 模式说明

2.4.8.1.1. 威胁分析

在通信传输场景中存在着“中间人攻击”的可能性，如下图示：Alice 发送给 Bob 的信息被中间人 Eve 窃听，如果 Alice 和 Bob 都不知情，将会带来严重后果。因为双方会认为私密内容没有被泄露，仍然按原计划进行。

因此实现对数据被窃听或泄露的主动感知就非常有必要。



图 31 通信传输攻击模型

2.4.8.1.2. 防护模型



图 32 通信传输防护模型

量子通信的优势在于可以感知窃听,从而使得窃听者不能获得信号,进而保证传递的信息从原理上不可能被计算破译,因而具有绝对安全性。量子通信使用的载体具有量子特性,例如电子、光子这些微观粒子会表现出量子特性。

利用量子载体的这种特性就可以发现窃听者。假设爱因斯坦要和薛定谔协商出一串密码,要求协商出的密码不能被其他人知道。他首先发送一串电子,电子的自旋方向是随机地处在平行、反平行、垂直于和反垂直于磁场。薛定谔随机地沿着磁场的方向或者垂直于磁场的方向进行测量。沿着磁场方向测量爱因斯坦沿着磁场方向(平行或者反平行)制备的电子自旋时,薛定谔得到平行或反平行的结果,和爱因斯坦发过来的一样。但是对于垂直或者反垂直磁场的电子,薛定谔的测量结果就是随机的平行或者反平行。薛定谔沿着垂直于磁场方向测量时的结果也类似。在传输了大量的电子之后,爱因斯坦公开每个电子的自旋方向是沿着于磁场方向还是垂直于磁场的方向(但不公布是平行或反平行,垂直或者反垂直),薛定谔公开对每个电子的测量方向(但不公布测量结果)。对于制备方向和测量方向相同的情况,两者的结果应该是一样的。如果中间有人窃听,就会改变电子自旋的方向,造成误码。他们可以公布一部分测量结果进行对比,得出误码率,根据误码率的大小判断窃听的程度。如果窃听不严重,它们就把测量结果作为密码,然后或者使用一次一密加密信息,或者使用其他经典密码加密信息,再使用经典通信传输密文,完成信息的传输。可以看到,量子保密通信实现了传统通信中做不到的一点,就是实时发现窃听行为^[28]。

2.4.8.2. 典型应用示例

量子通信协议 BB84 由 Bennett 和 Brassard 于 1984 年首次提出，也是使用和实验最多的量子密钥分发方案之一。BB84 协议不仅是目前最接近实用化的量子通信协议，而且也是其他量子通信协议的基础。该协议描述如何利用光子的偏振态来传输信息进行量子密钥分发:发送方 Alice 和接收方 Bob 用量子信道(如果光子作为量子态载体，对应的量子信道就是传输光子的光纤)来传输量子态;同时双方通过一条公共经典信道(如因特网)比较测量基矢和其他信息交流，进而两边同时安全地获得或共享一份相同的密钥。公共信道的安全性不需考虑，BB84 协议在设计时已考虑到了两种信道都被第三方(Eavesdropper, 通常称为 Eve)窃听的可能。

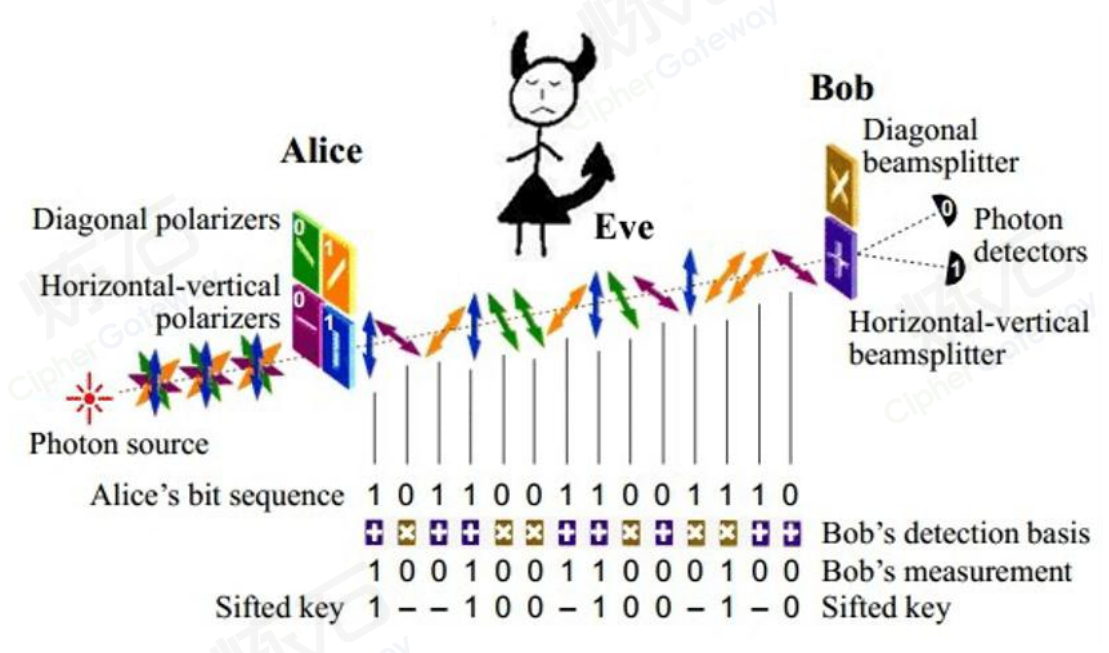


图 33 基于 BB84 协议的量子密钥分发

利用 BB84 协议中的量子状态的测不准原理和不可克隆定理，我们可以在合法通信中检测出扰动，进而判定双方通信过程中是否存在窃听，从而打破信息暴露之后自己却毫无感知的被动局面。

（三）数据存储（数据资产安全）

2.4.9. 应用内数据加密

2.4.9.1. 模式说明

2.4.9.1.1. 威胁分析

传统的信息安全侧重在网络层面以攻防对抗方式为主，通过诸如禁止访问等手段打造安全的网络边界，应用系统本身并没有内建安全机制，数据仍然以“裸奔”的形式存在。然而数据是随着业务需求在系统中频繁流动的，在生命周期的各个阶段都面临泄露的风险。近年来更是由于数据分析挖掘、交换共享等新应用场景出现，数据在动态使用过程中泄露风险剧增，企业或机构普遍面临以下问题：

1. 内部人员泄露数据

组织内部人员比如研发、测试和 DBA 人员，因为工作需要能够接触到生产数据库、测试数据库、备份数据库，要想拿走这些明文数据是很容易的。

2. 外部黑客窃取数据

外部黑客利用系统基础设施层、网络层和应用层等存在的安全漏洞或者网络安全配置缺陷对系统进行远程入侵，非法实施“拖库”操作。

3. 缺乏事后追责的能力

由于没有高置信度的审计功能或者诸如数字水印等“后手”机制，事后追责也变得非常艰难。

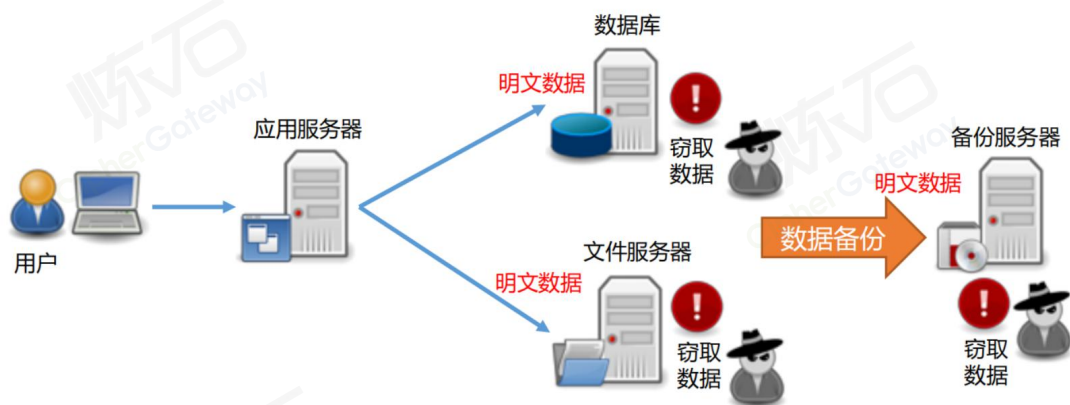


图 34 明文数据在各个阶段都面临被窃取的风险

2.4.9.1.2. 防护模型

应用系统是数据“必经之路”，在应用系统这一“咽喉要道”上，使用基于国密算法的加密手段，可赋予应用系统内建安全，达到以下效果：

- 1.利用加密技术将敏感字段加密，以密文的形式流转 to 下一个环节，比如数据处理、数据存储、数据分析环节。
- 2.密文数据必须回到应用层进行解密，确保数据处理全过程中不出现漏点，从而建立不可绕过的数据安全锚点。
- 3.在应用中可以获取登录用户身份信息，结合用户身份实现“主体到人、客体到字段”级细粒度访问控制。
- 4.在应用系统中的“安全锚点”处可以建立高置信的审计机制，为数据泄密事件发生后的复盘、追责、堵漏洞提供支持。

5.在应用系统中，通过分析访问用户的行为，可发现异常操作，并施加阻断和预警。

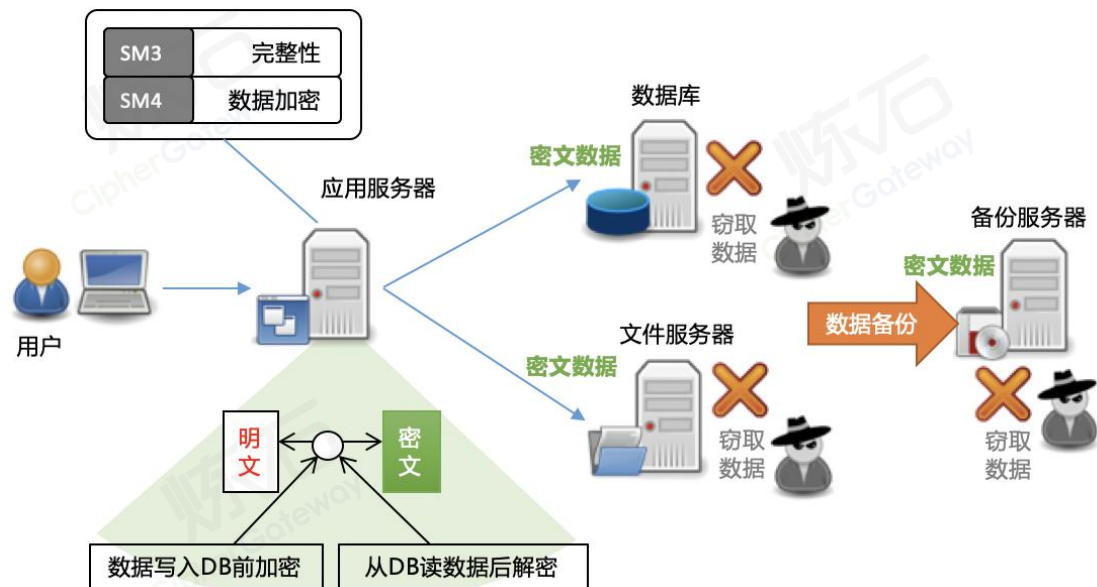


图 35 使用密码技术防止应用内威胁

应用内数据加密常用的手段有：内部集成密码 SDK、采用 CASB 代理网关以及应用内 AOE 加密手段等。由于重点面向结构化数据加密，从算法选择上，除了分组密码算法，还支持 FPE 格式保留加密等。

2.4.9.2. 典型应用示例

2.4.9.2.1. 应用内加密（集成密码 SDK）

应用内加密（集成密码 SDK）是指应用系统通过开发改造的方式，与封装了加密业务逻辑的密码 SDK 进行集成，并调用其加解密接口，使目标应用系统具备数据加密防护能力。

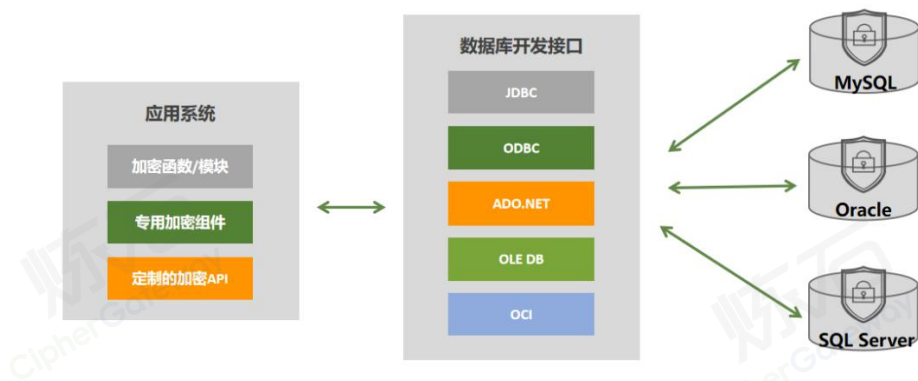


图 36 应用内加密（集成密码 SDK）技术原理

应用内加密（集成密码 SDK）的优势是适用范围广和灵活性高。

缺点是：

（1）需要对应用系统开发改造，时间周期较长，后期实施和维护成本较高，也面临大量代码改造带来的潜在业务风险；

（2）对业务开发人员来说，正确合规使用密码技术具有一定门槛。

2.4.9.2.2. CASB 代理网关

CASB 代理网关（Cloud Access Security Broker）是一种委托式安全代理技术，将网关部署在目标应用的客户端和服务端之间，无需改造目标应用，只需通过适配目标应用，对客户端请求进行解析，并分析出其包含的敏感数据，结合用户身份，并根据设置的安全策略对请求进行脱敏等访问控制，可针对结构化数据和非结构化数据同时进行安全管控。

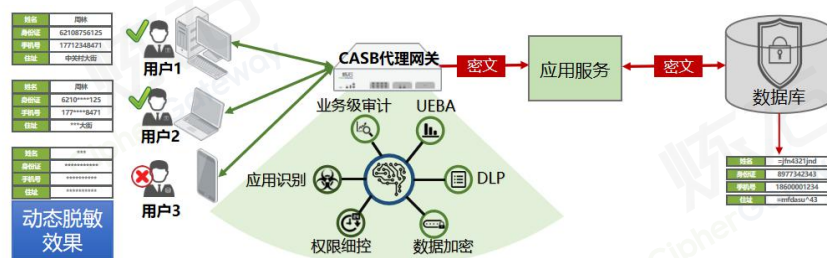


图 37 CASB 代理网关技术原理

由于 CASB 代理网关位于应用服务和用户端之间，该位置可以获取到丰富的业务上下文，可以基于用户、资源、操作和业务属性，灵活利用访问者所对应属性集合决定是否有权访问目标数据，比如部门、区域、职位、动作、目标数据类型、时间，以及其他条件等，从而在复杂业务场景下实现对数据的安全防护。但是实施成本较高。

2.4.9.2.3. 应用内加密（AOE 面向切面加密）

应用内加密（AOE 面向切面加密）技术，能以免开发改造方式，实现应用系统中结构化数据和非结构化数据的存储加密，并提供细粒度访问控制、丰富脱敏策略、以及数据访问审计功能，为应用打造全面有效且易于实施的数据安全保护。其实现原理是将数据库加解密插件部署在应用服务中间件，结合旁路部署的数据安全管理平台、密钥管理系统，通过拦截入库 SQL，将数据加密后存入数据库。

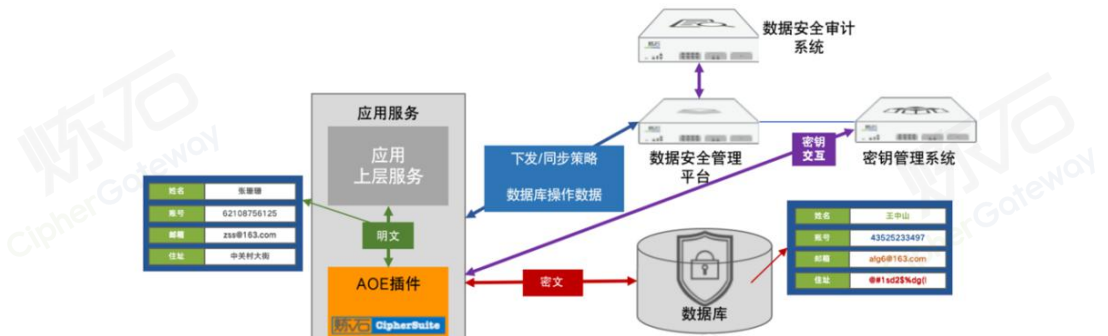


图 38 应用内加密（AOE 面向切面加密）技术原理

主要适用于企业在应用层想要实现免开发改造的、可敏捷实施的高性能数据安全防护。该加密方式支持结构化/非结构化数据的加密，可与应用开发解耦，灵活性高。进一步的，该加密方式可支持分布式部署、集中式管控，既可针对单个应用防护，也可以针对上百个应用的批量保护。

由于企业实际应用系统错综复杂，涉及到多样化的编程语言与框架，这对 AOE 面向切面加密技术的实现提出较高的工程化实现挑战。

2.4.10. 数据库存储加密

2.4.10.1. 模式说明

2.4.10.1.1. 威胁分析

结构化数据集中存储在数据库服务器中，在内部没有安全防护措施的情况下，风险极大，容易受到以下威胁：

1. 内部越权获取数据

一般在正规的 IT 组织中，研发或测试人员只能操作开发库或测试库，而开发库中或测试库中可能会有从生产库导出的数据，或者出于调试程序、排查错误的需要，不可避免地会接触生产库，存在敏感数据泄露的风险。

另外对 DBA 的管理容易“一刀切”，没法做到数据权限的精细化管控，DBA 要导出整个生产库的数据很容易。这种由于内部管理不到位导致的数据泄露事件占整体数据安全事件的七成以上。

2. 外部黑客拖库

对于有价值的数据库而言，一直是外部黑客觊觎的目标。外部黑客通过寻找网络漏洞进入数据库服务器，可以拖走数据库文件。

3. 无意识地泄露

研发人员或系统维护人员在日常工作中形成的日志文件，里面也会记录敏感数据，比如个人隐私信息，账号信息，公司商业机密信息等，而这些日志文件如

果没有妥善保管或销毁，容易流向员工个人电脑甚至是互联网上。此外，存储介质的更换、维修或者报废等环节，也面临数据泄露风险。



图 39 存储的数据面临被窃取的威胁

2.4.10.1.2. 防护模型

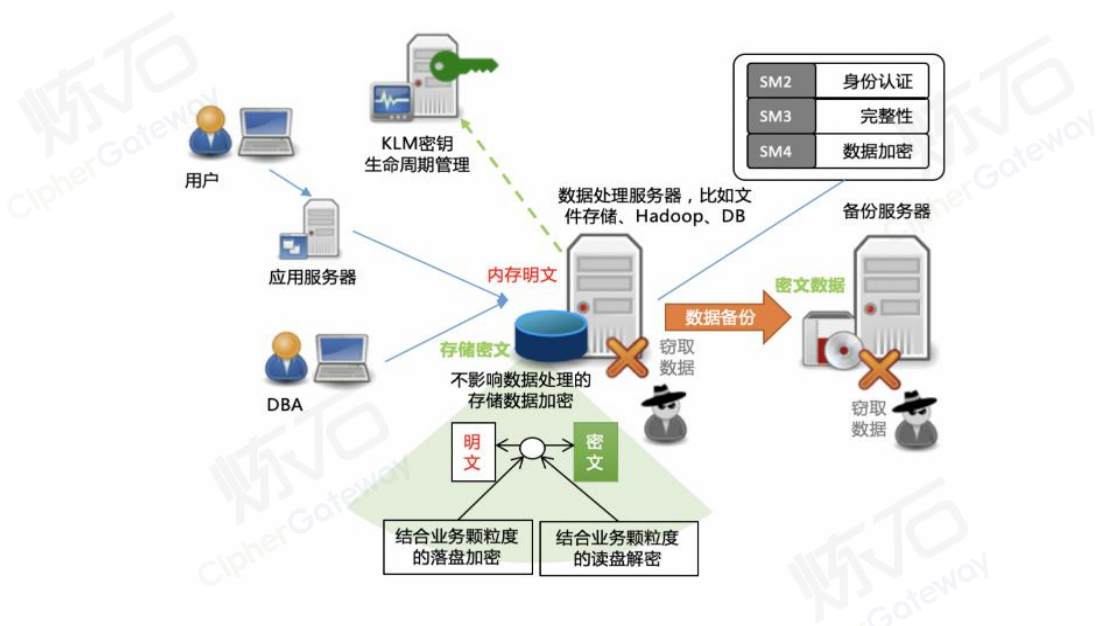


图 40 使用密码技术保护存储的数据

防护重点是给数据本身加一层贴身防护，即围绕数据库应用、数据库存储服务，采用基于国密算法的密码技术，利用包括加密网关、外挂加密、透明数据加密等技术，对数据库文件、表空间、表字段等进行不同层面的加密保护，可防范数据被窃取的风险。

2.4.10.2. 典型应用示例

2.4.10.2.1. UDF 用户自定义函数加密

UDF (User Defined Function) 用户自定义函数是在已有数据库功能的基础上扩展更丰富的业务需求，其原理是在数据库支持的形式上，通过定义函数名称及执行过程，实现自定义的处理逻辑。UDF 用户自定义函数加密，是通过 UDF 接口实现数据在数据库内的加解密。

UDF 的优势是扩展能力强，适用于对数据有“定制化实现”的场景化需求，能够根据用户的业务需求，对数据实现丰富多样的加解密处理。缺点是通用性低，需要根据不同数据库的类型，做相对应的定制化实现，并且在存储过程或 SQL 中加以调用。

2.4.10.2.2. 数据库外挂加密

数据库外挂加密指通过针对数据库定制开发外挂进程，使进入数据库的明文先进入到外挂程序中进行加密，形成密文后再插入数据库表中。这种技术使用“触发器”+“多层视图”+“扩展索引”+“外部调用”的方式实现数据加密，可保证应用完全透明。通过扩展的接口和机制，数据库系统用户可以通过外部接口调

用的方式实现对数据的加解密处理。视图可实现对表内数据的过滤、投影、聚集、关联和函数运算，在视图内实现对敏感列解密函数的调用，实现数据解密。

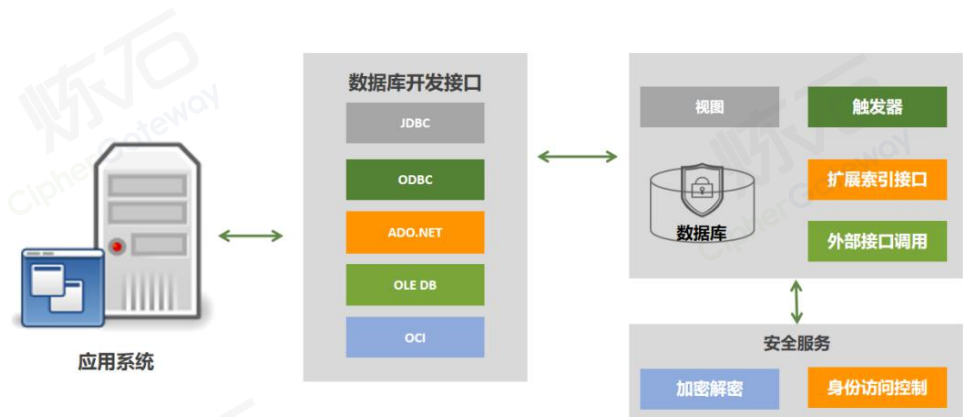


图 41 数据库外挂加密技术原理

使用数据库外挂加密技术的缺点有：

- (1) 支持的数据库种类有限，仅支持 Oracle 等少量数据库类型；
- (2) 数据库性能损耗较高，会对数据库的读写性能存在明显影响；
- (3) 可扩展性差。

2.4.10.2.3. TDE 透明数据加密

透明数据加密（Transparent Data Encryption，简称为 TDE）是在数据库内部透明实现数据存储加密、访问解密的技术，Oracle、SQL Server、MySQL 等数据库默认内置此功能。数据在落盘时加密，在数据库内存中是密文，当攻击者“拔盘”窃取数据，由于数据库文件无法获得密钥而只能获取密文，从而起到保护数据库中数据的效果。



图 42 透明数据加密技术原理

透明数据加密技术适用于对数据库中的数据执行实时加解密的应用场景,尤其是在对数据加密透明化有要求,以及对数据加密后数据库性能有较高要求的场景中。在实际使用中,可根据 Oracle 等内置 TDE 的密钥管理接口,将默认“软密钥钱包”升级为外部密钥管理系统,以增强密钥安全性。

方案的优势是:

(1) 独立权控体系。与数据库外挂加密类似,使用插件形式的透明数据加密技术,同样可以在外置的安全服务中提供独立于数据库自有权控体系之外的权限控制体系;

(2) 性能损耗较低。

缺点有:

(1) 防护颗粒度较粗;

(2) 数据库类型适用性上有限制。透明数据加密因使用插件技术,对数据库的版本有较强依赖性,且仅能对有限几种类型的数据库实现透明数据加密插件,在数据库类型适用性上有一定限制。

2.4.10.2.4. 数据库加密网关

数据库加密网关是部署在应用服务器和数据库服务器之间的代理网关设备，通过解析数据库协议，对传入数据库的数据进行加密，从而获得保护数据安全的效果。

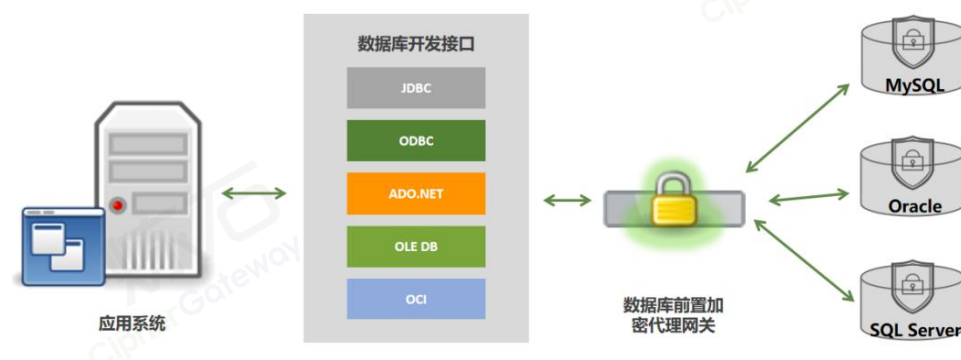


图 43 数据库加密网关技术原理

数据库加密网关可以为数据库提供“入库加密、出库解密”的防护，可以建立数据库用户的访问控制，实现企业内部人员的敏感数据访问授权精细化，可以防数据库拖库以及拦截非法 SQL。

优势是可以实现应用系统与加解密功能分离。相比较于传统的应用内加密（集成密码 SDK）技术，数据库加密网关技术具有独立性，能够使用户从高度复杂且繁重的加密解密处理逻辑的开发工作解放出来。

但是对于 Oracle 等采用私有通信协议（不开源）的商业数据库，安全厂商提供的数据库加密网关破解协议的方案存在法律风险。同时要实现高性能和高可用难度更大大。

2.4.11. 文件存储加密

2.4.11.1. 模式说明

2.4.11.1.1. 威胁分析

文件数据跟随业务在各层之间高速流转，其同样遵循数据全生命周期这一规律，也不可避免会面临下面的威胁：

1. 内部人员泄露威胁：

在缺乏权限控制或管理不严的组织中，内部员工接触到的文件数据常常是不受限制的。他们可以随意拷贝、外发公司的文件数据。

2. 数据文件本身缺乏主动安全机制

数据在 PC 端和应用服务端都以明文存储，缺乏必要的加密手段，存在员工泄露、拔盘或黑客入侵非法复制等数据泄露风险；

3. 缺乏审计难以追责

缺乏基于业务操作行为的审计和分析功能，一旦出现问题不容易追责。

4. 安全防护预警能力弱

缺乏基于业务操作行为的事中预警和阻断、通知功能。

2.4.11.1.2. 防护模型

数据全生命周期包括：收集、存储、使用、加工、传输、提供、公开七个阶段，在各个阶段都会面临数据泄露的风险，而存储阶段是数据处理最密集，最集中的阶段。数据文件不仅存储在服务端，也存储在终端。对于数据本身，通过加

2.4.11.2.2. FDE 全磁盘加密

全磁盘加密（Full Disk Encryption，简称 FDE）是指通过动态加解密技术，对磁盘或分区进行动态加解密的技术。FDE 的动态加解密算法位于操作系统底层，其所有磁盘操作均通过 FDE 进行：当系统向磁盘上写入数据时，FDE 首先加密要写入的数据，然后再写入磁盘；反之，当系统读取磁盘数据时，FDE 会自动将读取到的数据进行解密，然后再提交给操作系统。

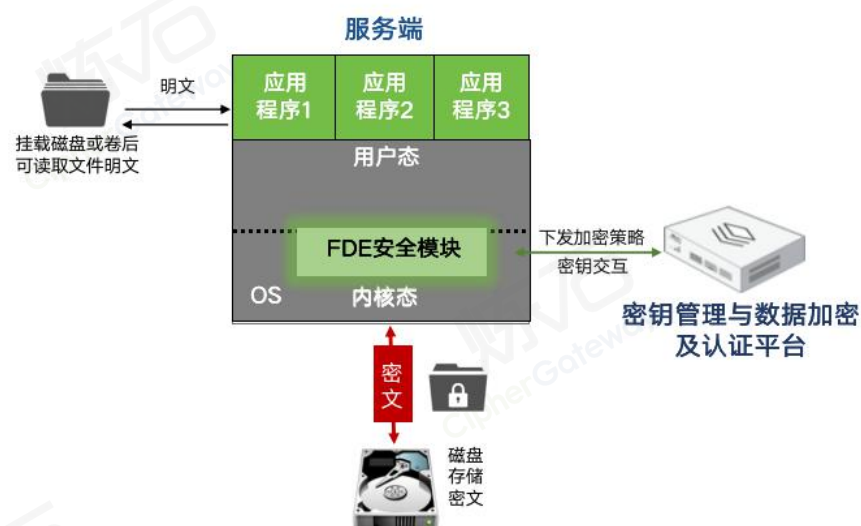


图 45 FDE 磁盘加密系统组成

其最大的优势是性能高、兼容性好，其次是部署、实施简单。但是相应的数据防护颗粒度粗。该加密技术因为缺少访问控制能力，因此，一旦磁盘挂载口令泄露，就有数据泄露的风险，仅能防范“拔硬盘”攻击。

2.4.11.2.3. DLP 终端加密

DLP（Data leakage prevention）终端加密技术，目的是管理企业终端上（主要是 PC 端）的敏感数据，其原理是在受管控的终端上安装代理程序，由代理程

序与后台管理平台交互，并结合企业的管理要求和分级分类策略，对下载到终端的敏感数据进行加密，从而将加密应用到企业数据的日常流转和存储中。信息被读取到内存中时会进行解密，而未授权复制到管控范围外则是密文形式，主要适用于非结构化数据的保护。

DLP 终端加密技术可以避免出现的数据泄漏场景：

- (1) 操作失误或无意识外发导致技术数据泄漏；
- (2) 通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据；
- (3) 离职人员通过 U 盘、移动硬盘等方式随意拷走机密资料；
- (4) 移动笔记本被盗、丢失或维修等造成数据泄漏。

但是 DLP 存在终端适配困难、运维成本高的问题。

(四) 数据使用（数据共享与安全兼得）

2.4.12. 基于差分隐私的数据匿名化

2.4.12.1. 模式说明

2.4.12.1.1. 威胁分析

攻击者可以根据被公开的一组信息以及攻击者已经获取到的背景知识，来推断出某客体其他敏感属性值。造成的后果就是尽管敏感信息没有被主动披露，但是仍然避免不了被泄露的后果^[29]。

2.4.12.1.2. 防护模型

1. 差分隐私

差分隐私是一种通用且具有坚实的数学理论支持的隐私保护框架,可以在攻击者掌握任意背景知识的情况下对发布数据提供隐私保护。

定义 1 差分隐私。设有随机算法 M , P_M 为 M 所有可能的输出构成的集合对于任意两个相邻最多相差一条记录的近数据集 D 和 D' 即 $D \Delta D' \leq 1$, 以及 P_M 的任何子集 S_M , 若算法 M 满足下列不等式则称算法 M 提供 ϵ -差分隐私保护;

$$\Pr [M(D) \in S_M] \leq \exp(\epsilon) \times \Pr [M(D') \in S_M] \quad (1)$$

其中: $\Pr [\cdot]$ 由算法 M 随机控制, 表示隐私披露的风险; 参数 ϵ 称为隐私保护预算, 用来控制算法 M 在两个邻近数据集上获得相同输出的概率的比值, 反映 M 所能够提供的隐私保护水平。

要实现差分隐私保护需要噪声机制的介入, 本文选用的噪声机制为拉普拉斯 (Laplace) 机制。该机制通过向确切的查询结果中加入服从 Laplace 分布的随机噪声来实现 ϵ -差分隐私保护, 记位置参数为 0, 尺度参数为 b 的 Laplace 分布为 $Lap(b)$, 其密度函数为:

$$p(x) = b/2 \exp(-|x|/b) \quad (2)$$

定义 2 Laplace 机制。给定数据集 D , 设有函数 $f: D \rightarrow \mathbb{R}^d$, 其敏感度为 Δf , 那么随机算法 $M(D) = f[D] + Y$ 提供 ϵ -差分隐私保护, 其中 $Y \sim Lap(\Delta f / \epsilon)$ 为随机噪声, 服从尺度参数为 $\Delta f / \epsilon$ 的 Laplace 分布。

2. 匿名化

数据匿名化是将数据集经过一定的变换之后,生成一种在一定范围内无差别的新数据集然后进行发布,使得攻击者无法根据发布出来的新数据集推导出某个个体是否具有敏感信息,从而实现对数据的隐私保护。

目前匿名化方案主要有泛化/隐匿技术和基于微聚集匿名化技术两种,其中泛化/隐匿技术是基于数据匿名化的一种典型技术,但存在的问题是不区分数值型数据与分类型数据,使得数据泛化后丢失了更多其数据的语义;其次是泛化的计算复杂度非常高^[30]。

2.4.12.2. 典型应用示例

在确保常规的网络安全前提下,数据拥有者一般都会对敏感数据进行加密保护,但是对其他非敏感数据不做处理。而攻击者可以根据被公开的信息结合攻击者已经获取到的背景知识,来推断出这些敏感数据。保护的方法是利用基于隐私的数据匿名化技术,对原始数据进行处理,生成扰动数据,在不影响下游数据统计、加工的前提下,最大限度保护数据安全。

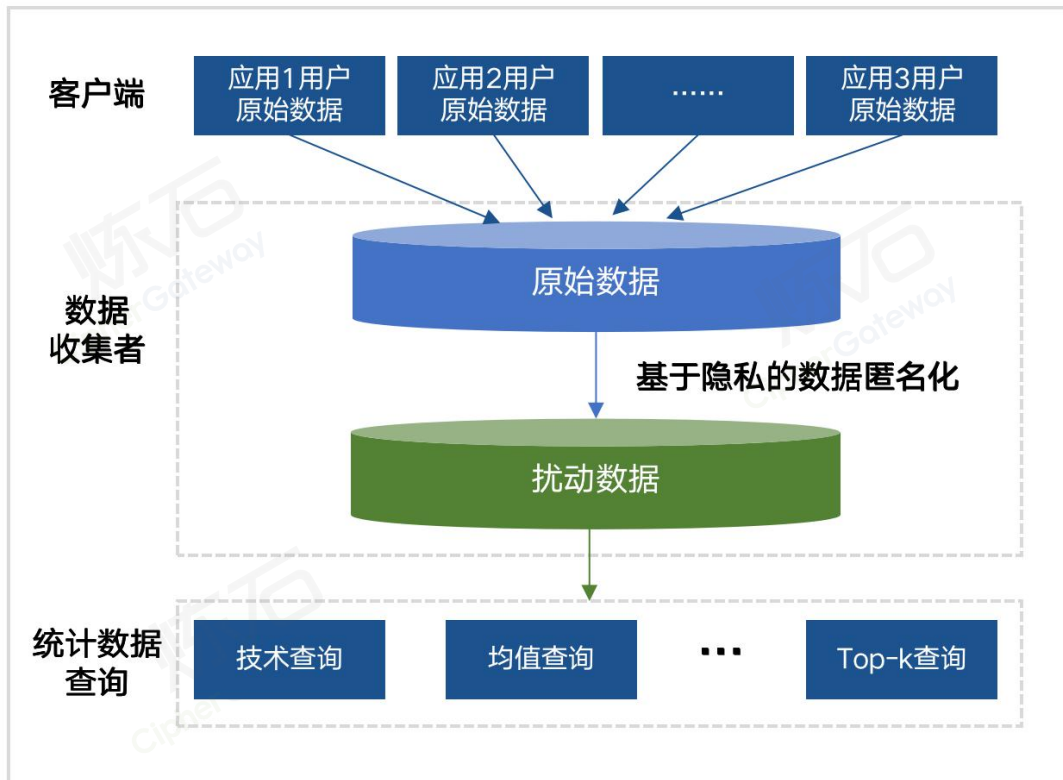


图 46 基于隐私的数据匿名化示意图

2.4.13. 基于属性加密的访问控制

2.4.13.1. 模式说明

2.4.13.1.1. 威胁分析

云计算、物联网等新型计算环境为我们提供了便捷的数据共享、融合计算等服务，极大地提高了对数据的处理效率，使计算和存储资源得到充分的利用，其中包含了大量的具有“所有权”特征的个人隐私数据。然而，普遍存在使用方权限过大，不受限访问导致隐私数据泄露事件频发。

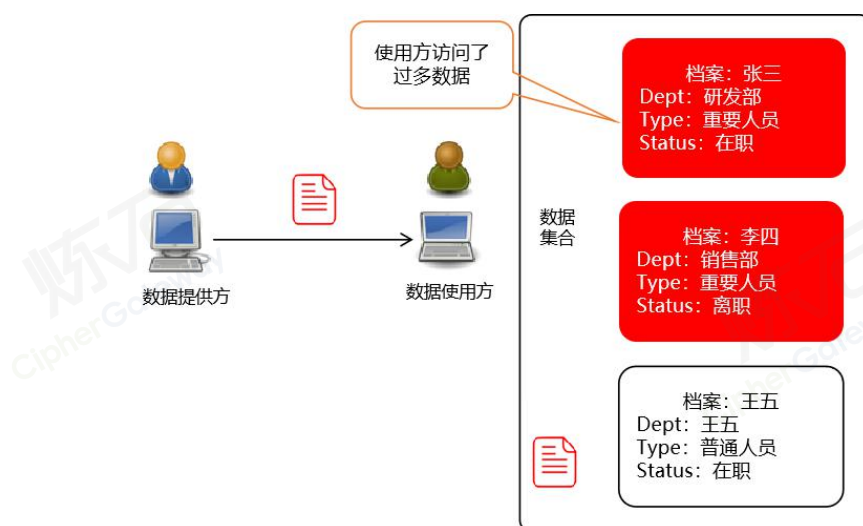


图 47 隐私数据泄露威胁

隐私数据泄露事件使得用户对通过新型计算环境获取数据服务时的数据安全性提出了质疑，隐私数据必须要满足“有限公开”原则，即只有授权用户才能搜索到授权允许访问的信息。

访问控制技术根据预先设定的访问控制策略，保障资源只能被合法用户执行合法操作，防止了信息的非授权访问。然而，新型计算环境所具有海量性、动态性、强隐私性等特点，给访问控制技术的应用带来了巨大的挑战，使得传统的面向封闭环境的访问控制模型如 DAC、MAC、RBAC 等难以直接适用于新型计算环境。

2.4.13.1.2. 防护模型

基于用户、资源、操作和运行上下文属性所提出的基于属性的访问控制 (Attribute-Based Access Control, ABAC) 将主体和客体的属性作为基本的决策要素，灵活利用请求者所具有的属性集合决定是否赋予其访问权限，能够很好地将策略管理和权限判定相分离。由于属性是主体和客体内在固有的，不需要手

工分配，同时访问控制是多对多的方式，使得 ABAC 管理上相对简单。并且属性可以多个角度对实体进行描述，因此可根据实际情况改变策略。除此之外，ABAC 的强扩展性使其可以同加密机制等数据隐私保护机制相结合，在实现细粒度访问控制的基础上，保证用户数据不会被分析及泄漏。

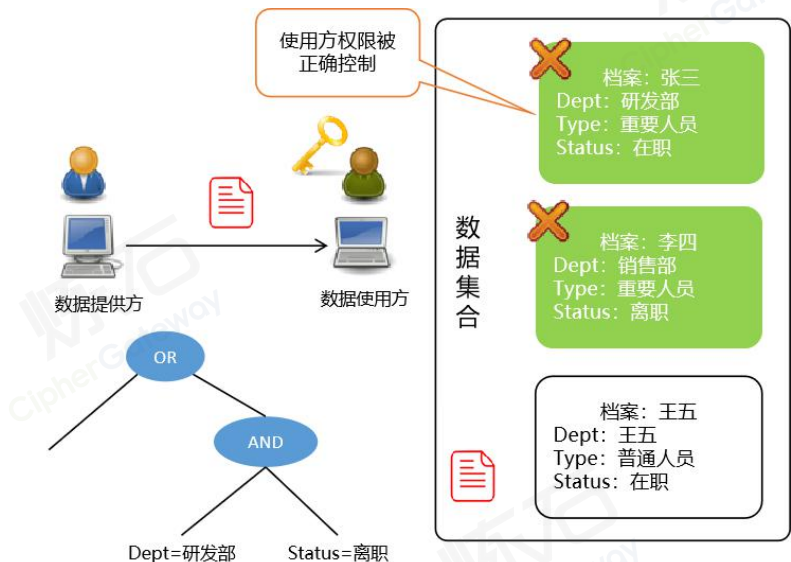


图 48 细粒度访问控制防护模型

ABAC 系统按其执行操作种类的不同可分为准备阶段和执行阶段。准备阶段主要负责收集构建访问控制系统所需的属性集合以及对访问控制策略进行描述。而执行阶段主要负责对访问请求的响应及对访问策略的更新。属性权威 (Attribute Authority, AA) 预先收集、存储和管理构建安全的访问控制所需的所有属性以及属性—权限之间的对应关系。因此为了构建安全的 ABAC，首先需从海量的类型各异的访问主体和访问客体挖掘出独立、完备的主体属性、客体属性、权限属性和环境属性集合，并构建这些属性同相关实体之间的关联关系。属性的独立性保证了属性集合中不存在意义相似的冗余属性，减小了系统的存储和管理负担。完备性则保证了属性集合可以提供访问控制系统所需的所有属性，

保证了系统的安全性。当获得属性集合后，需要对属性与权限之间的对应关系进行分析。当获取独立完备的属性集合以及属性－权限对应关系后，策略管理点（Policy Administration Point, PAP）利用这些信息对访问控制策略进行形式化描述。

在执行阶段中，当接收到原始访问请求（NAR）之后，策略实施点（Policy Enforcement Point, PEP）向 AA 请求主体属性、客体属性以及相关的环境属性，并根据所返回的属性结果集构建基于属性的访问请求（AAR）并将 AAR 传递给策略决策点（Policy Decision Point, PDP），PDP 根据 AA 所提供的主体属性、客体属性以及相关的环境属性，对用户的身份信息进行判定。通过与 PAP 进行交互，根据 PAP 提供的策略查询结果对 PEP 转发来的访问请求进行判定，决定是否对访问请求授权，并将判定结果传给 PEP，最终由 PEP 执行判定结果。但是在 ABAC 中用户的身份是由一系列属性组成的集合来表示，具有较强的匿名性，这种匿名性导致用户可能滥用其所拥有的属性带来的权限。通过引入身份认证机制可以有效保证用户所提供属性的可靠性及数据源的不可否认性，增强访问控制系统的安全性。同时新型计算环境中用户和设备的动态特性带来了权限的频繁变动，需要对这些变动实时响应，更改相应的权限，保证系统安全可靠的运行。

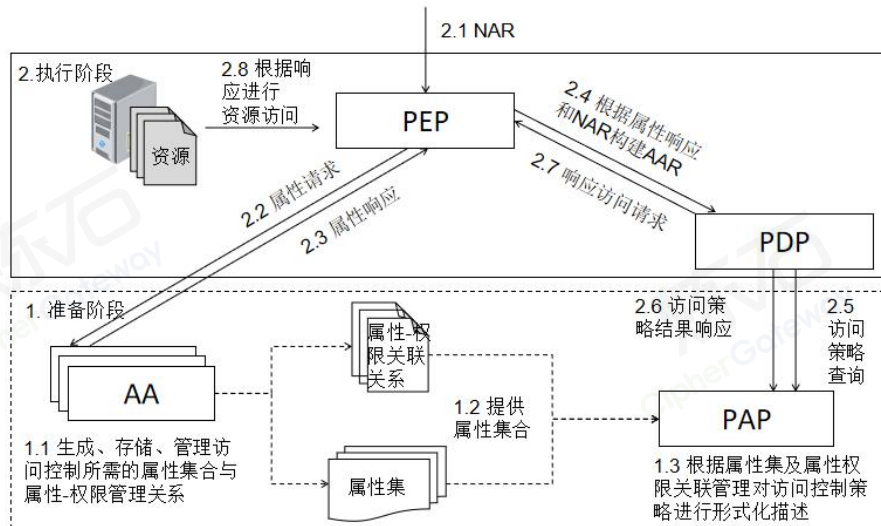


图 49 ABAC 机制框架示意图

2.4.13.2. 典型应用示例

典型应用为基于属性的加密。

虽然传统的 ABAC 有效控制了用户对资源的访问操作，但其仅实现了对用户访问过程的控制。为了最大限度地保护数据的隐私安全，实现更细粒度的访问控制，研究者们提出了基于属性的加密机制（Attribute-Based Encryption, ABE）。ABE 实现了对数据机密性的访问控制。其采用非对称密码机制并利用属性作为加解密的关键要素，将属性同密文和用户密钥相结合。当用户属性与密文属性的公共集合满足加密时访问结构所规定的参数时才能解密相应数据。

ABE 机制也可分为准备阶段和执行阶段。准备阶段中 AA 的任务同传统 ABAC 中相同，负责预先收集，存储和管理构建安全的访问控制所需的所有属性。Authority 根据不同的访问结构及属性设计访问控制策略，并将这些策略封装在资源加密密钥或用户解密密钥中。

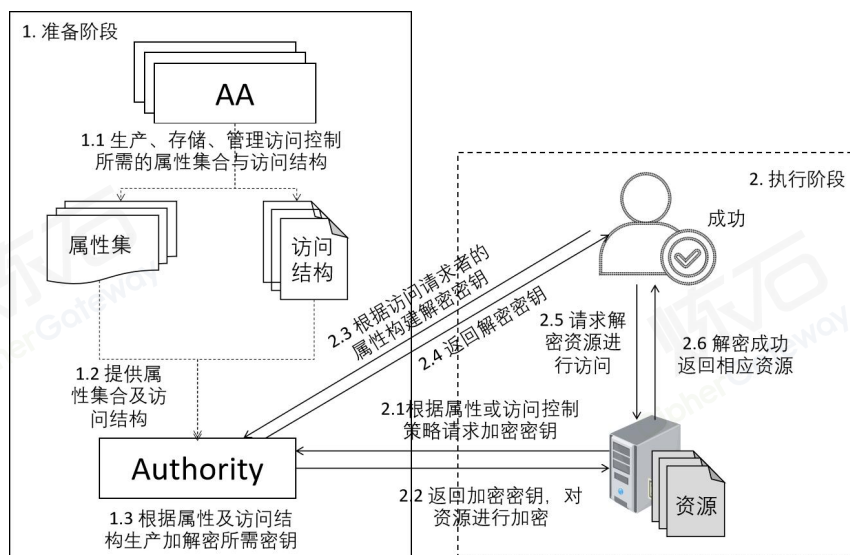


图 50 ABE 机制框架示意图

在执行阶段中，用户通过 AA 获取相关的属性并根据自身属性向 Authority 请求解密私钥，之后利用所获取的密钥对密文进行解密并返回最终结果。

2.4.14. 锚点解密的防绕过数据安全

2.4.14.1. 模式说明

2.4.14.1.1. 威胁分析

传统的加密与访问控制组合模式中，加密施加在数据库侧，访问控制通过 4A 或 IAM 策略中心下发认证和权限决策。如下图所示，这种模式下解密和权限是两个决策点，加密设备将数据解密后以明文形式传输到服务端，数据解密无法和权限体系结合，加解密和访问控制的分离带来威胁敞口，攻击者可以绕过访问控制，从威胁敞口直接窃取数据。同时，数据库加密设备与 IAM 策略中心需要重复定义字段级的安全策略，造成重复配置、增大维护难度。



图 51 数据访问控制机制被绕过

数据在服务端可被攻击者直接窃取，另一方面访问控制可以被绕过，攻击者也可以窃取数据，同时审计置信度较低，这既带来数据泄露的威胁，也是对安全机制本身的破坏。

2.4.14.1.2. 防护模型

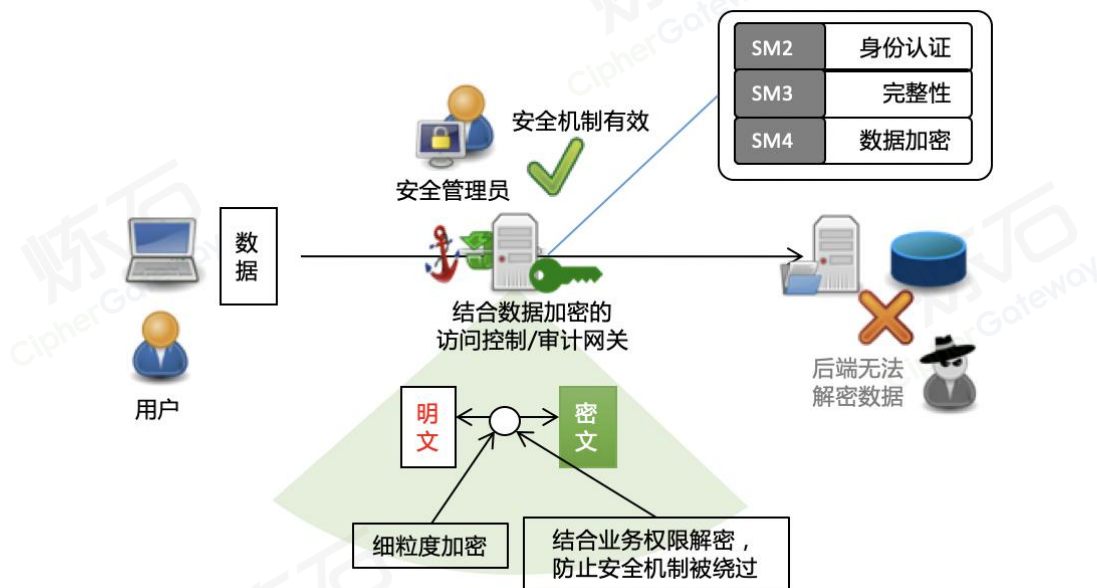


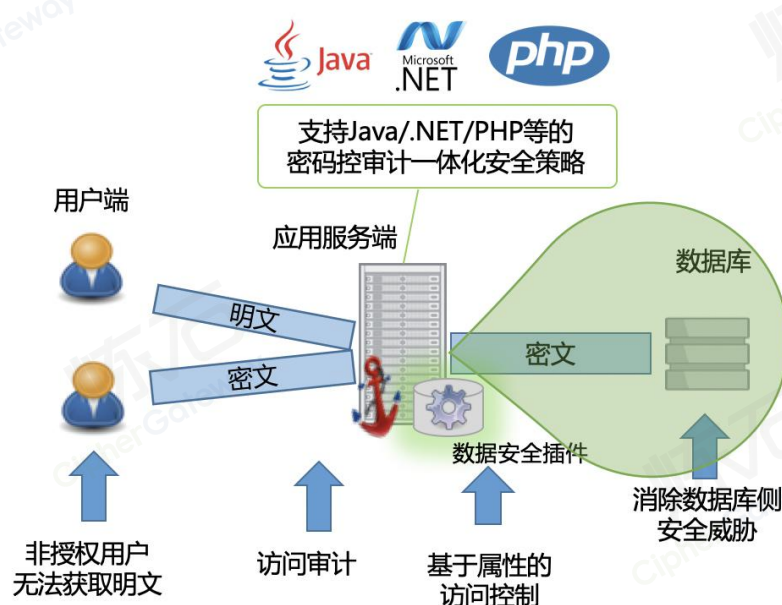
图 52 基于密码控审一体化的防绕过机制

基于密码技术，用加密构建一个数据的集中控制点，要有效使用数据，必须到这一点进行解密，而在解密前要对身份进行认证，并对访问行为进行审计，留存日志提供高置信度审计，打造无法绕过的安全机制。

将密码技术与细粒度访问控制以及安全审计结合，可以形成“防绕过”的安全机制。通过识别应用中的访问主体，可实现“主体到人、客体到字段”的细粒度访问控制。

2.4.14.2. 典型应用示例

在数据加密的基础上再实施访问控制策略，可以打造有效的数据防护。如下图所示，CASB 插件模式把数据解密与访问控制、审计等技术结合，共同构建“防绕过”的数据安全防护体系。同时，在解密的节点上做访问控制和审计，访问控制的策略就难以被绕过，这时审计也具有高置信度。CASB 插件模式支持第三方数据库审计系统，以独立于业务应用之外的方式实现审计。通过对审计日志进行完整性保护，保证可事后追责。



2.4.15. 不可信环境中的数据运算

2.4.15.1. 模式说明

2.4.15.1.1. 威胁分析

不可信环境指的是能够独立完成分配的计算任务但是无法保证计算任务的机密性和完整性的资源。比如：随着大数据时代的到来，云计算得到了广泛的应用，进而衍生出云存储这一重要存储模式，它能够为企业和个人提供大容量的存储平台、具有易于管理，扩展性高、低成本等特点。云存储模式的出现，存储用户不再需要购买昂贵的设备，只需要支付少量的费用，就可以将自己的数据存储云服务器上，更加的方便、快捷。数据外包实际是用户放弃对数据的最终控制权，数据的安全性和完整性成为影响用户选择云存储的主要影响因素。

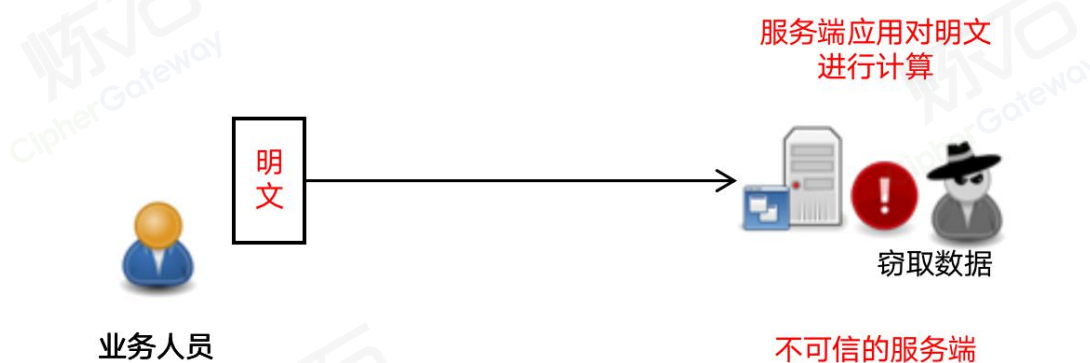


图 54 不可信服务端对明文进行计算示意图

2.4.15.1.2. 防护模型

一方面要利用不可信服务环境的计算资源，另一方面又要确保数据万无一失，实现“环境不可信但数据可信”的目标，可以在客户端对数据进行加密之后再送到服务端进行处理，服务端应用对密文进行处理和计算，并且能够返回正确的结果到客户端。在此过程中，密钥一直掌握在数据拥有者的手里，潜伏在服务端的攻击者无法获取数据明文。

常见的不可信环境中密文运算方案有：同态加密、MPC 多方计算、零知识证明等隐私计算技术。

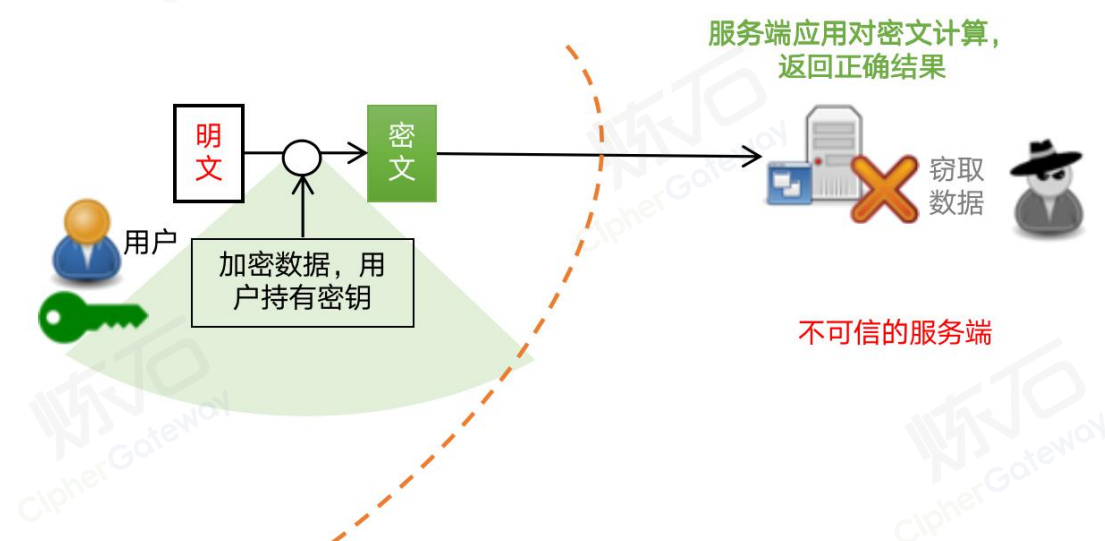


图 55 不可信服务端环境运算示意图

2.4.15.2. 典型应用示例

2.4.15.2.1. FHE 全同态加密

随着互联网的发展，尤其是云计算概念的诞生，人们在加密数据搜索与处理等方面的需求日益增加，大大推动了全同态加密方向的科学研究。与此同时，自Gentry 的创新性工作发表以来，关于全同态加密的研究工作开始出现了新的高潮，被广泛应用于多种实际环境。

下面是全同态加密的一些典型应用：

1. 全同态加密一般性应用框架

密码协议是大多数安全模块中必备的环节，从广义上讲，所有的密码协议都是安全多方计算的一个特例。它们广泛应用于金融交易、社交网络、实时监控、信息管理等多个领域。常见的密码协议中，通常包括多个参与者，他们可能是可信方（例如用户自己、经过认证的参与者）或不可信方（未经认证的参与者）。理论上，凡是存在不可信方的协议都具备全同态加密应用的可能。因此，全同态加密的大部分应用都可视作安全多方计算的范畴。

当不可信方需要对敏感数据进行搜索、分析、处理等操作时，协议的其他参与者不希望不可信方掌握明文数据，因此可以采用全同态加密方案，让不可信方直接对密文进行操作，实现等同于对原始数据直接进行处理的效果，从而完成用户的需求。我们给出全同态加密的一般性应用框架，如下图所示：

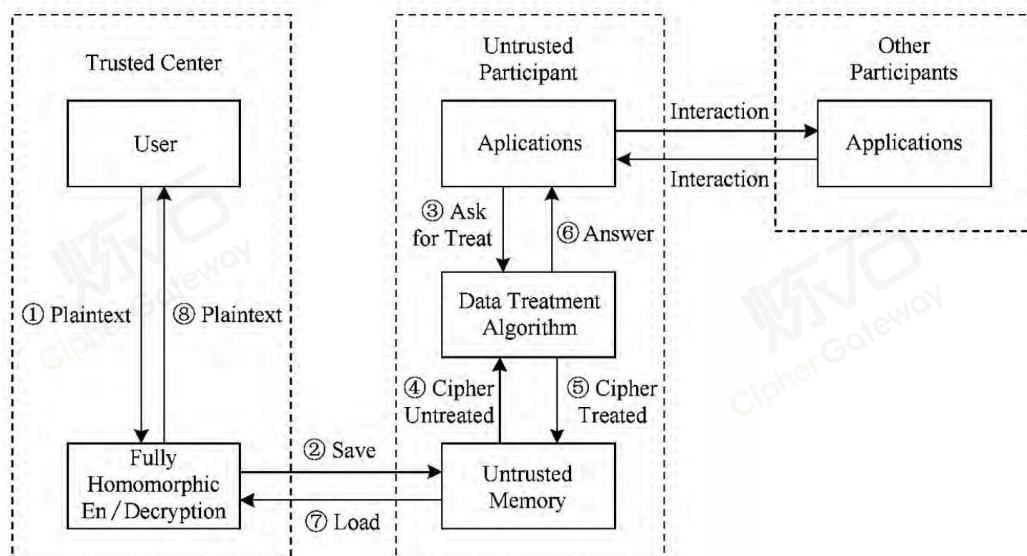


图 56 全同态加密的一般性应用框架

加密数据处理方法简述如下：假设存在全同态加密函数 $Enc_k(x)$ ，首先用户用自己的私钥 k 对需要处理的数据 m 进行同态加密 $c = Enc_k(x)$ ，然后将加密数据 c 上传到云端服务器。服务器能够对加密数据 c 直接进行处理，得到 $c' = f(c) = f(Enc_k(x))$ ，然后将处理后的密文 c' 返回给用户。用户收到 $c' = f(c) = f(Enc_k(x)) = Enc_k(f(m))$ 后，利用自己的私钥 k 对其进行同态解密，得到已经处理好的明文数据 $f(m)$ 。

2. 云计算中的全同态加密

云存储安全是云计算领域的重要安全问题之一。为解决数据隐私保护的问题，常见的方法是由用户对数据进行加密，把加密后的密文信息存储在服务端。然而，当用户需要服务器提供数据搜索、分析、处理等功能时，传统加密方案难以实现，但全同态加密为之提供了实现的可能。

(1) 云计算中的加密数据检索

随着云计算技术的广泛应用，服务器端存储的加密数据必将呈爆炸式增加，对加密数据的检索成为一个迫切需要解决的问题。现有的加密数据检索算法包括线性搜索、公钥搜索和安全索引等，这些算法可以快速地检索出所需信息，但是它们只适用于小规模数据的检索，而且代价很高。基于全同态加密技术的数据检索方法可以直接对加密的数据进行检索，不但能保证被检索的数据不被统计分析，还能对被检索的数据进行简单的运算，同时保持对应的明文顺序。

数据检索有多种方法，如向量空间模型等。首先对文档进行分词和词干化，即从文档中抽取出能表征文档主要内容特征和形式特征的检索词，以形成文档的向量表示。然后将得到的检索词和待检索文档进行加密，并储存至云服务器。采用了全同态加密方案后，当服务器需要检索加密文档时，可直接提交加密后的检索词。此时每个文档都可根据所提交的关键词进行权重向量表示，对用全同态加密后的词频和倒排文档频率进行操作可以得到权重：

$$W_{i,k} = \frac{(\lg f_{ik} + 1.0) \times \lg \frac{N}{n_k}}{\sqrt{\sum_{k=1}^l \left[(\lg f_{ik} + 1.0) \times \lg \frac{N}{n_k} \right]^2}}$$

其中， $f_{i,k}$ 为检索词 T_k 在文档 D_i 中出现的频率， N 为整个文档集包含的文档数， n_k 为整个文档集中含检索词 T_k 的文档数。该权重反映了关键词与文档的相关度，因而可以根据大小进行排序，筛选出用户需要的文档。用户得到加密文档后，用私钥对文档解密即可得到原始文档，整个过程如下图所示^[31]

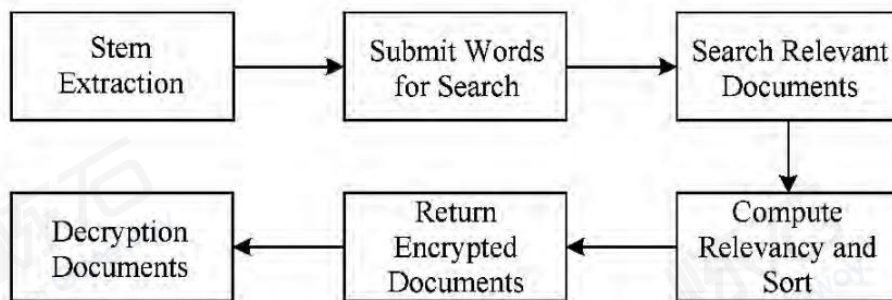


图 57 基于全同态的数据检索过程

(2)云计算中的加密数据处理

云计算中的加密数据处理和云计算中加密数据检索的思路类似。首先对待处理的关键数据进行加密和特殊标记，以与普通加密数据区分开来，然后再上传到服务器。服务器会直接对密文数据进行操作来完成用户的需求，并将处理后的密文返回给用户。目前人们对加密数据处理已经开始了一定的应用研究。

3.电子投票

在计票的快捷准确、人力和开支的节省、投票的便利性等方面有着传统投票方式无法企及的优越性。而设计安全的电子选举系统是全同态加密的一个典型应用。文献描述了一个简单的电子选举方案：1）若有同态函数 $Enc_k(x_1 + x_2) = Enc_k(x_1) \times Enc_k(x_2)$ ，选民将自己的选票进行加密 $C_i = Enc_k(M_i)$ ，其中 $M_i \in \{0, 1\}$ ；2），投票中心收集同态加密后的选民选票 C_i ，投票中心基于全同态加密方案的同态性质对加密后的选票 C_i 进行计票 $C = C_1 \times C_2 \times \dots \times C_n$ ，得到经过同态加密后的选举结果 $C = Enc_k(M_1 + M_2 + \dots + M_n)$ ；3）只有拥有解密密钥的某个可信机构才能够对加密后的选举结果进行解密，公布选举结果。在上述过程中，选票收集与计票完全对加密后的选票数据进行操作，不需要

使用任何解密密钥。因此，任何一个主体或机构都可以完成计票员的职责，无论其是否可信。

4. 数字水印

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记，这种标记通常是不可见的，只有通过专用的检测器或阅读器才能提取。如何应对复杂网络环境下数据隐藏与数字水印系统的安全挑战，是目前需要迫切解决的问题。针对数字水印的一种主要的安全性攻击手段是非授权检测攻击，即攻击者在未经授权的情况下对含有水印的载体进行检测，以确定水印是否存在，进而猜测或破译水印的含义，甚至去除载体中的水印并嵌入一个伪造的水印。文献^[32]提出的基于全同态加密的数字水印方案可以有效地抵抗这种攻击。该方案首先利用全同态加密体制对水印信号与原始载体进行加密，然后将加密后的水印嵌入到原始载体中。在用户检测水印之前，必须首先对含有水印的载体进行同态解密，从而保证解密后的水印信号与含水印的载体之间没有明显的相关性。在解密含水印的载体之后，可以通过计算解密后的载体与水印信号之间的相关度，判断水印的存在性进而提取水印。下图描述了传统的数字水印方案与基于全同态加密的数字水印方案的区别：

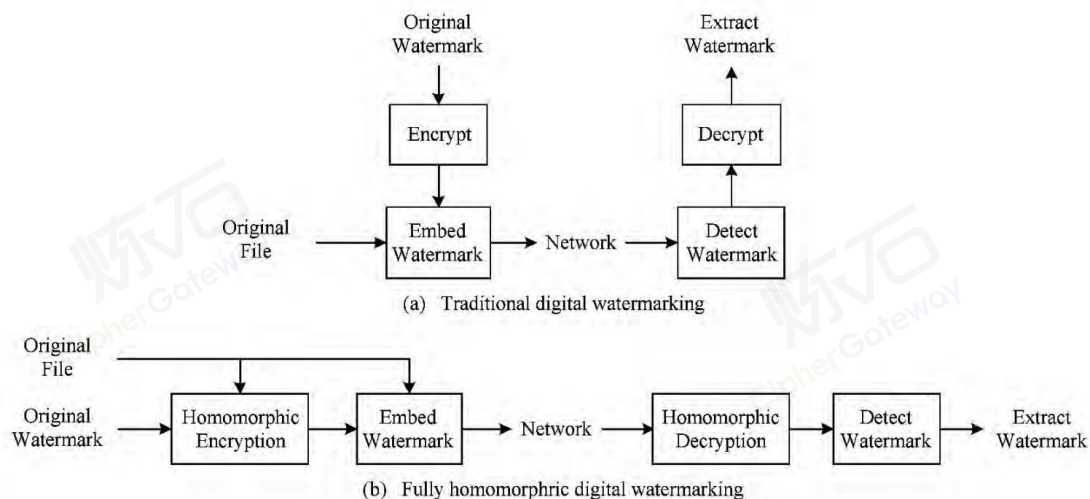


图 58 传统数字水印与基于全同态加密的数字水印的区别

全同态加密在云计算、电子商务等实际中的重要应用使其受到密码学家越来越多的关注^[33]。

2.4.15.2.2. MPC 安全多方计算

1.安全多方计算简介

安全多方计算解决了在一些互不信任的参与方之间联合计算一个函数的问题。该技术最早是由姚期智院士在 1982 年时提出的百万富翁问题引出的。这个问题描述了“两个百万富翁希望知道谁更富有一些，但他们互相不希望知道对方财富的具体信息。那么，这样一个对话应该如何进行呢？”

具体而言，安全多方计算中， n 个计算参与方分别持有数据 x_1, x_2, \dots, x_n ，协议目的是利用各方秘密数据计算一个预先达成共识的函数 $y_1, \dots, y_n = f(x_1, x_2, \dots, x_n)$ ，此时任意一方可以得到对应的结果 y_i ，但无法获得其他任何信息。这种协议所达成的目标可以类比为如下理想模型：所有计算参与方将他们各自的数据发送给一个可信第三方，之后在第三方本地进行函数计算并返回结果。

而安全多方计算则代替这个场景下的可信第三方。例如，假设有 3 个参与方分别拥有隐私输入 x 、 y 、 z ，他们同意计算如下函数的结果 $F(x, y, z) = \max(x, y, z)$ ，并同时保护自己数据隐私。如果本次计算结果为 z ，那么第三个参与方即知道他的输入是最大值，而另外两方知道他们的输入不等于最大值 z 。这个简单的例子可以推而广之到每一方都有一些输入和输出，以及函数对不同参与方的输出不同的情景。

2. 安全多方计算安全模型

安全多方计算不只是一个单独的协议，而是一个在不断丰富和成长的解决方案集合，其中每一个方案都有不同的性质和性能。这里先规定参与计算的各参与方角色：输入方负责将敏感数据输入到安全计算中；结果方需要得到安全计算的全部或者部分结果；计算方负责联合进行本次计算。

任何一个参与安全多方计算的参与方都会担任其中一种或多种角色，比如金融衍生品场外交易匹配应用场景中，参与交易的买方和卖方同时扮演了上面 3 种角色；而提供密钥管理系统的服务提供方，会同时持有上述 3 种角色，但不同的运算机器会扮演不同的角色。

安全多方计算可被看作一个分布式计算机程序的一组指令，这个程序由一系列由所有参与方提前达成共识的固定交互步骤构成，每个参与方输入一段秘密信息并且获得最终输出。构建这种协议的直观方式是构造一个将输入映射到输出的随机映射，也即普通函数的一般化形式，因为普通函数不包含任何内在随机性，在这个过程中，安全多方计算会关注两个方面的特性：

(1) 输入隐私性：从协议执行中所暴露出来的信息不能推导出任意参与方的隐私输入，除去那些可以通过计算结果反推出的部分。

(2) 鲁棒性：任何协议能容忍的敌对合谋参与方子集都不能通过分享信息或者篡改指令来使得诚实方输出一个错误结果。

安全多方协议是一种不依赖于可信个人或者机构的密文计算技术。因此，这种技术可以创立比现有机构更有公信力的机构。一些已被验证或值得开发的解决方案包括：第一，利用安全多方计算去整合现有的可信机构，从而获得更可信和自然的解决方案；第二，利用参与方的对立利益来增加安全多方计算的可信度，如金融衍生品场外交易匹配系统；最后，可通过安全多方计算的分布式安全优势，将信任分发到一组参与方中，使得攻击者需要处理一个更为复杂的多方攻击问题^[34]。

2.4.15.2.3. ZKP 零知识证明

零知识证明(Zero-Knowledge Proof)是由 Shafi Goldwasser、Silvio Micali、和 Charles Rackoff 在 1985 提出的。指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

零知识证明的思想被广泛运用在密码学和区块链领域，Zcash 是首个使用零知识证明机制的区块链系统，它可提供完全的支付保密性，同时仍能够使用公有区块链来维护一个去中心化网络。

零知识证明被广泛应用于多个领域，如数据的隐私保护、身份认证、去中心化存储、区块链、数字金融等，并且未来应用或更加广泛。由此可见，掌握零知识证明的原理和应用就显得格外重要^[35]。

2.4.15.2.4. 区块链隐私保护

区块链具备六大特性：去中心化、不可篡改、可追溯、自治性、开放性和匿名性。目前主流的公链平台如比特币、以太坊仍然是明文直接上链，因转移 / 交易数据完全公开，泄露了用户的隐私信息。为解决相关问题，出现了 CoinJoin、TumbleBit、Monero 等方案。这些方案一定程度上解决了匿名性的问题，却仍然无法适应复杂应用环境下的转移 / 交易数据的隐私保护。2017 年底，以太坊创始人 Vitalik Buterin 总结了有关区块链隐私保护的现有工作，并探索了以太坊的 4 种解决方案，即渠道、混合器、环签名和零知识证明。其强调，尽管零知识证明效率低下且难以实施，但其既能不泄露数据隐私，又能证明数据的真实性，仍然是以太坊隐私问题的最有力解决方案。2019 年，Rehmani 等提出了一种基于公共区块链的分布式共乘服务，利用智能合约和零知识证明实现了用户隐私安全的保护。

除此之外，现在越来越多的区块链应用选择仅将数据的哈希值上链，如以闪电网络技术和雷电网络技术为代表的链下隔离通道方案、以 Fabric 为代表的多链通道隔离技术。显然这些方案因没有将真正的数据上链，虽然降低了链的存储压力，但链下数据存在易泄露、易破坏等诸多问题，导致真正应用时数据失效的可能增大。

轻量级同态加密是处理长数据加密的理想方法。在上链之前，先对转移 / 交易数据和余额信息进行轻量级加密，且存储在该链上，当链上的所有用户访问链中的信息时，仅看到的是经过同态加密后的信息，从而有效地保护如账户的资金等隐私信息^[36]。

2.4.16. 可验证结果的计算外包

2.4.16.1. 模式说明

2.4.16.1.1. 威胁分析



图 59 外包计算威胁

随着云计算和大数据时代的到来，用户与服务提供者计算能力不对等的现象愈加突出，如何安全有效地进行外包计算引起了人们的广泛关注。所谓外包计算，就是计算能力较弱的用户将私有数据外包给计算能力更强的服务提供者(如云服务器等)，由服务提供者返回最终的计算结果。但是，服务提供者并不是完全可信的，它们有可能泄露用户隐私数据，或返回错误的计算结果。因此，如何保护用户隐私、并有效验证外包服务的计算结果具有重要的理论价值与现实意义。

2.4.16.1.2. 防护模型

可验证外包计算（verifiable outsourcing computation）是指对云外包计算结果正确性的验证^[37]。在完成隐私保护的外包计算后，用户接收计算结果并向云服务供应商（CSP）提出验证请求，由 CSP 返回一些证据。用户通过验证该证据，可以判断云计算结果是否准确无误。可验证外包计算的一般化流程如下图所示，除正确性保护之外，可验证外包计算有时也具备抗抵赖和防止伪造的特殊功能。

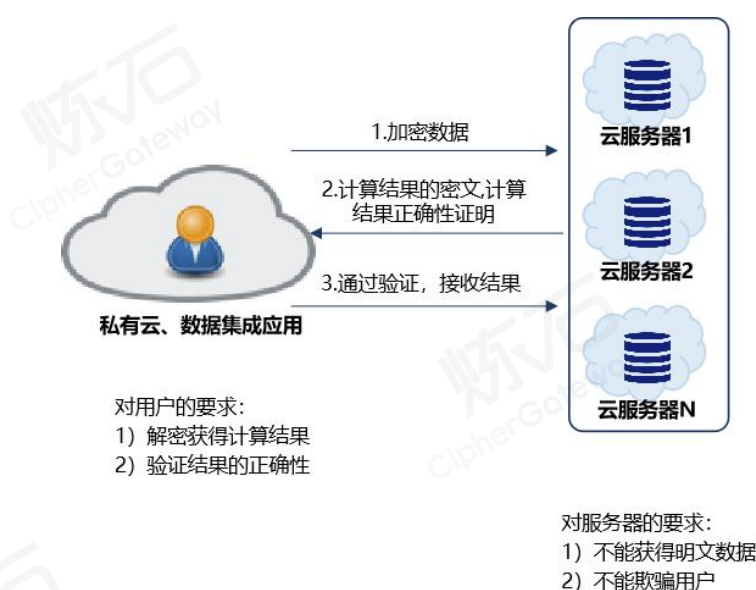


图 60 可验证外包计算流程

流数据规模的快速增长为可验证外包计算方案带来了严峻的挑战。例如天气预报、流量管理、市场分析等应用场景，资源受限的数据所有者通常会连续地收集、产生数据流，并将它们立即外包给云端服务器。此后，CSP 如何为外包计算结果构造有效的证据，使其顺利通过用户检验且无法伪造，是可验证计算中的一个新问题。现有研究已经实现了流数据在分组聚合查询与线性代数查询中的可验证性，并支持数据值动态更新。

2.4.16.2. 典型应用示例

典型应用为可验证大型线性方程组求解外包计算。

针对目前大型线性方程组求解在外包计算中遇到的用户信息泄露、计算结果被篡改等问题,提出一种安全高效的^[38]可验证外包计算方案。通过随机置换和线性方程组的恒等变换,构造了新的具备相似解的线性方程组,避免了当前数据伪装方案易受求解公因式法攻击的问题,同时提高了客户端的验证效率,降低了空间复杂度。性能分析表明,该方案具有极高的效率。

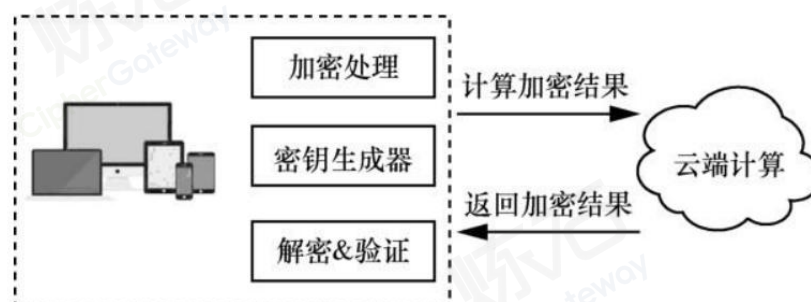


图 61 外包计算模型

客户端:在客户端,用户的工作主要包括数据加密和数据解密验证这 2 个方面。在数据加密阶段,客户端利用密钥生成器,随机生成密钥值。然后,利用方程组的恒等变换和矩阵的可逆变换对增广矩阵进行处理,实现数据加密。在解密验证阶段,客户端通过逆变换将矩阵还原,然后找出解向量中添加的随机值,验证其是否正确,同时将原方程组的解向量随机代入方程组中的几个等式中,验证其正确性。

云服务器端:云服务器端的主要工作是根据用户发送的数据信息,如实地进行求解线性方程组的运算。客户端并不关心服务器以何种方式进行求解运算,只需要其能够返回运算结果,即线性方程组的解向量。

2.4.17. 封装业务逻辑的可信运算环境

2.4.17.1. 模式说明

2.4.17.1.1. 威胁分析



图 62 应用运行环境存在风险

随着移动互联网、物联网等新型计算环境的普及，安全问题愈发严重，尤其是恶意代码攻击严重威胁着用户的隐私和财产安全^[39]。这些安全威胁主要利用计算平台上的安全漏洞进行攻击，根本原因在于计算平台缺乏体系架构上的主动防御手段。因此，如何在体系架构上实现主动防御机制，从底层芯片出发，提供基于硬件的平台完整性和机密性保护的整体安全解决方案，已经成为目前面临的根本问题。

2.4.17.1.2. 防护模型

可信计算是一种主动防御技术。它利用硬件属性作为信任根，系统启动时逐层度量，建立一种隔离执行的运行环境，保障计算平台敏感操作的安全性，从而实现可信代码的保护。

1. 可信平台模块

TCG 可信计算平台提供了受保护的能力、对完整性度量进行存储和报告的能力、平台证明三个基本特征。受保护能力是由具有访问被屏蔽位置权限的命令组成的命令集；完整性度量指得到影响平台完整性的量度，存储上述所得值且将其摘要放入平台配置寄存器的过程；证明即确定信息是否真实，外部实体可以验证其被屏蔽的位置和受保护的程度以及信任根。TCG 提出的可信平台模块 TPM 被业界广泛的应用。TPM 具有平台数据保护功能，存储与报告完整性功能，对资产进行保护功能，其他辅助功能，对身份进行认证的功能以及密码学运算等功能等。TPM 的硬件构成如下图所示：

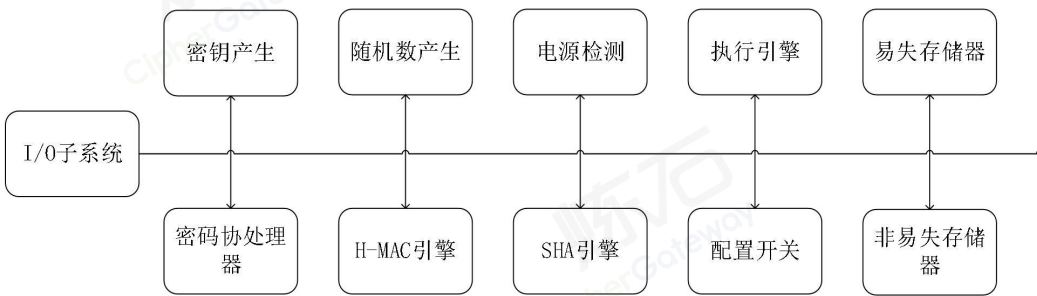


图 63 TPM 硬件构成

此外，TCMU（中国可信计算工作组）同样提出了可信计算平台模块 TCM。TCM 的目标为建立安全信任根基。TCM 核心功能为对平台的完整性进行量度，建立平台免疫力；作为平台身份的唯一标识；提供了密钥保护和硬件及密码学计算。

2.可信运行环境

TEE（Trusted Execute Environment）叫做可信运行环境，与 REE（Rich Execution Environment）相对应。参考 TEE System Architecture v1.1 规范文档，可得知 TEE 系统架构如下图所示。

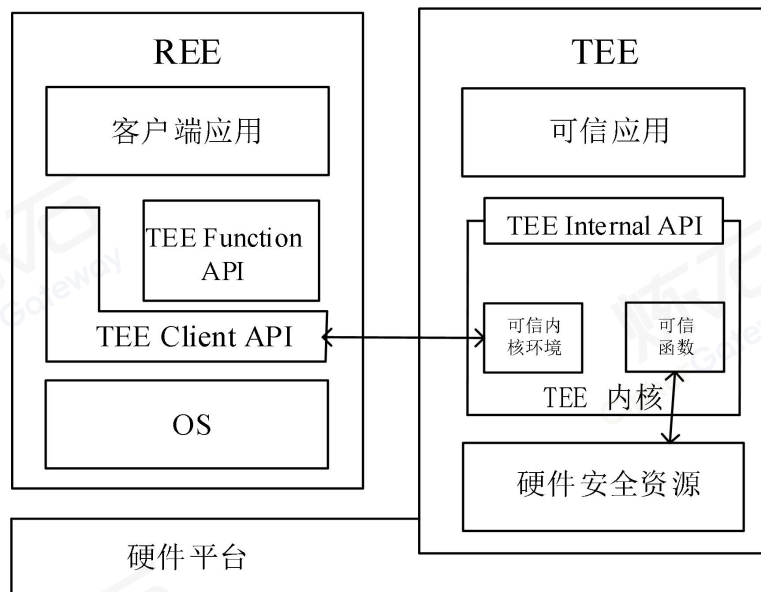


图 64 TEE 系统架构

系统架构分成了三部分：REE 环境、TEE 环境以及硬件平台，其中 REE 与 TEE 相互分离，同时他们的硬件资源同样相互分离。两个分离的环境通过 API 进行数据交互。

2.4.17.2. 典型应用示例

金融数据密码机主要用于金融领域内的数据安全保护，基于国密算法的金融数据密码机是应用层节点数据密码机，是一个物理安全的实体，承担主机安全模块（Host Security Module）的作用，能够实时地为主机提供密钥管理、消息验证、数据加密、签名的产生和验证等密码服务，保证数据从产生、传输、接收到管理整个过程的安全性、有效性、完整性、不可抵赖性等安全问题。相比通用功能的服务器密码机，金融数据密码机封装了金融系统的专有业务逻辑。

标准 GM/T 0045-2016 规定了金融数据密码机产品的功能要求、硬件要求、业务要求、安全性要求等。¹

(1) 根据金融业务系统的需求，金融数据密码机采用基于对称密码体制的三层密钥体系结构，如下图所示。分别为主密钥、次主密钥和数据密钥三层。金融数据密码机中的密钥采用“自上而下的逐层保护”的分层保护原则，即主密钥保护次主密钥，次主密钥保护数据密钥。所有的密钥都不能以明文形态出现在金融数据密码机外部，必须采用加密或者知识拆分的方式进行密钥的导入/导出。其中数据密钥直接被用户使用，提供金融数据的加解密等服务。

A 主密钥。主密钥是一种密钥加密密钥，其主要作用是保护其下层密钥的安全传输和存储。主密钥的存储必须采用强安全措施，不能以明文方式出现在密码机外。主密钥可采用加密存储或微电保护存储方式。采用微电保护的存储方式时，密钥可以明文方式存储，但需要设计有销毁密钥的触发装置，当触发装置被触发时，销毁存储的所有密钥。

B 次主密钥。次主密钥是一种密钥加密密钥，其主要作用是保护数据密钥的安全传输、分发和存储。由于采用的是对称密码机制，因此一般需要通过离线分发的方式进行密钥的分享。

C 数据密钥。数据密钥是实际保护金融业务数据的密钥，直接用于加密或校验各类应用数据，包括 PIN 密钥和 MAC 密钥等。数据密钥一般不在密码机中长期存储，多个密码机在共享次主密钥的基础上，利用次主密钥保护各类数据密钥的安全传输以完成数据密钥的共享。数据密钥的使用最为频繁，一般需要按时更新。

¹ 原文链接：<https://blog.csdn.net/Lapedius/article/details/109153695>

(2) 金融数据密码机的接口符合 GM/T 0045-2016 的接口要求。不同于设备接口规范的 API 接口形式，金融数据密码机的接口直接以网络数据包格式的形式定义，可利用 SOCKET 编程直接调用。其接口主要分为几大类：

磁条卡应用接口：主要支持各类密钥的生成、注入、合成和转加密。

IC 卡应用接口：主要支持数据加解密、数据转加密、脚本加解密、MAC 计算等。

基础密码运算服务接口：提供最基本的各类密码计算服务，包括 SM2 签名验签、加密解密、SM4 加密解密、SM3 消息摘要等。

金融数据密码机支持密钥存储、密码机生成密钥后可以将其存储在内部的安全存储区域内，用户通过密钥索引号进行调用。有些情况下，金融数据密码机生成密钥后不将其存储在本地，而是利用主密钥加密后导出给用户；用户需要进行密码计算时，将由主密钥加密的密钥作为接口参数传给密码机，然后密码机解密该密钥后使用。这样的做法可以保证密钥不以明文形式出现在金融数据密码机外。

2.4.18. 基于密码的数字水印追溯

2.4.18.1. 模式说明

2.4.18.1.1. 威胁分析

自 20 世纪 90 年代以来，数字出版浪潮开始席卷全球，深刻改变了出版的载体形态、存储手段、传播形式、销售业态和阅读方式，但同时授权、盗版活动也借助新技术越来越猖獗。数字产品几乎允许一切可能形式的编辑，极易篡改或伪

造且难以察觉，无法保证原作品的完整性和真实性，数字产品违规外发可导致短时间内无差别、低成本、大规模的“克隆”，这些都严重威胁到数字产品权利人的合法利益，而追踪打击、侵权取证和司法鉴定变得更加困难。



图 65 数据违规外发

2.4.18.1.2. 防护模型

数字水印技术的提出弥补了传统密码学在多媒体内容安全保护上的不足，被广大学者们公认为是版权保护的一种有效方法。数字水印技术作为一种典型的信息隐藏技术，将标识信息（如：商标、版权声明、图章、电子签名等标识性内容）隐藏在数字内容（图像、音视频、文档、软件、三维网格、光盘水印、磁带水印）中。数字水印的嵌入原则上不影响数字载体的使用价值，且数字水印也应该是不易被探知、篡改和擦除的，并且能够把水印信息和数字载体内容更好的关联，并以此来确定数字内容的版权归属、认证数字内容来源的真实性、确认数字内容的跟踪侵权行为。数字水印是保护信息安全、实现文件防篡业务溯源、版权保护的有效办法。

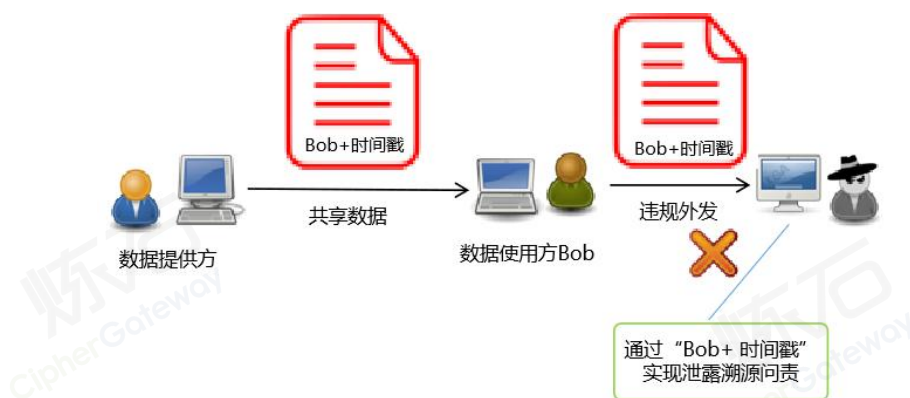


图 66 基于时间戳实现可追溯数字水印

如在数据共享的过程中,数据提供方将使用方的身份及时间戳等信息作为数字水印一起写入数字载体中后发送给使用方 Bob,若数据从 Bob 处违规外发,可根据水印信息准确追溯到外泄主体及相关信息。

数字水印处理系统基本框架如下图所示^[40]:

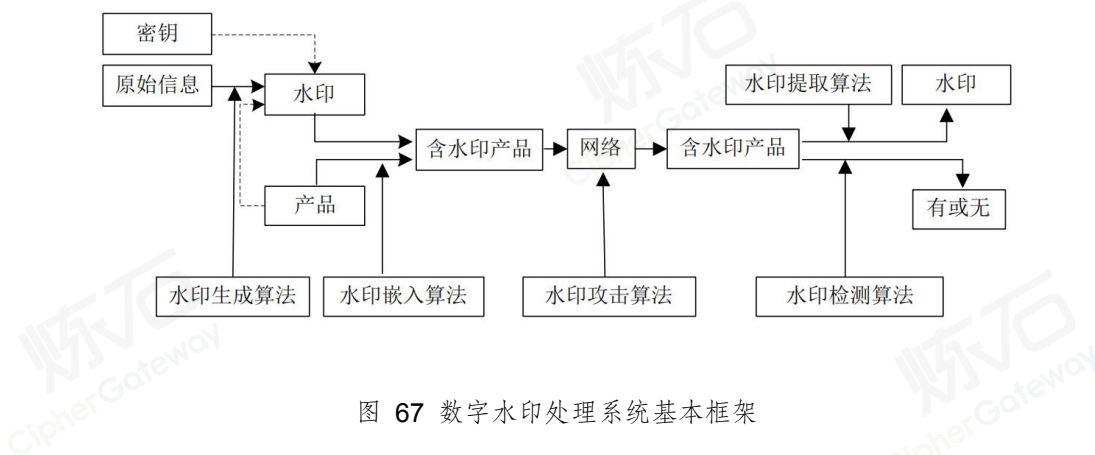


图 67 数字水印处理系统基本框架

数字水印系统包含嵌入器和检测器两大部分。嵌入器至少具有两个输入量：一个是原始信息,它通过适当变换后作为待嵌入的水印信号；另一个是要在其中嵌入水印的载体作品。水印嵌入器的输出结果为含水印的载体作品,而检测器负责判断水印是否存在,若存在则输出为所嵌入的水印信号。首先根据原始信息、密钥和原始数字产品并基于水印生成算法共同生成水印,然后基于水印嵌入算法将水印信息嵌入到数字产品之中。含水印产品在网络传输过程中受到水印攻击算

法攻击之后,可以采用水印检测算法检测水印是否存在或基于水印提取算法提取水印信息,进而完成版权或内容真实性认证。

对于一个完整的数字水印通用模型而言,至少应该包括水印生成、水印嵌入和水印恢复三个部分。

水印生成过程中,同时为了增强水印安全性,水印信息有必要进行加密等预处理。设原始图像为 I , 水印为 W , 密钥为 K , 则水印嵌入过程可用下式来描述:

$$I_w = F(I, W, K)$$

式中 F 表示水印嵌入算法, 如下图所示。

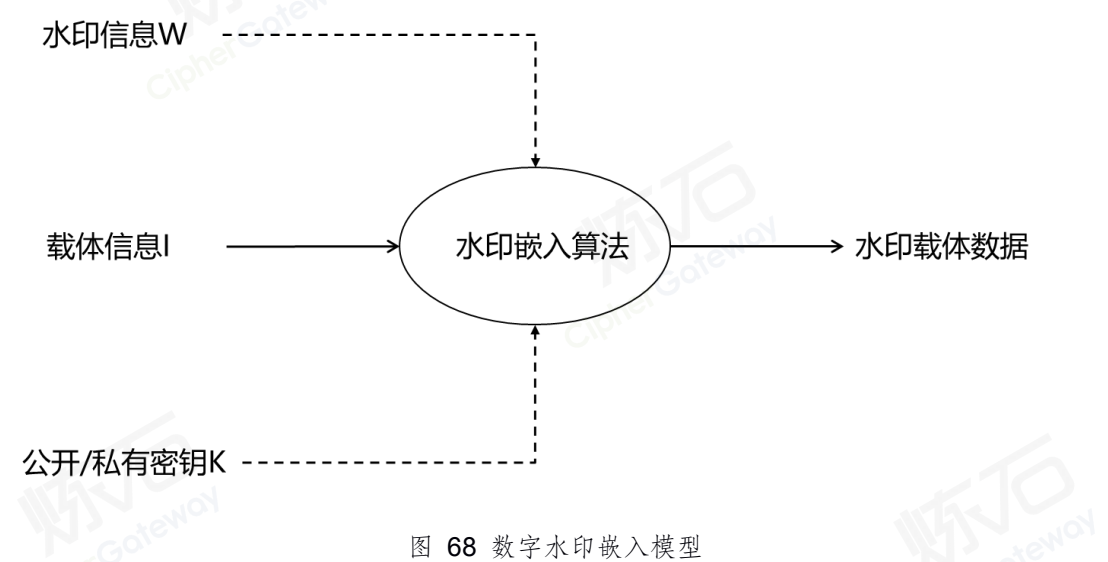


图 68 数字水印嵌入模型

水印恢复时,首先判断待测图像中水印的存在性问题,如果待测图像中存在水印,则提取出水印,如下图所示:

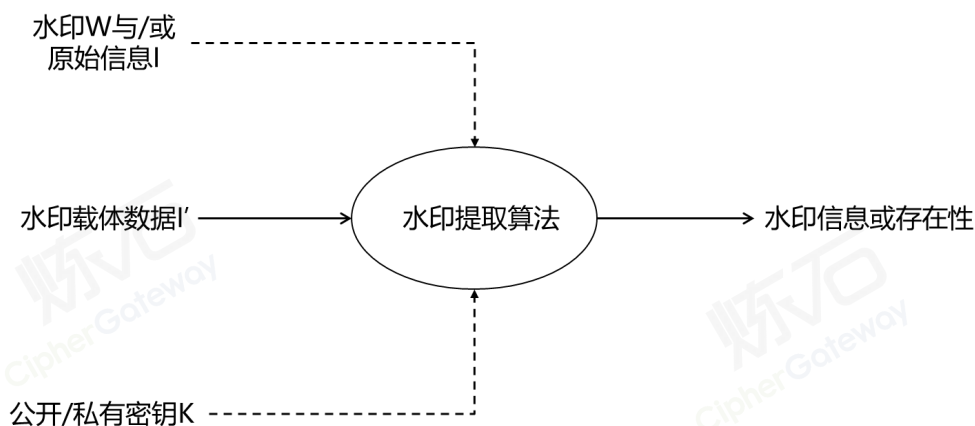


图 69 数字水印恢复模型

2.4.18.2. 典型应用示例

1. 数字水印

数字水印技术问世以来，经多方努力，发展迅速，其应用也非常广泛^[41]。主要体现在以下几个方面：

1) 版权保护

用于版权保护的水印大多数是鲁棒水印，一般而言，要求水印能够抵抗各种类型的攻击，提取的水印可以充分证明数字作品的版权。

2) 内容认证

即通过对从嵌入水印后的数字作品中提取的水印进行分析，判断数字作品的内容是否被篡改。

3) 票据防伪

即在支票、货币、电子票据等票据中嵌入水印信息，在使用时通过对水印进行检测可判断票据的真伪。

4) 拷贝控制

拷贝控制是指为防止作品的非法拷贝，水印检测器被集成在录制设备中，当检测到禁止拷贝的水印，则设备自动停止拷贝。其中，水印检测可通过特定的硬件或软件来实现。

5) 操作跟踪

在数字作品中加入用于操作跟踪的水印后，即可通过水印得到副本的操作记录，作品的所有者或创作者可在每份副本中加入不同水印，从而可记录不同的副本的去向，以达到对拷贝进行跟踪的目的。

2. 电子签章系统

电子签章系统是以数字签名、数字水印技术为核心，以印章图像为载体，基于 COM 中间件技术对电子图章的版权保护机制，实现对特定文件的签名、加密和认证^[42]。任何未通过认证的用户，均无法获取文件信息，从而达到了保护文件隐私与机密的目的。随着加密技术的日益成熟，电子签章系统的安全性也得到了进一步提升。现阶段常用的电子签章系统，已经形成了 PKI 与数字水印两大技术体系，每个体系下又包含了数字认证、数字签名、易损水印、鲁棒水印等多种类型。熟练运用这些技术，将使电子签章系统的实用价值得到更好体现。

融合了 PKI 与数字水印技术的电子签章系统，分为服务器端和客户端两大模块。其中，在服务器端有一台签章证书管理器，主要负责签章证书的新建、查看、删除、导出等任务。同时，提供专门的新建证书库，用于存放所有经由该签章证书管理器签发的证书，方便进行查询、调用。在客户端，又包括了手写签名、MyAddin 组件、seal 控件三个模块。其中，MyAddin 组件的功能是对用户提交的待加密文档，进行验证、签名、盖章和解锁；而 seal 控件的主要作用是对电子签章进行验证、锁定、解锁、查看等。具体组成如下图所示：

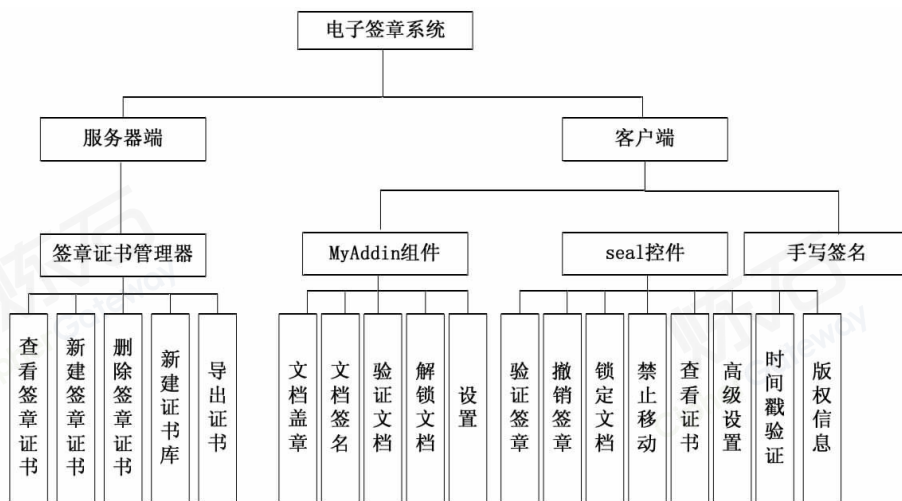


图 70 电子签章系统的组织架构

2.4.19. 基于密码校验的防篡改

2.4.19.1. 模式说明

2.4.19.1.1. 威胁分析

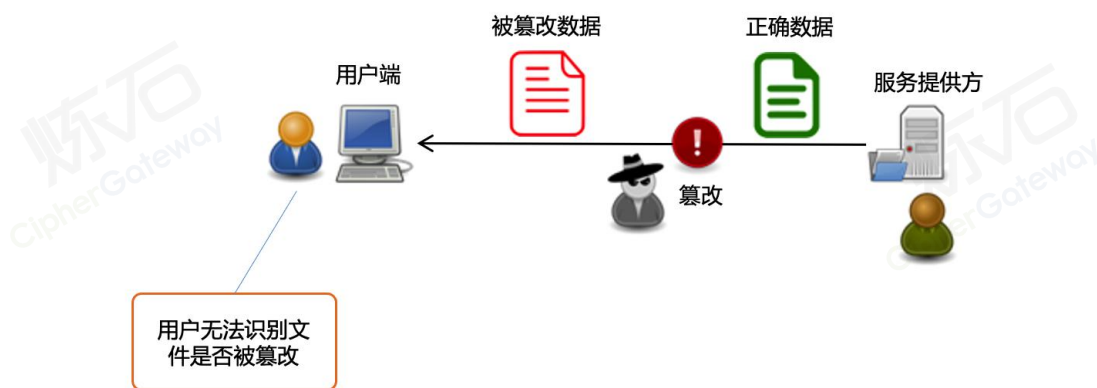


图 71 数据获取过程中存在被篡改威胁

数据安全性不言而喻，在全面信息化、电子化环境下，在对数据资源进行开发和利用的过程当中，所产生的数据内容将有很大概率出现被泄露、丢失及遭受篡改的风险。这类面临安全风险问题的数据，在内容上具体涵盖了数字档

案内容、知识产权、个人隐私数据等。而数据所面临的安全风险主要源于数据失真、传输共享泄露、关键信息缺失等。出现信息失真是指在数据传输与迁移过程当中，遭受旁人篡改及出现数据无法识别的情况；信息泄密则是指信息遭受计算机网络病毒（如木马病毒）攻击，直接致使数据泄露或遭到破坏；而关键数据缺失大部分是由于存储载体故障所致。

2.4.19.1.2. 防护模型



图 72 基于密码校验的防篡改

服务提供方在向用户传输数据前,采用 SM2 私钥对数据进行签名,结合 SM3 计算散列值,并将签名数据及散列值发送至用户端。用户接收到数据后,可进行 SM3 计算对比散列值, SM2 进行签名验证, 确保数据没有被篡改。

采用密码校验实现防篡改应用广泛, 具体总结以下几种方式:

1. 哈希值校验防篡改

哈希值校验技术是一种针对特征值实施校验的算法^[43],其中特征值是指档案管理中电子文件结合某种特定的算法最终核算所得的数值。通俗理解类似于人的指纹验证,因为电子文件特征值具有独特性。因此,采用该技术可通过比较同一

电子文件前后哈希值的差异来判断是否遭受缺损、篡改等情况。具体而言，哈希值校验技术也被业内人士称之为信息摘要和散列值，其主要是借助随机字母和数字的形式来组合为特定的长度，且具备独特的比特串。电子文件进行储存时，HMAC 也同步保存。最后在鉴别电子文件是否遭受缺损和篡改时，可采取 HMAC 实施校验。

2. 数字签名防篡改

数字签名本身是一种电子化数据类型，它和档案管理中的电子文件密切相关。使用数字签名技术主要用于辨别档案管理中文件签署人的身份情况，同时以此来表明签署人真正认可电子文件的内容信息。数字签名技术在应用过程中，主要体现为以下几个方面：

（1）用于身份认证。数字签名技术是一种签名使用者面向认证方注册登记，申请获得数字证书的全过程。

（2）签署发送方电子文件。数字签名技术在获取电子文件哈希值后，针对哈希值计算签名，因哈希值本身的不可逆特点，因此签名哈希值等同于电子文件签名。

（3）网络传输。数字签名技术具体是指签署发送方电子文件数字签名后进行封装处理，并最终将签名结果发送至接收方。

（4）接收方验证。数字签名技术主要是对签名后的电子文件进行哈希值验证。

3. 时间戳防篡改

时间戳技术重点在于保障数据文件的日期及时间信息，其经过加密处理后形成专属的凭证文件。在具体操作上，时间戳的嵌入也是与哈希值相结合，将所收

取电子文件的日期结合哈希值特性，生成数字签名。因此，时间戳的形成和数字签名的生成过程较为类似，先是将需要嵌入时间戳的文件以哈希值算法来生成哈希值，然后发送至时间戳服务系统，由此对文件的哈希值添加时间信息，并进行数字签名。

4. 区块链防篡改

区块链是由多种区块严格依照时间顺序来形成有序链接的数据结构，区块本身具备存储和共享数据的功能，在存储上细分为区块头与区块体。其中区块头专门记录区块特征信息，涵盖区块高度、区块哈希值、版本号、前一个区块的哈希值、时间戳等。而区块体则用于对某段时间发生的交互信息进行记录的功能，当区块头和区块体信息进行打包并数字签名后，即可面向全体区块实施网络广播，由此数据交互的所有节点信息都将被记录。考虑到其中存在多数节点同时参与的情况，区块链本身在整个形成过程当中，通常会基于某种共识机制在诸多节点当中选取出最早完成数据打包的节点，并促使其具备区块权限，进而发展成为区块链的下个区块。通常区块链形成后无法更改，一旦进行数据交互，则节点必将对所储存信息实施核实验证，如此发现存在篡改行为，则节点所记录任何数据都将作废，需拷贝正确记录来进行节点交互。

2.4.19.2. 典型应用示例

典型应用是基于 EFI 的文件完整性保护。

要实现针对 EFI (Extensible Firmware Interface 可扩展固件接口) 的攻击可能篡改可执行文件的摘要值，需要根据策略对每一个被加载文件的摘要值进行

签名，而在以后的每一次启动时，系统会验证签名，这样就保证了每一个驱动文件的完整性^[44]。

当第一次初始化系统时，根据策略选择某一哈希算法对每一个加载时需要验证的文件进行哈希运算，得到一个固定长度的哈希值，用签名算法的私钥对哈希值签名，把得到的签名值和公钥写入需要验证文件的文件头中，整个过程如下图

(a) 所示。签名算法使用的私钥用 TPCM 中的密钥树来管理。

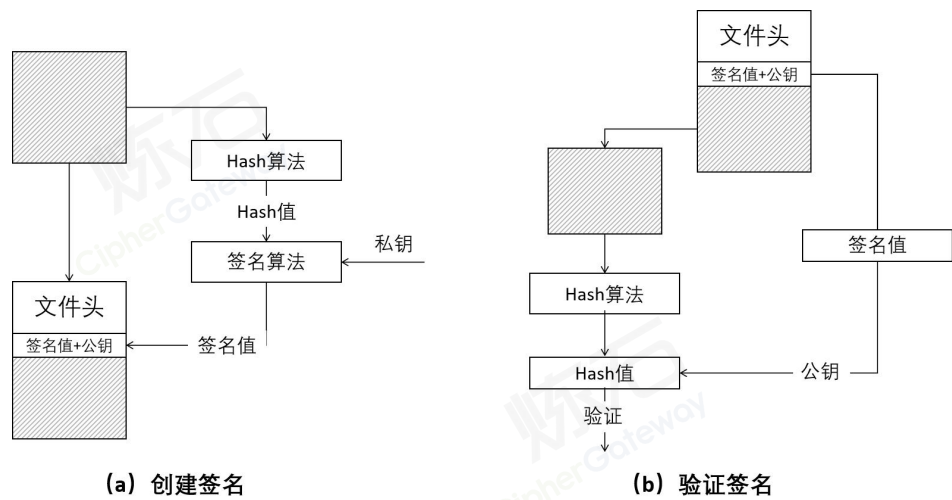


图 73 文件完整性验证过程

以后每次启动系统加载文件时会读取存放在文件头中的签名值和公钥，用签名算法的公钥对签名值解密，得到定长的哈希值。同时对文件抽取出文件头以后的部分进行哈希运算，得到相同长度的哈希值。对这两个哈希值进行比较，如果一致，说明文件未被篡改或破坏；如果不同，说明文件已被篡改或破坏，系统会提示用户文件被破坏，并询问用户是否继续加载。过程如上图中 (b) 所示。

需要加载的可执行文件通过验证后才能真正被加载，这样就保证了被加载文件的真实性与完整性。对文件完整性的验证是可信链传递过程中最重要的部分，只有通过验证，信任才能继续往下一级传递。每个需要度量的文件都有唯一对应的测量值，并且对它进行了签名保存。同时对连接哈希值的计算在 TPCM 芯片内

部完成，并存放在 PCR 中，保证了测量值的高可靠性。当某个可执行文件被篡改或不可信文件将被加载时，系统可以及时发现并请求用户选择策略，然后按策略执行。

2.4.20. 基于私钥签名的责任认定

2.4.20.1. 模式说明

2.4.20.1.1. 威胁分析

目前数据交互频繁，若交互双方产生权益纠纷，而数据发送方对其发送行为矢口否认，无法对信息交互的数据进行追溯，则很难对纠纷进行责任认定。

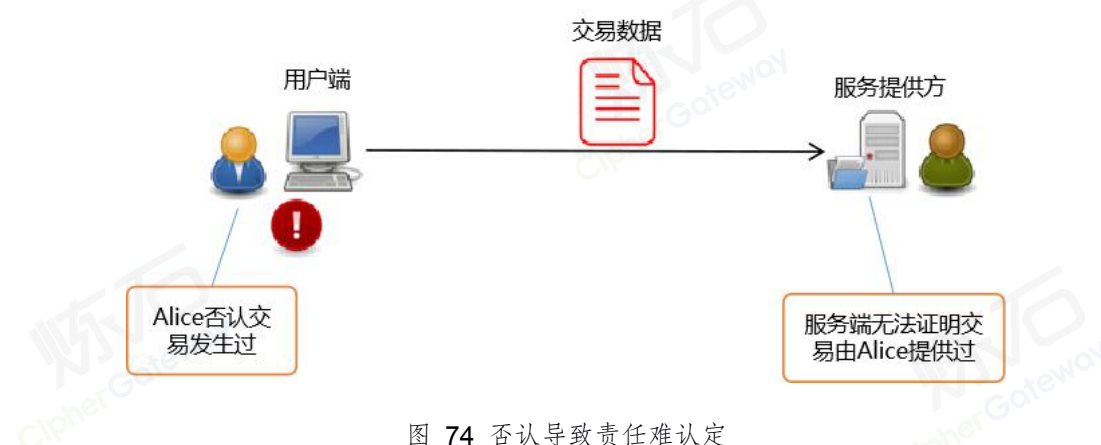


图 74 否认导致责任难认定

因此，需建立可靠的责任认定和抗抵赖机制，确保在业务流程中产生的数据可追溯。在实际应用中，当安全需求不是为了数据的保密，而是为了保证数据的可靠性及数据源的不可否认性，满足这种要求的方法就是使用数字签名技术。数字签名具有的完整性、不可否认性及不可伪造性（身份唯一性）的性质有效保证了信息传输的安全，是信息安全的核心技术之一。

2.4.20.1.2. 防护模型

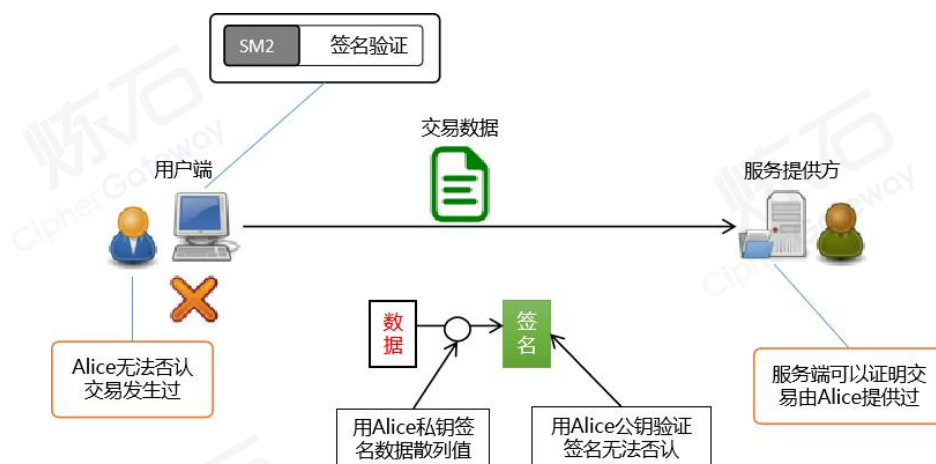


图 75 基于私钥签名责任认定防护模型

消息的接收者可以根据数字签名来判断消息发送者的身份信息。一个数字签名体制一般由两个部分构成——签名算法（Signature Algorithm）、验证算法（Verification Algorithm）。

（1）签名算法：由签名者保存，签名密钥、签名加密算法。它的作用是对消息进行签名。

（2）验证算法：可以通过验证算法检验消息的数字签名，判断签名的真伪，验证签名的人可以利用公开的验证算法和验证密钥验证签名，十分方便。签名者的公钥是公开的，私钥是保密的，并利用私钥对消息 m 进行数字签名操作，验证者收到消息签名对后，利用公钥对消息的签名进行验证。

一个基本的数字签名方案的组成如下图所示。

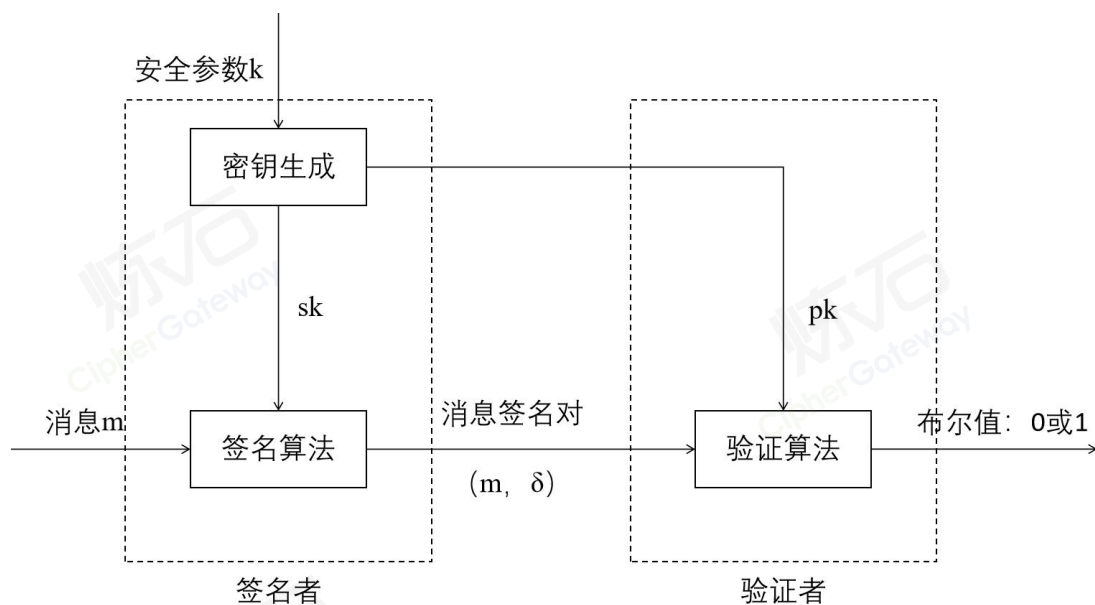


图 76 数字签名方案的基本组成

在上图中，签名者用自己的私钥 sk 对消息 m 进行签名操作，验证者利用签名者的公钥 pk 可以验证消息签名者的身份，确定消息的来源是否正确。除非知道签名者的私钥，否则任何人都不能篡改其他人的签名，并且任何人都无法否认自己的签名。如果对于签名的合法性，签名者和验证者产生了分歧，则可通过可信第三方进行仲裁。

2.4.20.2. 典型应用示例

典型应用是签名验签服务器。

签名验签服务器是用于服务端的适用于基于公钥密码基础设施专用的密码设备²。为应用实体提供基于 PKI 体系和数字证书的数字签名、验证签名等运算功能，可以保证关键业务信息的真实性、完整性和不可否认性，主要用于数字证

² 引自 <https://blog.csdn.net/Lapedius/article/details/109061513>

书认证系统，也可以用于电子银行、电子商务、电子政务等基于 PKI 的业务系统，为这类业务系统提供数字证书的管理和验证服务。

签名验签服务器在软硬件组成上与服务器密码机基本类似。厂商可在 GM/T0018-2012《密码设备应用接口规范》的基础上，对服务器密码机进一步封装，实现签名验签功能，满足应用系统对数字签名和验证的需求。

3. 密码技术集聚创新原力

本章以商用密码技术标准及应用案例的形式,对常见的商用密码基础产品进行介绍,并说明这些密码产品的创新趋势。

3.1. 基础算力类

3.1.1. 密码卡

3.1.1.1. 产品概述

密码卡产品是以 PCI Express 为总线接口的密码设备,支持对称运算、杂凑运算、非对称运算、产生真随机数等密码运算功能,同时提供完备的数据加解密功能、密钥管理及存储功能等。



图 77 PCI-E 密码卡

3.1.1.2. 标准规范

- GB/T 15843.2-2008《信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制》
- GB/T 17964-2008《信息安全技术 分组密码算法的工作模式》
- GM/T 0002-2012《SM4 分组密码算法》
- GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》
- GM/T 0004-2012《SM3 密码杂凑算法》
- GM/T 0005-2012《随机性检测规范》
- GM/T 0006-2012《密码应用标识规范》
- GM/T 0018-2012《密码设备应用接口规范》
- GM/T 0028-2014《密码模块安全技术要求》
- GM/T 0039-2015《密码模块安全检测要求》

3.1.1.3. 应用要点

密码卡产品一般具备以下应用功能：

- 物理随机数的采集：内置由国家密码管理局批准使用的双路物理噪声源芯片，提供真随机数序列的生成。
- 对称运算：支持 SM1 和 SM4 分组密码算法，可实现 ECB 和 CBC 工作模式的数据加密、解密运算。

- 哈希运算：可对数据实现基于 SM3 密码杂凑算法的 HASH 运算。
- MAC 运算：可对数据实现基于 SM1 和 SM4 分组密码算法的 MAC 运算。
- HMAC 运算：可对数据实现基于 SM3 密码杂凑算法的 HMAC 运算。
- 非对称运算：支持 DH 算法、支持 SM2 椭圆曲线公钥密码算法，可实现对数据的加密/解密以及签名/验签。
- 密钥管理：支持符合国家密码管理局安全性要求的密钥结构体制，密钥的产生、存储、使用、更换、销毁、备份及恢复均符合国家密码管理局的安全设计要求。
- 用户鉴别：提供基于角色的用户鉴别，可通过口令、USBKey 或口令+USBKey 实现用户权限控制。
- 其它：支持用户对卡内专属非易失性存储空间进行读写操作。
- 国际公开算法：支持 AES、SHA-512 以及 RSA-2048、RSA-4096 。

3.1.1.4. 创新趋势

密码卡是一种密码设备,通过各种密码算法为上层应用系统提供加解密、数字签名等密码运算服务。从安全方面考虑,密码卡需要具备高速运算的特点,并且需要通过虚拟化技术实现高并发性。在云化趋势和政策合规性的双重驱动下,“密码+云”的融合成为大势所趋,密码卡需要支持虚拟化、支持云密码机虚拟化,实现密码运算资源的动态调整,为应用提供按需、高效、弹性、可扩展的密码虚拟化服务。

3.1.2. 密码套件

3.1.2.1. 产品概述

密码套件（密码 SDK）能够帮助用户安全、高效的引入密码能力，提高其安全水平，应用系统通过开发改造的方式，与封装了加密业务逻辑的密码 SDK 进行集成。

3.1.2.2. 标准规范

- 《GM / T 0003-2012 SM2 椭圆曲线公钥密码算法》
- 《GM / T 0009-2012 SM2 密码算法使用规范》
- 《GM / T 0010-2012 SM2 密码算法加密签名消息语法规范》
- 《GM / T 0004-2012 SM3 密码杂凑算法》
- 《GM / T 0002-2012 SM4 分组密码算法》
- 《GM / T 0044-2016 SM9 标识密码算法》
- 《GM / T 0024-2014 SSL VPN 技术规范》
- 《GM / T 0028-2014 密码模块安全技术要求》
- 《GM / T 0039-2015 密码模块安全检测要求》

3.1.2.3. 应用要点

密码 SDK 包含提供加密能力的密码算法库和提供建立安全连接能力的 TLS 协议库，在支持国际通用密码算法及标准 TLS 协议之外，还提供国产商用密码算法（SM2、SM3、SM4、SM9 等 SM 系列算法）以及基于 SM 系列算法套件的 TLS 协议。基于密码算法及 TLS 协议库的支持，应用软件可以获得完整、持续的数据全生命周期安全保护。

密码套件的应用优势：

(1) 适用范围广

应用系统的开发商可以自行解决数据加解密的绝大多数问题，对数据库系统本身或第三方的数据安全厂商没有依赖。

(2) 灵活性高

应用服务端加密，是针对于应用服务器的加密方式，因为应用服务端加密可与业务逻辑紧密结合，在应用系统开发过程中，灵活地对相关业务中的敏感数据进行加密处理，且使用的加密函数、加密密钥等均可根据业务逻辑需求进行灵活选择。

密码套件的应用挑战：

(1) 需要对应用系统开发改造

应用系统加密的实现需要应用系统开发投入较大的研发成本，时间周期较长，后期实施和维护成本较高，也面临大量代码改造带来的潜在业务风险。

(2) 对应用开发人员要求高

对业务开发人员来说，正确合规使用密码技术具有一定门槛。比如在实际应用中，会出现应用开发人员密钥使用不合规或安全风险等情况。

(3) 需要高性能国密 SDK

目前国密算法在主流服务器和终端上软件实现还存在性能瓶颈问题，通过集成国密 SDK 使应用系统具备数据加密能力的同时，应充分保障应用系统性能，力争对业务影响降低最小，这就需要高性能国密 SDK 为应用系统提供高速的数据加解密服务。

3.1.2.4. 创新趋势

数据安全发展趋势，密码套件要重视软件产品面临的安全风险，大力推动密码技术与操作系统、数据库等基础软件以及云计算、区块链等新兴技术的融合应用，构建关键软件产品安全保障体系。面对大量的存量应用系统，通过开发改造应用重构安全的成本极高，而增量应用很快又成为存量，要解决此类问题，需要探索一种将安全能力与应用高效结合的创新技术手段。面向关键软件的密码安全，尤其在数据安全方面，可以在数据流转环节探索“面向切面的数据安全技术”，让安全能力既与业务流程深度融合，又在技术上解耦。密码套件除了在操作系统兼容性、新技术融合度、密码高性能，更需要增加密码套件基于中间件的使用便利性，使得密码更好用。

3.1.3. 智能密码钥匙

3.1.3.1. 产品概述

智能密码钥匙具备身份认证、密钥管理能力，可提供密码服务的终端密码设备，其作用是存储用户秘密信息，完成数据加解密、数据完整性校验、数字签名、访问控制等功能。智能密码钥匙一般使用 USB 接口形态，因此也被称作 USB Token 或者 USB Key。

3.1.3.2. 标准规范

- GM/T 0016-2012《智能密码钥匙应用接口规范》
- GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》
- GM/T 0027-2014《智能密码钥匙技术规范》
- GM/T 0048-2016《智能密码钥匙密码检测规范》

3.1.3.3. 应用要点

1. 结合产品应用逻辑，理解智能密码钥匙的密钥体系结构

下图展示了智能密码钥匙中的密钥体系结构。

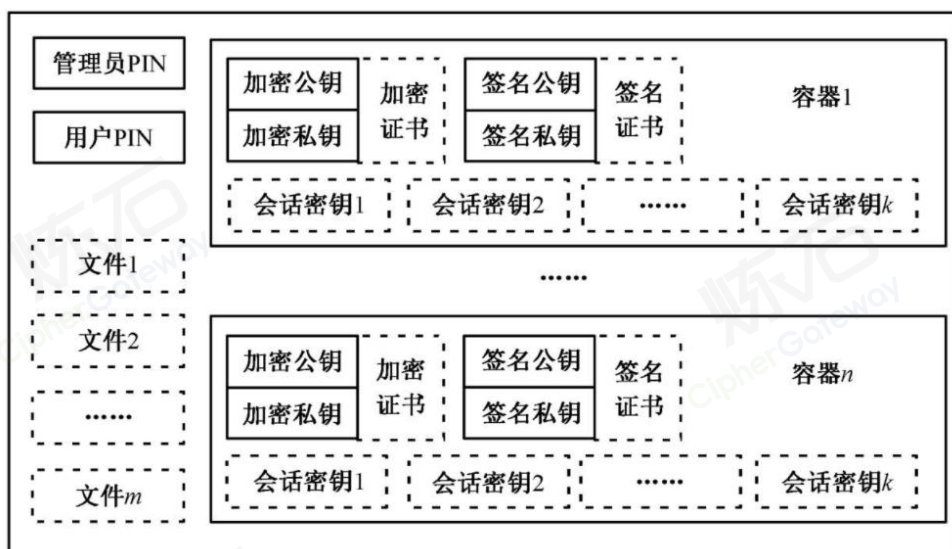


图 78 智能密码钥匙应用逻辑结构图

本产品一般基于非对称密码体制，至少支持三种密钥：设备认证密钥、用户密钥、会话密钥。

2. 智能密码钥匙初始化时，应区分出厂初始化和应用初始化。
3. 应使用商用密码算法进行密码运算。
4. 应注意口令PIN和对称密钥的存储和使用安全。
5. 在签名前应执行身份鉴别，以保证签名密钥的使用安全。

3.1.3.4. 创新趋势

智能密码钥匙用于各种安全设备终端，如密码机、虚拟专用网络、VPNC认证系统等，广泛用于电子政务、网上银行、电子商务、企业ERP等领域，可为用户提供身份认证、电子签章、文件加密、保密通信和移动存储加密等服务。随着业务应用的发展出现了动态令牌智能密码钥匙、存储型智能密码钥匙、蓝牙型智能密码钥匙、时钟存储性智能密码钥匙、SD型智能密码钥匙、指纹型智能密码

钥匙、高速度智能密码钥匙、音码型智能密码钥匙等。随着基础科技的进步、应用环境的发展、安全形势的变化，未来智能密码钥匙的发展趋势包括以下方面。

1. 性能更高

随着技术的发展智能密码钥匙核心部件的安全芯片的运算能力不断提高。

- (1) 内部存储空间更大，能够存储更多、体积更大的密钥，实现计算更复杂、安全强度更高的算法；
- (2) 运算速度更快，以 RSA 签名为例从原来的每秒几次升到每秒十几次甚至几十次，更好地满足了强调速度的应用环境；
- (3) 通信速率更高，新的智能卡芯片能够在保证稳定性的前提下搭配高速 USB 控制器，显著提高了 USB Key 与主机之间的数据传输速率。

2. 产品细分应对应用环境变化

保障互联网应用的安全，是智能密码钥匙产品的主要用途之一。随着通信技术的发展，传统的以 PC 为平台的互联网应用也随之延伸到了移动互联网设备平台上。面对应用环境的日益复杂和多样化发展的趋势，使用单一形态、单一接口的智能密码钥匙产品来应对是困难的，需要对应用环境进行细分，研发系列化、个性化的智能密码钥匙产品，分别针对不同特性的应用环境。例如，除 USB 之外支持其他接口（如 SD、耳机、红外、蓝牙等）的智能密码钥匙产品、能够通过切换设备类型消除与第三方软件冲突的智能密码钥匙产品、能识别操作系统类型并自动选择合适的通信协议的智能密码钥匙产品等。

3.1.4. 服务器密码机

3.1.4.1. 产品概述

服务器密码机作为通用型密码机产品,主要为应用提供最为基础和底层的密钥管理和密码计算服务,是可以提供多种国产商用密码算法(SM1、SM2、SM3、SM4),并能够保证密钥和密码算法安全性,具有很高的安全性和实用价值。下图是典型的服务器密码机软/硬件架构。

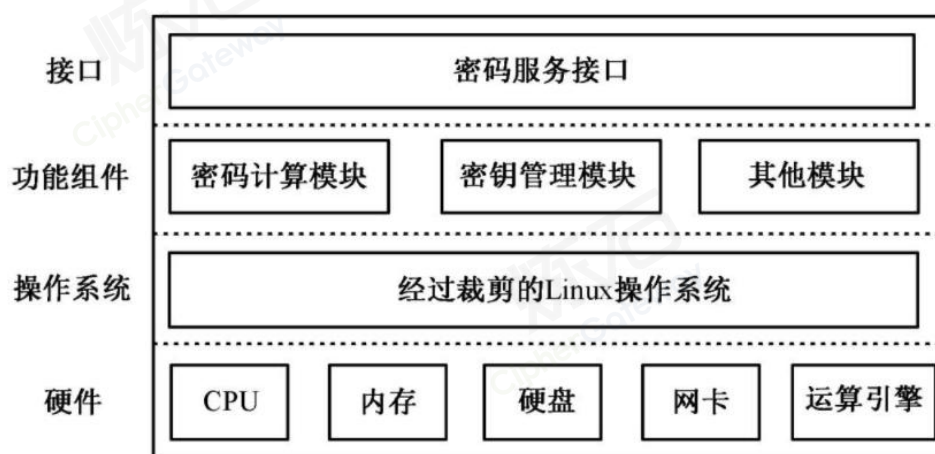


图 79 典型的服务器密码机软/硬件架构

3.1.4.2. 标准规范

- GM/T 0002-2012 《SM4 分组密码算法》
- GM/T 0003-2012 《SM2 椭圆曲线公钥密码算法》
- GM/T 0004-2012 《SM3 密码杂凑算法》
- GM/T 0005-2012 《随机性检测规范》
- GM/T 0006-2012 《密码应用标识规范》

- GM/T 0018-2012 《密码设备应用接口规范》
- GM/T 0030-2014 《服务器密码机技术规范》

3.1.4.3. 应用要点

1. 应结合服务接口类型，理解服务器密码机产品的密钥体系结构

服务器密码机必须至少支持三层密钥体系结构，包括管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥。



图 80 服务器密码机密钥体系结构

- (1) 管理密钥：管理密钥主要是用于保护服务器密码机中密钥和敏感信息安全的密钥，它一般与应用无关，而与设备的安全性设计相关，与外部应用没有关联，其使用不对应用系统开放。
- (2) 用户密钥：用户密钥是用户的身份密钥，包括签名密钥对和加密密钥对。签名密钥对由服务器密码机生成，用于实现用户签名、验证、身份鉴别等，代表用户或应用者的身份；而加密密钥对则由密钥管理系统下发到设备中，主

要用于对会话密钥的保护和数据的加解密等。用户密钥存储在服务器密码机内部的安全存储区域。

- (3) 设备密钥：与用户密钥类似，设备密钥是服务器密码机的身份密钥，包括签名密钥对和加密密钥对，用于设备管理，代表服务器密码机的身份。设备密钥的签名密钥对在设备初始化时通过管理工具生成或者安装，加密密钥由密钥管理系统下发到设备中，设备密钥对存储在服务器密码机内部的安全存储区域。
 - (4) 密钥加密密钥：密钥加密密钥是定期更换的对称密钥，用于在预分配密钥情况下，对会话密钥的保护。密钥加密密钥通过密码设备管理工具生成或安装，与用户密钥和设备密钥存储在不同的存储区。
 - (5) 会话密钥：会话密钥是对称密钥，一般直接用于数据的加解密。会话密钥使用服务器密码机的接口生成或导入，使用时利用句柄检索。为了保证会话密钥的安全，它不能以明文形态进出密码机，服务器密码机的接口采用数字信封、密钥加密密钥加密传输或者密钥协商等方式进行会话密钥的导入/导出。
2. 应结合具体密码服务，理解服务器密码机的接口类别和调用。

相关接口类型包括：

- (1) 设备管理类：主要是对于密码设备、会话、私钥权限的管理，包括打开/关闭设备、创建/关闭会话、获取/释放私钥使用权限等
- (2) 密钥管理类：主要涉及会话密钥生成、密钥的导入/导出、密钥销毁等密钥生命周期管理

- (3) 非对称算法运算类函数：主要包括数字签名的计算和公钥加解密操作
- (4) 对称算法运算类函数：主要包括对称加解密和 MAC 的计算
- (5) 杂凑运算类函数：主要支持杂凑的多包运算
- (6) 文件类函数：对内存存储的文件进行管理

3.1.4.4. 创新趋势

虽然目前国内密码市场仍以硬件为主,但随着云计算的普及和国家对密码管理思路的演进,密码应用必将在合规的前提下,走向更为灵活易用的软件化。未来外挂式的单体密码设备或将消失,密码将走向与基础软硬件融合、与云融合、与信息化业务融合,包括密码在内的信息安全能力将成为信息化的内生特性。

云计算、大数据等环境催生密码技术新的应用场景,服务器密码机的发展趋势之一是支持多租户云模式,基于云密码资源池解决方案,可根据负载动态调整云密码机的处理能力,实现密码算力的动态调整,为应用提供按需、高效、可扩展的密码服务。云服务器密码机也可根据应用的需求动态伸缩,按需调配资源,同时应用所需的加解密功能也应能动态的按需加载。

3.1.5. 签名验签服务器

3.1.5.1. 产品概述

为应用实体提供基于 PKI 体系和数字证书的数字签名、验证签名等运算功能的服务器,可以保证关键业务信息的真实性、完整性和不可否认性,主要用于数

字证书认证系统，也可以用于电子银行、电子商务、电子政务等基于 PKI 的业务系统，为这类业务系统提供数字证书的管理和验证服务。

进一步的，签名验签服务器的辅助模块“时间戳服务器”，基于 PKI 技术的时间戳权威系统对外提供精确可信的时间戳服务，为信息系统中的时间防抵赖提供基础服务。

3.1.5.2. 标准规范

- GM/T 0029-2014 《签名验签服务器技术规范》
- GM/T 0018-2012 《密码设备应用接口规范》
- GM/T 0002-2012 《SM4 分组密码算法》
- GM/T 0003-2012 《SM2 椭圆曲线公钥密码算法》
- GM/T 0004-2012 《SM3 密码杂凑算法》
- GM/T 0005-2012 《随机性检测规范》
- GM/T 0009-2012 《SM2 密码算法使用规范》
- 国际标准 RFC3161 和 RFC2630 两种时间戳协议的时间戳

3.1.5.3. 应用要点

签名验签服务器在软/硬件组成上与服务器密码机基本类似。对服务器密码机进一步封装，实现签名验签功能，满足应用系统对数字签名和验证的需求。

签名验签服务器可以通过三种方式提供服务：

1. API 调用方式。用户通过 GM/T 0020-2012《证书应用综合服务接口规范》中规定的 API 接口访问签名验签服务器。
2. 通用请求响应方式。通过 GM/T 0029-2014 的附录 A“消息协议语法规则”中规定的协议，请求者将数字签名、验证数字签名等请求发送给签名验签服务器，由签名验签服务器完成签名验签服务并返回结果。
3. HTTP 请求响应方式。其工作原理与请求响应模式类似，不同的是将消息格式从二进制的 ASN.1 格式，转换为易于在 Web 应用和 HTTP 协议中传递的文本格式。通过 GM/T 0029-2014 的附录 B“基于 HTTP 的签名消息协议语法规则”的 HTTP 请求发送给签名验签服务器，由签名验签服务器完成签名验签服务并返回结果。

3.1.5.4. 创新趋势

传统签名验签服务器基于硬件架构的服务模式，在业务开发、系统运维、业务规划上存在很多问题，且难以适合云计算及移动互联网的业务场景。

未来创新趋势支持统一管理的签名验签服务平台能有效解决以上问题，服务平台能共用签名验签服务器，提高服务器密码硬件算力的利用率，所有底层硬件设备统一管理，即便出现故障容易替换新硬件，无需重新导入证书。

数字经济下丰富的应用场景，比如电子合同、互联网医院、电子保单等，普遍需要将签名验签与特定业务流程深度结合，将传统密码产品延伸演进到依赖密码技术的业务产品。这或许也是整个密码产品的潜在发展演进方向。

3.2. 应用场景类

3.2.1. 数字证书认证系统

3.2.1.1. 产品概述

数字证书认证系统是对生命周期内的数字证书进行全过程管理的安全系统。数字证书认证系统必须采用双证书机制，并按要求建设双中心。一般的数字证书认证系统的逻辑结构如下图所示。

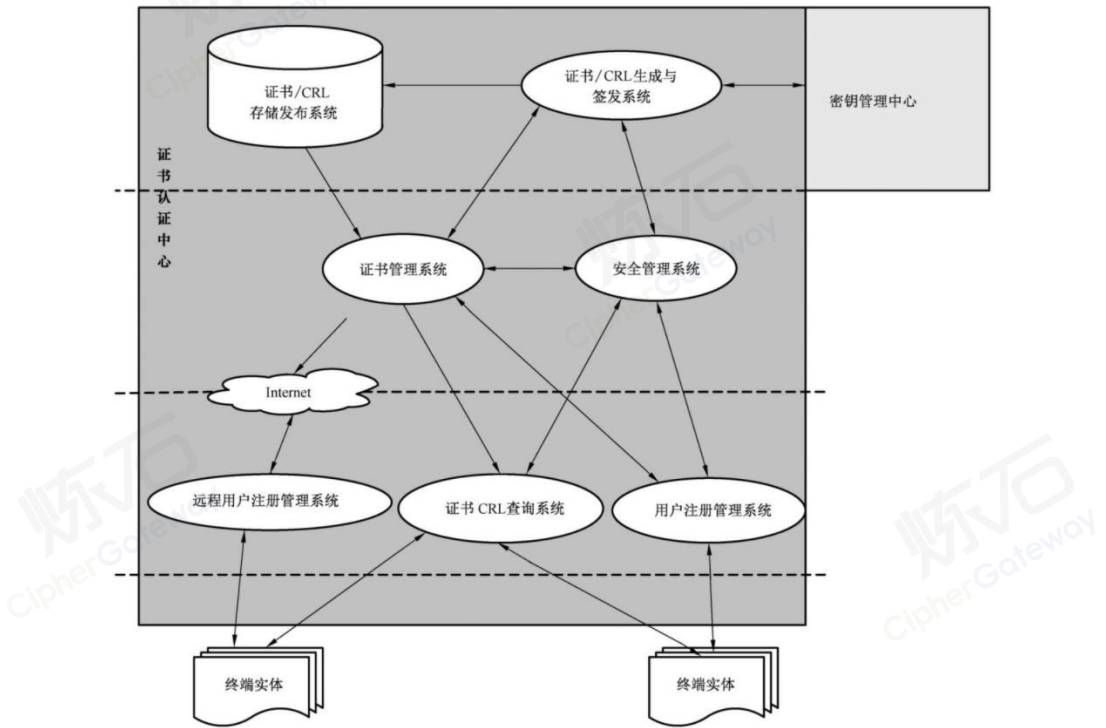


图 81 数字证书认证系统的逻辑结构图

提供了对生命周期内的加密证书密钥对进行全过程管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档和密钥恢复等。

电子商务是数字证书认证系统的典型应用场景之一。交易各方通过认证机构获取各自的数字证书。交易产生之前要对交易各方进行身份鉴别，通过认证机构颁发的数字证书以及数字签名技术完成网上交易双方的身份鉴别，并实现交易过程中对传输数据的保密性、完整性和行为的不可否认性。

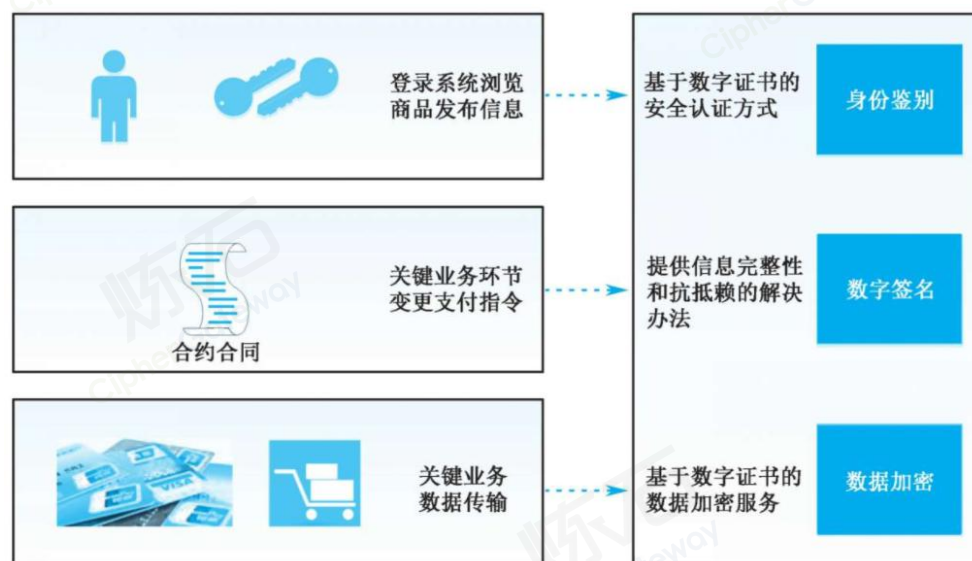


图 82 数字证书认证系统在电子商务中的应用

3.2.1.2. 标准规范

- GM/T 0014-2012 《数字证书认证系统密码协议规范》
- GM/T 0015-2012 《基于 SM2 密码算法的数字证书格式规范》
- GM/T 0034-2014 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》
- GM/T 0020-2012 《证书应用综合服务接口规范》
- GM/T 0037-2014 《证书认证系统检测规范》

- GM/T 0038-2014《证书认证密钥管理系统检测规范》
- GM/T 0043-2015《数字证书互操作检测规范》

3.2.1.3. 应用要点

第三方电子认证服务机构的数字证书认证系统的建设、检测和使用应满足上述标准的相关要求，非第三方电子认证服务机构（如自建CA）的数字证书认证系统的建设、检测、运行及管理，可参照以上标准。下面将根据上述标准给出应用要点。

1. 证书认证系统的检测类别有产品和项目之分，不同的类别对应的检测内容也不同。
2. 应采用双证书机制，并建设双中心。
3. 应使用商用密码算法进行密码运算。
4. 应遵循相关标准以满足密码服务接口的要求。
5. 应对CA和KM的管理员进行分权管理。
6. 应为证书认证系统进行物理区域划分，并进一步对KM物理区域进行划分。
7. 应配置安全策略保障网络安全。
8. 应有数据备份和恢复策略，能够实现对系统的数据备份与恢复。
9. 应保障系统各组件间通信安全。

3.2.1.4. 创新趋势

数字证书底层基于公钥密码体制，为个人或单位用户提供身份证明，其未来创新除了完善本身的管理流程之外，主要依赖于加密技术的创新和发展，比如更安全、更高效的加密算法。此外，证书的生成、管理以及发放方式等存在创新发展的空间。

3.2.2. CASB 数据加密平台

3.2.2.1. 产品概述

CASB 数据加密平台是一款集数据加解密、访问控制、动态脱敏、策略管理和密钥管理等功能于一体的数据安全产品。

CASB 数据加密平台主要由数据加密插件、数据安全管理和密钥管理系统组成。其中数据加密插件部署在应用系统的服务端，逻辑上处在应用系统和数据库之间，应用系统写入数据和读取数据时都会流经数据加密插件，写入数据时数据加密插件对数据加密，使数据以密文的形式在数据库内存储，读取数据时，数据加密插件对密文数据进行解密，将解密后的明文传送至应用系统前端，整个加解密过程对应用系统的用户端是透明的；数据安全平台负责为数据加密插件提供管理、加解密和脱敏策略配置等可视化管理服务；密钥管理系统负责提供密钥支持和密钥管理服务。

3.2.2.2. 标准规范

- 《中华人民共和国网络安全法》

- 《中华人民共和国密码法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》
- 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
- 《GB/T 37092-2018 信息安全技术 密码模块安全要求》
- 《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》
- 《GM / T 0002-2012 SM4 分组密码算法》
- 《GM / T 0003-2012 SM2 椭圆曲线公钥密码算法》
- 《GM / T 0004-2012 SM3 密码杂凑算法》
- 《GM / T 0009-2012 SM2 密码算法使用规范》
- 《GM / T 0010-2012 SM2 密码算法加密签名消息语法规范》
- 《GM / T 0024-2014 SSL VPN 技术规范》
- 《GM / T 0028-2014 密码模块安全技术要求》
- 《GM / T 0039-2015 密码模块安全检测要求》

3.2.2.3. 应用要点

(1) 结构化数据加密保护

针对数据库中存储的结构化数据，业务数据安全防护平台可以实现重要敏感字段的加密保护，具体功能如下：

- 1) 用户可以根据企业分类分级的结果或者实际需求，选择对重要敏感字段进行加密。即使数据库文件被非法复制或者存储文件丢失，也不会导致真实敏感数据的泄露；
- 2) 能对结构化数据实现精确到字段级的精细化防护，对于没有授权的用户绕过数据加密插件，即使窃取硬盘或拷贝数据也无法解密读取，可有效做到“防拔盘、防拖库”；
- 3) 支持国密 SM4 算法，可对不同字段采用不同加密算法不同密钥进行加密；
- 4) 对手机号、身份证号、Email 等有固定格式的字段能实现保留格式的加密；
- 5) 根据应用系统用户身份权限等进行细粒度访问控制，支持“主体到应用内用户，客体到数据库字段级”，实现对应用系统用户侧的数据脱敏和访问控制。

(2) 非结构化数据加密保护

针对文件类的非结构化数据，可实现落盘加密，读盘解密。通过数据安全管理平台可以进行加解密策略配置和细粒度的访问控制，支持对指定的文件夹进行加密，此时该文件夹（及其子文件夹）的文件在保存时被加密；支持通过白名单机制控制应用系统访问非结构化数据，即经过授权的应用，可以正常访问数据，获取的是明文；未经授权的应用或者直接拷贝文件数据，只能获取密文数据。

(3) 访问控制（动态脱敏）

支持在数据解密节点上，对敏感数据通过设置遮掩等方式实现动态脱敏，可实时将脱敏后的结果展示在应用前端。

动态脱敏是在生产环境中应用读取敏感数据的过程中实现，先经过插件解密，接着由插件根据脱敏策略进行脱敏，再将脱敏后的结果返回应用前端，性能上不影响正常业务，用户无延迟感知。

动态脱敏的基本原理是通过脱敏算法将敏感数据进行遮蔽、变形，将敏感级别降低后对外展示。插件中包含脱敏引擎，引擎中内置了常用的脱敏算法，并且支持根据用户需求定制脱敏算法。解密后的敏感数据由脱敏引擎根据已经设置的脱敏算法进行计算处理，得到脱敏后的结果返回应用前端展示。



图 83 数据动态脱敏

3.2.2.4. 创新趋势

CASB 数据加密平台未来创新集中在四个方面：一是底层加密技术的更新换代，主要体现在加密算法性能提升、更安全的密钥机制、新的加密算法、新的加密技术应用等；二是平台业务模式的演化，包括平台本身的功能性能升级、插件端功能性能升级等；三是应用场景的创新，确保适配越来越多的应用场景，比如

云环境、虚拟化等领域；四是部署实施的优化，平台将朝着更加自动化、智能化方向演进。

3.2.3. 金融数据密码机

3.2.3.1. 产品概述

金融数据密码机主要是针对特定应用场景，在通用型的服务器密码机基础上，进一步封装了特定接口，以便于应用调用。

3.2.3.2. 标准规范

密码行业标准中，已发布 7 项与密码机产品相关的标准，包括 3 项技术规范和 3 项配套的检测规范，以及 1 项与服务器密码机相关的接口规范 GM/T 0018-2012《密码设备应用接口规范》。下表给出了不同类型的密码机所要遵循的技术和检测规范。

表 5 不同类型的密码机所要遵循的技术和检测规范

	技术规范	检测规范
服务器密码机	GM/T 0030-2014 《服务器密码机技术规范》	GM/T 0059-2018 《服务器密码机检测规范》
签名验签服务器	GM/T 0029-2014 《签名验签技术规范》	GM/T 0060-2018 《签名验签服务器检测规范》

金融数据密码机	GM/T 0045-2016 《金融数据密码机技术规范》	GM/T 0046-2016 《金融数据密码机检测规范》
---------	------------------------------	------------------------------

3.2.3.3. 应用要点

金融数据密码机主要用于金融领域内的数据安全保护，提供 PIN 加密、PIN 转加密、MAC 产生、MAC 校验、数据加解密、签名验证及密钥管理等金融业务相关功能。金融数据密码机除用于金融行业实际业务外，还可以提供基本的密码算法服务，为通用业务提供密码计算服务。

3.2.3.4. 创新趋势

金融数据密码机作为多种密码能力的提供者，其未来创新趋势是在金融领域其他的高安全业务中应用，或者延伸其他广泛行业的高安全业务场景。

3.2.4. VPN 虚拟专用网络

3.2.4.1. 产品概述

虚拟专用网络（VPN）技术是指使用密码技术在公用网络中构建临时的安全通道的技术。通过 VPN 技术提供的安全功能，用户可以实现在外部对企业内网资源的安全访问。

3.2.4.2. 标准规范

- GM/T 0022-2014 《IPSec VPN 技术规范》

- GM/T 0023-2014 《IPSec VPN 网关产品规范》
- GM/T 0024-2014 《SSL VPN 技术规范》
- GM/T 0025-2014 《SSL VPN 网关产品规范》
- GM/T 0026-2014 《安全认证网关产品规范》
- GB/T 32922-2016 《信息安全技术 IPSec VPN 安全接入基本要求与实施指南》

3.2.4.3. 应用要点

VPN 商用密码产品的设计、检测和使用应遵循标准上述标准，下面将根据上述产品标准给出 6 个应用要点。

1. 应使用商用密码算法进行密码运算。
2. 应结合具体密码协议，理解 VPN 产品的密钥体系结构。
3. 应注意 IPSec VPN 的数据报文封装模式，其分为隧道模式和传输模式，其中隧道模式是必备功能，用于主机和网关的 VPN 实现。
4. 应注意 SSL VPN 的工作模式，其分为客户端—服务端模式和网关—网关模式两种。
5. 应理解 IPSec VPN 中 AH 和 ESP 协议提供的安全功能。IPSec VPN 产品的安全报文封装协议分为 AH 协议和 ESP 协议。
6. 应注意对管理员的分权管理机制，并采用基于数字证书方式对管理员身份进行鉴别。

管理员应持有表征用户身份信息的硬件装置，与登录口令相结合登录系统，进行管理操作前应通过身份鉴别。

3.2.4.4. 创新趋势

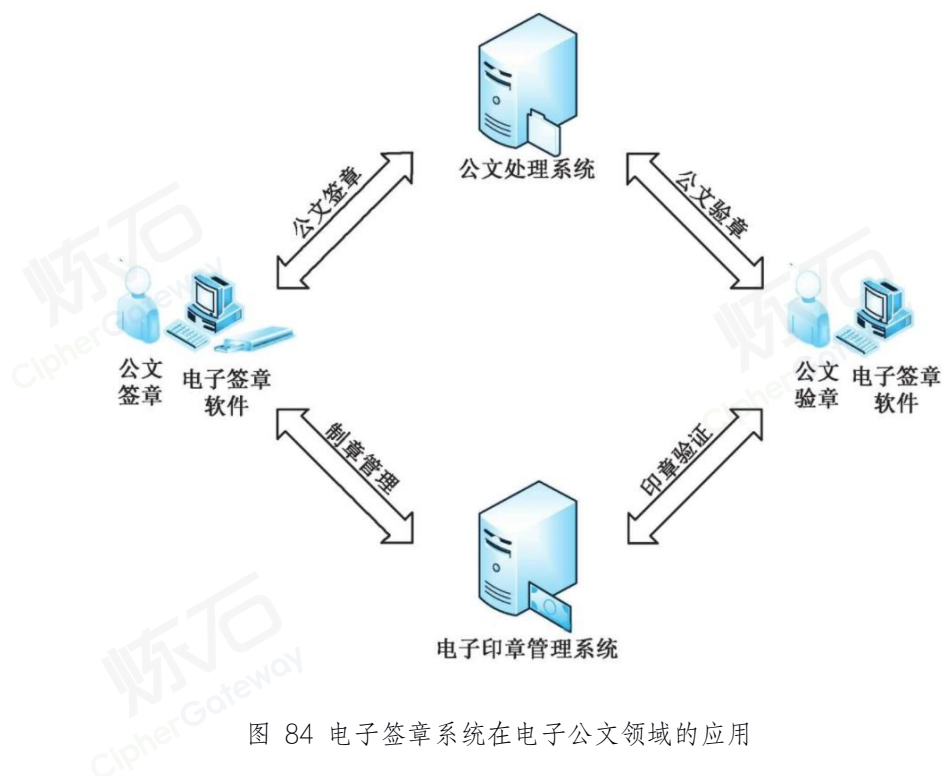
VPN 是基于各种安全协议在公众网络中建立安全隧道，提供专用网络的功能和作用。在未来发展中，支持更高带宽的高性能产品，和零信任网络结合形成以身份为中心的安全方案。

3.2.5. 电子签章系统

3.2.5.1. 产品概述

电子签章将传统印章与电子签名技术进行结合，通过采用密码技术、图像处理技术等，使电子签名操作和纸质文件盖章操作具有相同的可视效果，让电子文档的电子签章具有了和传统印章一样的功能。同时，电子签章基于公钥密码技术标准体系，以电子形式对电子文档进行数字签名及签章，确保了“签名”文档来源的真实性和文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。

在电子公文领域的应用中，电子签章可以和公文处理系统结合。



3.2.5.2. 标准规范

- GM/T 0031-2014 《安全电子签章密码技术规范》
- GM/T 0047-2016 《安全电子签章密码检测规范》
- GB/T 33190-2016 《电子文件存储与交换格式版式文档》
- GB/T 33481-2016 《党政机关电子印章应用规范》

3.2.5.3. 应用要点

下面将根据上述产品标准给出应用要点。

1. 应使用商用密码算法进行密码运算。
2. 应注意电子印章和电子签章二者在数据格式上的关联和区别。
3. 电子印章的验证。

4. 电子签章的生成。

5. 电子签章的验证。

3.2.5.4. 创新趋势

当前，电子签章行业经过几年的发展，迎来了爆发期，国内也出现了若干行业头部企业，通过各自的签章平台（以 SaaS 为主）服务于众多企业。随着近两年区块链技术的风行，电子签章与区块链技术的结合将会是电子印章未来的发展趋势之一。当然，区块链底层也是基于加密技术（哈希和非对称加密），但区块链具有创新的密码应用模式，由多方共同维护账本，不可篡改，不可抵赖，不会丢失。去中心化的思路解决了第三方安全和信任问题，因此，区块链将为电子签章行业带进一个更加可信的时代。

3.2.6. 身份鉴别系统

3.2.6.1. 产品概述

身份鉴别系统是面向业务网各应用系统平台提供身份鉴别服务的系统，可对各类业务网中应用系统的用户身份进行集中管理并实现身份鉴别和授权。身份鉴别系统的密码应用主要解决用户身份真实性、单点登录场景下鉴别协议的安全性、鉴别和授权过程中敏感数据传输和存储的安全性等问题。

3.2.6.2. 标准规范

- GB / T 15843.6-2018 信息技术 安全技术 实体鉴别 第 6 部分：采用人工数据传递的机制
- GB / T 34953.2-2018 信息技术 安全技术匿名实体鉴别 第 2 部分：基于群组公钥签名的机制
- GMT 0032-2014 基于角色的授权与访问控制技术规范
- GMT 0034-2014 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范
- GMT 0037-2014 证书认证系统检测规范
- GMT 0038-2014 证书认证密钥管理系统检测规范

3.2.6.3. 应用要点

1. 密码应用需求

身份鉴别系统在日常运行和管理过程中，密码应用需求主要包括：

- (1) 身份鉴别需求。对登录系统的用户以及使用身份鉴别系统获取用户登录状态的应用系统进行身份鉴别，保证用户和应用系统身份的真实性。
- (2) 关键数据的安全存储需求。保证用户信息、应用系统信息等关键数据在存储过程中的保密性和完整性。
- (3) 关键数据的安全传输需求。保证用户信息、访问令牌等关键数据在传输过程中的保密性或完整性。

2. 密码应用架构

身份鉴别系统包括身份鉴别服务器、数据库服务器、服务器密码机和 SSL VPN 等。业务网终端用户在访问应用系统前，身份鉴别系统需要对其进行身份鉴别；身份鉴别后获取授权来访问应用系统。身份鉴别系统密码应用部署如下图所示，具体说明如下：

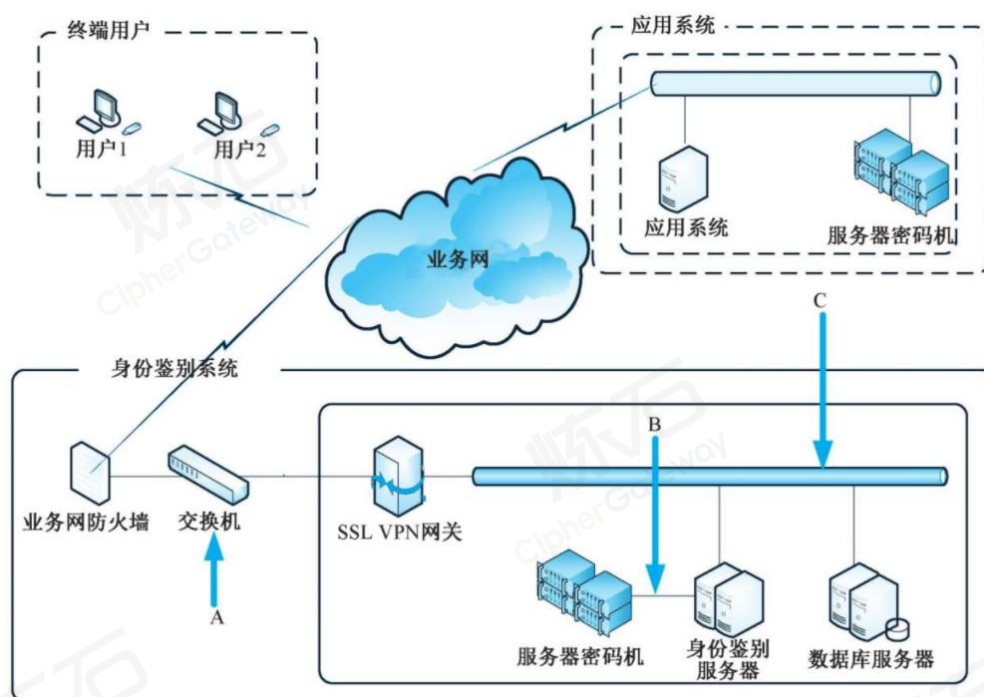


图 85 身份鉴别系统密码应用部署图

- (1) 在机房部署 SSL VPN 网关，用于安全通信链路的构建。SSL VPN 网关是身份鉴别服务器的外部访问出口，确保通信安全。
- (2) 在机房部署身份鉴别服务器，调用服务器密码机，完成身份鉴别协议逻辑的实现。
- (3) 在机房部署服务器密码机，为身份鉴别服务器提供数字签名、验证签名和数据加解密等密钥管理和密码运算服务。

3.2.6.4. 创新趋势

身份鉴别系统是一项利用多种加密技术的综合应用模式，一方面跟随加密技术的发展而同步发展，另一方面随着其他新技术的兴起以及身份鉴别机制的变革而升级，在未来，创新趋势是与 IAM 身份管理系统深度结合，并且与多因素认证融合。

3.3. 管理支撑类

3.3.1. 密钥管理系统

3.3.1.1. 产品概述

实现对业务系统中各种密钥的全生命周期集中管理。密钥管理系统密码应用方案设计的重点是建立完善的密钥管理体系，以满足其他业务系统对于对称密码体制和非对称密码体制的密钥服务需求。

3.3.1.2. 标准规范

不同行业、不同应用场景下，密钥管理系统的构建方法各不相同，并没有一个通用的密钥管理标准进行约束。

3.3.1.3. 应用要点

1. 密码应用需求

密钥是密钥管理系统的核心。在密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等整个生命周期过程中，都需要通过密码技术对密钥进行保护，以确保密钥的全生命周期安全。密钥管理系统的密码应用需求主要包括以下内容：

- (1) 密钥的安全分发需求。密钥管理中心主密钥/密钥对在本地存储,不进行传输；其他密钥一般采用离线方式或在线方式进行传输，并配以保密性和完整性保护措施。
- (2) 关键设备的安全管理需求。在远程管理设备时，实现鉴别信息的防窃听，保证系统资源访问控制信息的完整性，对各类设备的日志记录进行完整性保护。
- (3) 业务系统密钥的安全需求。保证密钥等关键数据在传输、存储过程中的保密性、完整性。
- (4) 密钥管理需求。对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等全生命周期安全管理，采用必要的密码技术保证各环节的密钥保密性和完整性。

2. 密码应用架构

密钥管理系统由密钥管理中心（KMC）和密钥管理分中心（SKMC）两部分组成，最上层的业务系统不在密钥管理系统的边界之内。作为密钥管理系统的核心区域，KMC 为多个不同需求的 SKMC 提供对称密钥和非对称密钥对的管理服务，通过离线分发方式向 SKMC 下发密钥。KMC 不直接面向业务系统，而 SKMC 则直接面向业务系统提供密钥管理服务。

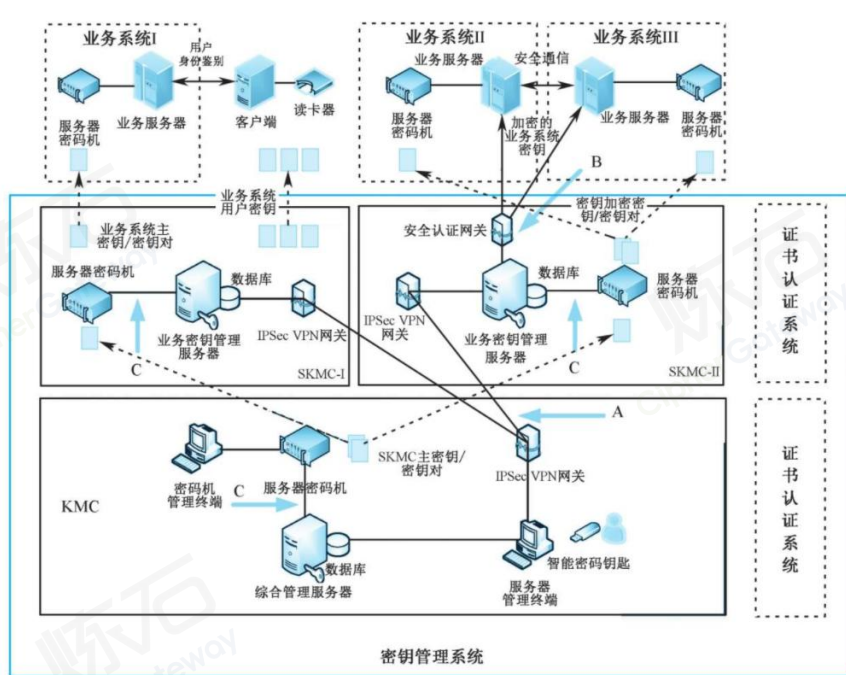


图 86 密钥管理系统密码应用部署图

(1) KMC 的架构和功能

KMC 的主要功能是为各个 SKMC 分发密钥。考虑到需要分发给 SKMC 的密钥相对较少，KMC 向 SKMC 分发密钥时采用离线分发方式：利用密钥存储介质采用人工传递的方式分发密钥。

KMC 主要包括综合管理服务器、服务器密码机、IPSec VPN 网关以及服务器管理终端等设备。

(2) SKMC 的架构和功能

SKMC 负责业务系统的对称密钥和非对称密钥的管理。密钥管理系统有两类 SKMC：SKMC-I 和 SKMC-II，分别为了满足不同应用场景下的应用系统需求。

3. 密钥体系

密钥管理系统“应用和数据安全”层面的密钥主要分为对称和非对称两类密钥体系。

(1) 对称密钥体系

密钥管理系统的对称密钥及其功能如下表所示。

表 6 密钥管理系统对称密钥列表

层次	密钥名称	功能
1	KMC 主密钥	用于分散 SKMC 主密钥
2	SKMC 主密钥	由 KMC 主密钥和 SKMC 信息进行密钥分散生成,用于业务系统主密钥和业务系统密钥加密密钥的分散。由 KMC 利用离线方式通过智能 IC 卡分发给 SKMC
3	业务系统主密钥	由 SKMC 主密钥和业务系统信息进行密钥分散生成,用于业务系统用户对称密钥的分散。由 SKMC 利用离线方式通过智能 IC 卡分发给业务系统
	业务系统密钥加密密钥	由 SKMC 主密钥和业务系统信息进行密钥分散生成,用于业务系统安全通信密钥的安全分发。密钥加密密钥实际上包含两个对称密钥,分别用于对待分发的密钥进行保密性和完整性保护。保密性保护算法是 SM4,完整性保护算法是 HMAC-SM3,即基于 SM3 的 HMAC 算法。SKMC 利用离线方式通过智能 IC 卡分发给业务系统

4	业务系统用户对称密钥	由业务系统主密钥和用户信息分散生成，用于业务系统 I 中的用户身份鉴别，SKMC 利用离线方式通过智能 IC 卡分发给业务系统用户
	业务系统安全通信密钥	由 SKMC 随机生成，用于业务系统 II 和 III 之间的安全通信。SKMC 利用业务系统密钥加密密钥（或业务系统密钥对，见表 5-6）加密后分发给业务系统。业务系统安全通信密钥也包含两个，分别用于对通信数据进行保密性和完整性保护。保密性保护算法是 SM4，完整性保护算法是 HMAC-SM3

(2) 非对称密钥体系

密钥管理系统利用 PKI 技术，完成非对称密钥体系的建立和证书的逐级签发，形成三层密钥体系，密钥管理系统中涉及的非对称密钥如下表所示。

表 7 密钥管理系统非对称密钥列表

层次	密钥	功能
1	KMC	密钥管理系统中主要使用 KMC 密钥对中的签名密钥对，进行 SKMC 证书的签发和验证
2	SKMC	密钥管理系统中主要使用 SKMC 密钥对中的签名密钥对，进行业务系统证书的签发和验证

3	业务系统密钥对	<p>业务系统使用的密钥对用于签发用户证书和安全通信等。</p> <p>SKMC 可以利用其中的加密公钥向业务系统在线分发密钥，基于 SM2 非对称加密对待分发的密钥同时进行保密性和完整性保护</p>
---	---------	--

4. 密码应用工作流程

密钥管理系统的密码应用工作流程如下：

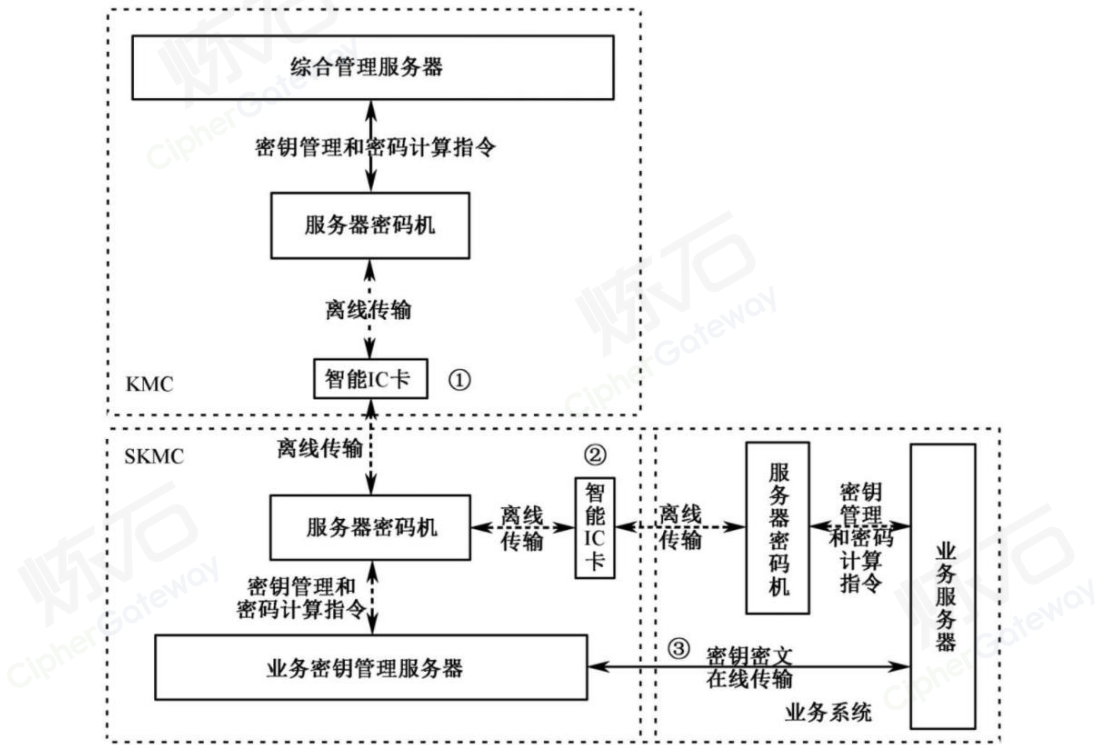


图 87 密钥管理系统的密码应用工作流程

- (1) KMC 向 SKMC 离线分发密钥。KMC 利用离线方式通过智能 IC 卡将 SKMC 主密钥和 SKMC（加密）密钥对从服务器密码机分发到 SKMC 的服务器密码机中。
- (2) SKMC-I 向业务应用系统 I 离线分发密钥，SKMC-II 向业务应用系统 II 和 III 离线分发密钥。SKMC-I 和 SKMC-II 都采用离线分发方式进行业务系统密钥

的分发，区别在于 SKMC-II 和业务系统之间传递的密钥是业务系统密钥加密密钥或业务系统（加密）密钥对，在步骤（3）中进行后续密钥的安全传输。

- (3) SKMC-II 向业务应用系统 II 和 III 在线分发密钥。SKMC-II 按照步骤（2）向业务应用系统 II 和 III 离线分发业务系统密钥加密密钥或（加密）密钥对完毕后，利用上述密钥对后续密钥进行加密分发。

3.3.1.4. 创新趋势

密钥管理系统的创新方向包括应用场景的适配，目前云场景、多租户、虚拟化需求迫切，支持 KMIP 等标准协议的 KMS 服务。

4. 密码能力融入业务流程

4.1. 数据安全本质是对数据重建访问规则

企业数字化转型伴随着数字化资产爆发式增长，数据作为最重要的生产要素，在企业应用系统内部高速流转、共享、协同，驱动业务效率提升，带来了巨大效益。与此同时，数据的高价值使之成为被觊觎的目标，数据安全威胁已经成为关乎企业命运的关键业务风险，这也对企业安全防护体系提出新需求。

近年来，国家高度重视数据安全。我国 2017 年生效的《网络安全法》对个人信息等数据保护提出明确要求；2018 年正式实施《信息安全技术个人信息安全规范》，并于 2020 年修订及实施新版；2019 年 10 月颁布、2020 年 1 月 1 日正式实施的《密码法》明确要求应用密码技术实现数据保护；2021 年 9 月 1 日正式实施《数据安全法》；2021 年 11 月 1 日正式实施《个人信息保护法》。

从安全技术理念看，美国国家安全局 NSA（National Security Agency）下属的 IAD（Information Assurance Directorate），是美国国防与政府防御体系的主要建设机构，早在 2013 年就提出“安全必须从以网络为中心，转向聚焦以数据为中心”；而美国国防部在 2019 年 2 月发布的《国防部云战略》白皮书，也明确提出“美国国防部的安全防护建设重点，在从边界防御，转向保护数据和服务”。

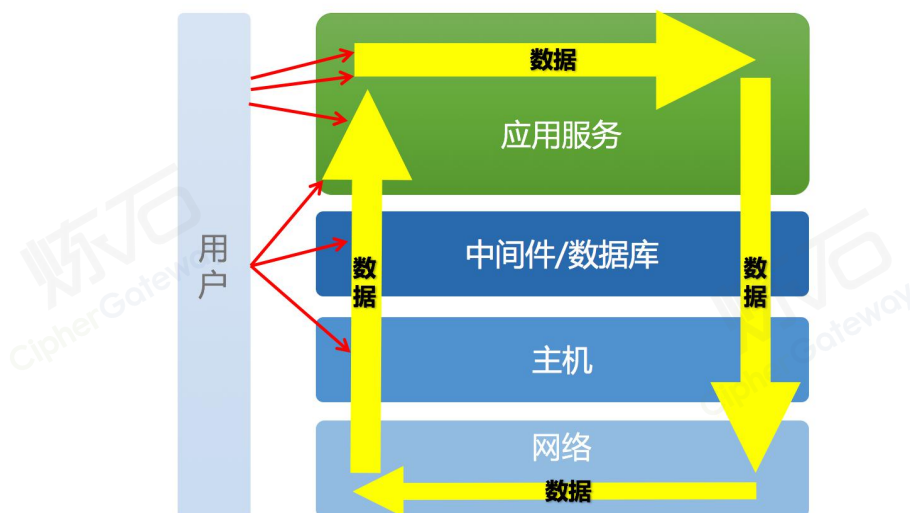


图 88 网络/主机和数据分别是两个正交的维度

参考上图，当前数字化转型围绕业务应用展开，应用由网络/主机/中间件/数据库等承载运行，而数据在各层次支撑组件中被共享流转。由此可见，网络/主机和数据是两个正交的维度，这也给数据安全防护带来挑战，由于 0-day 漏洞不可避免、以及 n-day 漏洞修复不及时所带来的攻击利用，网络/主机所依赖的基于“防漏洞”方式的数据保护，从防护效果来讲是不确定的防护手段。而数据加密、去标识化等技术手段施加了对数据的访问规则，重建、延伸并增强了对数据本身的安全机制，能够提供更为确定的防护效果。

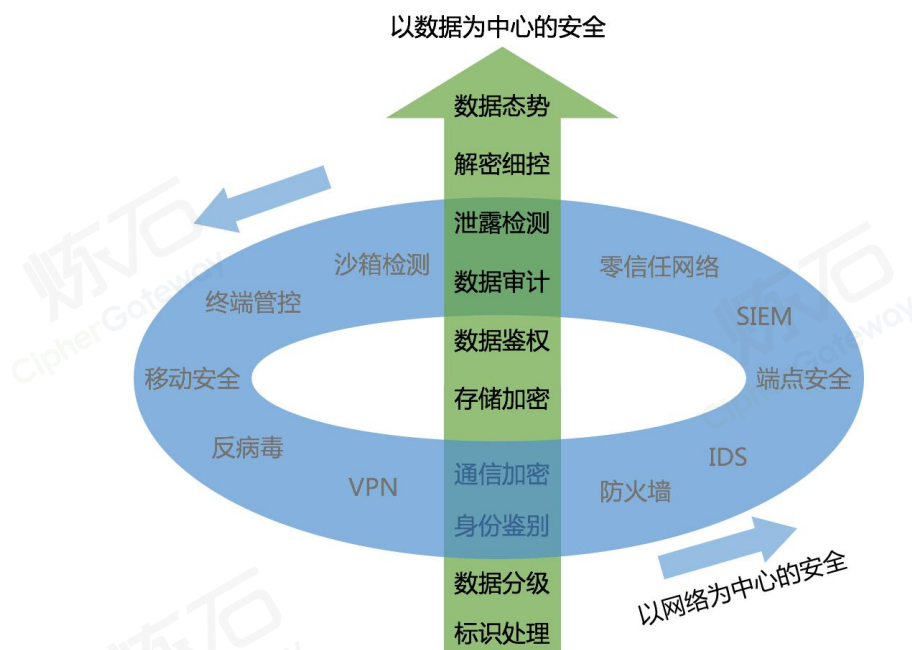


图 89 网络与数据并重的新安全建设体系

内部威胁和外部入侵是数据泄露两大原因。企业过去保护数据，是在网络侧采用各层次“防漏洞”的方式，但来自业务人员的内部威胁始终存在，同时安全漏洞目前看也无法避免，难以彻底解决网络入侵。所以对数据本身直接进行加密和访问控制，是实现数据防护最有效的手段。安全技术本身也正在从“以网络为中心的安全”，向“聚焦以数据为中心的安全”演进。

“以网络为中心的安全”是保证数据安全的前提和基石，而“以数据为中心的安全”以数据为抓手实施安全保护，能够更有效增强对数据本身的防护能力，二者高度关联、相互依赖、叠加演进。从产业背景看，过去 20 年是 IT 时代，侧重于主机/网络/应用等方面的安全建设。而今天进入 DT 时代 (Data Technology)，数据的重要性和主导性被提升到新高度，与之对应的，企业安全建设理念也将提升为“网络与数据并重的新安全建设体系”。

着眼当下，数据安全所面临的问题不是做的过多导致冗余，而是出血口太多、防护能力达不到。事实上，应用系统、安全产品、基础设施都潜藏着漏洞，或者

存在考虑不周的安全设计缺陷。好的安全理念应该是以网络与数据并重为新建设方向，面向失效的安全机制，通过有联动协同的纵深安全机制，构建有效防线。特别的，从针对数据本身进行主动式防护出发，将包含密码技术在内的数据安全技术组合赋能给具体行业安全问题，比发掘一个适用于所有行业的通用问题，更符合用户的实际需求。

4.2. 安全技术从基础设施演进到业务应用

从空间维度看，企业信息化架构包含基础设施、平台、业务应用等层次，数据在不同层之间持续流转，并且数据越往上层，价值点越多。数据在基础设施与平台层时，缺失业务含义、价值点低，比如磁盘加密产品的安全控制颗粒度是比较粗的。而数据在业务应用层时，才具有丰富的业务上下文含义。

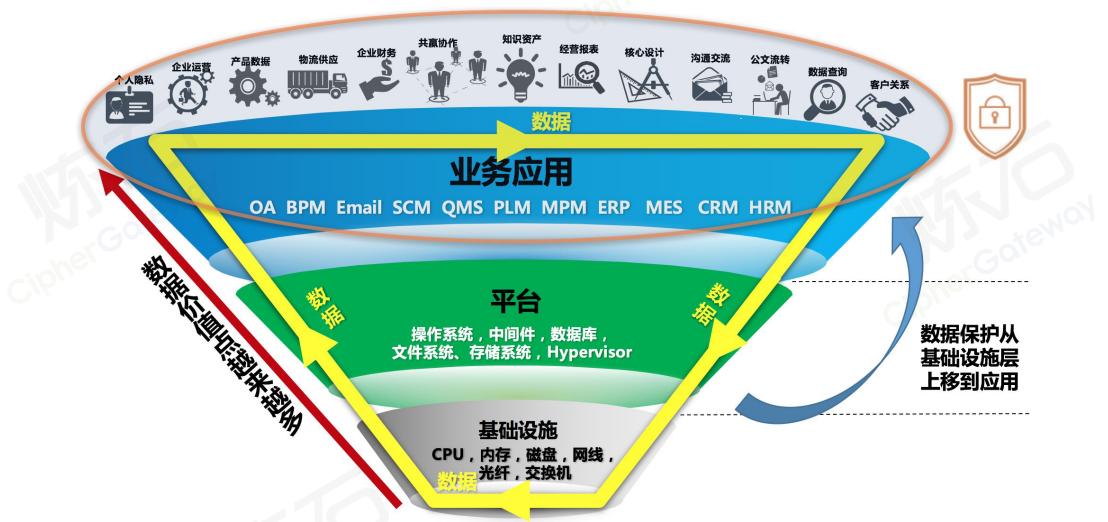


图 90 数据安全从以基础设施为抓手，演进到以应用为抓手

传统数据安全包括传输加密（VPN 等）、磁盘加密、数据库 TDE 等，侧重从基础设施或平台层防护数据，而对应用层数据流转缺失保护。但是，应用层恶意

用户的攻击行为，往往发生在看似合理的业务操作中，具有更高的隐蔽性；而且内部用户更容易接触到组织的核心知识资产等敏感信息，危害更大；另外，接触业务应用层的内部人员数量，要远大于接触基础设施层和软件平台的。

由于数据主要在业务应用中被共享流转，所以业务应用层是实现数据安全的关键抓手，然而企业应用普遍缺失内生安全能力，所以业务应用层的数据安全防护是当前数据安全的建设重点、也是薄弱环节。面向业务应用层的数据安全机制，能够建立细粒度的数据安全访问机制，有效应对数据泄露威胁。数据安全技术正在从“以基础设施为抓手的传统数据安全”，演进到“以业务应用为抓手的新数据安全”。企业应用生态既包含传统套装软件、行业软件、自建应用等，也包含新型的 SaaS（Software as a Service），这种差异性也催生了不同的数据安全技术。

4.3. 密码安全融合打造面向业务实战防护

数据安全的技术机制包括加密、访问控制、审计、追溯等。本质上，访问控制和审计等技术，通常需要在“安全边界”上实施执行，比如安全网关、或应用系统等。而在新一代 IT 架构中，数据被更充分流转和共享，网络边界和数据边界都被打破了，仅靠应用内的访问控制难以防范存储归档数据的违规外拷等场景，而此时数据访问日志的覆盖率也存在缺失、导致审计不可信。

密钥是对数据保密性的浓缩，带密钥的散列值（消息认证码）是对数据完整性的浓缩，数据很大但密钥很小。数据流动快、边界范围大，但密钥管控严、边界范围小，所以加密的核心价值是将数据边界收缩到密钥边界，缩小了安全敞口。

在数据流转的咽喉要道，通过密钥管控，采用密码机集中解密处理或基于远程密管的分布式节点解密处理等方式，可以“重构出新的数据边界”，进而在新边界上将数据解密与访问控制、审计等机制紧密结合，无论数据存储在哪里，都需要回到“锚点”解密后再实施安全控制规则，保证访问控制不会被绕过。CASB 面向切面加密即是“锚点”解密的落地实践。



图 91 数据安全密码防护体系

面向切面加密的 CASB 插件模式中，数据安全插件就位于数据流转的咽喉位置，在数据加解密的锚点，施加支持 ABAC（Attribute Based Access Control，基于属性的访问控制）的访问控制策略，提供防绕过的数据防护机制，并支持可追溯、防篡改的第三方数据操作审计，每条日志支持主体追溯到人，保证可事后追责。CASB 插件模式会配套支持多级密钥派生的密钥管理平台，根密钥由双随机数芯片物理真随机产生，并保存在硬件密码卡中，不会以明文形式导出，密钥备份采用标准的分散备份方案，由企业内指定人员授权后可进行密钥恢复操作，保障在密管设备发生故障损坏情况下可以在新设备中安全恢复密钥。

实际上，CASB 面向切面加密是对云访问安全代理技术进行再次创新的 CASB 插件模式，是一种面向企业应用施加保护的、可敏捷实施的密码数据安全技术，可应对云上或待上云自建应用的安全威胁，因为其不仅限于保护 SaaS，所以也可称为 Critical Application Security Broker，关键应用安全代理。将插件软件包复制到应用中间件指定目录，再经过简单配置，应用无需再进行任何源代码修改，即可实现任意指定字段的数据库存储加密（防范内部 IT 人员、外部黑客等），同时实现结合登录用户身份的数据动态脱敏和审计（防范内部业务人员越权），进而提供“主体到应用内用户，客体到字段级”的细粒度数据安全防护能力。插件与安全策略管理平台以及密钥管理系统进行交互，获取加解密策略以及密钥。

数据安全产品最关键的是对数据结构识别，CASB 插件模式通过部署在应用中间件的数据安全插件，唤醒了沉睡中的数据操作 API，比如 SQL 规范、数据源接口、文件操作接口等，巧妙解决了数据结构的识别问题，所以 CASB 插件模式可以看做是一种改进版的 CASB API 模式实现。CASB 插件模式无需改造应用，即可通过配置施加安全策略，增强应用内生安全能力，打造“以业务应用为抓手的数据安全密码防护体系”。无论是企业云迁移应用，还是私有部署应用，均可快速部署和敏捷实施。典型场景包括政企客户的个人信息保护、企业商业秘密保护、政府、央企、金融等行业国密整改、军工与保密行业数据保护等。CASB 插件模式可针对单个应用防护、也可以针对几十个应用批量保护，同时支持敏感字段等结构化数据、和文档文件等非结构化数据。在提升数据安全防护能力的同时，不改变应用的运行机制，也不影响企业现有系统的稳定性，保障企业业务不中断。

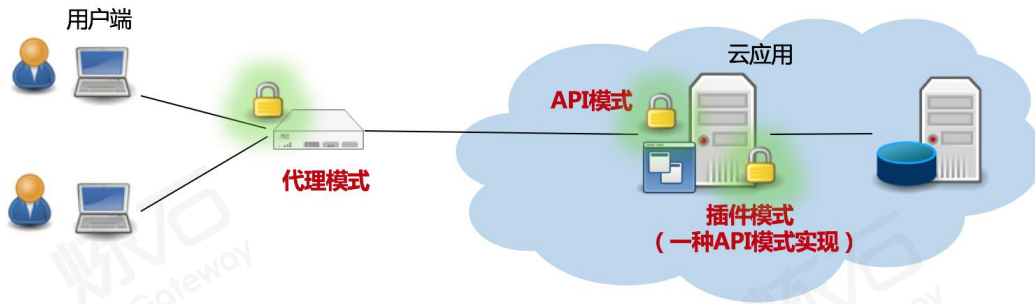


图 92 CASB 的三种交付模式部署对比

表 8 CASB 的三种交付模式技术对比

方案	CASB 代理模式 (串网关)	CASB API 模式 (改代码)	CASB 插件模式 (切面安全)
技术本质	网关侧分析和代理应用请求； 以适配方式增强数据安全与业务安全；	云应用开放 API 扩展外部安全服务； 以集成方式增强云应用安全能力；	应用内识别用户数据操作； 以配置方式增强数据安全；
优缺点分析	实施成本中，应用免改造但需适配； 云访问安全代理（SaaS）、 关键应用安全代理（应用云迁移、私有应用）；	实施成本中，需要开发改造应用； 云访问安全代理（SaaS）；	实施成本低，仅需配置安全策略； 关键应用安全代理（应用云迁移、私有应用）；

对比上述表格，CASB 插件模式是对源自美国的 CASB 云访问安全代理技术的重要创新，也是面向云场景的新数据安全技术，可面向企业批量应用敏捷实施数据防护，实现服务侧数据存储加密、用户侧数据动态脱敏、高置信度数据访问审

计等功能，兼具 API 模式“内生安全”和应用免改造“敏捷实施”两大优势，可有效防护云上或待上云的各种自建应用，具有广阔的应用场景和发展空间。



5. 密评合规重构安全防护

5.1. 密码应用典型性问题分析

国家正在大力推进密码工作，普及密码技术的应用，但是我国的商用密码应用仍有极大的发展空间。密码产品、技术和服务只有得到合规、正确、有效应用，才能发挥安全支撑作用。在实际应用中，由于用户（信息系统应用开发商）有可能不用、乱用、错用密码技术，导致应用系统的安全性得不到有效保障^[56]。

5.1.1. 密码应用不广泛

由于行业无强制性密码应用要求，制约了密码应用的发展，导致很多需要使用密码进行保护的场景，并未使用密码。信息系统应用开发商对密码在安全防护中的重要地位缺乏认识，为节省成本而忽视密码技术。由于缺乏密码算法、协议等技术支撑，信息系统中数据的保密性、真实性、完整性和不可否认性得不到保障。

同时，不同行业的信息系统对密码产品、技术及服务的性能要求、应用场景、手段和管理方法等都不尽相同，因此不同行业应根据其行业特点尽快出台对应的商用密码应用指导性文件。目前商用密码推广还处于起步阶段，针对密码应用、管理等相关规定，各行业无明确强制性的密码应用安全要求，可能会面临管理、技术、成本等各方面的问題，制约了商用密码的应用发展。

5.1.2. 密码应用不规范

在密码标准化建设工作中，我国虽然已发布 SM 系列国密算法，但密码应用方面的标准体系还不够完善。同时信息系统应用开发商缺乏对密码重要作用的认识，不严格执行密码标准，不规范调用密码技术，导致系统无法对接，甚至出现安全漏洞。

随着移动互联网、物联网、云计算等新业态的快速发展，密码应用标准的缺失将成为阻碍行业发展、数据互联互通的障碍。现行密码标准与关键信息基础设施、重点行业的密码应用要求难以契合，商用密码标准化推进难度大，导致了商用密码未能规范应用。

5.1.3. 密码应用不安全

由于开发人员缺乏对密码算法、技术标准的正确理解，在密码应用的过程中，经常会出现密码错误应用的情况发生。如果信息系统应用开发商对密码应用缺乏技能和经验，不清楚合规性要求，不了解密码算法的类型、协议参与方的角色要求、关键参数的类型和规模等基本知识，错误调用密码技术，就会不可避免地产生安全漏洞。常见的案例包括系统中使用了已被破解的密码算法（如 MD5、SHA-1 等），密码支撑资源被错误调用等。

密码技术不用、乱用、错用都将导致系统安全问题，因此，合规、正确、有效使用密码技术是信息系统应用开发商必须熟练掌握的基本能力。同时准确结合用户安全需求，从而在信息系统密码安全应用的建设过程中做到“正确规范”。

5.2. 密评为密码合规提供基线

5.2.1. 密评发展历程

密评最早是在 2007 年提出，经过十几年的积累，密评制度体系不断完善成熟，其发展历程大致可以分为以下 5 个阶段^[56]。

5.2.1.1. 阶段一：奠定期

制度奠定期从 2007 年 11 月至 2016 年 8 月。2007 年 11 月 27 日，国家密码管理局印发 11 号文件《信息安全等级保护商用密码管理办法》，要求信息安全等级保护商用密码测评工作由国家密码局指定的测评机构承担。2009 年 12 月 15 日，国家密码管理局印发管理办法实施意见，进一步明确了密码测评有关要求。

5.2.1.2. 阶段二：集结期

再次集结期从 2016 年 9 月至 2017 年 4 月。国家密码管理局成立起草小组，研究起草《商用密码应用安全性评估管理办法（试行）》。2017 年 4 月 22 日，正式印发《关于开展密码应用安全性评估试点工作的通知》（国密局（2017）138 号文），在七省五行业开展密评试点。

5.2.1.3. 阶段三：建设期

体系建设期从 2017 年 5 月至 2017 年 9 月。国家密码管理局成立密评领导小组，研究确定了密评总体架构，并组织有关单位起草 14 项制度文件。2017 年 9 月 27 日，国家密码管理局印发《商用密码应用安全性测评机构管理办法（试行）》

《商用密码应用安全性测评机构能力评审实施细则（试行）》《信息系统密码应用基本要求》（后以密码行业标准 GM/T 0054 形式发布）和《信息系统密码测评要求（试行）》，密评制度体系初步建立。

5.2.1.4. 阶段四：试点期

密评试点开展期从2017年10月至今。试点开展过程同时也是机构培育过程，包括机构申报遴选、考察认定、发布目录、开展试点测评工作并提升测评机构能力、总结试点经验、完善相关规定。2019年上半年对第一批密评试点做了评审总结，对参与试点的27家机构进行能力再评审，择优选出16家扩大试点，对另外11家机构给予6个月能力提升整改期。2019年10月，开始启动第二批密评试点工作。

5.2.1.5. 阶段五：推广期

随着《密码法》于2020年1月1日起正式实施，密评也逐渐进入推广期。从前期的试点、政策驱动到组织机构开始主动开展密评工作，特别的，中国密码学会密评联委会于2020年12月发布了密评指引文件，并于2021年12月进行了更新；密评遵循的标准《GM/T 0054-2018 信息系统密码应用基本要求》（2018年2月8日发布并实施），也升级为国家标准《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》（2021年3月9日发布，2021年10月1日实施），标志着密评体系已经基本确立，密评有了量化评估、高风险判定的指引等测评的依据标准，开始进入快速推广和发展的阶段。

5.2.2. 密评开展依据

“密评”的全称是“商用密码应用安全性评估”，指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估^[45]。

那为什么要做密评呢？一方面，开展密评工作是国家法律法规的强制要求，是网络安全运营者的法定责任和义务；另一方面，开展密评是商用密码应用正确、合规、有效的重要保证，是检验网络和信息系​​统安全性的重要手段。

5.2.2.1. 密评是法律法规强制要求

开展密评，是国家相关法律法规提出的明确要求，同时也是赋予网络安全运营者的法定责任和义务。

1. 《中华人民共和国密码法》

第二十七条：法律、行政法规和国家有关规定要求使用密码进行保护的关键信息基础设施，其运营者应当使用密码进行保护，自行或者委托密码检测机构开展密码应用安全性评估。

2. 《商用密码应用安全性评估管理办法(试行)》

第十条：关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次。

3. 《网络安全等级保护条例（征求意见稿）》

第四十七条：第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密

码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。

4.《国家政务信息化项目建设管理办法》

第十五条：项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

第二十五条：项目建设单位提交验收申请报告时应当附上密码应用安全性评估报告等材料。

因此，开展密评是广大网络安全运营者落实法律法规要求，履行网络安全义务的一项重要责任。

5.2.2.2. 密评是网络和信息系統安全的重要保证

1.密评是商用密码应用的重要推动力

商用密码应用的正确、合规、有效，是网络和信息系統安全的关键所在，而密评工作的开展可以促进商用密码应用做到合规、正确和有效，是商用密码应用正确、合规、有效的重要推动力。

2.密评是应对网络与数据安全形势的需要

通过密评可以及时发现密码应用过程中存在的问题，为网络和信息安全提供科学的评价方法，逐步规范密码的使用和管理，从根本上改变密码应用不广泛、不规范、不安全的现状，确保密码在网络和信息系統中得到有效应用，切实构建起坚实可靠的网络安全密码保障。

3.密评是系统安全维护的必然要求

密码应用是否合规、正确、有效，涉及密码算法、协议、产品、技术体系、密钥管理、密码应用多个方面。因此，需委托专业机构、专业人员，采用专业工具和专业手段，对系统整体的密码应用安全进行专项测试和综合评估，形成科学准确的评估结果，以便及时掌握密码安全现状，采取必要的技术和管理措施。

综上所述可以看出，密码体系是网络与数据安全环境的基础，而密码评测是建立健全密码安全体系最重要的考量，是网络安全和信息系统安全建设的重要组成部分，因此开展密评工作具有非常重要的意义。

5.2.3. 密评适用对象

《密码法》第二十七条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

《商用密码应用安全性评估管理办法（试行）》第三条、第二十条：涉及国家和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位（以下简称责任单位）应当健全密码保障体系，实施商用密码应用安全性评估。

重要领域网络和信息系统的包括：

- 基础信息网络
- 涉及国计民生和基础信息资源的重要信息系统
- 重要工业控制系统
- 面向社会服务的政务信息系统
- 关键信息基础设施
- 网络安全等级保护第三级及以上信息系统

自 2021 年 9 月 1 日起施行的《关键信息基础设施安全保护条例》中明确了关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

司法部、网信办、工业和信息化部、公安部负责人在就《关键信息基础设施安全保护条例》有关问题回答了记者提问时，对于关键信息基础设施如何认定的问题?是这样回答的：《条例》从我国国情出发，借鉴国外通行做法，明确了关键信息基础设施的定义和认定程序。一是明确关键信息基础设施的定义。二是明确关键信息基础设施所在行业 and 领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门。三是明确由保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并组织认定本行业、本领域的关键信息基础设施。四是规定关键信息基础设施发生较大变化，可能影响其认定结果时，运营者应当及时报告保护工作部门，由保护工作部门重新认定。

《关键信息基础设施确定指南（试行）》中明确的关键信息基础设施认定标准有：

1. 网站类

（符合以下条件之一的，可以认定为关键信息基础设施）

（1）门户网站

（2）重点新闻网站

（3）日均访问量超过 100 万人次的网站

（4）一旦发生网络安全事故，可能造成以下影响之一的：

- 影响超过 100 万人工作、生活；
- 影响单个地市级行政区域 30%以上人口与的工作、生活；
- 造成超过 100 万个人信息泄露；
- 造成大量机构、企业敏感信息泄露；
- 造成大量地理、人口、资源等国家基础数据泄露；
- 验证损害政府形象、社会秩序或危害国家安全。

(5) 其他应该认定为关键信息基础设施。

2.平台类

(符合以下条件之一的，可以认定关键信息基础设施)

(1)注册用户超过 1000 万或活跃用户(每日至少登录一下)数超过 100 万；

(2)日均成交订单额或交易额超过 1000 万元；

(3)一旦发生网络安全事故，可能造成以下影响之一的：

- 造成 1000 万元以上的直接经济损失；
- 直接影响超过 1000 万人工作、生活；
- 造成超过 100 万人个人信息泄露；
- 造成大量机构、企业敏感信息泄露；
- 造成大量地理、人口、资源等国家基础数据泄露；
- 严重损害社会和经济秩序或危害国家安全。

(4) 其他应该认定为关键信息基础设施；

3.生产业务类

(符合以下条件之一的，可以认定关键信息基础设施)

(1) 地市级以上政府机关面向公众服务的业务系统或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统；

(2) 规模超过 1500 个标准机架的数据中心；

(3) 一旦发生网络安全事故，可能造成以下影响之一的：

- 影响单个地市级行政区 30%以上人口的工作、生活；
- 影响 10 万人用水、用电、用气、用油、取暖或交通出行等；
- 导致 5 人以上死亡或 50 人以上重伤；
- 直接造成 5000 万元以上经济损失；
- 造成 100 万人个人信息泄露；
- 造成大量机构、企业敏感信息泄露；
- 造成大量地理、人口、资源等国家基础数据泄露；
- 严重损害社会和经济秩序或危害国家安全。

(4) 其他应该认定为关键信息基础设施。

同时《信息安全等级保护商用密码管理办法》中也明确规定：“国家密码管理局和省、自治区、直辖市密码管理机构对第三级及以上信息系统使用商用密码的情况进行检查”。在国家密码管理局印发的《信息安全等级保护商用密码管理办法实施意见》中规定“第三级及以上信息系统的商用密码应用系统，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行”。这些制度明确了信息安全等级保护第三级及以上信息系统的商用密码应用和测评要求。此外，在新版《网络安全等级保护条例》（征求意见稿）明确要求在规划、建设、运行阶段开展密码应用安全性评估。

5.2.4. 密评政策法规

为规范密评工作，国家密码管理局制定印发了《商用密码应用安全性评估管理办法（试行）》、《商用密码应用安全性测评机构管理办法（试行）》、《商用密码应用安全性测评机构能力评审实施细则（试行）》等管理文件，对测评机构、网络与信息系统责任单位、管理部门提出要求，对评估程序、评估办法、监督管理等进行明确，对测评机构审查认定工作提出要求。

5.2.4.1. 《商用密码应用安全性评估管理办法（试行）》

1. 出台背景和目标

为发挥密码在维护安全与促进发展综合平衡中的重要支撑作用，我国法律法规和政策性文件都对密码应用提出明确要求。在此背景下，国家密码管理局制发《商用密码应用安全性评估管理办法（试行）》（以下简称《办法》），目标是明确国家和省（部）密码管理部门在密码应用安全性评估中的指导、监督和检查职责；明确重要信息系统的建设、使用、管理单位在评估工作中的主体责任；依法培育测评机构，规范评估行为，以评促改、以评促用，形成规范有序的密码应用安全性评估审查机制，并与网络安全等级保护等已有制度做好衔接。

2. 主要内容

《办法》聚焦于建立密评审查机制、规范密评工作，规定了测评机构、网络与信息系统责任单位、管理部门的权利义务，明确了评估程序、评估方法、监督管理等内容。

《办法》共四章二十二条。

(1) 第一章是总则。明确了制定《办法》的目的和立法依据，对密码和密码应用安全性评估进行定义，明确适用范围和管理机构职能。

(2) 第二章介绍了评估程序。规定了责任单位和测评机构职责，提出独立、客观、公正的评估原则，对重要信息系统如何实施密码应用安全性评估做出规定。

(3) 第三章介绍了监督管理。规定密码管理部门要不定期开展评估专项检查和抽查工作，对测评机构进行监督检查，明确其他主管部门应将密评情况作为网络与信息系统安全检查的重要内容。

(4) 第四章是附则。分别对《办法》实施前已投入使用的重要信息系统、未设立密码管理机构的有关部门，以及不在《办法》所列范围内的其他网络与信息系统如何开展密评做出规定。

3. 密评工作与网络安全等级保护工作的关系

《办法》的制定充分考虑了与网络安全等级保护（简称“等保”）的结合和相互衔接。《办法》根据《网络安全法》《商用密码管理条例》及国家关于网络安全等级保护和重要领域密码应用的有关要求制定，对网络安全等级保护第三级及以上信息系统提出密码应用安全性评估要求。

5.2.4.2. 《商用密码应用安全性测评机构管理办法（试行）》

1. 适用范围

根据《商用密码应用安全性评估管理办法（试行）》确定的在试点期间的主要原则，为规范培育商用密码应用安全性测评机构，《商用密码应用安全性测评机构管理办法（试行）》提出了试点期间对测评机构的管理原则，适用在中华人

民共和国境内对商用密码应用安全性测评机构的监督管理，也适用于对测评机构、测评人员及其测评活动的管理与规范。

2. 测评机构遴选的基本原则

测评机构遴选应按照“依法合规、公正公开、客观独立”的原则有序开展。

3. 测评机构的监管主体

国家密码管理局根据各省部密码管理部门的推荐，负责测评机构的受理、能力评审和监督检查等。

4. 测评机构的基本条件

申请测评机构应具备以下条件：在中华人民共和国境内注册，由国家投资、法人投资或公民投资成立的企事业单位；要求产权关系明晰，注册资金 500 万元以上；成立年限在 2 年以上，从事信息系统安全相关工作 1 年以上，无违法记录；要求具备与从事系统测评相适应的独立、集中、可控的工作环境，测评工作场地应不小于 200 平方米；具备必要的检测设施、设备，使用的设施设备应满足实施密评工作的要求；具备完善的人员结构，包括专业技术人员和管理人员，通过“密码应用安全性评估人员考核”的人员数量不少于 10 人；具有完备的安全保密管理、项目管理、质量管理、人员管理、培训教育、客户管理和投诉处理等规章制度。

5. 申请测评机构应提交的材料

申请测评机构应提交的材料主要包括：①《商用密码应用安全性测评机构申请表》。②从事与商用密码相关工作情况的说明。③开展测评工作所需的软硬件及其他服务保障设施配备情况。④管理制度建设情况（需要提供相关制度的文本

文件)。⑤申请单位及其测评人员基本情况(需要提供人员的基本信息)。⑥申请单位认为有必要提交的其他材料。

6.测评机构的申请流程

国家密码管理局设立申请材料初审工作组,对申请材料进行初审,出具初审结论。初审结果按程序报批后,告知申请单位。通过初审的申请单位,应在60个工作日内参加培训、考核和能力评审。测评人员培训、考核工作由国家密码管理局委托的机构承担,申请单位应当确保本单位测评人员全程参加。考核通过后,测评人员方可参加密码应用安全性评估工作。

7.测评机构的责任和义务

测评机构的设施环境以及人员是保证测评质量的重要基础。测评机构的地址或测评实验室的位置发生变化,则需要对新设施和环境进行额外的考核,以核实其是否仍能够满足本办法的要求。

8.测评机构的监督检查

监督检查是保证测评机构能力持续性的重要途径,也是在测评初期保证测评队伍质量、建立测评体系信誉的主要途径。密码管理部门会着重对以下过程进行监督检查:测评人员的完整性、测评能力是否保持、质量管理体系运行的合规性、测评过程是否由有资质的测评人员执行及测评报告的准确性和公正性等。测评项目实施过程中,测评机构应接受国家密码管理局的监督管理。测评机构应当在年底编制密评工作报告,并报送国家密码管理局。国家密码管理局、测评机构所属省部密码管理局对测评机构负有监督检查职责,根据需要开展测评机构检查工作。

9.测评机构的法律责任

测评机构有下列情形之一的，国家密码管理局应责令其限期整改；情节严重的，予以通报或做出其他严肃处理。①未按照有关标准规范开展测评或未按规定出具测评报告的。②严重妨碍被测评信息系统正常运行，危害被测评信息系统安全的。③未妥善保管、非授权占有或使用密码应用安全性评估相关资料及数据文件的。④分包或转包测评项目，以及有其他扰乱测评市场秩序行为的。⑤限定被测评单位购买、使用指定信息安全和密码相关产品的。⑥测评人员未通过培训考核，但从事密码应用安全性评估工作的。⑦未按本办法规定提交材料、报告情况或弄虚作假的。⑧其他违反密码应用安全性评估工作有关规定的行为。

测评机构有下列情形之一的，国家密码管理局应取消其商用密码应用安全性测评机构试点资格。①因单位股权、人员等情况发生变动，不符合商用密码应用安全性测评机构基本条件的。②故意泄露被测评单位工作秘密、重要信息系统数据信息的。③故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假未如实出具测评报告的。④自愿退出测评机构目录的。测评人员有下列行为之一的，责令测评机构督促其限期改正；情节严重的，责令测评机构暂停其参与测评工作；情形特别严重的，从密码应用安全性测评人员名单中移除，并对其所在测评机构进行通报。①未经允许擅自使用或泄露、出售密码应用安全性评估工作中收集的数据信息、资料或测评报告的。②测评行为失误或不当，影响重要领域网络与信息系统安全或造成运营使用单位利益损失的。③其他违反密码应用安全性评估工作有关规定的行为。测评机构及其测评人员违反本办法的相关规定，给被测评信息系统运营使用单位造成严重危害和损失的，由相关部门依照有关法律法規予以处理。任何单位和个人如发现测评机构、测评人员有违法、违规行为的，可向国家密码管理局举报、投诉。

5.2.4.3. 《商用密码应用安全性测评机构能力评审实施细则（试行）》

《商用密码应用安全性测评机构能力评审实施细则（试行）》通过对申请机构的组织管理能力、测评实施能力、设施和设备安全与保障能力、质量管理能力、风险防范能力等进行公平、公正、独立、客观的能力评审，为规范测评机构的建设和管理、提高测评机构能力提供支撑。

1. 实施细则的主要内容

实施细则阐述了商用密码应用安全性测评机构能力评审工作中相关机构的工作职责、评审工作的具体流程、评审结果的量化及认定等。

2. 基本原则

申请单位能力评审遵循公平、公正、独立、客观的原则。

3. 适用范围

适用于对申请单位的能力评审。

4. 工作职责

国家密码管理局组织对申请单位的测评能力进行评审。能力评审实行专家组负责制。国家密码管理局在能力评审中的具体职责包括：①负责能力评审工作的组织管理，审核申请资料的完整性与规范性。②建立并维护能力评审专家库。③设立评审专家组，在能力评审专家库随机抽取评审专家，指定专家组组长，由专家组负责对申请单位的能力进行评估、判定。④负责与申请单位的沟通协调，组织并监督现场评审。⑤负责出具能力评审结论。

5. 评审程序

国家密码管理局组成评审专家组，组织专家评审。评审分为材料核查、现场评审、综合评议三个阶段。

(1) 材料核查。专家组对照评审内容和要求对申请单位提交的材料进行查阅，重点对《商用密码应用安全性测评机构申请表》和《商用密码应用安全性测评机构能力评估申请表》进行审阅。对需要现场核实的内容予以记录，以备现场评审时核查。

(2) 现场评审。专家组前往申请单位，采取查看、问询、模拟测试、问卷考试等形式，对照《商用密码应用安全性测评机构能力要求》对测评机构的基本情况、人员结构、测评实验室条件、仪器设备条件、测评实施能力、质量管理能力和风险控制能力七个方面进行评审。专家组根据现场评审情况，对照《商用密码应用安全性测评机构能力评审专家评分表》逐项量化评价。

(3) 综合评议。专家组组长主持召开会议，综合材料审查和现场评审情况进行研讨和评议，汇总专家评分情况，填写《商用密码应用安全性测评机构能力评审汇总表》，提交国家密码管理局。在第二批测评机构试点培育中，将增加实际测评能力仿真评价的环节，确保申请机构有实战经验，而且能力特别突出。

6. 工作要求

测评机构能力评审工作过程中，专家组应遵循如下要求：遵守法律法规和技术规范要求，坚持客观、独立、科学、公正的原则，专家对量化评价负责；按时参加评审活动，认真履行职责，廉洁自律，不得借评审谋取私利；遵守相关保密规定，对评审中接触到的有关情况负有保密责任；有下列情形之一的，专家应当主动向国家密码管理局申请回避，如未主动申请回避，一经发现，取消其专家资格。

①专家担任申请单位技术顾问等职务的。②专家所在单位与申请单位存在利益关系的。③专家与申请单位存在利益关系的其他情况。

7.《商用密码应用安全性测评机构能力要求》

《商用密码应用安全性测评机构能力评审实施细则（试行）》的附件《商用密码应用安全性测评机构能力要求》，对测评机构能力提出了具体要求。主要包括基本情况、人员结构、测评实验室条件、仪器设备条件、测评实施能力、质量管理能力和风险控制能力等方面的要求。

5.2.5. 密评遵循标准

密评工作应当遵循国家法律法规及相关标准。密评机构开展密评工作应当遵循上密码管理政策、相关密码标准和指导性文件要求，遵循独立、客观、公正的原则。

密评标准主要有以下标准：

- 《GM/T 0054-2018 信息系统密码应用基本要求》
- 《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》
- 《信息系统密码测评要求（试行）》
- 《商用密码应用安全性评估测评过程指南（试行）》
- 《商用密码应用安全性评估管理办法（试行）》
- 《商用密码应用安全性评估作业指导书》
- 《商用密码应用安全性评估测评工具使用需求说明书》

在 2021 年 10 月 1 日以前，密评依据的主要标准是国家密码管理局于 2018 年 2 月 8 日发布并实施的《GM/T 0054-2018 信息系统密码应用基本要求》（简

称“GM/T 0054 标准”) 等标准，对信息系统的规划、建设、运行三个阶段的密码应用情况进行安全性评估。

2021 年 10 月 1 日，国家市场监管总局、国家标准化管理委员会发布的《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》（简称“GB/T 39786 标准”）正式施行后，密评工作依据的主要标准变为 GB/T 39786 标准。而 GB/T 39786 标准是在 GM/T 0054 标准基础上修订完善而来的，是由行业标准升级为了国家标准。

5.2.5.1. GM/T 0054-2018 标准

2018 年 2 月，国家密码管理局发布了 GM/T 0054-2018 《信息系统密码应用基本要求》（简称 GM/T 0054 标准），对信息系统中如何应用密码提出了基本要求，是当前指导、规范和评估信息系统中商用密码应用的标准依据。GM/T 0054 标准提出了总体要求、密码功能要求、密码技术应用要求、密钥管理和安全管理共 5 个方面的相关要求。

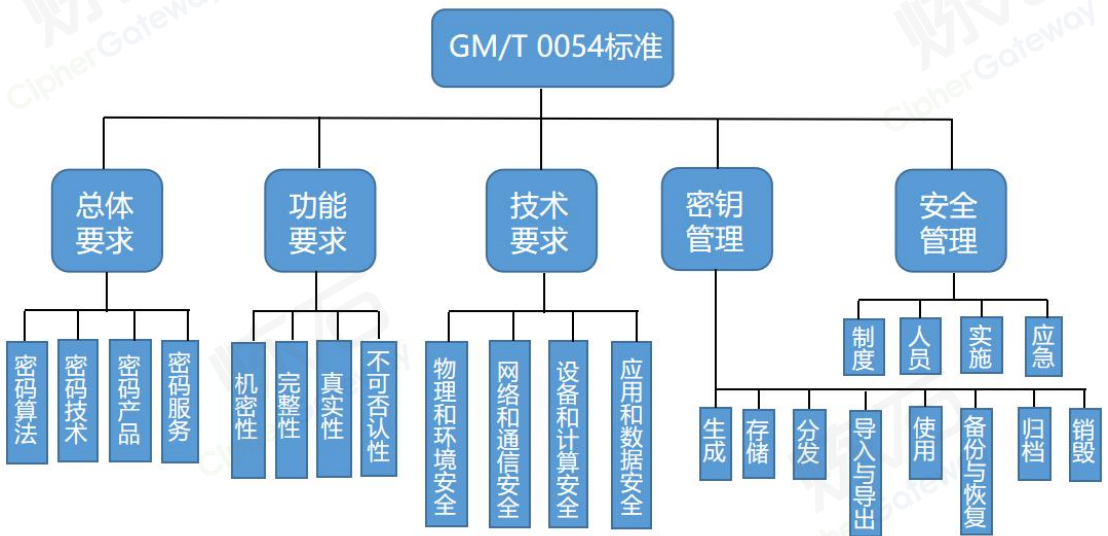


图 93 GM/T 0054 标准基本要求架构图

1.总体要求

总体要求是所有信息系统都需遵循的基本要求，其中：

- 密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
- 密码技术应遵循密码相关国家标准和行业标准；
- 密码产品与密码模块应通过国家密码管理部门检测认证；
- 密码服务应通过国家密码管理部门许可。

2.密码功能要求

密码功能要求是对密码在信息系统中功能作用的阐述，主要包括机密性、完整性、真实性和不可否认性。

3.密码技术应用要求

密码技术应用要求是对密码产品应用的密码技术要求，主要包括物理和环境安全、网络和通信安全、设备和计算安全以及应用和数据安全等。

4.密钥管理

密钥管理是对密码应用过程中对密钥管理提出的明确要求。信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。

5.安全管理

安全管理主要包括制度、人员、实施、应急等部分内容。

5.2.5.2. GB/T 39786—2021 标准

2021 年 3 月 9 日，国家市场监督管理总局、国家标准化管理委员会正式发布国家标准 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》（以下简称 GB/T 39786），已于 2021 年 10 月 1 日正式实施。“信息系统密码应用基本要求”从行业标准 GM/T 0054 上升为国家标准 GB/T 39786，是商用密码应用与安全性评估工作的重要里程碑，对促进我国密码事业发展，进一步规范密码应用，具有重要意义。

GB/T 39786 标准从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层提出密码应用技术要求，保障信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性；并从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求，为信息系统提供管理方面的密码应用安全保障。

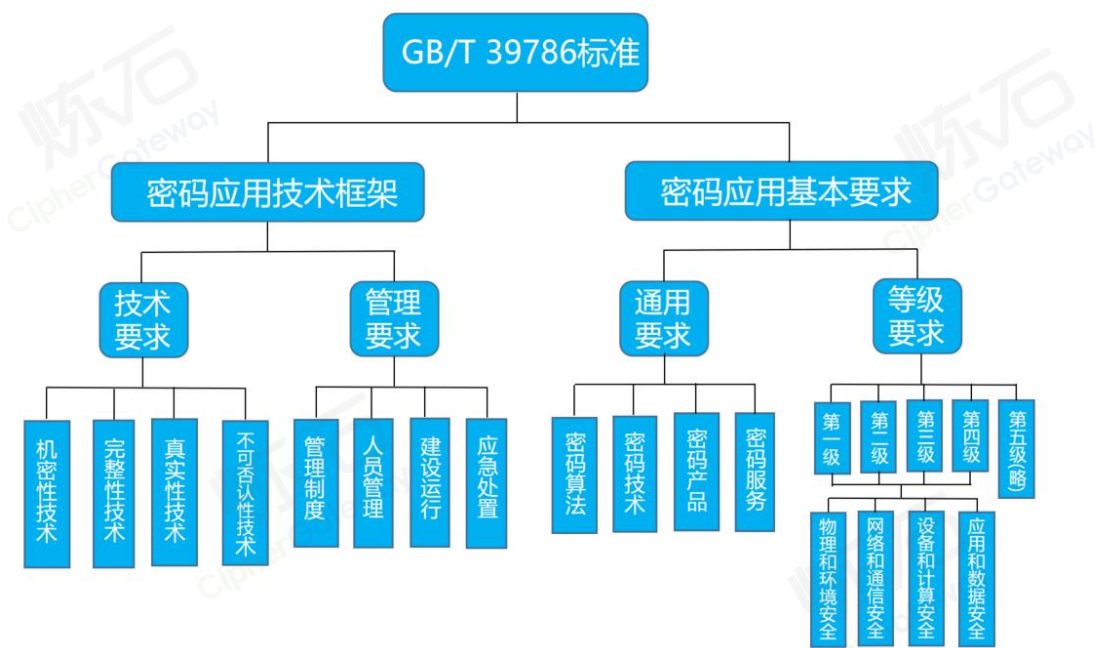


图 94 GB/T 39786 标准基本要求架构图

1、密码应用技术要求

技术要求主要由机密性、完整性、真实性、不可否认性四个密码安全功能维度构成.具体保护对象或应用场景描述如下:

1.机密性技术要求保护对象

使用密码技术的加解密功能实现机密性.信息系统中保护的对象为:

- 身份鉴别信息;
- 密钥数据;
- 传输的更要数据;
- 信息系统应用中所有存储的重要数据。

2.完整性技术要求保护对象

使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性,信息系统中保护的对象为:

- 身份鉴别信息;
- 密钥数据;
- 日志见录;
- 访问控制信息;
- 重要信息资源安全标记
- 重要可执行程序;
- 视频监控音像记录;
- 电子门禁系统进出记录;
- 传输的重要数据;

- 信息系统应用中所有存储的重要数据。

3.真实性技术要求应用场景

使用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现真实性,信息系统中应用场景为:

- 进入重要物理区域人员的身份鉴别;
- 通信双方的身份鉴别;
- 网络设备接入时的身份鉴别;
- 重要可执行程序来源真实性保证;
- 登录操作系统和数据库系统的用户身份鉴别;
- 应用系统的用户身份鉴别。

4.不可否认性技术要求保护对象

使用基于公钥密码算法的数字签名机制等密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性。

2、密码应用管理要求

管理要求由管理制度、人员管理、建设运行、应急处置等四个密码应用管理维度构成,具体如下:

- 密码应用安全管理相关流程制度的制定、发布、修订的规范性要求;
- 密码相关安全人员的密码安全意识以及关键密码安全岗位员工的密码安全能力的培养,人员工作流程要求等;
- 建设运行过程中密码应用安全要求及方案落地执行的一致性和有效性要求;

- 处理密码应用安全相关的应急突发事件的能力要求。

3、密码应用基本要求

GB/T 39786 标准对信息系统密码应用划分为自低向高的五个等级，参照国家标准 GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》（以下简称 GB/T 22239）的等级保护对象应具备的基本安全保护能力要求，提出密码保障能力逐级增强的要求，使用一、二、三、四、五表示。信息系统管理者按照业务实际情况选择相应级别的密码保障技术能力及管理能力的描述如下：

第一级，是信息系统密码应用安全要求等级的最低等级，要求信息系统符合通用要求和最低限度的管理要求，并鼓励使用密码保障信息系统安全；

第二级，是在第一级要求的基础上，增加操作规程、人员上岗培训与考核、应急预案等管理要求，并要求优先选择使用密码保障信息系统安全；

第三级，是在第二级要求的基础上，增加对真实性、机密性的技术要求以及全部的管理要求；

第四级，是在第三级要求的基础上，增加对完整性、不可否认性的技术要求；

第五级（略）。

本文以第三级密码应用基本要求为例，全面介绍信息系统在物理和环境安全、网络和通信安全、计算和设备安全、应用和数据安全以及安全管理等 5 个方面的基本要求。

第三级密码应用基本要求如下：

1.物理和环境安全

- 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；

- 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；
- 宜采用密码技术保证视频监控音像记录数据的存储完整性；
- 以上如采用密码服务,该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
- 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

2.网络和通信安全

- 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
- 宜采用密码技术保证通信过程中数据的完整性；
- 应采用密码技术保证通信过程中重要数据的机密性；
- 宜采用密码技术保证网络边界访问控制信息的完整性；
- 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性；
- 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
- 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

3.设备和计算安全

- 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
- 远程管理设备时，应采用密码技术建立安全的信息传输通道；
- 宜采用密码技术保证系统资源访问控制信息的完整性；
- 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；
- 采用密码技术保证日志记录的完整性；

- 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；
- 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
- 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

4.应用和数据安全

- 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；
- 宜采用密码技术保证信息系统应用的访问控制信息的完整性；
- 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
- 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
- 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
- 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
- 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
- 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；
- 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
- 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

5.安全管理

(1) 管理制度

使用密码技术的信息系统应符合以下管理制度要求：

- 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
- 应根据密码应用方案建立相应密钥管理规则；
- 应对管理人员或操作人员执行的日常管理操作建立操作规程；
- 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
- 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
- 应具有密码应用操作规程的相关执行记录并妥善保管。

（2）人员管理

使用密码技术的信息系统应符合以下人员管理要求：

- 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
- 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：
 - 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；
 - 对关键岗位建立多人共管机制；
 - 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；
 - 相关设备与系统的管理和使用账号不得多人共用。
- 应建立上岗人员培训制度，对于涉及密码操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；

- 应定期对密码应用安全岗位人员进行考核；
- 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

(3) 建设运行

本级要求包括：

- 应依据密码相关标准和密码应用需求，制定密码应用方案；
- 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照本标准附录 B；
- 应按照应用方案实施建设；
- 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
- 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

(4) 应急处置

本级要求包括：

- 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
- 事件发生后，应及时向信息系统主管部门进行报告；
- 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

5.2.5.3. 标准升级后的变化

GB/T 39786-2021（以下简称 GB/T 39786）标准为 GM/T 0054-2018（以下简称 GM/T 0054）标准的升级版，由行业标准升级到了国家标准，因此 GB/T 39786

标准内容更加规范，要求更加明确，逻辑更加清晰，同时对于密评实际执行过程中遇到的问题也做了相应的修订，使得密评工作能够更加有序、快速的推进开展。

GB/T 39786 整体上按照不同的密码应用级别，针对每个级别分别提出技术要求和管理要求，随着级别的提升，对密码应用的要求程度越来越强。其中对于不同级别的技术要求，又从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面分别提出，而各个级别、各个层面均需要共同遵循标准第 5 章所提出的通用要求^[46]。

与 GM/T 0054 相比，GB/T 39786 加强了与 GB/T 22239-2019（以下简称 GB/T 22239）的衔接，明确了不同等级信息系统所使用密码产品的安全级别要求，并结合密评工作实践对内容进行了优化，使之更为科学合理，其中主要的变化有四个方面。

1. 行文结构有变化

GM/T 0054 采用了“先分层，后分级”的行文结构，按照物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面，以及单独的管理层面，分别描述每层中第一级到第四级信息系统的密码应用要求。

GB/T 39786 则改为了“先分级，后分层”的行文结构，按照信息系统密码应用第一级到第五级，分别描述每级的密码应用技术要求和管理要求，其中第五级为“略”。这种变化使得相应级别信息系统的责任单位，能够更为直观的查阅标准。

2. 完整性要求的变化

GB/T 39786 总体上将 GM/T 0054 第三级对完整性要求的约束程度由“应”调整为“宜”，第四级维持“应”。这项调整可以与 GB/T 22239 形成更好的衔接。

在 GB/T 22239 中，对于网络安全等级保护第三级的数据完整性要求是“应采用校验技术或密码技术”进行完整性保护，见 GB/T 22239 的 8.1.2.2 和 8.1.4.7；对于网络安全等级保护第四级提出“应采用密码技术”进行完整性保护，见 GB/T 22239 的 9.1.2.2。为与上述网络安全等级保护要求相衔接，在 GB/T 39786 中也做了相应的调整。

需要说明的是，信息系统责任单位对于约束程度为“宜”的条款要求，并非可以随意选择不遵循该条款（即“不适用”）。

3.对密码产品安全性级别要求的变化

GM/T 0054 对于第三级信息系统，对密码产品的配用采用了“宜采用符合 GM/T 0028 的三级及以上”的描述。在工作实践中发现这种描述使得三级系统对于“宜”的解释空间较大，甚至会出现采用一级产品是否符合要求的争议。

为明确对密码产品安全性的门槛，GB/T 39786 对第三级信息系统的密码产品配用要求更改为“应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》（以下简称 GB/T 37092）[4]二级及以上”，仍维持第四级信息系统的密码产品“应达到 GB/T 37092 三级及以上”的要求。这样既降低了主观解释的不确定性，使得密码应用和安全性评估的客观依据更为明确，也使得第三级和第四级系统有了显著区分。

需要说明的是，信息系统所使用密码产品的安全级别遵循 GB/T 37092，经商用密码产品认证后确定，在产品认证证书上标明。商用密码应用安全性评估活动中，不对具体密码产品做考察，而是在确保实际使用的密码产品与产品认证证书的一致性后，直接采信产品检测认证的结果。对于应取得而未取得认证证书的商用密码产品，《信息系统密码应用高风险判定指引》将其视作高风险项之一。

4. 密钥管理要求的变化

相比于 GM/T 0054 在正文中对不同等级信息系统提出环节逐渐增多的密钥管理要求的做法，GB/T 39786 在正文中重点对密钥管理与使用提出管理性质的要求，将密钥管理生命周期所涉及技术环节内容移至标准的资料性附录 A。

这项调整是从标准衔接和可操作性角度考虑的。GM/T 0054 对密钥生命周期各环节的要求，本质上是对实现密钥产生、存储、分发、使用等功能的密码产品的技术要求，这些密钥管理的能力基本上是由密码产品来实现的。如前所述，密码应用安全性评估并不对密码产品进行重复检测，而是直接采信密码产品检测认证的结果。从与 GB/T 37092 衔接的角度，GB/T 39786 就不宜再重复规定密码产品的密钥管理安全能力。因此，GB/T 39786 一方面在通用要求部分对密钥管理所依托的密码产品和密码服务进行约束，另一方面从 GB/T 37092 不涉及的管理角度对密钥管理提出要求，如 8.5 “管理制度”中要求密码应用安全管理制度包含密钥管理的制度、8.6 “人员管理”中要求设置密钥管理员等。而将原 0054 中对密钥管理的技术要求修改后移入资料性附录。

5. 关于“应”“宜”“可”和不适用项的理解

GB/T 39786—2021 对于每一个密码应用要求项，采用“应”“宜”或“可”来表达不同的约束程度。国家标准 GB 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》（以下简称 GB 1.1）[11]的附录 C 对“应”“宜”或“可”给出了解释：“应”表示应该、只准许，“宜”表示推荐、建议，“可”表示可以、允许。但对于信息系统责任单位而言，在制定密码应用方案时，如何综合考量“应”“宜”或“可”的要求项哪些需要响应，仅就 GB 1.1 的这个定义是难以明确的。

《信息系统密码应用测评要求》从测评的角度出发，对测评实践中如何把握“应”“宜”或“可”进行了进一步解释：

——对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第6章相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。

——对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第6章相应的测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照第6章相应的测评指标要求进行测评和结果判定。

——对于“应”的条款，密评人员应按照第5章和第6章相应的测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

测评指标为“不适用”主要有以下3种情况：

(1) 条款所对应的保护对象或安全需求不存在。例如对于“应采用密码技术保证设备中的重要信息资源安全标记的完整性”，如果不对信息资源设定安全标记，则本项的保护对象不存在，在测评时相应指标设定为“不适用”。

(2) 根据信息系统的密码应用方案和方案评审意见确定是否作为“不适用”项。需要注意的是，这种“不适用”的情况仅针对“宜”的条款。当然，在这种情况下认定为“不适用”项，密评机构仍有责任进一步核实，若评估认为所描述的风险控制措施无效或不足以控制风险，则仍需将其纳入测评范围；

(3) 由信息系统责任单位自行决定是否作为“不适用”项。需要注意的是，这种“不适用”的情况仅针对“可”的条款。信息系统责任单位具有自主选择权，鼓励但不强制采用密码技术满足对应要求。

5.2.6. 密评核心内容

密评对象是采用商用密码产品、技术、服务而建成的网络和信息系统。密评内容主要涵盖商用密码应用安全的三个方面，分别是合规性、正确性、有效性。

5.2.6.1. 商用密码应用合规性评估

商用密码应用合规性评估主要是指判定网络和信息系统使用的密码算法、密码协议、密钥管理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。网络和信息系统使用的密码产品和密码服务是否经过国家密码管理部门核准或由具备资格的机构认证合格。

5.2.6.2. 商用密码应用正确性评估

商用密码应用正确性评估主要是指判定密码算法、密码协议、密钥管理、密码产品和密码服务是否使用正确，即系统中使用的密码产品是否取得商用密码产品认证证书，或者系统中采用的标准密码算法、协议和密钥管理机制是否按照相应的国家和行业密码标准进行正确的设计和实现；自定义密码协议、密钥管理机制的设计和实现是否正确，安全性是否满足要求，密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确。

5.2.6.3. 商用密码应用有效性评估

商用密码应用合规性评估主要是指判定网络和信息系统中的密码应用是否在网络和信息系统的运行过程中发挥了效用，是否满足了信息系统的安全需求，是否有效解决了信息系统面临的安全问题。

5.2.7. 密评等保关系

5.2.7.1. 密评与等保的联系

密评对象主要包含关键基础设施、第三级等级保护对象和部分重要的信息系统；等级测评对象基本涵盖了全部的网络和信息系统，第三级以上的网络安全等级保护对象一般也是关基和密评的评估对象；关键基础设施是等级测评和密评共同的评估对象^[47]。

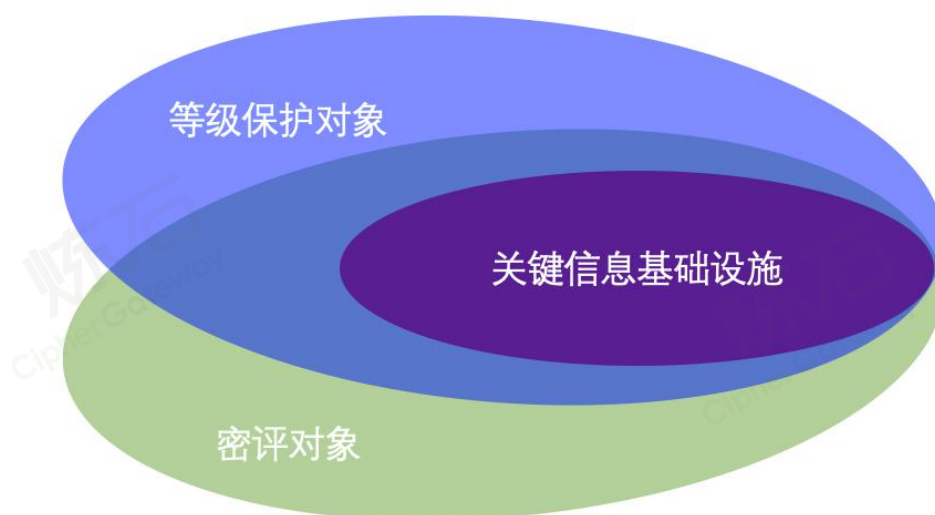


图 95 等保和密评评估对象以及关基三者之间的关系

5.2.7.2. 密评与等保的区别

1、评测目的不同

《密码法》中明确规定，法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护。关键信息基础设施运营者，应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。

《网络安全法》中明确规定，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，依据相关规定开展等级保护工作，通过等级测评来检验网络系统的安全防护能力，识别系统可能存在的安全风险。

因此，密评主要针对信息系统密码应用的合规性、正确性、有效性进行评估，等级保护测评主要是对信息系统网络安全防护能力进行测评，二者评估目的不同。

2、评估内容不同

等级测评和密评的主要参考标准和评估内容如下：

表 9 等级测评和密评的主要参考标准和评估内容

类别	等级测评	密评
基本要求	GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》	GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
评估实施指南	GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》	商用密码应用安全性评估测评过程指南
主要评估内容	<ul style="list-style-type: none"> ■ 安全物理环境 ■ 安全通信网络 ■ 安全区域边界 ■ 安全计算环境 ■ 安全管理中心 ■ 安全管理制度 ■ 安全管理机构 ■ 安全建设管理 ■ 安全运维管理 	<ul style="list-style-type: none"> ■ 总体要求 <ul style="list-style-type: none"> ● 密码算法 ● 密码技术 ● 密码产品 ● 密码服务 ■ 密码功能要求 <ul style="list-style-type: none"> ● 机密性 ● 完整性 ● 真实性 ● 不可否认性 ■ 密码技术应用要求 <ul style="list-style-type: none"> ● 物理和环境安全 ● 网络和通信安全 ● 设备和计算安全 ● 应用和数据安全 ■ 密钥管理 <ul style="list-style-type: none"> 生成、存储、分发、导入、导出、备份、恢复、归档、销毁 ■ 安全管理 <ul style="list-style-type: none"> ● 管理制度

		<ul style="list-style-type: none"> ● 人员管理 ● 建设运行 ● 应急处置
--	--	--

3、评估流程不同

商用密码应用安全评估的工作流程主要包括确定评估对象、开展测评工作、输出密码测评报告、密评结果上报四个阶段；等级保护测评工作主要包括五个规定动作：定级、备案、建设整改、等级测评、监督检查。

4、评测结果不同

密评的测评结论有符合、部分符合、不符合，网络安全等级保护评估结论为优、良、中、差。密评和等级测评在测评过程中，都会依据资产、威胁、脆弱性进行赋值，通过计算风险值来判定风险，风险结论有高、中、低。当网络和信息系统存在高风险时，等级测评和密评的结论均为不符合（差）。

5.2.8. 密评机构名单

国家密码管理局于 2021 年 6 月 11 日，依据《中华人民共和国密码法》以及商用密码应用安全性评估有关管理规定,发布了最新一期《商用密码应用安全性评估试点机构目录》，有 48 家密评机构在列³。

³ 引用自 https://www.oscca.gov.cn/sca/xwdt/2021-06/11/content_1060863.shtml

表 10 商用密码应用安全性评估试点机构目录

机构名称	注册地
工业和信息化部密码应用研究中心	北京
中国电力科学研究院	北京
中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)	北京
中国金融电子化公司	北京
中国科学院软件研究所	北京
中国科学院数据与通信保护研究教育中心	北京
中金金融认证中心有限公司	北京
中科信息安全共性技术国家工程研究中心有限公司	北京
公安部第一研究所	北京
北京市电子产品质量检测中心	北京
北京软件产品质量检测检验中心	北京
电力行业信息安全等级保护测评中心第一 测评实验室（北京卓识网安技术股份有限公司）	北京
北京信息安全测评中心	北京

北京银联金卡科技有限公司	北京
交通运输信息安全中心有限公司	北京
国家广播电视总局广播电视科学研究院	北京
国家信息中心（国家电子政务外网管理中心）	北京
国家信息技术安全研究中心	北京
国家密码管理局商用密码检测中心	北京
教育部教育管理信息中心	北京
天津云安科技发展有限公司	天津
中互金认证有限公司	天津
河北翎贺计算机信息技术有限公司	石家庄
北方实验室（沈阳）股份有限公司	沈阳
长春市博鸿科技服务有限责任公司	长春
上海市信息安全测评认证中心	上海
公安部第三研究所（公安部信息安全等级保护评估中心、国家网络与信息系统安全产品质量监督检验中心）	上海
智巡密码（上海）检测技术有限公司	上海

国电南京自动化股份有限公司	南京
江苏省信息安全测评中心	无锡
杭州安信检测技术有限公司	杭州
浙江省电子信息产品检验研究院	杭州
浙江东安检测技术有限公司	杭州
安徽科测信息技术有限公司	合肥
福建金密网络安全测评技术有限公司	福州
江西智慧云测安全检测中心有限公司	鹰潭
山东省电子信息产品检验院（中国赛宝（山东）实验室）	济南
山东道普测评技术有限公司	济南
河南中科安永科技有限公司	郑州
长沙中安密码检测有限公司	长沙
工业和信息化部电子第五研究所（中国赛宝实验室）	广州
广州竞远安全技术股份有限公司	广州
深圳市网安计算机安全检测技术有限公司	深圳
重庆巽诺科技有限公司	重庆

成都市信息系统与软件评测中心	成都
成都创信华通信息技术有限公司	成都
新疆天行健信息安全测评技术有限公司	乌鲁木齐
新疆量子通信技术有限公司	乌鲁木齐

5.3. 密码应用安全性评估标准

5.3.1. 密评测评要求

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》^[48]编制的《信息系统密码应用测评要求》^[49]将信息系统密码应用测评要求分为通用测评要求和密码应用测评要求。其中，通用测评要求对“密码算法和密码技术合规性”和“密钥管理安全性”提出测评要求，适用于第一级到第五级的信息系统密码应用测评；密码应用测评要求，对信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面提出了第一级到第四级密码应用技术的测评要求，并对管理制度、人员管理、建设运行和应急处置四个方面提出了第一级到第四级密码应用管理的测评要求。通用测评要求的内容不单独实施测评，也不单独体现在密码应用安全性评估报告的单元测评结果和整体测评结果中，仅供密码应用测评要求的测评实施引用。

5.3.1.1. 通用测评要求

对于信息系统中采用的商用密码算法、技术、产品、服务，需要对其密码应用的合规性、正确性和有效性进行评估。

- 密码算法核查

- 了解信息系统使用的算法名称、用途、位置、执行算法的设备及其实现方式；
- 核查密码算法是否符合国家或者行业标准或取得国家密码管理部门同意其使用的证明文件。

- 密码技术核查

- 核查密码协议、密钥管理等密码技术是否遵循密码相关国家标准和行业标准；
- 若密码技术由合规的密码产品实现，则重点评估密码技术使用是否遵循密码相关国家标准和行业标准。

- 密码产品核查

- 核查相关部件和设备是否取得国家密码管理部门颁发的商用密码产品型号证书或被主管部门认可的测评机构出具的合格测评报告。

- 密码服务核查

- 核查信息系统使用第三方提供的电子认证服务等密码服务是否获得国家密码管理局颁发的密码服务许可证，且证书在有效期内。

5.3.1.2. 物理和环境安全测评要求

在物理和环境安全方面需要以密码技术实现物理访问控制,以及对电子门禁记录与视频监控记录进行完整性保护等要求，具体要求见下表。

表 11 物理和环境密评测评要求

测评对象	测评要求
身份鉴别	采用密码技术进行物理访问身份鉴别（真实性）。（第一级到第四级）
电子门禁记录数据存储完整性	采用密码技术保证电子门禁系统进出记录数据的存储完整性。（第一级到第四级）
视频监控记录数据存储完整性	采用密码技术保证视频监控音像记录数据的存储完整性。（第三级到第四级）

5.3.1.3. 网络和通信安全测评要求

在网络和通信安全方面需要以密码技术实现网络传输过程的通信双方真实性、数据机密性、完整性保护等要求，具体要求见下表。

表 12 网络和通信密评测评要求

测评对象	测评要求
身份鉴别	1) 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。（第一级到第三级） 2) 采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。（第四级）
通信数据完整性	采用密码技术保证通信过程中数据的完整性。（第一级到第四级）
通信过程中重要数据的机密性	采用密码技术保证通信过程中重要数据的机密性。（第一级到第四级）
网络边界访问控制信息的完整性	采用密码技术保证网络边界访问控制信息的完整性。（第一级到第四级）
安全接入认证	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。（第三级到第四级）

5.3.1.4. 设备和计算安全测评要求

在设备和计算安全方面需要以密码技术实现设备用户身份真实性、远程鉴别信息机密性、重要文件完整性保护等要求，具体要求见下表。

表 13 设备和计算密评测评要求

测评对象	测评要求
身份鉴别	采用密码技术对登录设备的用户进行身份鉴别，保证

	用户身份的真实性。（第一级到第四级）
远程管理通道安全	远程管理设备时，采用密码技术建立安全的信息传输通道。（第三级到第四级）
系统资源访问控制信息完整性	采用密码技术保证系统资源访问控制信息的完整性。（第一级到第四级）
重要信息资源安全标记完整性	采用密码技术保证设备中的重要信息资源安全标记的完整性。（第三级到第四级）
日志记录完整性	采用密码技术保证日志记录的完整性。（第一级到第四级）
重要可执行程序完整性、重要可执行程序来源真实性	采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。（第三级到第四级）

5.3.1.5. 应用和数据安全测评要求

在应用和数据安全方面需要以密码技术实现身份真实性,数据传输和存储的机密性、完整性、行为不可抵赖性等要求，具体要求见下表。

表 14 应用和数据密评测评要求

测评对象	测评要求
身份鉴别	采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。（第一级到第四级）
访问控制信息完整性	采用密码技术保证信息系统应用的访问控制信息的完

	整性。（第一级到第四级）
重要信息资源安全标记完整性	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。（第三级到第四级）
重要数据传输机密性	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。（第一级到第四级）
重要数据存储机密性	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。（第一级到第四级）
重要数据传输完整性	采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。（第一级到第四级）
重要数据存储完整性	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。（第一级到第四级）
不可否认性	在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。（第三级到第四级）

5.3.1.6. 密钥管理测评要求

密钥安全是密码应用安全的重中之重，要在密码应用方案中以单独章节描述各个层面密码应用所涉及的密钥，明确其种类和生命周期过程保护措施，以及所涉及的密码设备。系统建设过程中，要制定密钥管理制度，清晰说明密钥管理的规则、相关方及其职责，在密钥各生命周期环节的操作规程，以及违反操作规程的惩处措施等。

密钥的生命周期管理，包括密钥生成、存储、使用、分发、导入导出、备份恢复、归档。对于信息系统内的密钥需要进行安全运行检查，理清密钥流转的关系，梳理出密钥流转表，即标明这些密钥是如何生成、存储、使用、分发、导入和导出、备份和恢复、归档、销毁，并核查是否满足要求，确认所有密钥管理的操作都是由符合规定的密码产品的密码模块实现，核查密码产品是否符合相应安全等级及以上安全要求。

5.3.1.7. 安全管理测评要求

不要忽视管理要求。从长期看，信息安全保障是管理因素大于技术因素的，要从信息系统风险控制的角度，结合业务过程充分、周全考虑并切实落实 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》所规定的管理制度、人员管理、建设运行、应急处置四个方面的管理要求。

基于 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的《信息系统密码应用测评要求》详述了制度管理、人员管理、建设运行、应急处置的密评的测评要求。

- 制度管理

- 核查各项安全管理制度是否包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度（第一级到第四级）。
- 建立相应密钥管理规则，比如密码应用方案、密钥管理制度及策略类文档，核查信息系统中密钥是否按照密钥管理规则进行生存周期的管理（第一级到第四级）。

- 核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程（第二级到第四级）。
- 核查是否定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定；对经论证和审定后存在不足或需要改进的密码应用安全管理制度和操作规程，核查是否具有修订记录。（第三级到第四级）。
- 核查相关密码应用安全管理制度和操作规程是否具有相应明确的发布流程和版本控制（第三级到第四级）。
- 核查是否具有密码应用操作规程执行过程中留存的相关执行记录文件（第三级到第四级）。

● 人员管理

- 应了解并遵守密码相关法律法规和密码管理制度（第一级到第四级）。
- 应设置密钥管理人员、安全审计人员、密码操作人员等关键岗位（第二级到第四级）。
- 建立上岗人员培训制度，应能够正确使用密码产品（第二级到第四级）。
- 定期对密码应用安全岗位人员进行考核（第三级到第四级）。
- 建立关键岗位人员保密制度和调离制度，核查人员离岗的管理文档是否规定了关键岗位人员保密制度和调离制度等；核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容（第一级到第四级）。

- 建设运行

- 规划阶段制定密码应用方案（第一级到第四级）。
- 制定密钥安全管理策略,核查密钥生存周期的各个环节是否符合要求（第一级到第四级）。
- 实施阶段应制定实施方案,选用被核准的密码产品和被许可的密码服务（第一级到第四级）。
- 投入运行前,应经测评机构进行安全性评估,评估通过后方可投入正式运行每年应委托测评机构开展评估（第一级到第二级）。
- 定期开展密码应用安全性评估及攻防对抗演习,有重大安全隐患时,应停止系统运行,制定整改措施,整改完成并通过评估方可投入运行（第三级到第四级）。

- 应急处置

- 应急策略

- ◆ 根据密码产品提供的安全策略,由用户自主处置密码应用安全事件（第一级）。
 - ◆ 制定密码应用应急策略,做好应急资源准备,当密码应用安全事件发生时,按照应急处置措施结合实际情况及时处置（第二级）。
 - ◆ 制定密码应用应急策略,做好应急资源准备,当密码应用安全事件发生时,立即启动应急处置措施,结合实际情况及时处置（第三级到第四级）。

- 事件处理

- ◆ 事件发生后，及时向信息系统主管部门进行报告（第三级）。

- ◆ 事件发生后，及时向信息系统主管部门及归属的密码管理部门进行报告。（第四级）

- 向有关主管部门上报处置情况

- ◆ 事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况（第三级到第四级）。

5.3.1.8. 不同等级保护密码应用要求

GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》对于每一个密码应用要求项，采用“应”“宜”或“可”来表达不同的约束程度。国家标准 GB 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》^[50]的附录 C 对“应”“宜”或“可”给出了解释：“应”表示应该、只准许，“宜”表示推荐、建议，“可”表示可以、允许。但对于信息系统责任单位而言，在制定密码应用方案时，如何综合考量“应”“宜”或“可”的要求项哪些需要响应，仅就 GB 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》的这个定义是难以明确的。为此，《信息系统密码应用测评要求》从测评的角度出发，对测评实践中如何把握“应”“宜”或“可”进行了进一步解释：

——对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。

——对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照相应的测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照相应的测评指标要求进行测评和结果判定。

——对于“应”的条款，密评人员应按照相应的测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

下表整理了信息系统等级保护1级到4级的密码要求强度，具体要求见下表。

表 15 信息系统等级保护 1 级到 4 级的密码要求强度

指标要求			一级	二级	三级	四级
技 术 要 求	物理和 环境安 全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	可	宜	应
		视频监控记录数据存储完整性	—	—	宜	应
		密钥服务	应	应	应	应
		密码产品	—	一级及	二级及	三级及

			以上	以上	以上
网络和通信安全	身份鉴别	可	宜	应	应
	通信数据完整性	可	可	宜	应
	通信过程中重要数据的机密性	可	宜	应	应
	网络边界访问控制信息的完整性	可	可	宜	应
	安全接入认证	—	—	可	宜
	密钥服务	应	应	应	应
	密码产品	—	一级及以上	二级及以上	三级及以上
设备和计算安全	身份鉴别	可	宜	应	应
	远程管理通道安全	—	—	应	应
	系统资源访问控制信息完整性	可	可	宜	应
	重要信息资源安全标记完整性	—	—	宜	应
	日志记录完整性	可	可	宜	应
	重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
	密钥服务	应	应	应	应
	密码产品	—	一级及以上	二级及以上	三级及以上
应用和	身份鉴别	可	宜	应	应

数据安 全	访问控制信息完整性	可	可	宜	应	
	重要信息资源安全标记完整性	—	—	宜	应	
	重要数据传输机密性	可	宜	应	应	
	重要数据存储机密性	可	宜	应	应	
	重要数据传输完整性	可	宜	宜	应	
	重要数据存储完整性	可	宜	宜	应	
	不可否认性	—	—	宜	应	
	密钥服务	应	应	应	应	
	密码产品	—	一级及 以上	二级及 以上	三级及 以上	
安 全 管 理	制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程	—	应	应	应
		定期修订安全管理制度	—	—	应	应
		明确管理制度发布流程	—	—	应	应
		制度执行过程记录留存	—	—	应	应
	人员	了解并遵守密码相关法律法规 和密码管理制度	应	应	应	应
		建立密码应用岗位责任制度	—	应	应	应
		建立上岗人员培训制度	—	应	应	应
		定期进行安全岗位人员考核	—	—	应	应

		建立关键岗位人员保密制度和 调离制度	应	应	应	应
	建设	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全 性评估	可	宜	应	应
		定期开展密码应用安全性评估 及攻防对抗演习	—	—	应	应
	应急	应急策略	可	应	应	应
		事件处置	—	—	应	应
		向有关主管部门上报处置情况	—	—	应	应

5.3.2. 密评测评过程

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》编制的《信息系统密码应用测评过程指南》^[51]中提出在测评活动开展前，需要对被测信息系统的密码应用方案进行评估，通过评估的密码应用方案可以作为测评实施的依据。测评实施包括四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动，测评流程见下图。



图 96 测评实施过程

测评实施流程具体包含哪些环节，可见下表。

表 16 测评实施流程的各环节

测评准备活动	方案编制活动	现场测评活动	分析与报告编制
(1) 项目启动 (2) 信息收集和分析 (3) 测评工具和表单准备	(1) 确定测评对象和测评指标 (2) 确定测评检查点 (3) 确定测评内容 (4) 编制测评方案	(1) 现场测评准备 (2) 现场测评和结果记录 (3) 结果确认和资料归还	(1) 单项测评结果判定 (2) 单元测评结果判定 (3) 整体测评 (4) 风险分析 (5) 测评结论形成 (6) 测评报告编制

5.3.2.1. 测评准备活动

1、工作目标

- (1) 启动测评项目
- (2) 收集被测信息系统相关资料
- (3) 准备测评所需资料
- (4) 为编制测评方案打下良好的基础

2、工作流程

测评准备活动的工作流程如下图：

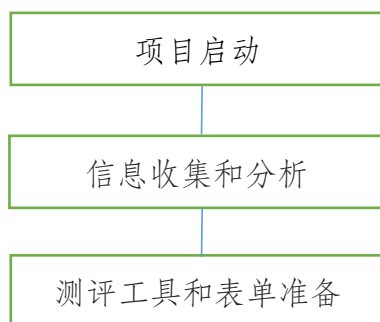


图 97 测评准备活动的工作流程

3、各环节工作

下面分别对项目启动、信息收集和分析、测评工具和表单准备这三个环节需要做的具体的工作内容做详述。

- 项目启动

- 编制项目计划书(包含项目概述、工作依据、技术思路、工作内容和项目组织等)。
- 被测评单位提供基本资料，初步了解被测信息系统。

- 信息收集和分析

- 被测评单位的管理架构、技术体系、运行情况、被测评系统商用密码总体描述文件、各种密码安全规章制度及相关过程管理记录、配置管理文档等。
- 填写系统调查表，调查被测系统的基本信息、行业特征、密码管理策略、网络及设备部署、软硬件、重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、业务安全保护等级、用户范围、用户类型、被测系统所处的运行环境及面临的威胁等。
- 沟通和确认，必要时安排一次现场调查。

- 工具和表单准备

- 调试测评工具清单，例如漏扫工具、渗透工具、性能测试工具、协议分析工具等。
- 准备和打印表单，主要包括授权书、风险确认书、文档交接单、会议记录表单、会议签到表单等。
- 在测评环境模拟被测信息系统架构,准备开发测评指导书，并进行必要的工具验证。

5.3.2.2. 方案编制活动

1、工作目标

- (1) 整理测评准备阶段中获取的信息系统相关资料。
- (2) 为现场测评活动提供最基本的文档和指导方案。

2、工作流程

方案编制活动的工作流程如下图：

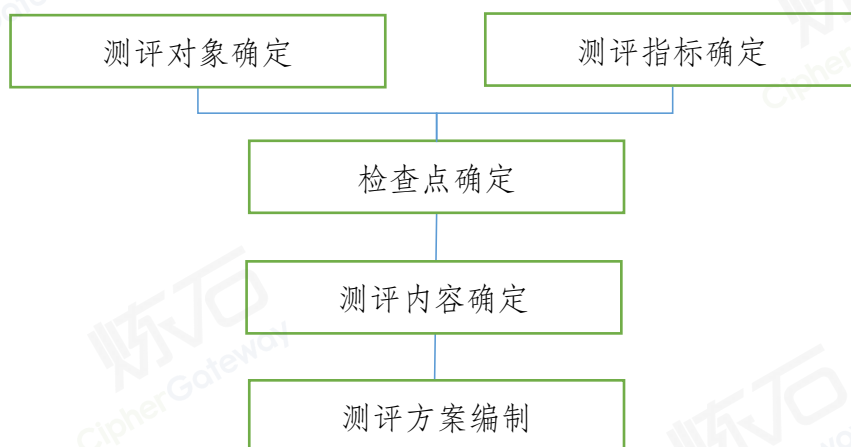


图 98 方案编制活动的工作流程

3、各环节工作

下面分别对确定测评对象、测评指标确定、测评检查点确定、测评内容确定、测评方案编制这五个环节需要做的具体的工作内容做详述。

- 确定测评对象

- 输入：完成的调查表格

- 工作：识别并描述被测信息系统的整体结构，包括物理环境、网络拓扑和外部边界连接、业务系统及相关硬件设备，相关商用密码技术应用情况；识别并描述被测信息系统的边界及边界设备、网络区域；根据业务类型及其重要程度进行资产和威胁评估。

- 输出：测评方案的测评对象部分

- 测评指标确定

- 输入：完成的调查表格，以及相关规章制度文件

- 工作：获得系统定级结果，并根据《信息系统密码测评要求》选择相应等级的测评指标；对确定的测评指标进行描述，并分析给出不适用项；由多个不同等级的信息系统组成的被测系统，应分别确定各个定级对象的测评指标。

- 输出：测评方案的指标部分

- 测评检查点确定

- 输入：被测系统的结构与密码应用信息

- 工作：列举需要接受现场检查的关键设备和检查内容。

- 输出：测评方案的测试检查点部分

- 测评内容确定

- 输入：完成的调查表格、测评方案已完成的部分、作业指导书

- 工作：依据相关制度和要求，将测评指标和测评对象结合，说明各测评对象所采取的测评方法，构成若干个可以具体实施测评的单元，并说明单元测评实施的工作内容。
 - 输出：测评方案的单元测评实施部分
- 测评方案编制
 - 输入：委托测评协议、完成的调查表格
 - 工作：编写测评项目概要、明确测评标准、估算测评工作量、安排项目组成员、编制工作内容实施计划等形成测评方案提交被测单位签字确认。
 - 输出：经过评估的测评方案

5.3.2.3. 现场测评活动

1、工作目标

- (1) 依据测评方案落实现场测评工作。
- (2) 取得报告编制活动所需的、足够的证据和资料。

2、工作流程

现场测评活动的工作流程如下图：

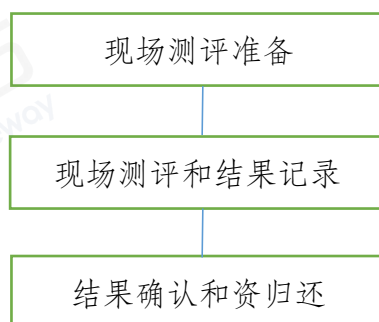


图 99 现场测评活动的工作流程

3、各环节工作

下面分别对现场测评准备、现场测评和结果记录、结果确认和资料归还这三个环节需要做的具体的工作内容做详述。

- 现场测评准备

- 召开测评现场首次会，介绍测评内容和计划,以及存在风险等。
- 被测评单位确认风险，做好应急和备份工作。
- 获得信息系统相关方的现场测评授权。
- 确认现场测评需要的各种资源。

- 现场测评和结果记录

- 开展访谈、文档审查、实地查看、工具测试等，并做好过程与结果的记录。
- 确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况。
- 测评结束后，确认测评工作是否对测评对象造成不良影响，测评对象及系统是否工作正常。

- 结果确认和资料归还

- 汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评。
- 召开测评现场结束会，现场确认和沟通证据源记录。
- 归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。

5.3.2.4. 分析和报告编制活动

1、工作目标

- (1) 汇总分析
- (2) 形成密码测评结论
- (3) 编制测评报告

2、工作流程

分析和报告编制活动的工作流程如下图：

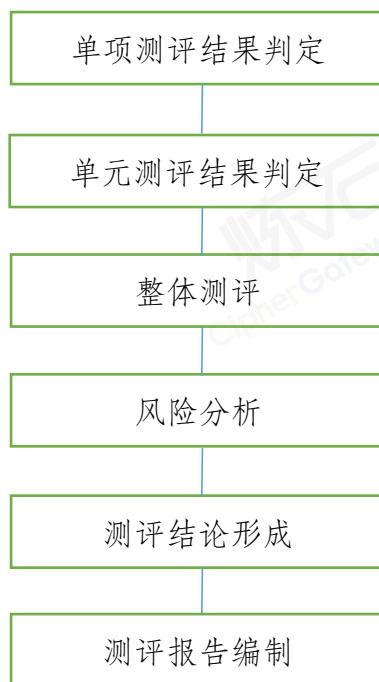


图 100 分析和报告编制活动的工作流程

3、各环节工作

下面分别对单项测评结果判定、单元测评结果判定、整体测评、风险分析、形成结论、编制报告这六个环节需要做的具体的工作内容做详述。

- 单项测评结果判定

- 针对单个测评项，结合测评对象分析测评证据，形成初步单项测评结果，作为测评结论的基础。
- 测评结果包含“符合”、“不符合”两种情况。
- “优势证据”原则。
- 单元测评结果判定
 - 对单项测评结果情况汇总、统计并形成单元测评结果。
 - 根据单项测评结果情况，单元测评结果分为，符合、不符合、部分符合、不适用。
- 整体测评
 - “部分符合”及“不符合”要求的单个测评项，与其他测评项的关联分析。
 - “部分符合”及“不符合”要求的单个测评项，与其他测评单元的关联分析。
 - “部分符合”及“不符合”要求的单个测评项，与其他层面的关联分析。
- 风险分析
 - 针对测评结果中部分符合项或不符合项所产生的安全问题，分析可能对被测信息系统造成的安全影响。
 - 根据威胁类型和威胁发生频率，结合资产价值的高低，对被测系统的安全风险进行赋值。
 - 结合被测系统安全保护等级，考虑对国家安全、社会秩序、公共利益以及对公民法人权益造成的风险。

- 形成结论

- 单元测评结果全部“符合”，则结论为“符合”。
- 单元测评结果有“不符合”，则结论为“不符合”。
- 单元测评结果没有“不符合”，有“部分符合”，则结论结合风险分析来综合判定。

- 编制报告

- 对一个测评委托单位应形成一份密码测评报告；如果一个测评委托单位内有多个被测系统，对每个被测系统均需要形成一份测评报告
- 报告包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法、单项测评、整体测评结果汇总、风险分析、测评结论以及整改建议等章节。

5.3.3. 密评高风险项

《信息系统密码应用高风险判定指引》^[52]是密评工作中的重要参考基线，也就是涉及到高风险的测评项为一票否决项，《信息系统密码应用高风险判定指引》遵循 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，由指标要求、适用范围、安全问题、可能的缓解措施和风险评价构成。要充分理解《信息系统密码应用高风险判定指引》的内容，需要对《信息安全技术 信息系统密码应用基本要求》有个充分的认识。

同时,《信息系统密码应用高风险判定指引》提及“由于信息系统密码应用场景的复杂性,本文件无法涵盖密码应用的所有高风险安全问题,对于本文件未涉及但确实可能会对信息系统造成严重安全隐患的安全问题,应结合信息系统的实际情况对相关安全问题所引发的风险等级做出客观判断。在某些情况下,受限于具体场景的安全需求和各项条件,本文件给出的安全问题也可能不会导致信息系统面临较高安全风险,在信息系统密码应用的规划、建设、运行及测评时应结合具体场景进行合理判定”,所以在使用《信息系统密码应用高风险判定指引》过程中,需要尊重科学合理利用的原则,一方面不可以胡乱解读,另一方面也不能太过教条化。

下面根据《信息系统密码应用高风险判定指引》整理出会被判为高风险的安全问题和可能的缓解措施。

高风险项为“一票否决”。

5.3.3.1. 通用要求

对于密码算法、密码技术、密码产品和密码服务会涉及高风险项的安全问题和可能的缓解措施,整理如下表。

表 17 密码算法、密码技术、密码产品和服务的高风险项

	安全问题	可能的缓解措施
密码算法	(1) 采用存在安全问题或安全强度不足的密码算法对重要数据进行保护,如 MD5、DES、SHA-1、RSA(不足 2048 比特)等密码算法;	无

	<p>(2) 采用安全性未知的密码算法，如自行设计的密码算法、经认证的密码产品中未经安全性论证的密码算法。</p>	
密码技术	<p>(1) 采用存在缺陷或有安全问题警示的密码技术，如 SSH 1.0、SSL 2.0、SSL 3.0、TLS 1.0 等；</p> <p>(2) 采用安全性未知的密码技术，如自行设计的密码通信协议、未经安全性论证的密码通信协议等。</p>	无
密码产品和密码服务	<p>(1) 使用自实现且未提供安全性证据的密码产品；</p> <p>(2) 使用的密码产品存在高危安全漏洞，如存在 Heartbleed 漏洞的 OpenSSL；</p> <p>(3) 密码产品的使用不满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件；</p> <p>(4) 选用的密码服务，其密码服务提供商不具有相关资质；</p> <p>(5) 存在可能会对密钥管理造成严重安全隐患的安全问题。</p>	无

5.3.3.2. 物理和环境安全的高风险项

对于物理和环境安全方面会涉及的高风险项的安全问题和可能的缓解措施，整理如下表。

表 18 物理和环境安全的高风险项

	安全问题	可能的缓解措施
身份鉴别（第二级及以上级别）	（1）存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； （2）未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要区域进入人员进行身份鉴别； （3）人员身份真实性的密码技术实现机制不正确或无效。	（1）基于生物识别技术（如指纹等）对重要区域进入人员进行身份鉴别； （2）重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等。

5.3.3.3. 网络和通信安全的高风险项

对于网络和通信安全方面会涉及的高风险项的安全问题和可能的缓解措施，整理如下表。

表 19 网络和通信安全的高风险项

	安全问题	可能的缓解措施
身份鉴别（第	（1）存在通用要求中密码算法、密码技术、	无

三级及以上 级别)	<p>密码产品和密码服务相关安全问题；</p> <p>(2) 未采用基于对称密码算法或密码杂凑算法的消息鉴别码 (MAC) 机制、基于公钥密码算法的数字签名机制等密码技术对通信实体进行身份鉴别 (第三级) /进行双向身份鉴别 (第四级)；</p> <p>(3) 通信实体身份真实性的密码技术实现机制不正确或无效；</p> <p>(4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书 (适用时)。</p>	
通信过程中 重要数据的 机密性 (第三 级及以上级 别)	<p>(1) 存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>(2) 未采用密码技术的加解密功能对通信过程中重要数据进行机密性保护；</p> <p>(3) 通信过程中重要数据机密性保护的密码技术实现机制不正确或无效；</p> <p>(4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书 (适用时)。</p>	<p>在“应用和数据安全”层面针对信息系统所有需要保护的重要数据传输采用符合要求的密码技术进行机密性保护，且加密后的数据流能够覆盖网络通信信道。</p>
安全接入认	(1) 存在通用要求中密码算法、密码技	无

证（第四级）	<p>术、密码产品和密码服务相关安全问题；</p> <p>（2）未采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对从外部连接到内部网络的设备进行接入认证；</p> <p>（3）安全接入认证的密码技术实现机制不正确或无效；</p> <p>（4）采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。</p>	
--------	--	--

5.3.3.4. 设备和计算安全的高风险项

对于设备和计算安全方面会涉及的高风险项的安全问题和可能的缓解措施，整理如下表。

表 20 设备和计算安全的高风险项

	安全问题	可能的缓解措施
身份鉴别（第三级及以上级别）	<p>（1）存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>（2）未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）</p>	<p>基于特定识别技术（如设备指纹、生物指纹等）保证用户身份的真实性。</p>

	<p>机制、基于公钥密码算法的数字签名机制等</p> <p>密码技术对登录设备的用户进行身份鉴别；</p> <p>(3) 用户身份真实性的密码技术实现机制不正确或无效。</p>	
<p>远程管理通道安全（第三级及以上级别）</p>	<p>(1) 存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>(2) 远程管理设备时，未采用密码技术建立安全的信息传输通道；</p> <p>(3) 信息传输通道所采用的密码技术实现机制不正确或无效；</p> <p>(4) 通过不可控网络环境进行远程管理，且鉴别数据以明文形式传输。</p>	<p>(1) 与业务网络物理隔离、采取相应的安全防护措施的专用管理网络(如带外管理网络)进行远程管理；</p> <p>(2) “网络和通信安全”层面使用 SSL VPN 网关、IPSec VPN 网关等相关设备建立专用的集中管理通道,且采用的密码技术符合要求。</p>

5.3.3.5. 应用和数据安全的高风险项

对于应用和数据安全方面会涉及的高风险项的安全问题和可能的缓解措施，整理如下表。

表 21 应用和数据安全的高风险项

	安全问题	可能的缓解措施
身份鉴别（第三级及以上级别）	<p>（1）存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>（2）未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录用户进行身份鉴别；</p> <p>（3）用户身份真实性的密码技术实现机制不正确或无效；</p> <p>（4）采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。</p>	<p>基于特定识别技术（如设备指纹、生物指纹、第三方身份鉴别服务等）保证用户身份的真实性。</p>
重要数据传输机密性（第三级及以上级别）	<p>（1）存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>（2）未采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护；</p> <p>（3）重要数据传输机密性保护的密码技术实现机制不正确或无效；</p> <p>（4）采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。</p>	<p>在“网络和通信安全”层面通信实体间采用符合要求的密码技术建立网络通信信道，且网络通信信道经评估无高风险。</p>

	时)。	
重要数据存储机密性(第三级及以上级别)	<p>(1)存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题;</p> <p>(2)未采用密码技术的加解密功能对重要数据在存储过程中进行机密性保护;</p> <p>(3)重要数据存储机密性保护的密码技术机制实现不正确或无效;</p> <p>(4)采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书(适用时)。</p>	无
重要数据存储完整性(第三级及以上级别)	<p>(1)存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题;</p> <p>(2)未采用基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对重要数据在存储过程中进行完整性保护;</p> <p>(3)重要数据存储完整性保护的密码技术实现机制不正确或无效;</p> <p>(4)采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书(适用时)。</p>	应用系统具有符合要求的身份鉴别措施,保证只有授权人员才能访问应用系统的重要数据,且定期对重要数据进行备份。

不可否认性 (第三级及以上)	<p>(1) 存在通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题；</p> <p>(2) 在可能涉及法律责任认定的应用中，未采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为和接收行为实现不可否认性；</p> <p>(3) 不可否认性的密码技术实现机制不正确或无效；</p> <p>(4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。</p>	无
-------------------	---	---

5.3.3.6. 密码应用管理要求的高风险项

对于密码应用管理要求会涉及的高风险项和可能的缓解措施，整理如下表。

表 22 密码应用管理要求的高风险项

	安全问题	可能的缓解措施
具备密码应用安全管理 制度（第二级及以上级别）	未建立任何与密码应用安全管理活动相关的管理制度，或相关管理制度不适用于当前被测信息系统。	无
制定密码应	信息系统未制定密码应用方案或密码应用	如被测系统通过测

用方案（第二级及以上级别）	方案未通过评审。	评发现不存在高风险安全问题，可酌情降低风险等级。
---------------	----------	--------------------------

5.3.4. 密评评分规则

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》编制的《商用密码应用安全性评估量化评估规则》^[53]对信息系统的密码应用情况给出了量化原则、量化评估框架、量化规则。

5.3.4.1. 测评对象评分规则

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。 $S_{i,j,k}$ 取值的示例可以见下表。

表 23 测评对象评分量化规则

符合情况	涉及情况			评分	示例
	密码使用有效性	密码算法/技术合规性	密码管理安全		
符合	✓	✓	✓	1	全部符合相关的要求
部分符合	✓	×	✓	0.5	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/技术不符合法律法规的规定和密码相关国家标准、行业标准的有关规定
	✓	✓	×	0.5	密码使用有效，使用的密码算法/技术符合法律法规的规定和密码相关国家标准、行业标准的有关规定，但是相关的密钥管理机制存在问题
	✓	×	×	0.25	密码使用有效，但使用的密码算法/技术不符合法律法规的规定和密码相关国家标准、行业标准的有关规定，相关的密钥管理机制也存在问题
不符合	×	/	/	0	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

说明：

- 1) 密码使用有效性：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；
- 2) 密码算法/技术合规性：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；
- 3) 密钥管理安全：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。

5.3.4.2. 测评单元评分规则

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：

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

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《信息系统密码应用测评要求》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。

5.3.4.3. 安全层面评分规则

每个测评单元相应的权重为 w_{ij} ，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：

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

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《信息系统密码应用测评要求》。

各个测评单元相应的权重 w_{ij} 见下表（其中“/”表示不适用）：

表 24 测评单元的权重

安全 层面	测评单元	测评单元的权重 w_{ij}			
		第一级	第二级	第三级	第四级
物理和 环境安 全	身份鉴别	0.4	0.7	1	1
	电子门禁记录数据存储完整性	0.4	0.4	0.7	0.7
	视频监控记录数据存储完整性	/	/	0.7	0.7
网络和 通信安 全	身份鉴别	0.4	0.7	1	1
	通信数据完整性	0.4	0.4	0.7	1
	通信过程中重要数据的机密性	0.4	0.7	1	1
	网络边界访问控制信息的完整性	0.4	0.4	0.4	0.7
	安全接入认证	/	/	0.4	0.7
设备和	身份鉴别	0.4	0.7	1	1

计算安全	远程管理通道安全	/	/	1	1
	系统资源访问控制信息完整性	0.4	0.4	0.4	0.7
	重要信息资源安全标记完整性	/	/	0.4	0.7
	日志记录完整性	0.4	0.4	0.4	0.7
	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
应用和数据安全	身份鉴别	0.4	0.7	1	1
	访问控制信息完整性	0.4	0.4	0.4	0.7
	重要信息资源安全标记完整性	/	/	0.4	0.7
	重要数据传输机密性	0.4	0.7	1	1
	重要数据存储机密性	0.4	0.7	1	1
	重要数据传输完整性	0.4	0.7	0.7	1
	重要数据存储完整性	0.4	0.7	0.7	1
	不可否认性	/	/	1	1
管理制度	具备密码应用安全管理制度	1	1	1	1
	密钥管理规则	0.7	0.7	0.7	0.7
	建立操作规程	/	0.7	0.7	0.7
	定期修订安全管理制度	/	/	0.7	0.7
	明确管理制度发布流程	/	/	0.7	0.7
	制度执行过程记录留存	/	/	0.7	0.7
人员管	了解并遵守密码相关法律法规和	0.7	0.7	0.7	0.7

理	密码管理制度				
	建立密码应用岗位责任制度	/	1	1	1
	建立上岗人员培训制度	/	0.7	0.7	0.7
	定期进行安全岗位人员考核	/	/	0.7	0.7
	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
建设运行	制定密码应用方案	1	1	1	1
	制定密钥安全管理策略	1	1	1	1
	制定实施方案	0.7	0.7	0.7	0.7
	投入运行前进行密码应用安全性评估	1	1	1	1
	定期开展密码应用安全性评估及攻防对抗演习	/	/	0.7	0.7
应急处置	应急策略	1	1	1	1
	事件处置	/	/	0.7	0.7
	向有关主管部门上报处置情况	/	/	0.7	0.7

5.3.4.4. 整体测评结果评分规则

每个安全层面相应的权重为 w_i ，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：

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

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。

各个安全层面相应的权重 W_i 见下表。

表 25 安全层面相应的权重

安全层面	测评单元	安全层面的权重 W_i
物理和环境安全	身份鉴别	10
	电子门禁记录数据存储完整性	
	视频监控记录数据存储完整性	
网络和通信安全	身份鉴别	20
	通信数据完整性	
	通信过程中重要数据的机密性	
	网络边界访问控制信息的完整性	
	安全接入认证	
设备和计算安全	身份鉴别	10
	远程管理通道安全	
	系统资源访问控制信息完整性	
	重要信息资源安全标记完整性	
	日志记录完整性	
	重要可执行程序完整性、重要可执行程序来源真实性	
应用和数据	身份鉴别	30

安全	访问控制信息完整性	
	重要信息资源安全标记完整性	
	重要数据传输机密性	
	重要数据存储机密性	
	重要数据传输完整性	
	重要数据存储完整性	
	不可否认性	
管理制度	具备密码应用安全管理制度	8
	密钥管理规则	
	建立操作规程	
	定期修订安全管理制度	
	明确管理制度发布流程	
	制度执行过程记录留存	
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
	建立密码应用岗位责任制度	
	建立上岗人员培训制度	
	定期进行安全岗位人员考核	
	建立关键岗位人员保密制度和调离制度	
建设运行	制定密码应用方案	8
	制定密钥安全管理策略	

	制定实施方案	
	投入运行前进行密码应用安全性评估	
	定期开展密码应用安全性评估及攻防对抗演习	
应急处置	应急策略	6
	事件处置	
	向有关主管部门上报处置情况	

5.3.4.5. 测评得分计算示例

1、计算思路

- 1) 第一步：对某一个安全层面来说，先针对某一个测评单元，计算出这个测评单元的各个测试对象的分值；
- 2) 第二步：利用这个测评单元的各个测试对象的分值，计算出算术平均值，也就是这个测评单元的分值（算术平均值）；
- 3) 第三步：这个安全层面包含多个测评单元，利用测评单元的权重，计算出这个安全层面的分值（加权平均值）；
- 4) 第四步：把每个安全层面的分值都计算出来后，利用每个安全层面的权重，就可以计算出整体测评结果（加权平均值）。

2、举例说明

- 1) 假设：

安全层面：物理和环境

测评单元：身份鉴别

测评对象：测评对象 A，测评对象 B，测试对象 C

表 26 身份鉴别单元测评对象得分情况

安全层面	测评单元	测评对象	测评对象得分
物理和环境安全	身份鉴别	测评对象 A	1
		测评对象 B	0.5
		测评对象 C	0

说明：

每个测试对象的得分是根据“密码使用是否安全”，“密码算法/技术是否合规”，“密钥管理是否安全”来综合打分的。全部符合得 1 分，部分符合得 0.5 分或者 0.25 分，全部不符合不得分（即 0 分）。

2) 通过测评对象的分值，计算出这个测评单元的得分（算术平均值）

$$\text{测评单元的得分} = \frac{1+0.5+0}{3} = 0.5$$

3) 假设：物理和环境安全层面，每个测评单元的得分如下：

表 27 物理和环境测评单元得分情况

安全层面	测评单元	测评单元得分	测评单元的权重（第三级）
物理和环境安全	身份鉴别	0.5	1
	电子门禁记录数据存储完整性	1	0.7
	视频记录数据存储完整性	0.5	0.7

利用测评单元的权重和测评单元的得分,通过加权平均计算出安全层面的得分:

$$\text{安全层面的得分: } \frac{0.5 \times 1 + 1 \times 0.7 + 0.5 \times 0.7}{1 + 0.7 + 0.7} = 0.6458$$

4) 假设: 每个安全层面的得分如下:

表 28 各安全层面得分

安全层面	安全层面的得分	安全层面的权重
物理和环境安全	0.6458	10
网络和通信安全	0.6842	20
设备和计算安全	0.7073	10
应用和数据安全	0.6148	30
管理制度	0.9222	8
人员管理	0.9079	8
建设运行	0.9205	8
应急处置	0.8542	6

利用安全层面的权重和安全层面单元的得分,通过加权平均计算出整体测评结果的得分:

整体测评结果的得分:

$$\frac{0.6458 \times 10 + 0.6842 \times 20 + 0.7073 \times 10 + 0.6148 \times 30 + 0.9222 \times 8 + 0.9079 \times 8 + 0.9205 \times 8 + 0.8542 \times 6}{100} \times 100 = 72.79$$

5.3.5. 密测评结论

按照商用密码应用“三同步一评估”要求，信息系统需要同步规划、同步建设、同步运行密码保障系统，并进行商用密码应用安全性评估。在规划阶段，评估的对象是信息系统的密码应用方案；在建设和运行阶段，评估的对象是实际的信息系统。

5.3.5.1. 方案评估结论

方案评估结论：{通过/不通过}。

方案评估结论格式如下：

受{委托单位}委托，{密评机构名称}于XX年XX月XX日至XX年XX月XX日，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》的第XX{（一~四）}级相关要求，对《XX系统密码应用方案》进行了商用密码应用安全性评估，结论为：{通过/不通过}。

5.3.5.2. 系统测评结论

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）。依据量化评估结果S的分值来判断系统评测结果：符合、基本符合、不符合。

1) 符合：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 39786—2021《信息安全技术 信息系统密码应用基本要求》相应等级要求；

2) 基本符合：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 39786-2021《信息安全技术 信息系统密码应用基本要求》相应等级要求；

3) 不符合：否则，判定被测信息系统不符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》相应等级要求。

网络运营者完成测评工作后，获取到“密评”测评报告后需将密评报告、密评结果上报主管部门及所在地区（部门）密码管理部门备案，测评机构上报国密局备案；等保三级及以上信息系统，评估报告还需由被测单位上报至系统受理备案(即等级保护定级备案)的公安机关。

5.4. 密评改造专业化技术方案

5.4.1. 密改总体框架

根据业务信息系统的等级保护情况，参照《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》对应指标要求，综合考虑业务信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。将采用密码技术措施和有效的安全管理措施，弥补业务信息系统在身份鉴别、安全传输、数据加密、完整性保护、不可否认等方面密码应用薄弱的环节，消除密码应用环节的不合规、不安全密码技术和密码算法，进一步提高业务信息系统的密码应用水平，提升业务信息系统的安全防护能力。



图 101 国标 GB/T39786 密码应用基本要求

方案的总体思路：业务数据动态流转于业务各个环节，以应用为抓手构建国密改造防护体系。针对信息系统应用终端的身份认证、数据传输和数据存储，以及业务数据流转各个环节所需的应用系统免改造加密、数据库免改造加密、数据传输加密、身份认证、数字签名、密钥管理等密码需求，对需要密码应用升级改造的系统进行国密改造。



图 102 国密改造整体密码应用技术框架

本节介绍了数据库免改造、应用免改造、高性能、低成本、轻部署、周期短、无风险、强合规、一站式国密改造最佳实践，可快速轻松通过密评。

5.4.2. 密改技术方案

根据业务信息系统的等级保护定级^[54]（三级）情况，参照《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》以下简称“基本要求”，对信息系统从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面进行风险分析和密码应用需求分析，并提出国密改造应对方案参考。

密评得分说明^[55]，按照一级到五级划分，满分 100 分，60 分及格，要求没有高风险项。其中物理和环境安全占 10 分、网络和通信占 20 分，设备和计算安全占 10 分、应用和数据安全占 30 分、管理制度 8 分、人员管理 8 分、建设运行 8 分、应急处置 6 分。

5.4.2.1. 物理和环境安全

1、安全风险分析

计算、存储、网络、安全等物理设备统一存放在机房内。机房所面临的风险包括：

1. 机房场地如果遭受到破坏，如人为、盗窃、破坏设备等，会对系统造成不可逆转的伤害；
2. 机房的基础设施故障如动力系统故障、机房空调故障、消防系统故障等，这些故障会对平台的业务安全运行带来隐患；
3. 非法人员进入机房，对软硬件设备和数据进行直接破坏，会对机房内数据资产造成严重损失；
4. 进出机房记录和视频监控遭到篡改，以掩盖非法人员进出情况。

表 29 物理和环境安全风险

密测评项	安全风险
身份鉴别	电子门禁系统使用的是若算法，容易被破解。
电子门禁记录数据完整性	电子门禁记录没有做完整性保护。
视频监控记录数据完整性	视频监控记录没有做完整性保护。

2、密码应用需求

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，本方案应满足的物理和环境安全需求如下：

1. 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
2. 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；
3. 宜采用密码技术保证视频监控音像记录数据的存储完整性；
4. 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
5. 以上采用的密码产品，应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》二级及以上安全要求。

需要采用符合密码相关国家、行业标准要求密码技术，实现对门禁进出记录和视频监控数据进行完整性保护。

表 30 物理和环境应用测评指标

测评单元	测评指标
身份鉴别	在电子门禁系统中，应使用密码技术的真实性服务来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。
电子门禁记录数据完整性	应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性。
视频记录数据完整性	应使用密码技术的完整性功能来保证视频监控音像记录的完整性。

3、物理和环境安全全国密改造

物理和环境安全保护的对象是信息系统所在机房重要区域的物理安全,包括进出机房的人员身份真实性、电子门禁系统进出记录数据的存储完整性、视频监控音像记录数据的存储完整性。在机房采用符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的电子门禁系统,使用 SM4 算法进行密钥分散,实现门禁卡的“一卡一密”,并基于 SM4 算法对人员身份进行鉴别,采用 HMAC-SM3 技术实现电子门禁系统进出记录和视频监控系统视频记录等数据存储完整性保护。

1) 安全门禁及视频监控系统组成

基于非接触式 CPU 卡的门禁系统的密码应用涉及应用系统、密钥管理及发卡系统。在应用系统中门禁系统由门禁卡、PSAM 卡、门禁读卡器、门禁控制器和后台管理系统构成,通过各设备内的密码模块对系统提供密码安全保护。其中包括:

- (1) 门禁卡内的密码模块:用于门禁读卡器对门禁卡进行身份鉴别时(鉴别门禁卡是否合法)提供密码服务(如计算鉴别码);
- (2) 门禁读卡器内的密码模块:用于对门禁卡进行身份鉴别时提供密码服务(如密钥分散、验证鉴别码等)。在门禁系统的安全性设计时,门禁读卡器内配备密码模块 PSAM 卡。

门禁系统设计符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》标准的要求。标准规定了针对采用非接触式卡的门禁系统,采用密码安全技

术时，系统中使用的密码设备、密码算法、密码协议和密钥管理的相关要求。适用于采用非接触卡的门禁系统相关产品的研制、使用和管理。

安全音视频监控系统主要由相关的硬件产品和软件管理平台组成。系统的功能是实现视频信息在处理、传输、存储、显示、控制和回放过程中的加密、解密、完整性生产与校验处理。

2) 安全门禁及视频监控系统密码应用

门禁卡和门禁读卡器之间采用 SM4 密码算法进行身份鉴别和数据加密通讯。

所有的认证都是由安装在门禁读卡器中的 PSAM 模块进行运算的。PSAM 模块支持标准国密 SM4 算法，并可以根据密钥长度自动选择算法，具有明文加 MAC、密文、密文加 MAC 三种方式的数据和密钥线路保护功能。

门禁系统中，读卡器获得门禁卡产生的身份鉴别信息后，将该需要鉴别的信息反馈给门禁控制器，并由门禁控制器鉴别门禁读卡器上传的鉴别信息，判断产生该鉴别信息的门禁卡是否合法，并完成开门动作，同时将信息传输给后台管理系统，做长期保存、查询、统计、考勤等。后台管理系统采用智能密码钥匙基于消息鉴别码机制实现门禁记录数据存储完整性保护。

通过国密音视频数据存储实现对音视频记录进行完整性保护，在客户端播放时，先进行完整性的校验，校验无误后正常播放，国密改造如下图所示。

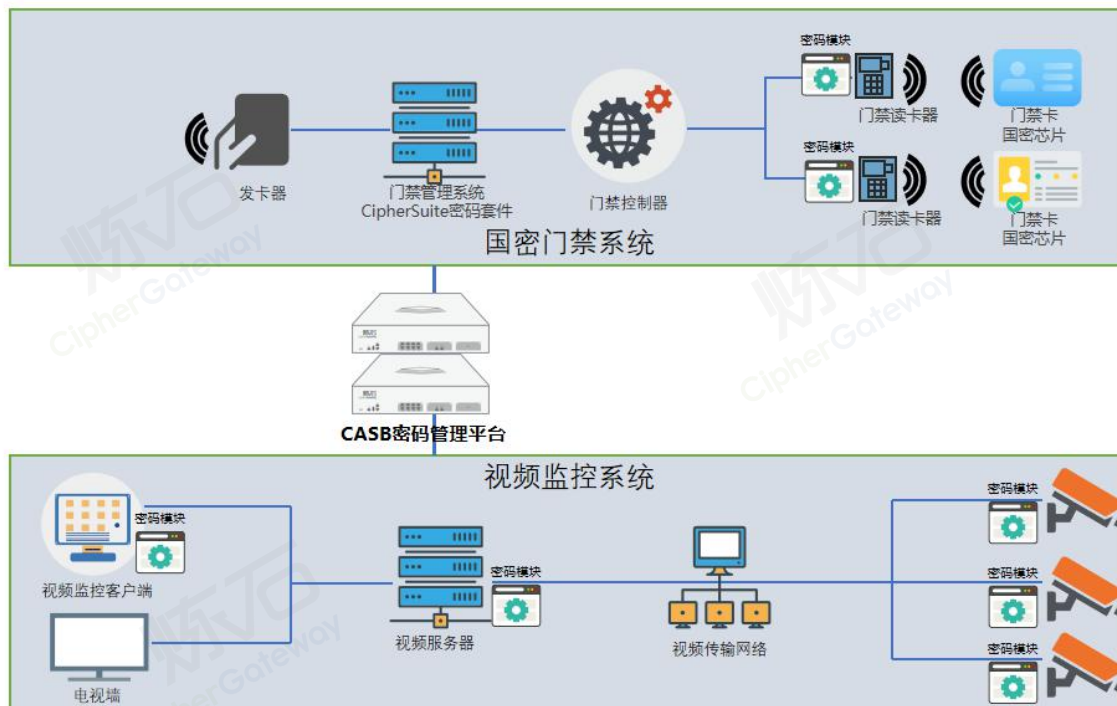


图 103 物理和环境改造图

物理和环境改造实现建议：

1) 身份鉴别：

部署国密算法的安全门禁系统，通过基于 SM4 算法进行密钥分散的 CPU 卡实现对人员身份进行鉴别，实现身份真实性。

2) 电子门禁记录数据的完整性：

在系统环境监控区部署密码数据安全模块和密钥管理与数据加密及认证平台，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系统视频记录等数据进行完整性保护。

3) 视频记录数据的完整性：

在系统环境监控区部署密码数据安全模块和密钥管理与数据加密及认证平台，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系统视频记录等数据进行完整性保护。

5.4.2.2. 网络和通信安全

1、安全风险分析

网络和通信过程中遇到的风险包括：

- 1) 链路可能会受到攻击，如 DDOS 攻击、流量攻击等，可能会导致业务系统全部瘫痪；
- 2) 链路发生故障导致资源和应用不可访问；
- 3) 非法设备从外部接入内部网络，或网络边界被破坏；
- 4) 通信传输过程中数据被非授权的截取、篡改，导致通信数据发生泄漏；
- 5) 关键节点存在恶意代码，导致对网络通信造成破坏等。

表 31 网络和通讯安全风险

测评单元	安全风险
身份鉴别	未在网络边界处使用密码设备或密码技术对网络区域进行保护。
访问控制信息完整性	没有使用密码技术实现边界访问控制信息的完整性。
通信数据完	未在网络边界处使用密码设备或密码技术对网络区域进行保护。

整性	
通信数据机 密性	未在网络边界处使用密码设备或密码技术对网络区域进行保护。
集中管理通 道安全	使用堡垒机对系统中的各设备进行管理、运维，未取得商用密码产品型号，设备使用 SSL 技术对集中管理通道进行保护。使用的密码算法包含 RSA2048、AES128、AES256、3DES、SHA1、SHA256、SHA384，它们都不是合规的密码算法。

2、密码应用需求

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，本方案应满足网络和通信安全的需求如下：

- 1) 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
- 2) 宜采用密码技术保证通信过程中数据的完整性；
- 3) 应采用密码技术保证通信过程中重要数据的机密性；
- 4) 可采用密码技术保证网络边界访问控制信息的完整性；
- 5) 可采用密码技术对从外部连接到内部网路的设备进行接入认证，确保接入的设备身份真实性。
- 6) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；
- 7) 以上采用的密码产品，应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》二级及以上安全要求。

需要采用支持国密 SSL 功能的 CipherSuite 密码模块和 SSLVPN 实现通信实体身份鉴别,保证通信实体身份的真实性,网络通信信道中数据的机密性和完整性;需要采用密码技术保障网络边界访问控制信息的完整性;需要采用密码技术保障对从外部连接到内部网络的接入设备身份的真实性。

3、网络和通信安全国密改造

网络和通信安全保护的对象是信息系统与外部实体之间网络通信的安全,包括通信实体身份的真实性、通信数据的机密性和完整性、以及网络边界访问控制信息的完整性。通过客户端使用国密浏览器、服务端部署 SSLVPN 网关,建立国密安全传输通道。通信前进行身份鉴别,握手成功后,使用数据加密密钥和校验密钥实现通信数据的机密性和完整性保护。同时 SSLVPN 采用 HMAC-SM3 技术实现访问控制信息的完整性保护。

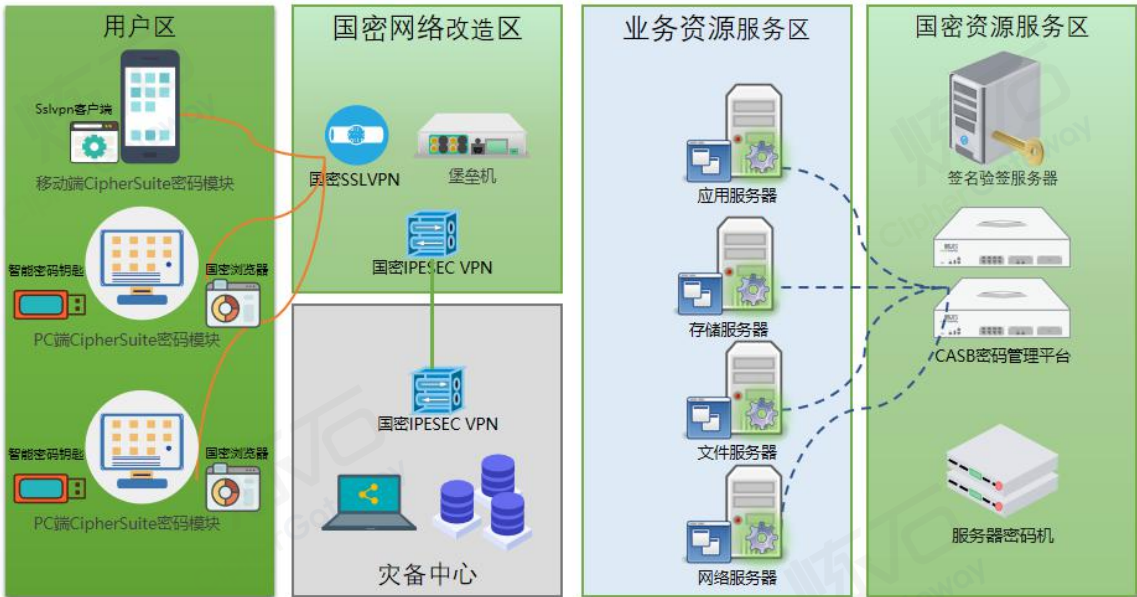


图 104 网络和通信改造图

网络和通信改造实现建议：

1. 身份鉴别：

部署安全接入网关，利用智能密码钥匙作为设备管理员的身份凭证，在设备管理员进行设备登录时对其身份进行鉴别。通过密码机和 CASB 安全管理平台生成分发密钥，实现 SM2 的身份鉴别。

2. 通信数据完整性：

通过安全接入网关，使用 SM3 算法的 MAC 消息鉴别码技术实现数据的完整性。

3. 重要数据机密性：

通过安全接入网关，使用 SM4 算法的对称加密实现机密性。密码套件 ECC_SM4_SM3。采用 SM4 对数据报文做加密运算实现，加密密钥通过 ECC_SM4_SM3 算法套件协商实现，定期更新。

4. 访问控制信息完整性：

安全接入网关具有网络边界访问控制功能，其他设备的访问控制信息列表通过 SM3 算法的 MAC 消息鉴别码技术实现数据的完整性。

5. 安全接入认证：

远程接入内网通过安全认证网关实现，内网采用 SM2 实现身份鉴别。

网络和通信安全层面使用的密码算法、密码技术、密钥管理由符合 GM/T 0025-2014《SSL VPN 网关产品规范》、GB/T 36968-2018《信息安全 技术 IPsec VPN 技术规范》、GB/T 37092—2018《信息安全技术密码模块安全要求》的 IPsec/SSL VPN 实现。

5.4.2.3. 设备和计算安全

1、安全风险分析

设备和计算操作过程中遇到的风险包括：

- 1) 设备被非法人员登录；
- 2) 用户口令遭到恶意破解，导致系统被入侵；
- 3) 系统遭到入侵后，删除账户、恶意分配账户权限、通过修改用户权限获取更高级别信息；
- 4) 对设备漏洞发动攻击；
- 5) 恶意调用系统资源，虚拟机逃逸；
- 6) 设备日志记录被非法篡改，以掩盖非法操作；
- 7) 远程登录设备时，身份鉴别数据被非法获取或非法使用；
- 8) 设备内重要程序和文件的来源不可信。

表 32 设备和计算安全风险

测评单元	安全风险
身份鉴别	应用服务器、数据中心数据库使用用户名与口令进行登录。 堡垒机使用用户名与口令进行登录，未使用密码技术。
远程管理身份鉴别 信息机密性	未使用合规的商用密码算法保护远程管理身份鉴别信息机密性。

访问控制信息完整性	堡垒机、应用库服务器、数据库都未使用密码技术实现访问控制信息的完整性保护。
重要程序或文件完整性	未采用可信计算技术实现系统运行过程中重要程序或文件完整性。
日志记录完整性	堡垒机、应用服务器、数据库未使用密码技术实现日志信息的完整性保护。

2、密码应用需求

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，本方案应满足设备和计算安全的需求如下：

- 1) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
- 2) 远程管理设备时，应采用密码技术建立安全的信息传输通道；
- 3) 宜采用密码技术保证系统资源访问控制信息的完整性；
- 4) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；
- 5) 宜采用密码技术保证日志记录的完整性；
- 6) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；
- 7) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

- 8) 以上采用的密码产品，应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》二级及以上安全要求；

需要采用密码技术保障登录设备的用户身份的真实性；远程管理设备时，需要采用密码技术建立安全的信息传输通道；需要采用密码技术保障系统资源访问控制信息、设备中的重要信息资源安全标记、日志记录的完整性以及重要可执行程序完整性，对其来源的真实性验证。

表 33 设备和计算测评指标

测评单元	测评指标
身份鉴别	应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息其有复杂度要求并定期更换。
远程管理身份鉴别信息机密性	在远程管理时，应使用密码技术的机密性服务来实现鉴别信息的防窃听。
访问控制信息完整性	应采用密码技术的完整性服务来保证系统资源访问控制信息的完整性。
敏感标记完整性	应使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性。
重要程序或文件完整性	应采用可信计算技术建立从系统到应用信任链，实现系统运行系统运行过程中重要程序或文件完整性保护。

日志记录完整性	应使用密码技术的完整性功能来对日志记录进行完整性保护。
---------	-----------------------------

3、设备和计算国密改造

设备和计算安全保护的对象是信息系统中各类设备和计算环境的安全,包括登录设备用户身份的真实性、远程管理时建立安全的信息传输通道、系统资源访问控制信息和日记的完整性等。采用基于智能密码钥匙的登录方式保证登录设备用户身份的真实性,使用国密 HTTPS 安全通道保证传输数据的机密性和完整性,采用数字签名技术实现设备上系统资源访问控制信息、日志记录和重要可执行程序完整性保护。

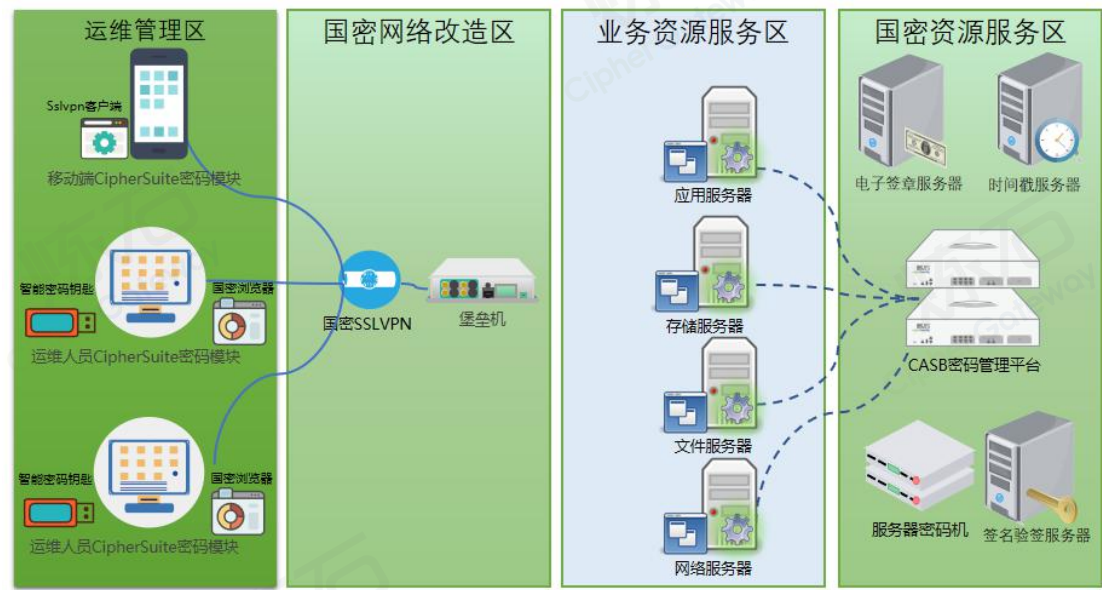


图 105 设备和计算改造图

设备和计算改造实现建议：

- 1) 身份鉴别：

在 PC 端部署国密浏览器，并向系统管理员配发智能密码钥匙，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息。

2) 远程通道管理安全：

采用智能密码钥匙、国密安全浏览器、SSLVPN 保障通信实体身份鉴别、接入通过 SSL/IPSEC VPN 网关安全认证、搭建的加密传输通道，对鉴别信息加密实现防窃听。

3) 访问控制信息完整性：

调用服务器密码机和 CASB 安全管理平台，使用 SM3 算法的 MAC 消息鉴别码技术实现数据的完整性。管理员身份鉴别通过智能密码钥匙实现，使用数字签名技术对应用服务器、数据库服务器管理员用户访问权限控制列表进行完整性保护。

4) 日志完整性：

通过调用 CASB 安全管理平台和服务器密码机，设置日志服务器安全策略，使用 SM3 算法的 MAC 消息鉴别码技术，使用 HMAC-SM3 对应用服务器、数据库服务器等设备日志进行完整性保护。

5) 重要可执行程序来源真实性和完整性：

在本系统应用服务区部署服务器密码机，智能密码钥匙，应用服务器中所有重要程序或文件在生成时通过调用服务器密码机使用 SM2 数字签名技术进行完整性保护，使用或读取这些程序和文件时，通过数字签名验证确认其完整性，公钥存储在只读安全介质中。

设备和计算安全层面所使用的密码算法、密码技术、密码服务、密钥管理符合 GM/T 0030-2014《服务器密码机技术规范》、GM/T 0027-2014《智能密码钥匙技术规范》、GB / T 37092-2018《信息安全技术密码模块安全要求》的智能密码钥匙、服务器密码机实现。

5.4.2.4. 应用和数据安全

1、安全风险分析

应用和数据面临的风险包括：

- 1) 业务系统被非法人员登录，导致业务系统被入侵；
- 2) 传输或存储的业务数据被其他应用获取、被外部攻击者非法获取；
- 3) 应用系统资源访问控制信息、应用日志记录被非法篡改，掩盖非法操作；
- 4) 应用程序、重要应用配置等重要信息被非法修改；
- 5) 数据发送者或接收者不承认发送或接受到数据，或者否认所做的操作和交易。

表 34 应用和数据安全风险

测评单元	安全风险
身份鉴别	使用用户名口令方式进行身份鉴别，未使用密码技术。
访问控制	未使用密码技术实现访问控制信息和敏感标记的完整性保护。
数据传输机密性	数据传输使用了 SSL 技术，机密性算法使用 AES256。

数据存储机密性	未使用密码技术实现数据存储机密性保护。
数据传输完整性	数据传输使用了 SSL 技术，完整性算法包含 SHA1、SHA256、SHA384。
数据存储完整性	未使用密码技术实现数据存储完整性保护。
日志记录完整性	系统未使用密码技术实现日志记录的完整性保护。
重要应用程序加载和卸载	系统未实现重要程序或文件完整性保护。

2、密码应用需求

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，本方案应满足应用和数据安全的需求如下：

- 1) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；
- 2) 宜采用密码技术保证系统资源访问控制信息的完整性；
- 3) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
- 4) 应采用密码技术保证信息系统应用的重要数据在传输、存储过程中的机密性；
- 5) 宜采用密码技术保证信息系统应用的重要数据在传输、存储过程中的完整性；

- 6) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；
- 7) 以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

以上采用的密码产品，应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》二级及以上安全要求

表 35 应用和数据测评指标

测评单元	测评指标
身份鉴别	应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。
访问控制	应使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记的完整性。
数据传输机密性	应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。
数据存储机密性	应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息、重要可执行

	程序等。
数据传输完整性	应采用密码技术保证重要数据在传输过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等。
数据存储完整性	应采用密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等。
日志记录完整性	应使用密码技术的完整性功能来实现对日志记录完整性的保护。
重要应用程序加载和卸载	应采用密码技术对重要应用程序的加载和卸载进行安全控制。

3、应用和数据安全改造

移动端 App 中部署符合 GM/T 0028-2014《密码模块安全技术要求》的移动端密码模块 CipherSuite（二级），在网络接入区边界部署符合 GM/T 0026-2014《安全认证网关产品规范》的安全认证网关，在系统基础设施区部署符合 GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》的证书认证系统，通过证书认证系统分别向移动端密码模块（二级）、安全认证网关配置数字证书，实现移动端登录应用用户的安全身份鉴别，防止非授权人员登录；在本系统业务办公区 PC 端部署国密安全浏览器，在业务服务区部署符合

GM/T 0025-2014《SSL VPN 网关产品规范》的 SSL VPN 安全网关，并向相关用户配发智能密码钥匙，实现对 PC 端登录应用用户的安全身份鉴别，防止非授权人员登录。

在网络接入区部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器，使用数字签名技术对统一身份认证系统应用用户访问权限控制列表进行完整性保护，防止应用资源被非授权用户获取。

在业务服务区分别部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机和符合 GM/T 0025-2014《SSL VPN 网关产品规范》的 SSL VPN 安全网关，应用通过调用服务器密码机，对移动端登录用户身份鉴别数据、PC 端登录用户身份鉴别数据、系统中流转的应用系统数据进行传输、存储机密性、完整性保护，实现身份鉴别数据、应用系统数据防窃取和防篡改保护；PC 端安全浏览器与 SSL VPN 安全网关之间使用合规的 SSL 协议，建立安全的数据传输通道，实现数据传输机密性、完整性保护。

应用通过调用部署在业务服务区的服务器密码机，使用 HMAC-SM3 对应用日志记录进行完整性保护，防止应用日志记录被非授权篡改。

在基础设施区部署符合 GM/T 0031-2014《安全电子签章密码技术规范》、GM/T 0033-2014《时间戳接口规范》的电子签章系统、时间戳服务器，使用密码技术对在系统中流转的应用系统数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性。

应用和数据安全层面所要求的密码算法、密码技术、密码服务、密钥管理由安全浏览器、符合 GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0029-2014《签名验签服务器技术规范》、GM/T

0030-2014《服务器密码机技术规范》、GM/T 0031-2014《安全电子签章密码技术规范》、GM/T 0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》、GM/T 0033-2014《时间戳接口规范》、GM/T 0014-2012《数字证书认证系统密码协议规范》、GM/T 0028-2014《密码模块安全技术要求》等标准要求的移动端密码模块（二级）、智能密码钥匙、安全认证网关、签名验签服务器、服务器密码机、电子签章系统、时间戳服务器和证书认证系统实现。

应用和数据安全保护的对象是应用及其数据的安全,包括登录应用系统用户身份的真实性、数据传输的机密性和完整性、数据存储的机密性和完整性等。通过身份认证系统实现登录应用系统用户的身份的真实性,通过国密浏览器和 SSL VPN 实现传输数据的机密性和完整性,通过数据加解密服务平台实现存储数据(如鉴别数据、用户数据、业务数据)的机密性。

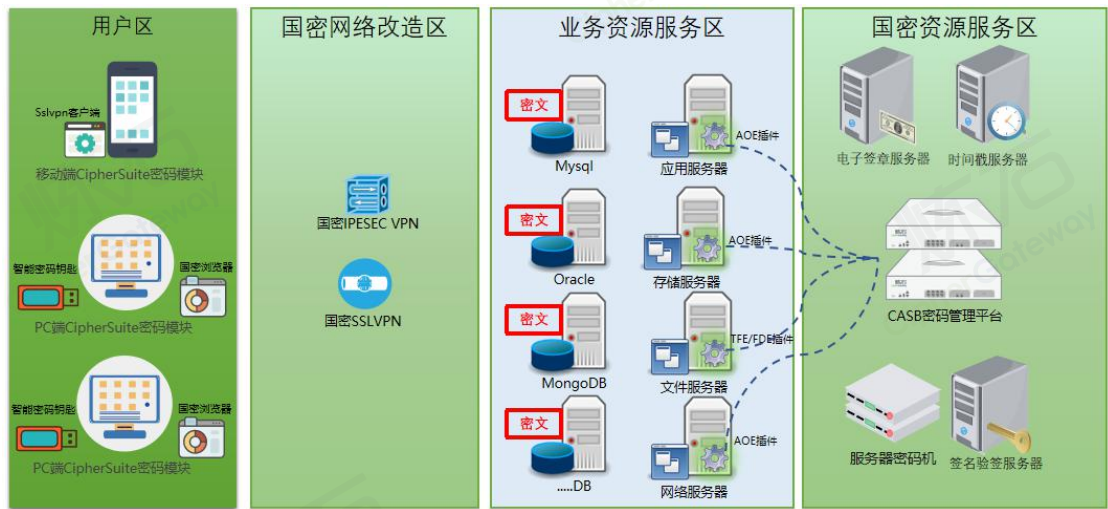


图 106 应用和安全改造图

应用和安全改造实现建议：

- 1) 身份鉴别：

部署数字证书系统、CASB 密码管理平台，服务器密码机、签名验签服务器，PC 端通过智能密钥实现身份鉴别，移动端通过密码模块实现系统用户身份鉴别。

2) 访问控制信息完整性：

部署密钥管理与数据加密及认证平台或签名验签服务器，调用 CASB 密码管理平台和服务器密码机，对业务应用系统访问控制策略、数据库表访问控制信息等使用 SM3 算法的 MAC 消息鉴别码技术实现数据的完整性。

3) 数据存储机密性：

通过 CASB 安全管理平台和 AOE 安全插件实现基于 SM4 算法对称加密。

4) 数据存储完整性：

调用 CASB 安全管理平台和服务器密码机，使用 SM3-HMAC 或者 SM4-GCM 实现存储数据的完整性保护。

5) 数据传输机密性和完整性：

数据传输机密性和完整，通过 SSL、IPSEC VPN 安全认证网关实现。

6) 不可否认性：

部署电子签章系统、时间戳服务器，通过 CASB 安全管理平台和智能密钥或密码模块，采用 SM2 算法的数字签名技术，并加盖时间戳，实现操作行为的不可否认性。

应用和数据安全层面所要求的密码算法、密码技术、密码服务、密钥管理符合 GM/T 0026-2014《安全认证网关产品规范》、GM/T 0029-2014《签名验签服

务器技术规范》、GM/T0030—2014《服务器密码机技术规范》、GB / T 37092—2018《信息安全技术密码模块安全要求》等标准要求的 IPSec/SSL VPN 综合安全网关、签名验签服务器、服务器密码机实现。

5.4.3. 密钥管理方案

5.4.3.1. 密钥管理需求分析

本方案应包括对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。以下给出各环节的密钥管理需求：

1. 密钥产生

密钥可以以随机产生、协商产生等不同的方式来生产。密钥在符合 GB/T 37092—2018《信息安全技术密码模块安全要求》的密码产品中产生是十分必要的，产生的同时可在密码产品中记录密钥关联信息，包括密钥种类。长度、拥有者、使用起始时间、使用终止时间等。

2. 密钥分发

密钥分发是密钥从一个密码产品传递到另一个密码产品的过程，分发时要注意抗截取、篡改、假冒等攻击，保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。

3. 密钥存储

密钥不以明文方式存储在密码产品外部是十分必要的，并采取严格的安全防护措施，防止密钥被非授权的访问或篡改。

公钥是例外，可以以明文方式在密码产品外存储、传递和使用，但有必要采取安全防护措施，防止公钥被非授权篡改。

4. 密钥使用

每个密钥一般只有单一的用途，明确用途并按用途正确使用是十分必要的。密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等。另外，有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性。

5. 密钥更新

密钥更新发生在密钥超过使用期限、已泄露或存在泄露风险时，根据相应的更新策略进行更新。

6. 密钥归档

如果信息系统中有密钥归档需求，则根据实际安全需求采取有效的安全措施，保证归档密钥的安全性和正确性。需要注意的是，归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档，则有必要生成审计信息，包括归档的密钥、归档的时间等。

7. 密钥撤销

密钥撤销一般针对公钥证书所对应的密钥。当证书到期后，密钥自然撤销；也可以按需进行密钥撤销，撤销后的密钥不再具备使用效力。

8. 密钥备份

对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密性和完整性。这与密钥存储的要求是一致的。密钥备份行为是审计涉及的范围，有必要生成审计信息，包括备份的主体、备份的时间等。

9. 密钥恢复

可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围，有必要产生审计信息，包括恢复的主体、恢复的时间等。

10. 密钥销毁

密钥销毁要注意的是销毁过程的不可逆，即无法从销毁结果中恢复原密钥。

密钥的安全是保证密码算法安全的基础。如何对密钥进行安全管理是密码产品、密码应用的设计开发人员关注的重点。

密钥生命周期指的是密钥从生成到销毁的时间跨度。不同的密钥有不同的生命周期：签名密钥对可能有数年的生命周期；而一些临时密钥的生命周期为单次会话，使用完毕后立即销毁。使用频率越高的密钥要求其生命周期尽量短。单个密钥的生命周期也不是固定的，如果密钥泄露应立即终止并销毁密钥。

此外，有些与安全相关的敏感参数也应该视同密钥进行安全防护，包括但不限于用户口令、密钥生成和密码计算过程中使用的随机数或中间结果。

5.4.3.2. 密钥管理改造

本系统选用通过检测认证的智能密码钥匙、IPSec/SSL VPN 综合安全网关、IPSec VPN 安全终端、签名验签服务器、服务器密码机、安全门禁系统、智能密码钥匙等商用密码产品。所用密码产品和密码模块具有国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，符合相关国家标准或密码行业规范要求。密码设备的密钥均存储在独立的硬件介质中。所有私钥不支持任何明文形式导出。其中签名密钥对由设备自身，通过双 WNG9 物理噪声源随机数发生器产生。

根据这些商用密码产品提供的安全策略，制定密钥管理方案，并严格遵照该方案进行使用和实施。

本方案中涉及的密钥主要包括用户密钥对、设备密钥对、应用密钥对、工作密钥和 HMAC 密钥。

1、密钥管理机制

本方案中涉及的密钥，其管理机制列表如下：

表 36 密钥管理机制

用户（管理员、非管理员）密钥对	
密钥生成	签名密钥对采用智能密码钥匙中的物理噪声源芯片产生 加密密钥对由 KMS 密钥管理系统产生
密钥存储	安全存储在智能密码钥匙的密钥存储区
密钥分发	不支持分发
密钥导入与导出	加密密钥对私钥通过用户签名公钥进行加密导入，加密密钥对公钥通过 PKCS#10 证书请求接口导入。
密钥使用	用于登录过程中的身份认证和密钥协商，关键业务操作过程中的数字签名
密钥备份与恢复	不支持密钥备份恢复
密钥归档	不支持密钥归档

密钥销毁	密钥存储区进行 0XFF 覆盖。
------	------------------

表 37 IPsec/SSL VPN 安全网关密钥管理机制

IPSec/SSL VPN 综合安全网关设备密钥对	
密钥生成	<p>签名密钥对内置 PCI-E 密码卡上的两片 WNG9 物理噪声源芯片异或产生。</p> <p>加密密钥对由 KMS 密钥管理系统产生</p>
密钥存储	安全存储在 PCI-E 密码卡上的密钥存储区
密钥分发	不支持分发
密钥导入与导出	加密密钥对私钥通过设备签名公钥进行加密导入，加密密钥对公钥通过 PKCS#10 证书请求接口导入。
密钥使用	用于登录过程中的身份认证和密钥协商
密钥备份与恢复	采用 3/5 门限机制进行加密备份恢复，备份恢复密钥分散存储在 5 只专用智能密码钥匙中。
密钥归档	不支持密钥归档
密钥销毁	密钥存储区进行 0XFF 覆盖。

表 38 堡垒机设备密钥管理机制

堡垒机设备密钥对	
密钥生成	<p>签名密钥对由内置 PCI-E 密码卡上的两片 WNG9 物理噪声源芯片异或产生。</p> <p>加密密钥对由 KMS 密钥管理系统产生</p>
密钥存储	安全存储在 PCI-E 密码卡上的密钥存储区
密钥分发	不支持分发
密钥导入与导出	加密密钥对私钥通过设备签名公钥进行加密导入，加密密钥对公钥通过 PKCS#10 证书请求接口导入。
密钥使用	用于登录过程中的身份认证和密钥协商
密钥备份与恢复	通过备份密钥进行备份恢复，备份密钥存储在智能密码钥匙中
密钥归档	不支持密钥归档
密钥销毁	密钥存储区进行 0xFF 覆盖。

表 39 业务系统密钥管理机制

业务系统密钥对

密钥生成	<p>签名密钥对密码机或签名验签与实践戳服务器内置 PCI-E 密码卡上的两片 WNG9 物理噪声源芯片异或产生。</p> <p>加密密钥对由 KMS 密钥管理系统产生</p>
密钥存储	安全存储在 PCI-E 密码卡上的密钥存储区
密钥分发	不支持分发
密钥导入与导出	加密密钥对私钥通过设备签名公钥进行加密导入，加密密钥对公钥通过 PKCS#10 证书请求接口导入。
密钥使用	用于访问控制信息、敏感数据、系统日志等施加数字签名，保证数据的完整性。
密钥备份与恢复	采用 3/5 门限机制进行加密备份恢复，备份恢复密钥分散存储在 5 只专用智能密码钥匙中。
密钥归档	不支持密钥归档
密钥销毁	密钥存储区进行 0xFF 覆盖。

表 40 工作密钥管理机制

工作密钥

密钥生成	由 KMS 密钥管理系统配套密码机产生真随机数，生成密钥素材。
密钥存储	加密存储在 KMS 密钥管理系统数据库中，加密密钥保存在配套密码机的 PCI-E 密码卡中。
密钥分发	支持数字信封分发方式，采用密文分发。
密钥导入与导出	通过密钥加密密钥导入到 KMS 密钥管理系统的备用库中。 不支持密钥明文导出。
密钥使用	用于敏感数据的存储加密和抽取解密。
密钥备份与恢复	采用 3/5 门限机制进行加密备份恢复，备份恢复密钥分散存储在 5 只专用智能密码钥匙中。
密钥归档	归档密钥加密保存在 KMS 密钥管理系统的历史库中。密钥加密密钥保存在配套密码机的 PCI-E 密码卡中。
密钥销毁	不支持密钥销毁。

2、密钥分级管理

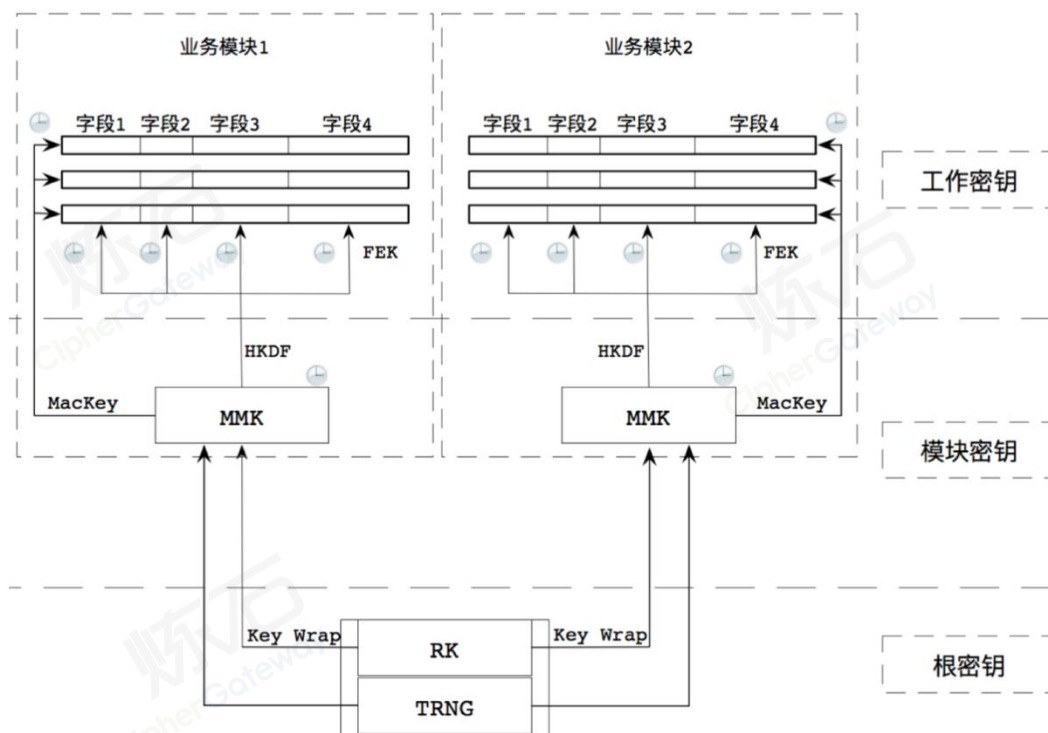


图 107 三层密钥体系图

三层密钥分别指根密钥 (Root Key, RK)，第二级密钥即模块主密钥 (Module Master Key, MMK)，以及用于加密具体数据的第三级密钥——工作密钥，以及可能需要的用于计算业务字段的消息认证码 (Message Authentication Code, MAC) 的 MacKey。

CipherSuite 会请求根密钥派生一个 MMK。MMK 在存储时，用 RK 对 MMK 进行 Key Wrap 保护 (读取时再用 RK 对 MMK 进行 Key Unwrap)。Key Wrap 遵循 RFC 3394 实现，而 RFC 3394 中采用的底层算法 AES 已被替换为 SM4 算法。同一个字段的字段值用同一个工作密钥进行加解密。工作密钥采用 RFC 5869 中的 HKDF-expand 方法从 MMK 进行派生。除了工作密钥之外，为了数据完整性保护的 MAC 计算也会需要密钥 MacKey。与工作密钥类似，MacKey 同样依据 RFC 5869 中的 HKDF-expand 方法从 MMK 进行派生。

5.4.4. 安全管理方案

5.4.4.1. 安全管理需求分析

1. 管理制度

本方案是使用密码技术的信息系统应符合以下管理制度要求：

- (1) 应具备密码应用安全管理制度，包括密码人员管理、密码管理、建设运行、应急处置、密码软硬件及介质管理制度；
- (2) 应根据密码应用方案建立相应密钥管理规则；
- (3) 应对管理人员或操作人员执行的日常管理操作建立操作规程；
- (4) 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
- (5) 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
- (6) 应具备密码应用操作规程的相关执行记录并妥善保管。

2. 人员管理

本方案是使用密码技术的信息系统应符合以下人员管理要求：

- (1) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
- (2) 应建立密码应用岗位责任制度，明确各岗位在安全系统中指责和权限；
- (3) 应建立上岗人员培训制度，对于涉及密码的操作和管理人员进行专门培训，确保其具备岗位所需专业技能；
- (4) 应定期对密码应用安全岗位人员进行考核；
- (5) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

3. 建设运行

本方案建设要求：

- (1) 应依据密码相关标准和密码应用需求，制定密码应用方案；
- (2) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照 GB / T 39786-2021 《信息安全技术 信息系统密码应用基本要求》附录 B 密码生存周期管理。
- (3) 应按照应用方案实施建设；
- (4) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
- (5) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

4. 应急处置

本方案应急处置要求

- (1) 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
- (2) 事件发生后，应及时向信息系统主管部门进行报告；
- (3) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

5.4.4.2. 安全管理改造

1、管理机构

为确保业务正常安全运行，建立并逐步健全一套自上而下的安全组织机构和有关管理的规章制度。

在国家及省密码管理局和密码专家的指导下建立密码安全领导小组,在局领导的直接管理下开展工作,通过技术人员与管理人員的密切协作逐步建立安全防范责任体系,将安全防范的责任逐级落实到每个具体操作人員的日常工作中。

密码安全管理小组由局分管领导担任组长负责系统的全面管理工作,由信息办公室负责人担任副组长负责系统的日常管理工作。

其中,密码安全管理小组职责如下:

- 1) 负责制定建设工程安管人員培训管理系统密码管理安全制度;
- 2) 明确工程安管人員培训管理系统密码建设单位、密码支撑单位、密码应用单位相关职责;
- 3) 指导下属信息系统密码应用单位,安全方针和密码保密策略等政策支持;
- 4) 制定试点工作计划、组织协调各项工作开展、质量把关、日常监督以及验收等;

密码承建、支撑单位职责如下:

- 1) 建设建设工程安管人員培训管理系统密码支撑体系;
- 2) 提供符合国家密码管理局要求的产品和服务;
- 3) 负责做好密码支撑和服务工作;

密码集成单位职责如下:

- 1) 负责集成密码应用的开发和测试工作;
- 2) 做好应用系统应用后的上线实施工作。

主要的日常运维管理负责人有:

- 1) 机房管理负责人:主要负责机房日常管理工作,包括定期检查门禁、监控、电源等设备的工作情况,保证安全设备长期有效等。

- 2) 设备运维负责人：主要负责系统硬件设备的定期检查，保证系统平稳运行。
当出现设备故障时，需确保 2 小时内恢复系统运行并排查设备故障。
- 3) 软件运维负责人：主要负责系统软件平台升级、维护及故障修复工作。每次升级需提前 48 小时报备管理对接人员，由管理对接人安排升级时间。但出现软件故障时，需确保 2 小时内恢复系统运行。
- 4) 网络运维负责人：主要负责保证系统网络畅通，负责网络应急保障。当出现网络故障时，需确保有备用线路供系统正常运行。
- 5) 密码安全运维负责人：主要负责各种密码设备、密码安全软硬件系统的日常维护工作，及安全漏洞排查等。
- 6) 售后支撑负责人：主要负责系统其他售后维护工作。
- 7) 厂家售后人员：负责密码设备的技术支撑。

2、管理人员

密码安全的管理人员，分为系统管理员、安全保密管理员、安全审计员和密钥管理人员、密码操作员，各角色的岗位职责如下：

1) 系统管理员

制定严格的规章制度并认真执行。建立完善的变更管理审核和批准制度，对任何可能影响系统正常运行的软硬件变更，包括更改设置、软硬件升级等，应及时登记报备。

系统管理员负责网络安全及系统安全，必须时刻注意网络安全及系统安全发展的动向，及时做好安全漏洞的防补工作。

2) 安全保密管理员

负责系统安全策略的制定与配置；负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

3) 安全审计员

负责定期对系统管理员、安全保密管理员、密钥管理人员、密码操作人员等的操作行为进行安全审计和监督检查，及时发现违规行为等。

(1) 定期对系统管理员的操作行为进行安全审计和监督检查，及时发现违规行为。

(2) 定期对安全管理员的操作行为进行安全审计和监督检查，及时发现违规行为。

(3) 定期对业务操作员等的操作行为进行安全审计和监督检查，及时发现违规行为。

(4) 对系统运行情况进行审计，形成审计报告。

4) 密钥管理人员

负责密钥的保管、监督、变更、撤消等操作，对任何可能变更密钥的操作，包括生成、更新、删除等，应及时登记报备。

5) 密码操作人员

负责密码设备的日常操作维护，包括查看设备基本信息、设备运行信息以及查看修改网络配置等。

(1) 密码设备的初始化；

(2) 密码设备、软件系统的配置管理；

(3) 密码设备的运维和故障处理。

3、管理制度

随着网络技术的发展，互联网规模的不断扩大，网络带宽的增加，软硬件平台下新安全漏洞的发现，危害网络安全的攻击手段将日益先进，且一旦发动攻击，受害对象的受损程度也将更加严重。因此，建立完善密码安全管理制度，也将有效防范系统性风险。

参照国家密码管理局相关规定，本单位制定了规范的密码安全管理制度和规范如下：

- 1) 日常安全管理规范
- 2) 安全保密制度
- 3) 密码安全管理制度

日常安全管理制度

1. 本单位员工应遵守安全保密制度。
2. 各部门应建立计算机信息系统数据备份制度，按照计算机安全管理的要求对备份数据进行保存。
3. 应采用相应的措施将内外网进行隔离，保证内部网信息安全。
4. 凡使用公用账号进行计算机联网的人，应自觉登记并遵守保密规定。
5. 任何人不得非法侵入内部网络进行破坏活动。
6. 任何人不能对计算机信息系统功能进行增加、删除、修改、干扰，影响计算机信息系统正常运行。
7. 任何人不得对计算机系统中存储、处理或者传输的数据和应用程序进行增加、删除、修改、复制等。
8. 不得私自下载内部计算机系统的信息资源。

9. 不准在私人交往和通信中泄露公司秘密。
10. 不准在公共场所谈论公司秘密。
11. 未经授权不得查阅他人电子邮件。
12. 不得冒用他人名义发送电子邮件。
13. 不得从事其它危害计算机信息系统安全的活动。
14. 认真接受保密教育。

安全保密制度

第一章 总则

1. 为了加强保密工作，保守秘密，根据《中华人民共和国保守国家秘密法》和《商用密码管理条例》等国家有关法规规定，制定本制度。
2. 秘密是指关系到政府的安全和利益，依照特定程序确定，在一定时间内只限一定范围的人员知悉的事项。
3. 工作人员都应当遵守本制度。

第二章 保密范围

4. 包括本制度第二条规定的下列秘密事项：
 - (1) 重大决策中的秘密事项
 - (2) 只限于在内部流通的制度文件、工作文档
 - (3) 机房安全管理中的秘密事项
 - (4) 商用密码产品以及商用密码技术
 - (5) 其他确定应当保密的事项
5. 本制度所称商用密码，是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品，包括如下：

- (1) 商用密码设备
- (2) 信息安全应用系统
- (3) 商用密码技术相关的纸张文档和电子文档
- (4) 程序源代码
- (5) 加解密算法

第三章 人员管理

- 6. 单位员工在其任职期间，必须遵守单位的保密规章制度，履行与工作岗位相应的保密职责，对于本制度第四条规定的单位秘密事项，必须做到不该说的不说、不该问的不问、不该看的不看、不该记录的不记录。
- 7. 员工除履行职务需要之外，未经单位事先书面同意，不得泄露、传播、公布、发表、传授、转让或者以其他任何方式使任何第三方（包括按照公司规定无权知悉该项秘密的单位其他员工）知悉属于单位或者虽属于他人但单位承诺有保密义务的技术秘密或商业秘密，也不得在履行职务之外使用这些秘密信息。
- 8. 从事涉密产品的采购、销售、运输以及保管的员工，对所接触和掌握的涉密技术承担保密责任。
- 9. 员工离职后在规定期限内仍应当保守在单位任职期间接触、知悉的属于单位或者虽属于第三方但单位承诺有保密义务的技术秘密和其他商业秘密信息，承担在单位任职期间一样的保密义务。
- 10. 对公司员工因违反单位规定，造成泄密事件，将依照有关法规及公司的奖惩规定，给予纪律制裁，解雇，直至追究法律责任。

11. 对单位员工泄露商用密码技术、非法攻击商用密码或者利用商用密码从事危害国家的安全和利益的活动，情节严重，构成犯罪的，依法追究刑事责任。

第四章 档案管理

12. 按照国家标准，档案的保管期限划分为永久、长期、短期三种，由单位负责人、部门负责人和档案人员组成鉴定小组，直接对档案进行鉴定，确定档案的保管期限。
13. 单位的档案资料只能由专人接触和保管，其他非相关人员不得无故翻阅、查看。在未经允许的情况下，任何人不得将单位档案资料以任何形式包括书面形式或电子形式带出单位。
14. 到期应销毁的档案,必须报经鉴定小组批准后，办理有关手续,由专人监销处理。凡涉及本制度第四条规定的单位秘密的文件资料的销毁处理，必须使用碎纸机，不准未经切碎作收购处理。
15. 对违反档案保密制度，泄露档案机密并造成损失的责任人，按有关规定视情节轻重给予处罚；构成犯罪的，依法追究刑事责任。

第五章 设备管理

16. 将所有涉密设备存放于机房和仓库中，机房和仓库工作人员应严格遵守相关的安全管理规定，所有涉密设备未经单位领导批准，一律不许带出。
17. 密钥存放在机房核心区保密柜的保密抽屉中，保密柜必须由两个管理员才能打开，保密抽屉的钥匙由领导保管，必须有三个上述的人员同时到场才可以取出密钥。
18. 实行严格的出入库管理。对所有单位设备，详细登记设备的生产单位的单位名称、法定代表人、组织机构代码以及设备的名称、型号及数量。

19. 定期和不定期的进行设备清查，所有的清查盘点必须记录在案。
20. 商用密码产品发生故障，必须由国家密码管理机构指定的单位维修。
21. 设备的报废须填写《设备报废申请表》，一般设备经维修部门和有关人员技术鉴定，出具报废鉴定证明，部门主管同意，领导批准，由单位统一回收和处理。报废、销毁商用密码产品，应当向国家密码管理机构备案。

密码安全管理制度

第一章 总则

1. 为了加强密码设备管理工作，确保安全使用密码，根据《中华人民共和国密码法》、《商用密码管理条例》、《信息系统密码应用基本要求》等国家有关法规规定，制定本制度。
2. 单位涉及密码管理、使用和运维等相关人员均需遵守本规定。

第二章 密码使用管理要求

3. 厅信息办公室统筹业务系统密码应用，执行统一规划、统一建设、统一管理和集中运维，各使用单位按规定流程申请密码资源。
4. 使用单位应当严格遵守相关保密制度，保管好个人数字证书，不得出借或使用他人证书登录信息系统。
5. 个人数字证书介质一旦丢失，应立即进行挂失，并按规定流程到证书发放机构申请新的证书和介质。

第三章 密码设备维护规定

6. 密码设备维护人员需经过培训，取得相关资质才能上岗，并需严格按照设备维护规范和使用说明开展维护工作。

7. 密码设备应当按照要求定期完成设备巡检、升级和维保工作，至少每半年集中检查一次，密码设备操作必须经过授权，且不得接入互联网访问。
8. 建立密码设备故障和应急保障机制，定期开展应急演练，确保设备发生故障时能及时恢复。
9. 加强密码设备的日常监控，评估系统安全风险，及时进行扩容和升级。

第四章 密码使用责任认定

10. 密码使用单位应当建立密码管理责任人，指定专人与市卫健局规信处对接，落实信息系统密码应用工作。
11. 密码使用单位应严格遵循相关要求使用密码技术完善系统的安全保护功能，因密码使用不当导致信息泄密、数据破坏的，追究相关单位密码管理部门和管理人员责任，并按要求整改。

第五章 人员考核

12. 由密码安全领导小组对本单位使用密码情况进行年度检查，并纳入责任单位相关人员考核。
13. 在当年密码应用考核中被处理的，原则上取消当年评优评先资格。
14. 在当年密码应用考核中表现突出的，按照相关规定给予表彰、评优评先。

第六章 密码安全培训

15. 定期举行密码安全培训，包括国家政策、法规、密码技术、设备培训、安全保密、使用培训等。
16. 一般人员培训应每年举行一次，设备维护培训不定期举行。

4、实施

完成密码应用方案编制后，用户单位可以委托密评机构对本方案进行评估，评估通过后，将本系统密码应用改造方案向用户单位所属地密码管理部门备案，并同步对业务信息系统进行密码应用改造，选用通过检测认证合格的商用密码产品，合规、正确、有效的建设密码保障系统。

依据评估通过的密码应用方案改造完成后，用户单位可以委托密评机构对业务信息系统进行密评，密评通过后上线运行，上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

5.4.4.3. 应急保障措施

1、组织保障

切实发挥好建设工作领导小组牵头协调作用，加强宏观指导，及时研究解决工作推进中的重大问题，推动工作高效开展。统筹规划、统一部署、协调推进，不断提高项目建设工作水平。建立主要领导负责制，加强项目工作力量的协调，构建统一领导、上下衔接、统筹有力的组织体系，充分落实项目建设工作，保障项目建设顺利推进。

2、人员保障

营造良好的学习实践环境，加强项目人才队伍建设，积极培养既精通业务又能运用互联网技术和信息化手段开展工作的综合型人才。将项目建设列入各部门和项目组成员学习培训内容，建立普及性与针对性相结合的培训机制，提高建

设意识和素质。强化互联网宣传，提升公众参与度，充分利用电视、广播、报刊、互联网等各类媒体，广泛宣传项目建设、服务新理念、新做法，加强对项目建设的舆论引导，积极协调高水平人才参与项目建设过程中。

3、应急

根据《基本要求》中安全管理应急方面的要求，对业务信息系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施；针对密码安全方面的应急响应措施包括：当业务信息系统发生密码相关安全事件时，在事发后 3 小时内向用户主管单位进行报告；事件处置完成后 2 个工作日内，向用户主管单位汇报安全事件发生情况及处置情况。

5.4.5. 安全合规分析

表 41 密码应用合规对照表

指标要求	密码技术应用点	采取措施	标准符合性(符合/不适用)	说明(针对不适用项说明原因及替代性措施)
物理和环境安全	身份鉴别	采用安全门禁卡和	符合	
	电子门禁记录数据存储完整性	读卡器实现进出机房人员身份的真实性	符合	

		安全门禁系统采用消息鉴别码技术保障电子门禁记录数据存储完整性		
	视频监控记录数据存储完整性	采用国密 NVR 保障视频记录数据存储完整性	符合	
网络和通信安全	身份鉴别	采用智能密码钥匙、国密浏览器、SSLVPN 保障通信实体身份鉴别、接入设备安全认证、通信数据机密性和完整性、访问控制信息的完整性	符合	
	通信数据完整性		符合	
	通信过程中重要数据的机密性		符合	
	网络边界访问控制信息的完整性		符合	
	安全接入认证		符合	
设备和计算安全	身份鉴别	采用智能密码钥匙、	符合	
	远程管理通道安全	国密浏览器、SSLVPN 实现登录设备用户	符合	

全		份鉴别、远程管理通道安全		
	重要信息资源安全标记完整性	系统不涉及	不适用	系统不涉及
	系统资源访问控制信息完整性	采用智能密码钥匙、服务器密码机实现重要数据的完整性	符合	
	日志记录完整性		符合	
	重要可执行程序完整性、重要可执行程序来源真实性		符合	
应用和数据安全	身份鉴别	采用身份认证系统、移动终端智能密码模实现应用用户身份鉴别	符合	
	重要信息资源安全标记完整性	系统不涉及	不适用	系统不涉及
	重要数据传输机密性	采用国密浏览器、	符合	
	重要数据传输完整性	SSLVPN 保障重要数据传输的机密性和	符合	

		完整性		
	重要数据存储机密性	采用数据加解密服务平台实现重要数据存储的机密性保护	符合	
	访问控制信息完整性	采用电子文件安全	符合	
	重要数据存储完整性	验证系统实现重要数据存储的完整性	符合	
	不可否认性	保护、关键操作行为的不可否认	符合	

5.4.6. 密改方案效果

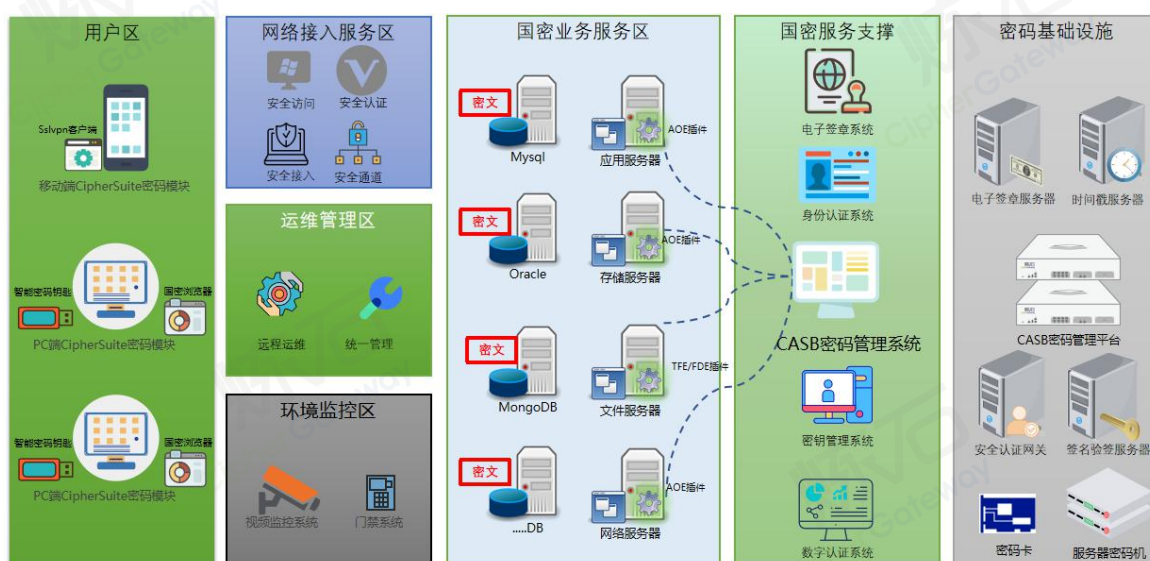


图 108 方案效果图

5.4.6.1. 以应用为抓手的数据安全密码防护体系

通过开发改造目标应用系统的方式来实现数据安全防护，需要投入大量的工作，而且已经上线运行的系统经过安全底层的改造，势必带来较大的风险，会影响到正常业务的开展。

将安全代理技术应用于本地应用中，可以在不改造应用的情况下，提供面向服务侧的数据存储加密、面向用户侧的动态脱敏及审计，以应用为抓手，打造“以密码技术为核心、多种技术相互融合的新数据安全防护体系”。

5.4.6.2. “主体到应用内用户、客体到字段”的权限细控

现有的应用系统访问控制粒度较粗，无法达到精细化管理的目的。将访问的客体精细到数据库中的字段或者存储系统中的文件，将数据访问的主体识别到具体应用中的用户，将加解密技术和访问控制技术相结合，在用户使用经过加密的数据时，都要回到应用中进行解密，而要解密就要先验证用户的身份，同时将用户的操作进行审计，这样就形成了无法绕过的细粒度安全访问控制。

5.4.6.3. 面向切面加密技术实现敏捷项目实施

实现面向切面的数据加密技术，在无需改造应用系统代码逻辑的前提下，将应用服务中的数据操作进行包装，使得经过此“切面”的所有数据操作都可以被进行过滤和加工，实现入库的数据的加密，读取库中的数据进行解密，与后端的数据库品牌或版本无关，可以完全解耦数据库。同时对于经过此切面的数据，可以进行“加工”，实现结合用户身份的动态脱敏。

5.4.6.4. 国密算法实现的高性能优化

高性能国密软件在保证了国密算法性能满足应用的同时,也符合国家对算法合规要求,保障密码技术自主可控。

CASB 业务数据加密平台支持国密 SM 系列算法,在单 CPU 上,国密 SM4 加解密速度突破 130Gbps,加密 10 亿条手机号仅耗时 20 秒(即每秒 5000 万条)。高性能密码实现保障信息系统的业务效率。此外,数据安全解决方案在目标应用服务器上完成数据加解密执行,不占用数据库服务器资源,对系统整体性能的影响较小。

5.4.6.5. 应用免改造,保障业务不中断

本国密改造方案既无需开发改造应用,也无需适配数据库,仅通过修改配置文件即可完成 AOE/TFE 插件的部署,实施简便快捷,不影响业务连续性。

1. 兼容复杂系统环境

CASB 业务数据加密平台能兼容多种数据库例如 Oracle、SQL Server、MySQL、PostgreSQL、MongoDB、人大金仓、达梦、大数据存储等,支持 char、varchar、clob、blob、json 等字段,支持数据库分库分表功能、ETL 采集数据加密及模糊查询功能,且支持结构化数据和非结构化数据的加密保护,满足数据加密的多种需求。

2. 实施成本低

CASB 业务数据加密平台同时支持云化、虚拟化、实体机等部署环境，且无需对每个应用系统和数据库进行适配，对于信息系统多、环境复杂的系统，该方案能大大降低实施成本。

5.4.6.6. 提供应用数据加密统一集中的数据安全管理平台

通过统一的数据安全管理平台，支持集中式管控、分布式部署、分阶段实施，政府管理者能够对分散于各信息系统中的重要数据进行统一的加密保护，实时掌握多个应用系统运行状况，对应用中所有数据加解密状态情况实现统一管理和监控，在提高安全性的同时，大大降低运维和管理成本。

5.4.7. 密改设备清单

表 42 密改软硬件设备建设清单

序号	品目名称	规格要求	数量	单位
1	智能密码 钥匙	系统用户/管理员登录身份鉴别，存储用户秘密信息 数字证书和私钥，完成数据加解密、完整性校验、 数字签名、访问控制等功能。	按需	个
2	国密 SSL、 IPSec VPN VPN 安全	用于 SSL 安全通道建立，配合 PC 端部署的国密浏览器，实现 PC 端到服务端之间数据传输机密性保护 实现服务端到服务端之间数据传输机密性保护，采用国密算法。	2	台

	网关			
3	国密浏览器	用于 SSL 安全通道建立，采用国密算法，服务端安全验证、客户端安全浏览。	按需	套
4	签名验签服务器	提供数字证书的数字签名、验证签名功能，支持与 CA 连接、应用管理（分配访问权限）、证书管理等功能。	2	台
5	时间戳服务器	为关键业务节点提供可信时间。	2	台
6	数字证书认证系统	证书生命周期管理，主要为设备/用户的身份鉴别提供真实性、身份验证、签名验签等信任服务。为设备/用户的身份鉴别提供真实性服务系统。	1	套
7	服务器密码机	用于密钥产生、密码运算、设备管理对重要业务数据进行存储机密性、完整性保护，密码运算服务。	2	台
8	加密插件	提供应用系统数据加解密算力，部署在应用服务器上，实现对数据安全和身份鉴别、访问控制等防护。针对结构化数据，对敏感信息等关键数据字段进行加密；针对非结构化数据，重要文件，图片等关键数据进行加密；实现关键数据的安全存储。对重要业务数据进行存储机密性、完整性保护，密码运算服务。提供高性能密码计算。	按需	个

9	<p>密钥管理与数据加密及认证平台</p>	<p>提供密钥生成、密钥派发、密钥存储等密钥管理系统支撑平台，提供加解密策略管理。密钥管理等安全能力的综合型硬件密码设备，为密码数据安全模块提供管理与支撑能力，并能与统一密钥管理中心交互实现全局管控。</p>	2	台
---	-----------------------	--	---	---

6. 附录

6.1. 密码基本知识

本节简要介绍密码的概念和作用，指出密码需要合规、正确、有效地使用，并对密码技术的核心内容：密码算法、基于密码的认证、密钥管理、密码协议、密码功能进行介绍。^[56]

6.1.1. 密码算法

现代密码学理论中，算法是密码技术的核心，常见的密码算法包括：对称密码算法、公钥密码算法和摘要密码算法。

6.1.1.1. 对称密码算法

对称密码算法加密过程与解密过程使用相同的或容易相互推导得出的密钥，即加密和解密两方的密钥是“对称”的。早期的密码算法都是对称形式的密码算法。对称密码加密和解密基本流程如下图所示。用户通过加密算法将明文变换为密文。只有掌握了同一个密钥和对应解密算法的用户才可以将密文逆变换为有意义的明文。

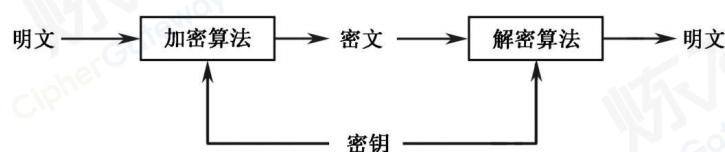


图 109 对称密码加密和解密基本流程

针对不同的数据类型和应用环境,对称密码有两种主要形式:一是序列密码,二是分组密码。

1. 序列密码和分组密码

(1) 序列密码和分组密码的区别

序列密码和分组密码都属于对称密码,区别在于序列密码是将密钥和初始向量作为输入,通过密钥流生成算法输出密钥流,然后将明文序列和密钥流进行异或,得到密文序列。分组密码首先对明文消息根据分组大小进行分组,再将明文分组、密钥和初始向量一起作为输入,通过分组加密算法直接输出密文分组。

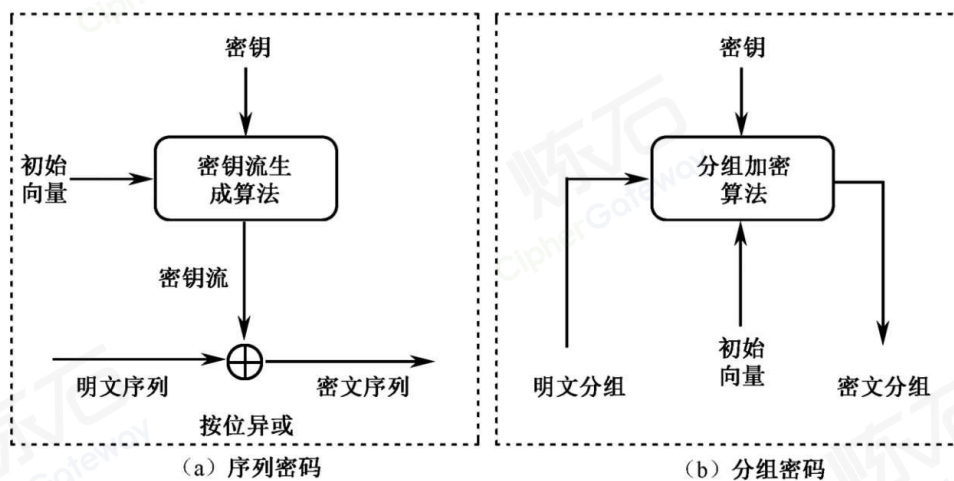


图 110 序列密码和分组密码的加密流程

(2) 初始向量

在对称密码的实际应用场景中,初始向量是一个在加密过程中起到引入随机性作用的随机数,即在加密一批明文数据之前,加密方先要随机生成一个初始向量,并将它和密钥一起输入到加密算法中。每次加密初始向量都必须重新生成,

初始向量的引入使得多次分别对同一明文数据使用相同的密钥进行加密,得到的密文是不同的。

2. 分组密码的工作模式

我国于 2008 年发布了规定分组密码算法工作模式的国家标准 GB/T 17964-2008《信息安全技术 分组密码算法的工作模式》。在分组密码算法中,根据分组数据块链接的组合模式不同,可以分为以下七种工作模式:电码本(ECB)模式、密文分组链接(CBC)模式、密文反馈(CFB)模式、输出反馈(OFB)模式、计数器(CTR)模式、分组链接(BC)模式、带非线性函数的输出反馈(OFB/NL)模式、GCM 模式。本节重点介绍常用的 ECB、CBC、CTR、GCM 模式。

(1) ECB 模式

ECB 模式是一种最直接的消息加密方法, ECB 模式的加密和解密流程如下图所示。

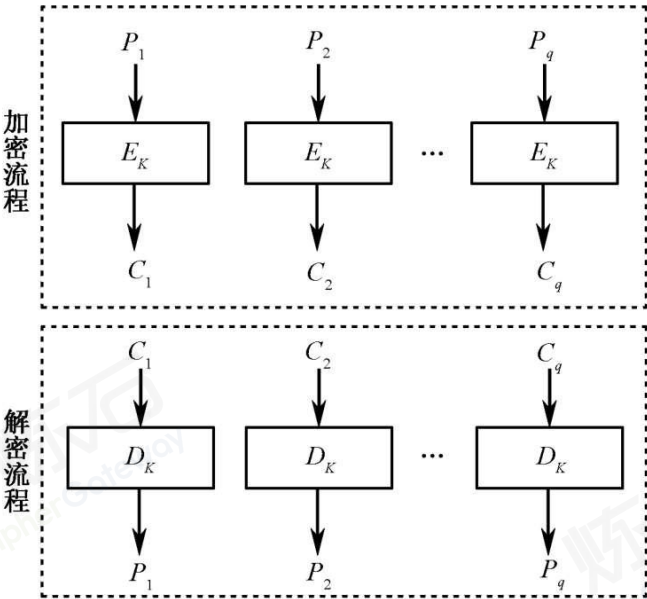


图 111 ECB 模式的加密和解密流程

可以看出 ECB 模式具有如下性质：

- 1) 对某一个分组的加密或解密可独立于其他分组进行；
- 2) 对密文分组的重排将导致明文分组的重排；
- 3) 不能隐蔽数据模式，即相同的明文分组会产生相同的密文分组；
- 4) 不能抵抗对分组的重放、嵌入和删除等攻击。因此，不推荐在应用中使用 ECB 模式。

(2) CBC 模式

在 CBC 模式下，每个明文分组在加密之前，先与反馈至输入端的前一组密文分组按位异或后，再送至加密模块进行加密。其中，IV 是一个初始向量，无须保密，但须随着消息的更换而更换，且收发双方必须选用同一个 IV。显然，计算的密文分组不仅与当前明文分组有关，而且通过反馈作用还与以前的明文分组有关。在解密过程中，初始值 IV 用于产生第一个明文输出；之后，前一个密文分组与当前密文分组解密运算后的结果进行异或，得到对应的明文分组。

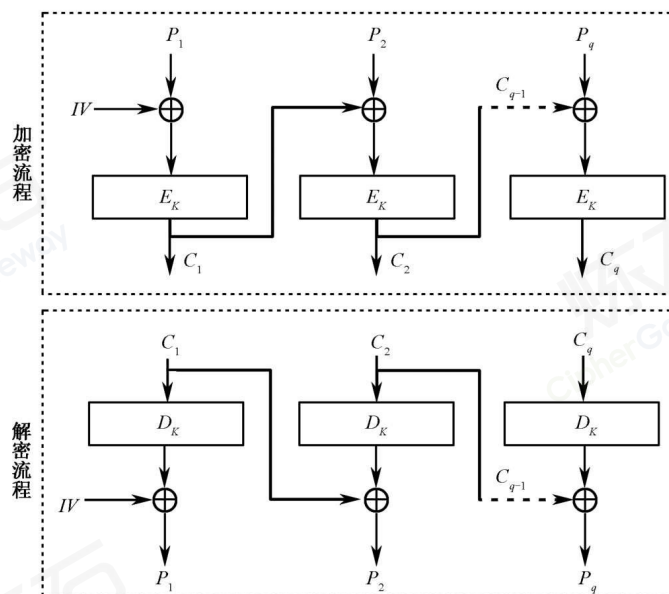


图 112 CBC 模式的加密和解密流程

CBC 模式具有如下性质：

- 1) 链接操作使得密文分组依赖于当前的和以前的明文分组，因此对密文分组的重新编排不会导致对相应明文分组的重新编排。
- 2) 加密过程使用 IV 进行了随机化，每次加密 IV 都必须重新生成，并且要保证 IV 的随机性。使用不同的 IV 可以避免 ECB 模式下每次对相同的明文使用相同的密钥加密生成相同的密文的弊端。
- 3) 加密过程是串行的，无法并行化；在解密过程中，通过两个相邻的密文分组执行解密操作可以获得明文分组，因此解密过程可以并行化。
- 4) 此外，CBC 模式还有一个重要用途：生成消息鉴别码（MAC），即使用最后一个分组的输出结果作为 MAC。MAC 可以用于检验消息的完整性、验证消息源的真实性等。

(3) CTR 模式

CTR 模式通过将逐次累加的计数器值进行加密来生成密钥流。CTR 模式的加密和解密流程如下图所示。

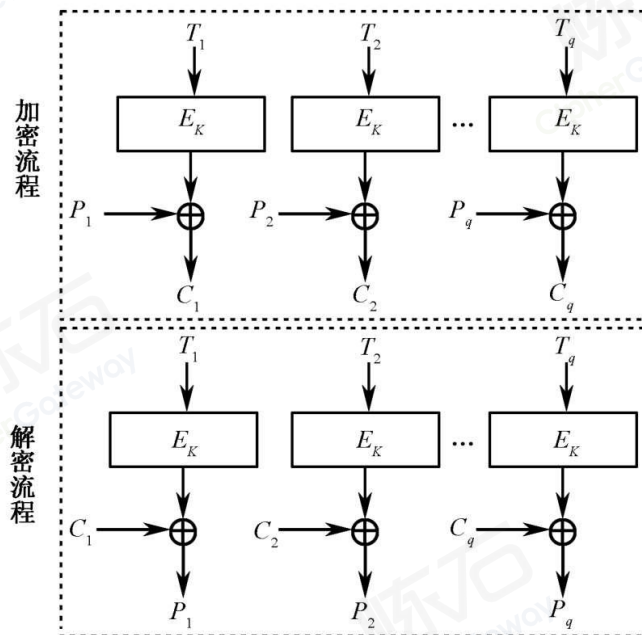


图 113 CTR 模式的加密和解密流程

此外，还有一种用法是将一个单独的 IV 与计数器值拼接在一起作为生成密钥流的输入分组，此时计数器值一般从 0 或 1 开始。需要注意的是，将 IV 与计数器值直接相加或异或后作为输入是不安全的，这样会导致选择明文攻击。

CTR 模式具有如下性质：

- 1) 支持加密和解密并行计算，可事先生成密钥流，进行加密和解密准备。
- 2) 只用到了分组密码算法的分组加密操作。
- 3) 错误密文中的对应比特只会影响解密后明文中的对应比特，即错误不会传播。

(4) GCM 模式

GCM 是认证加密模式中的一种，是遵循 EtM 方式（先加密后认证 Encrypt-then-MAC, EtM）在一个算法内部同时完成消息加密和 MAC 码计算的可认证加密模式，内部组合了 CTR 模式和 GMAC 算法。在实际应用场景中，有些信息是不需要保密，但信息的接收者需要确认它的真实性，例如源 IP，源端口，目的 IP 等。因此，可以将这一部分作为附加消息加入到 MAC 值的计算当中。下图的 E_k 表示用对称密钥 k 对输入做 SM4 加密。

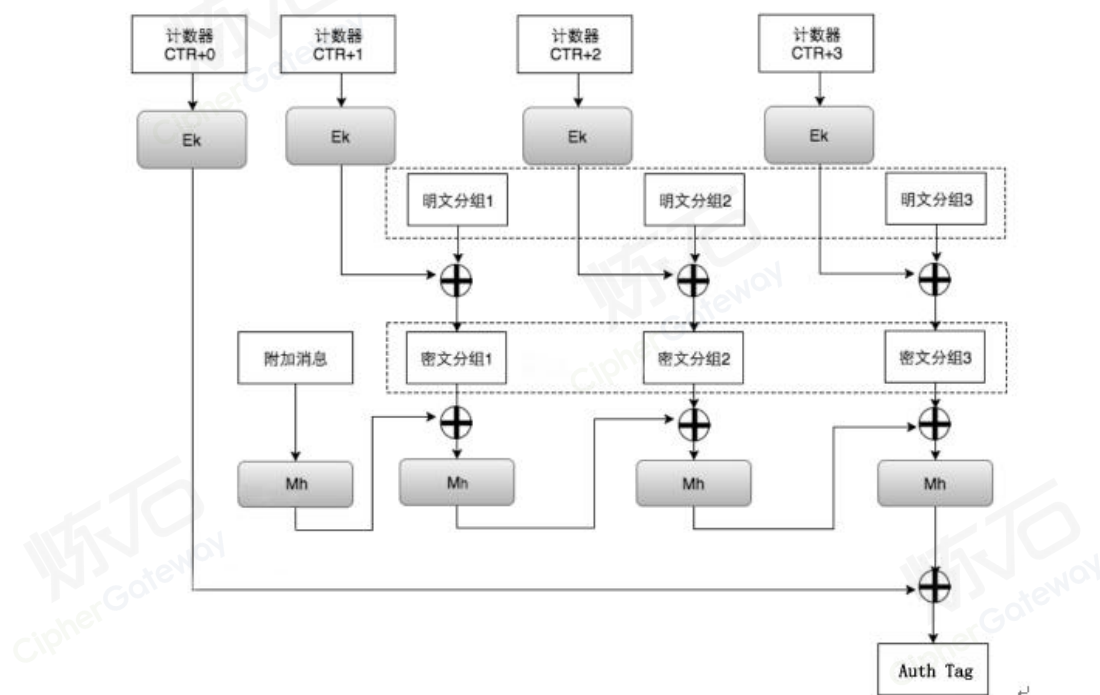


图 114 GCM 模式的加密流程

GCM 模式具有如下性质：

- 1) 能同时确保数据的保密性、完整性及真实性。
- 2) 可以提供附加消息的完整性校验。

3. ZUC 序列密码算法

ZUC（祖冲之密码算法）是我国发布的商用密码算法中的序列密码算法，可用于数据保密性保护、完整性保护等。

(1) ZUC 算法的结构

ZUC 算法由线性反馈移位寄存器（LFSR）、比特重组（BR）、非线性函数 F 三个基本部分组成，如图 7 所示。ZUC 算法结构在逻辑上分为上、中、下三层，其中上层是 16 级 LFSR，中间层是 BR，下层是非线性函数 F。

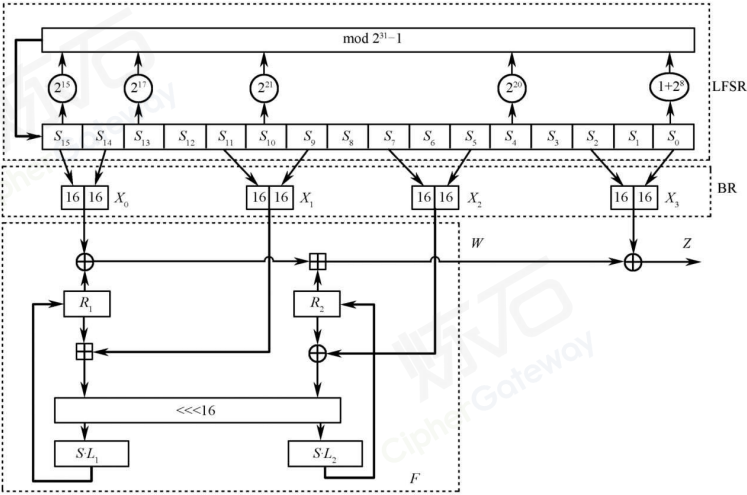


图 115 ZUC 算法结构

(2) ZUC 算法的使用

在生成密钥流时,ZUC 算法采用 128 比特的初始密钥和 128 比特的 IV 作为输入参数，共同决定 LFSR 里寄存器的初始状态。

(3) 基于 ZUC 的两种算法

- 1) 基于 ZUC 的机密性算法 128-EEA3。主要用于 4G 移动通信中移动用户设备和无线网络控制设备之间的无线链路上通信信令和数据的加密和解密。

- 2) 基于 ZUC 的完整性算法 128-EIA3。主要用于 4G 移动通信中移动用户设备和无线网络控制设备之间的无线链路上通信信令和数据的完整性校验，并对信令源进行鉴别。其主要技术手段是利用完整性算法 128-EIA3 产生 MAC，通过对 MAC 进行验证，实现对消息的完整性校验。

(4) ZUC 算法的安全性

ZUC 算法在设计中引入了素数域运算、比特重组、最优扩散的线性变换等先进理念和技术，体现了序列密码设计上的发展趋势。通过对其三层结构的综合运用，ZUC 算法具有很高的理论安全性，能够有效抵抗目前已知的攻击方法，具有较高的安全冗余，并且算法速度快，软/硬件实现性能都比较好。

4. SM4 分组密码算法

SM4 算法是我国发布的商用密码算法中的分组密码算法。为配合 WAPI 无线局域网标准的推广应用，SM4 算法于 2006 年公开发布，并于 2012 年 3 月发布为密码行业标准，2016 年 8 月转化为国家标准 GB/T 32907-2016《信息安全技术 SM4 分组密码算法》。

(1) SM4 算法描述

SM4 分组密码算法是一个迭代分组密码算法，数据分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构（非平衡 Feistel 结构）。Feistel 结构的特色是加密和解密的算法结构完全一致，在硬件实现上加密和解密使用完全相同的电路。解密过程只需要把加密过程中产生的轮密钥逆序排列就能从密文分组中恢复出明文分组。

迭代加密算法的基本结构如下图所示。明文分组经过迭代加密函数变换后的输出又成为下一轮迭代加密函数的输入，如此迭代 32 轮，最终得到密文分组。

每一轮迭代的函数是相同的，不同的是输入的轮密钥。

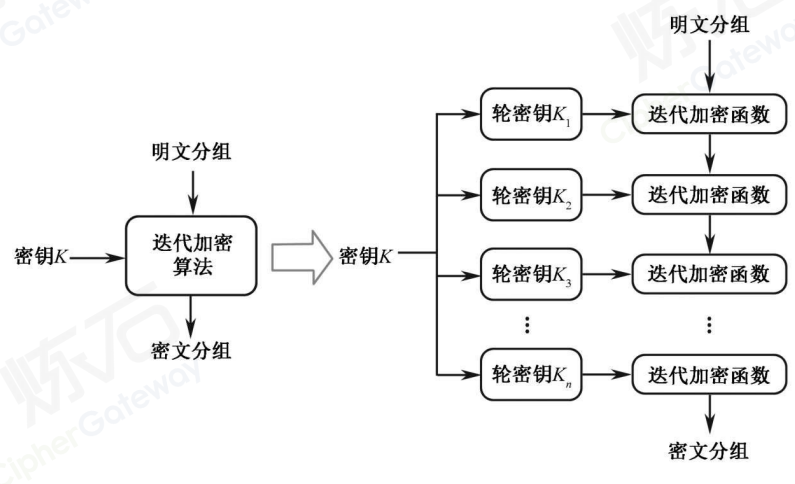


图 116 迭代加密算法的基本结构

SM4 算法中密钥扩展算法和加密算法的结构如下图所示。

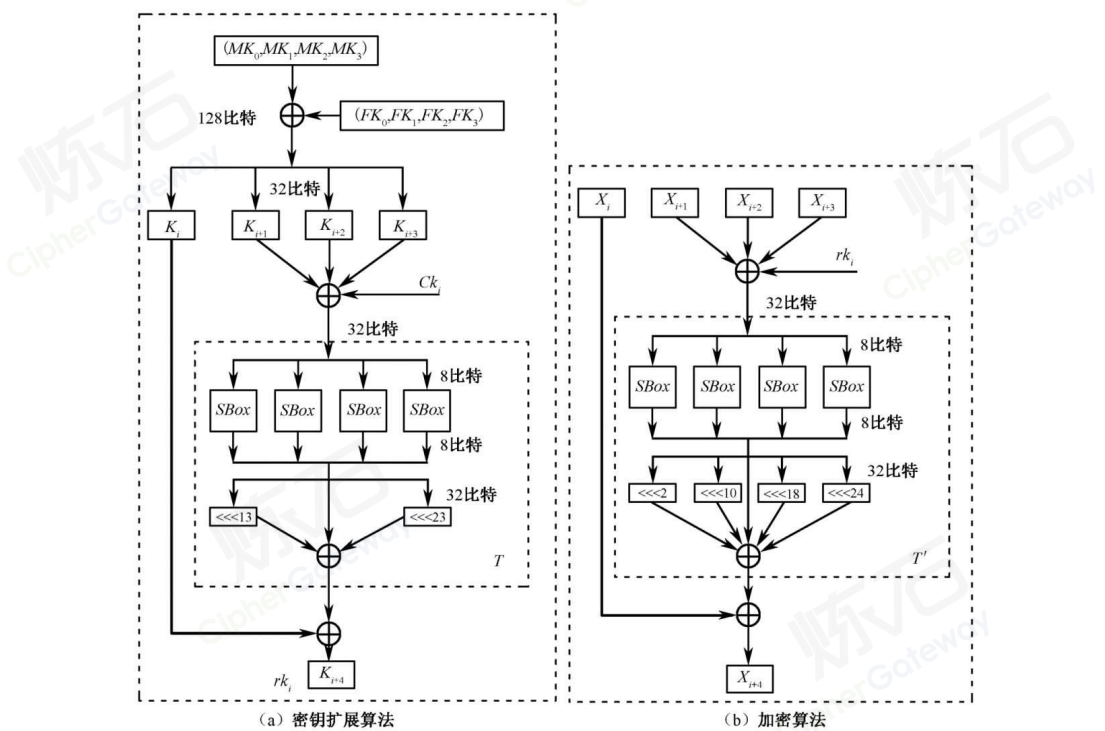


图 117 SM4 算法结构图

(2) SM4 算法的性能和安全性

SM4 算法具有安全高效的特点，在设计和实现方面具有以下优势：

- 1) 在设计上实现了资源重用，密钥扩展过程和加密过程类似。
- 2) 加密过程与解密过程相同，只是轮密钥使用顺序正好相反，它不仅适用于软件编程实现，更适合硬件芯片实现。
- 3) 轮变换使用的模块包括异或运算、8 比特输入 8 比特输出的 S 盒，还有一个 32 比特输入的线性置换，非常适合 32 位处理器的实现。

在安全性上，SM4 算法的密钥长度是 128 比特，其安全性与 AES-128 是相当的。在实现效率方面，由于 SM4 密钥扩展和加密算法基本相同，且解密时可以使用同样的程序，只需将密钥的顺序倒置即可。

5. 国外对称密码算法 AES

常见的国外对称密码算法主要有 DES、3DES 和 AES。本节将重点对目前使用最广泛的 AES 算法进行介绍。

AES 算法是美国联邦政府采用的一种分组密码算法标准，用来替代 DES 并被广泛使用。AES 算法的分组长度是 128 比特，密钥长度支持 128 比特、192 比特或 256 比特。支持不同密钥长度的 AES 算法分别用 AES-128、AES-192、AES-256 表示，三者密钥的长度不同，加密的轮数也不同。AES-128、AES-192 和 AES-256 的加/解密思路基本一样，只是密钥扩展算法的过程略有不同，加密和解密的轮数会适当增加，但加/解密的操作是一样的。

表 43 AES 基本特性

AES	密钥长度（比特）	分组长度（比特）	加密轮数
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

6.1.1.2. 非对称密码算法

非对称密码算法又称公钥密码算法，既可用于加密和解密，也可用于数字签名，打破了对称密码算法加密和解密必须使用相同密钥的限制，很好地解决了对称密码算法中存在的密钥管理难题。公钥密码算法包括公钥加密和私钥签名两种主要用途。SM2、SM9 算法是我国颁布的商用密码标准算法中的公钥密码算法，其中，基于 SM2 算法的数字签名技术已在我国电子认证领域广泛应用。

1. 公钥密码模型

公钥加密算法加密和解密使用不同的密钥。其中加密的密钥可以公开，称为公钥；解密的密钥需要保密，称为私钥。公钥、私钥是密切关联的，从私钥可推导出公钥，但从公钥推导出私钥在计算上是不可行的。

(1) 公钥加密算法

由于公钥密码运算操作计算复杂度较高，公钥加密算法的加密速度一般比对称加密算法的加密速度慢很多，因此公钥加密算法主要用于短数据的加密，如建立共享密钥。在执行公钥加密操作前，需要先查找接收者的公钥，然后用该公钥加密要保护的消息。当接收方接收到消息后，用自己的私钥解密出原消息。

(2) 数字签名算法

数字签名算法主要用于确认数据的完整性、签名者身份的真实性和签名行为的不可否认性等。与公钥加密算法使用公钥、私钥的顺序不同，数字签名使用私钥对消息进行签名，使用公钥对签名进行验证。

2. SM2 椭圆曲线公钥密码算法

SM2 椭圆曲线公钥密码算法（简称 SM2 算法）是基于椭圆曲线离散对数问题。由于基于椭圆曲线上离散对数问题的困难性要高于一般乘法群上的离散对数问题的困难性，且椭圆曲线所基于的域的运算位数要远小于传统离散对数的运算位数，因此，椭圆曲线密码体制比原有的密码体制更具优越性。

(1) 椭圆曲线密码基础知识

椭圆曲线上的两个基本运算是点加和倍点，它们用来构造点乘算法。点乘运算是椭圆曲线机制最核心，也是最耗时的运算。ECC 的数字签名、加密、密钥交换算法都要求计算椭圆曲线点乘运算，其计算效率直接决定着签名/验证、加/解密运算的速度。

(2) SM2 算法介绍

SM2 算法主要包括数字签名算法、密钥交换协议和公钥加密算法三个部分。

下面主要对 SM2 的数字签名算法、密钥交换协议和公钥加密算法进行介绍。

1) SM2 数字签名算法

在执行签名的生成过程之前，要用密码杂凑函数对用户的可辨别标识、部分椭圆曲线系统参数和用户的公钥杂凑值以及待签名消息进行压缩；在验证过程之前，要用密码杂凑函数对用户的可辨别标识、部分椭圆曲线系统参数和用户的公钥杂凑值及待验证消息进行压缩。

GB/T 32918.2-2016 规定了 SM2 数字签名算法，包括数字签名生成算法和验证算法，并给出了数字签名与验证示例及相应的流程，可以满足多种密码应用中的身份鉴别和数据完整性、信息来源真实性的安全需求。

2) SM2 密钥交换协议

密钥交换，又称密钥协商，是两个用户 A 和 B 通过交互的信息传递，用各自的私钥和对方的公钥来商定一个只有他们知道的秘密密钥。这个共享的秘密密钥通常用在对称密码算法中。

GB/T 32918.4-2016 规定了 SM2 密钥交换协议，并给出了密钥交换与验证示例及相应的流程，可满足通信双方经过两次或可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。

3) SM2 公钥加密算法

GB/T 32918.3-2016 规定了 SM2 公钥加密算法，并给出了消息加密和解密示例以及相应的流程。

(3) SM2 算法的安全性和效率

以 SM2 公钥加密算法为例，它的安全性主要体现在三个方面：

- 1) 算法具备单向性，即未授权的第三方在未得到私钥的情况下，从密文计算出明文在计算上是不可行的；
- 2) 算法产生的明文和密文具备不可区分性，即恶意第三方对于给定的密文无法区分出其是由给定的两个明文中的哪一个加密而来；
- 3) 密文具备不可延展性，即第三方无法在不解密密文的前提下，通过简单扩展密文来构造出新的合法密文。
- 4) 与 RSA 算法相比，SM2 算法具有以下优势：
 - 安全性高。256 比特的 SM2 算法密码强度已超过 RSA-2048，与 RSA-3072 相当。
 - 密钥短。SM2 算法使用的私钥长度为 256 比特，而 RSA 算法通常至少需要 2048 比特，甚至更长。
- 5) 私钥产生简单

RSA 私钥产生时需要用到两个随机产生的大素数，除了需要保证随机性外，还需要用到素数判定算法，产生过程复杂且速度较慢；而 SM2 私钥的产生只需要生成一个一定范围内的 256 比特的随机数即可，因此产生过程简单，存在的安全风险也相对较小。

6) 签名速度快

同等安全强度下，SM2 算法在用私钥签名时，速度远超 RSA 算法。

(4) SM2 算法的使用

为规范 SM2 算法的使用，2012 年我国发布了 GM/T 0009-2012《SM2 密码算法使用规范》和 GM/T 0010-2012《SM2 密码算法加密签名消息语法规范》，2017 年发布更新版本国家标准 GB/T 35276-2017《信息安全技术 SM2 密码算法使用规范》和国家标准 GB/T 35275-2017《信息安全技术 SM2 密码算法加密签名消息语法规范》。这些标准为 SM2 密码算法的使用制定了统一的数据格式和使用方法。

GM/T 0009-2012 定义了 SM2 算法的密钥数据格式、加密数据格式、签名数据格式和密钥对保护数据格式，并对生成密钥、加密、解密、数字签名、签名验证、密钥协商等计算过程进行了规范。GM/T 0010-2012 定义了使用 SM2 密码算法的加密签名消息语法。

3. SM9 标识密码算法

标识密码（IBC）是在传统的公钥基础设施（PKI）基础上发展而来的，除了具有 PKI 的技术优点外，主要解决了在具体安全应用中 PKI 需要大量交换数字证书的问题，使安全应用更加易于部署和使用。

2016 年，我国发布了标识密码算法标准 GM/T 0044-2016《SM9 标识密码算法》。同 SM2 数字签名算法一起，SM9 数字签名算法也在 2017 年被 ISO 采纳，成为国际标准 ISO/IEC 14888-3 的一部分。

(1) SM9 算法介绍

1) SM9 算法采用的基本技术

SM9 密码算法涉及有限域和椭圆曲线、双线性对及安全曲线、椭圆曲线上双线性对的运算等基本知识和技术。SM9 密码算法的应用与管理不需要数字证书、证书库或密钥库。

2) SM9 数字签名算法

用椭圆曲线对实现的基于标识的数字签名算法包括数字签名生成算法和验证算法。签名者持有一个标识和一个相应的私钥，该私钥由密钥生成中心通过主私钥和签名者的标识结合产生。签名者用自身私钥对数据产生数字签名，验证者用签名者的标识生成其公钥，验证签名的可靠性，即验证发送数据的完整性、来源的真实性和数据发送者的身份。

3) SM9 密钥交换协议

该协议可以使通信双方通过对方的标识和自身的私钥经两次或可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。该秘密密钥可作为对称密码算法的会话密钥，协议中可以实现密钥确认。

4) SM9 密码密钥封装机制和加密算法

密钥封装机制使得封装者可以产生和加密一个秘密密钥给目标用户，而唯有目标用户可以解封装该秘密密钥，并把它作为进一步的会话密钥。用椭圆曲线对实现基于标识的密钥封装机制，封装者利用解封装用户的标识产生并加密一个秘密密钥给对方，解封装用户则用相应的私钥解封装该秘密密钥。用椭圆曲线对实现的基于标识的加密与解密算法，使消息发送者可以利用接收者的标识对消息进行加密，唯有接收者可以用相应的私钥对该密文进行解密，从而获取消息。

5) SM9 密码算法参数定义

SM9 密码算法使用 256 比特的 Barreto–Naehrig(BN)曲线。该算法标准的第 5 部分定义了曲线参数，并给出了数字签名算法、密钥交换协议、密钥封装机制、公钥加密算法示例。

(2) SM9 算法的安全性和效率

目前，没有发现明显影响双线性对密码系统应用的安全性风险。SM9 密码算法能够避免弱椭圆曲线的选取问题，并抵抗常见的针对椭圆曲线的攻击方式，安全性远远高于同类算法。

4. 国外公钥密码算法 RSA

常见的国外公钥密码算法有 RSA、椭圆曲线数字签名算法等。下面重点对 RSA 进行介绍。

(1) RSA 算法简介

RSA 算法基于大整数因子分解难题设计，因其原理清晰、结构简单，是第一个投入使用，也是迄今为止应用最广泛的公钥密码算法，可用于数字签名、安全认证等。1992 年，RSA 算法纳入了国际电信联盟制定的 X.509 系列标准。RSA 算法的公钥相当于两个素数的乘积，而私钥则相当于两个独立的素数。

(2) 算法安全性和效率

需要注意的是，1024 比特及以下密钥长度的 RSA 算法目前已经不推荐使用。在当前应用中，为保证安全，应该至少选用 RSA-2048 算法。在效率方面，由于

达到相当安全强度时，RSA 密钥长度要远长于 ECC 算法，因此私钥计算的执行效率要比 ECC 算法慢数倍。

6.1.1.3. 摘要算法

摘要算法也称作“杂凑算法”、“散列算法”或“哈希算法”。密码摘要算法对任意长度的消息进行压缩，输出定长的消息摘要或杂凑值。

一般来说，摘要算法具有如下性质：

- (1) 抗原像攻击：摘要函数是单向的，从消息计算杂凑值很容易，但从杂凑值推出消息是困难的。
- (2) 抗第二原像攻击：输入的任何微小变化都会使摘要结果有很大不同。
- (3) 强抗碰撞性：要发现不同的输入映射到同一输出在计算上是困难的。

1. 密码摘要算法的结构

摘要算法有多种构造方式，常用的是 M-D 结构、海绵结构。MD5、SHA-1、SHA-2 和我国的 SM3 都采用了 M-D 结构，SHA-3 采用的是海绵结构。下面主要对 M-D 结构进行简要介绍。

M-D 结构，先对经过填充后的消息进行均匀的分组，而后消息分组顺序进入压缩函数 F，如图 10 所示。压缩函数 F 先由初始向量进行初始化，结合上一组消息的结果和本组消息产生一个中间值，最后一个压缩函数的结果即是最终的摘要值。这样，很长的消息也很容易被压缩到一个固定的比特长度。它的安全性取决于压缩函数的安全性。研究表明，如果压缩函数具有抗碰撞能力，那么摘要算

法也具有抗碰撞能力。因此，要设计安全摘要函数，最重要的是设计具有抗碰撞能力的压缩函数。

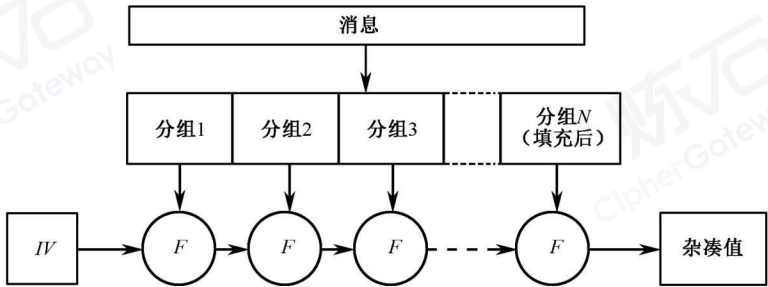


图 118 M-D 结构

2. 密码摘要算法的应用

密码摘要算法的直接应用就是产生消息摘要，进一步可以检验数据的完整性，被广泛应用于各种不同的安全应用和网络协议中。例如，用户收到消息后，计算其摘要值，并与发送方提供的结果做比对，如果二者一致，则基本认为消息在传送过程中没有遭到篡改。

需要注意的是，单独使用摘要算法并不能保证数据的完整性，因为在传输信道不安全的情况下，攻击者可以将消息和摘要值一同篡改，即在修改或替换消息后重新计算一个摘要值。因此，用于完整性保护时，摘要算法常常与密钥一同使用，生成的摘要值称为 MAC，这样的摘要算法称为带密钥的摘要算法。此外，摘要算法也与公钥密码算法一同使用来产生数字签名。

3. SM3 密码摘要算法

我国商用密码标准中的密码摘要算法是 SM3 算法。SM3 于 2012 年发布为密码行业标准 GM/T 0004-2012《SM3 密码杂凑算法》，并于 2016 年转化为国家标

准 GB/T32905-2016《信息安全技术 SM3 密码杂凑算法》。2018 年 10 月，SM3 算法正式成为国际标准。

(1) SM3 算法介绍

SM3 算法采用 M-D 结构，输入消息经过填充、扩展、迭代压缩后，生成长度为 256 比特的摘要值。SM3 算法的实现过程主要包括填充分组和迭代压缩等步骤。

(2) SM3 算法的安全性和效率

SM3 算法在 M-D 结构的基础上，新增了 16 步全异或操作、消息双字介入、加速雪崩效应的 P 置换等多种设计技术，能够有效避免高概率的局部碰撞，有效抵抗强碰撞性的差分分析、弱碰撞性的线性分析和比特追踪等密码分析方法。公开文献表明，SM3 算法能够抵抗目前已知的攻击方法，具有较高的安全冗余。在实现上，SM3 算法运算速率高，灵活易用，支持跨平台的高效实现，具有较好的实现效能。

SM3 算法在结构上和 SHA-256 相似，消息分组大小、迭代轮数、输出长度均与 SHA-256 相同。但相比于 SHA-256，SM3 算法增加了多种新的设计技术，从而在安全性和效率上具有优势。在保障安全性的前提下，SM3 算法的综合性能指标与 SHA-256 在同等条件下相当。

(3) HMAC

HMAC 是利用摘要算法，将一个密钥和一个消息作为输入，生成一个消息摘要作为输出。HMAC 可用作数据完整性检验，检验数据是否被非授权修改；也可用作消息鉴别，保证消息源的真实性。例如，IPSec 和 SSL 协议中均用到了 HMAC，

将其用于完整性校验和数据源身份鉴别。我国国家标准 GB/T 15852.2-2012《信息技术安全技术消息鉴别码第 2 部分：采用专用杂凑函数的机制》对 HMAC 算法进行了规范。

4. 国外摘要算法

常见的国外摘要算法有 MD5 密码摘要算法和安全摘要算法系列算法。SHA 系列算法主要包括 SHA-0、SHA-1、SHA-2 和 SHA-3。

MD5 算法：MD5 算法可用于数字签名、完整性保护、安全认证、口令保护等。MD5 算法首先将输入的信息划分成若干个 512 比特的分组，再将每个分组划分成 16 个 32 比特的子分组，经一系列变换后，最终输出 128 比特的消息摘要。根据王小云教授提出的分析方法，2005 年国际密码学家给出了 MD5 算法的碰撞实例，后来又成功伪造了 SSL 数字证书。目前，一部智能手机仅用 30 秒就可以找到 MD5 算法的碰撞。这些研究成果的碰撞案例表明 MD5 算法已不再适合实际应用。

SHA-1 算法：

SHA-1 设计思想基于 MD4 算法，在很多方面也与 MD5 算法有相似之处，其输入长度应小于 2^{64} 比特，消息摘要长度为 160 比特。2005 年，我国王小云教授首次给出了 SHA-1 的碰撞攻击，复杂度为 2^{69} 次运算。

2017 年 2 月，荷兰计算机科学与数学研究中心和谷歌研究人员合作找到了世界首例针对 SHA-1 算法的碰撞实例，生成了两个 SHA-1 算法消息摘要完全相同但内容截然不同的文件，针对 SHA-1 算法的攻击从理论变为现实，继续使用 SHA-1 算法存在重大安全风险，这标志着 SHA-1 算法继 MD5 算法后也将退出历

史舞台。2017 年 4 月，国家密码管理局发布了使用 SHA-1 密码算法的风险警示，要求相关单位遵循密码国家标准和行业标准，全面支持和应用 SM3 等密码算法。

SHA-2 算法：

SHA-2 算法虽然也是基于 M-D 结构，但是增加了很多重大变化以提升安全性。SHA-2 算法支持 224、256、384 和 512 比特四种长度的输出，包含 6 个算法：SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256。其中，SHA-256 和 SHA-512 是主要算法，其他算法都是在这两者基础上输入不同初始值，并对输出进行截断。目前没有发现对 SHA-2 算法的有效攻击。

SHA-3 算法：

与 MD5、SHA-1、SHA-2 算法等采用经典 M-D 结构不同，SHA-3 算法在设计上采用了新的结构——“海绵”结构。与 SHA-2 算法类似，SHA-3 算法也包含多个算法：SHA3-224、SHA3-256、SHA3-384、SHA3-512、SHAKE128、SHAKE256。

6.1.2. 密码协议

保障信息的安全不能单纯依靠安全的密码算法，还需要通过安全的密码协议在实体之间安全地分配密钥或其他秘密信息，以及进行实体之间的鉴别等。密码协议是指两个或两个以上参与者使用密码算法时，为达到加密保护或安全认证目的而约定的交互规则。

6.1.2.1. 密钥交换协议

在使用对称密码进行保密通信之前，必须向通信双方分发密钥使得双方共享密钥。然而在公钥密码出现之前通信双方建立共享密钥是一个困难问题。相对于对称密码，公钥密码的一个优点就是可以在不安全的信道上进行密钥交换。密钥交换协议旨在让两方或者多方在不安全的信道上协商会话密钥，从而建立安全的通信信道。

1. Diffie-Hellman 密钥交换协议

1976 年 Diffie 和 Hellman 提出公钥密码学概念，并提出了著名的 Diffie-Hellman 密钥交换协议。用户 A 和用户 B 之间的 Diffie-Hellman 密钥交换协议如下图所示。

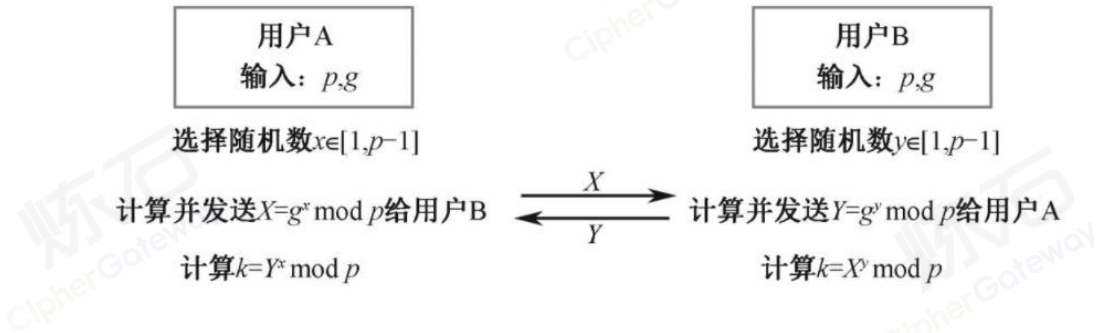


图 119 经典 Diffie-Hellman 密钥交换协议

然而，Diffie-Hellman 密钥交换协议只能提供建立会话密钥的功能，并不能抵抗中间人攻击，同时也不能提供相互鉴别的安全保障。

2. MQV 密钥交换协议

在经典 Diffie-Hellman 密钥交换协议的基础上, MQV 密钥交换协议在协议交互过程中用到了双方公钥信息, 只有拥有相应私钥的用户才能计算出与对方相同的会话密钥, 从而达到隐式鉴别的效果。

3. SM2 密钥交换协议

SM2 密钥交换协议为 MQV 的一个变种, 同样具有鉴别通信双方身份真实性的功能。该协议可满足通信双方经过两次信息传递过程, 计算并获取一个由双方共同决定的会话密钥。

6.1.2.2. 实体鉴别协议

实体鉴别机制用于证实某个实体就是他所声称的实体, 待鉴别的实体通过表明它确实知道某个秘密来证明其身份。我国国家标准 GB/T 15843 规定了进行实体鉴别的机制, 这些机制定义了实体间的信息交换, 以及需要与可信第三方的信息交换。

实体鉴别应用机制包括单向鉴别和相互鉴别两种。单向鉴别是指使用该机制时两实体中只有一方被鉴别, 相互鉴别是指两个通信实体运用相应鉴别机制对彼此进行鉴别。其中单向鉴别按照消息传递的次数, 又分为一次传递鉴别和两次传递鉴别; 相互鉴别根据消息传递的次数, 分为两次传递鉴别、三次传递鉴别或多次传递鉴别。如果采用时间值或序号, 则单向鉴别只需一次传递, 而相互鉴别则需两次传递; 如果采用使用随机数的“挑战—响应”方法, 单向鉴别需两次传递, 相互鉴别则需三次或四次传递 (依赖于所采用的机制)。

6.1.2.3. 综合密码协议

IPSec 协议和 SSL 协议是两个较为综合的密码协议，支持采用多种密码技术为通信交互中的数据提供全面安全保护，包括数据保密性、完整性校验、数据源身份鉴别和抗重放攻击等。不同的是，IPSec 工作在网络层，而 SSL 工作在应用层和传输层之间。IPSec 一般用于两个子网之间的通信，称为站到站的通信；SSL 一般用于终端到子网之间的通信，称为端到站的通信。

1. IPSec

IPSec 协议是国际组织 IETF 以 RFC 形式公布的一组 IP 密码协议集，其基本思想是将基于密码技术的安全机制引入 IP 协议中，实现网络层的通信安全。IPSec 最初是针对 IPv6 网络环境开发的，却首先在 IPv4 网络中广泛部署。考虑到当前网络设备对 IPSec 协议实现的兼容性，目前 IPSec 在 IPv4 和 IPv6 是一项建议的可选服务。

我国于 2014 年发布了密码行业标准 GM/T 0022-2014《IPSec VPN 技术规范》，其对 IPSec 协议技术进行了规范。

2. SSL

SSL 协议是网络上实现数据安全传输的一种通用协议，采用浏览器/服务端（B/S）结构是 SSL 协议的一种典型实现方式。

我国于 2014 年发布了密码行业标准 GM/T 0024-2014《SSL VPN 技术规范》，对 SSL 协议技术进行规范。标准 GM/T 0024-2014 参考了 TLS 1.1 版本，并在 TLS

1.1 握手协议中增加了 ECC、IBC 身份鉴别模式和密钥交换模式，取消了 DH 密钥交换方式，修改了密码套件的定义以使其支持商用密码算法。

6.1.3. 密码认证

6.1.3.1. 单向散列函数

1. 什么是单向散列函数

单向散列函数，又称单向 Hash 函数、杂凑函数，就是把任意长度的输入消息串变化成固定长的输出串且由输出串难以得到输入串的一种函数。这个输出串称为该消息的散列值。一般用于产生消息摘要，口令加密等。^[57]

单向散列函数有一个输入和一个输出，其中输入称为消息，输出称为散列值。单向散列函数可以根据消息的内容计算出散列值，而散列值就可以被用来检查消息的完整性。

单向散列函数根据消息的内容计算出散列值。

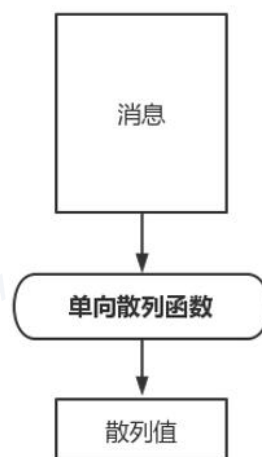


图 120 单向散列函数

2. 单向散列函数的实际应用

(1) 检测软件是否被篡改

可以使用单向散列函数来确认下载的软件是否被篡改。很多软件，尤其是安全相关的软件都会把通过单向散列函数计算出的散列值公布在官方网站上。用户在下载到软件之后，可以自行计算散列值，然后与官方网站公布的散列值进行对比。通过散列值，用户可以确认自己所下载到的文件与软件作者所提供的文件是否一致。

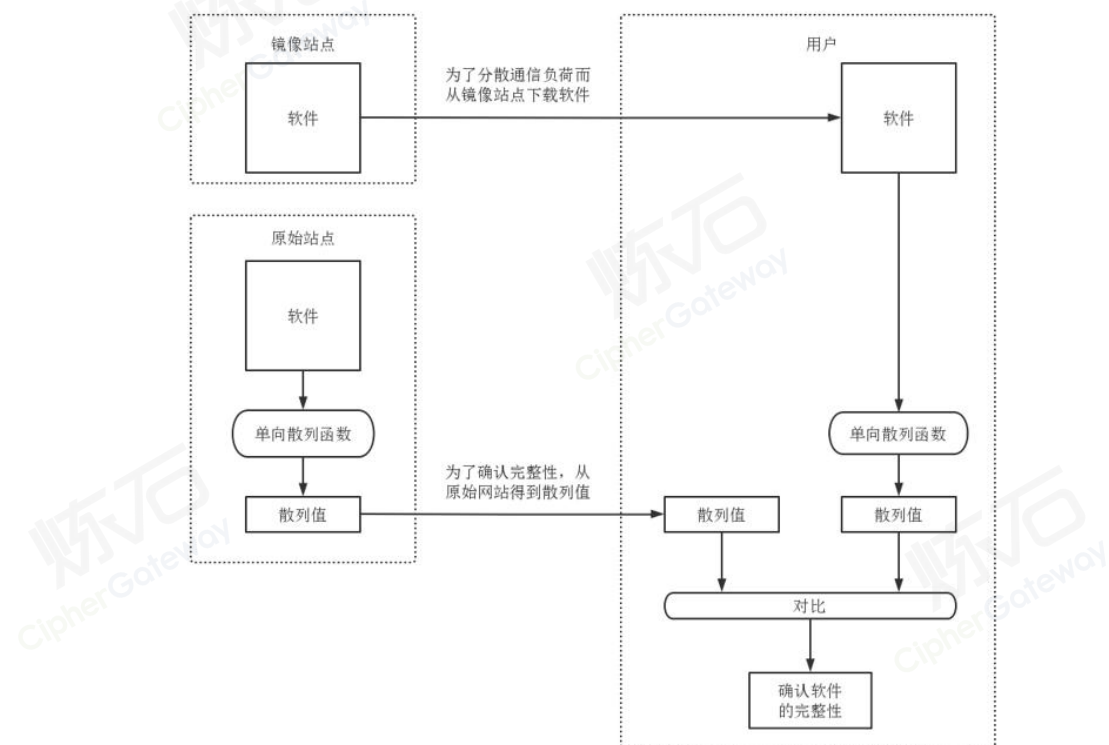


图 121 使用单向散列函数检测软件是否被篡改

(2) 基于口令的加密

单向散列函数也被用于基于口令的加密。PBE 的原理是将口令和盐(salt,通过伪随机数生成器产生的随机值)混合后计算其散列值,然后将这个散列值用作加密的密钥。通过这样的方法能够防御针对口令的字典攻击。

(3) 消息认证码

使用单向散列函数可以构造消息认证码。消息认证码是将“发送者和接收者之间的共享密钥”和“消息”进行混合后计算出的散列值。使用消息认证码可以检测并防止通信过程中的错误、篡改以及伪装。

(4) 数字认证

在进行数字签名时也会使用单向散列函数。数字签名是现实社会中的签名和盖章这样的行为在数字世界中的实现。数字签名的处理过程非常耗时,因此一般不会对整个消息内容直接施加数字签名,而是先通过单向散列函数计算出消息的散列值,然后再对这个散列值施加数字签名。

(5) 伪随机数生成器

使用单向散列函数可以构造伪随机数生成器。密码技术中所使用的随机数需要具备“事实上不可能根据过去的随机数列预测未来的随机数列”这样的性质。为了保证不可预测性,可以利用单向散列函数的单向性。

(6) 一次性口令

使用单向散列函数可以构造一次性口令。一次性口令经常被用于服务器对客户端的合法性认证。在这种方式中,通过使用单向散列函数可以保证口令只在通信链路上传送一次,因此即使窃听者窃取了口令,也无法使用。

3. 单向散列函数的具体例子

(1) MD4、MD5

MD4 能够产生 128 比特的散列值。不过，随着寻找 MD4 散列碰撞的方法被提出，现在它已经不安全了。

MD5 能够产生 128 比特的散列值。MD5 的强抗碰撞性已经被攻破，也就是说，现在已经能够产生具备相同散列值的两条不同的消息，因此它也已经不安全了。

MD4 和 MD5 中的 MD 是消息摘要（Message Digest）的缩写。

(2) SHA-1、SHA-2

SHA-1 是一种能够产生 160 比特的散列值的单向散列函数。1993 年被作为美国联邦信息处理标准规格发布的是 SHA,SHA-1 已经被列入“可谨慎运用的密码清单”，即除了用于保持兼容性的目的以外，其他情况下都不推荐使用。

SHA-1 的强抗碰撞性已于 2005 年被攻破⁴，也就是说，现在已经能够产生具备相同散列值的两条不同的消息。

SHA-2 共包含下列 6 种版本，从表中可以看出，这 6 种 SHA-2 实质上都是由 SHA-256 和 SHA-512 这两种版本衍生出来的，其他的版本都是通过将上述两种版本所生成的结果进行截取得到的。

表 44 6 种版本的 SHA-2

名称	输出长度	内部状态长度	备注
SHA-224	224	32×8=256	将 SHA-256 的结果截掉 32 比特
SHA-256	256	32×8=256	

⁴ 2005 年针对 SHA-1 的碰撞攻击算法及范例是由山东大学王小云教授的团队提出的，在 2004 年王小云团队就已经提出了针对 MD5、SHA-0 等散列函数的碰撞攻击算法。

SHA-512/224	224	64x8=512	将 SHA-512 的结果截掉 288 比特
SHA-512/256	256	64x8=512	将 SHA-512 的结果截掉 256 比特
SHA-384	384	64x8=512	将 SHA-512 的结果截掉 128 比特
SHA-512	512	64x8=512	

(3) RIPEMD-160

RIPEMD-160 是一种能够产生 160 比特的散列值的单向散列函数。RIPEMD-160 是欧盟 RIPE 项目所设计的 RIPEMD 单向散列函数的修订版。这一系列的函数还包括 RIPEMD-128、RIPEMD-256、RIPEMD-320 等其他一些版本。在《CRYPTREC 密码清单》中，RIPEMD-160 已经被列入“可谨慎运用的密码清单”，即除了用于保持兼容性的目的以外，其他情况下都不推荐使用。

RIPEMD 的强抗碰撞性已经于 2004 年被攻破，但 RIPEMD-160 还尚未被攻破。

(4) SHA-3

在 2005 年 SHA-1 的强抗碰撞性被攻破的背景下，NIST 开始着手制定用于取代 SHA-1 的下一代单向散列函数 SHA-3、SHA-3 和 AES 一样采用公开竞争的方式进行标准化。

6.1.3.2. 消息认证码

1. 什么是消息认证码

消息认证码是一种确认完整性并进行认证的技术，简称为 MAC。

消息认证码的输入包括任意长度的消息和一个发送者与接收者之间共享的密钥，它可以输出固定长度的数据，这个数据称为 MAC 值。

根据任意长度的消息输出固定长度的数据，这一点和单向散列函数很类似。但是单向散列函数中计算散列值时不需要密钥，相对地，消息认证码中则需要使用发送者与接收者之间共享的密钥。

要计算 MAC 必须持有共享密钥，没有共享密钥的人就无法计算 MAC 值，消息认证码正是利用这一性质来完成认证的。此外，和单向散列函数的散列值一样，哪怕消息中发生 1 比特的变化，MAC 值也会产生变化，消息认证码正是利用这一性质来确认完整性的。

后面我们会讲到，消息认证码有很多种实现方法，大家可以暂且这样理解：消息认证码是一种与密钥相关联的单向散列函数。

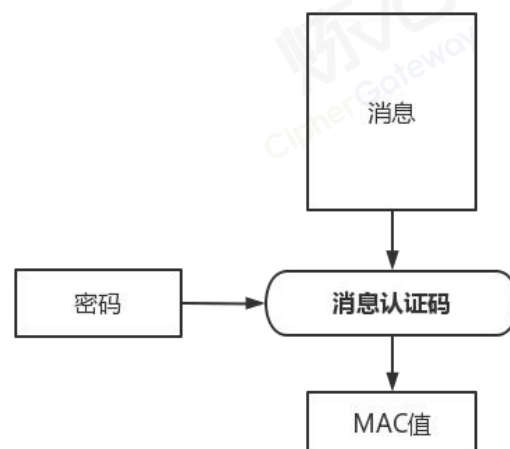


图 122 消息认证码

2. 消息认证码实现方法

(1) 使用单向散列函数实现

使用 SHA-2 之类的单向散列函数可以实现消息认证码，其中一种实现方法称为 HMAC。

(2) 使用分组密码实现

使用 AES 之类的分组密码可以实现消息认证码。

将分组密码的密钥作为消息认证码的共享密钥来使用，并用 CBC 模式将消息全部加密。此时，初始化向量（IV）是固定的。由于消息认证码中不需要解密，因此将除最后一个分组以外的密文部分全部丢弃，而将最后一个分组用作 MAC 值。

(3) 其他实现方法

此外，使用流密码和公钥密码等也可以实现消息认证码。

3. 消息认证码应用

下面我们来介绍几个消息认证码在现实世界中应用的实例

(1) SWIFT

银行和银行之间是通过 SWIFT 来传递交易消息的。而为了确认消息的完整性以及对消息进行验证，SWIFT 中使用了消息认证码。

(2) IPsec

IPsec 是对互联网基本通信协议——IP 协议(Internet Protocol)增加安全性的一种方式。在 IPsec 中，对通信内容的认证和完整性校验都是采用消息认证码来完成的。

(3) SSL/TLS

SSL/TLS 是我们在网上购物等场景中所使用的通信协议。SSL/TLS 中对通信内容的认证和完整性校验也使用了消息认证码。

6.1.3.3. 数字签名

1. 什么是数字签名

数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。它是一种类似写在纸上的普通的物理签名，但是在使用了公钥加密领域的技术来实现的，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。数字签名是非对称密钥加密技术与数字摘要技术的应用。^[58]

2. 数字签名使用

数字签名是具法律效力的，正在被普遍使用。2000 年，中华人民共和国的新《合同法》首次确认了电子合同、电子签名的法律效力。2005 年 4 月 1 日起，中华人民共和国首部《电子签名法》正式实施。

3. 数字签名应用

(1) 安全信息公告

一些信息安全方面的组织会在其网站上发布一些关于安全漏洞的警告，那么这些警告信息是否真的是该组织所发布的呢？如何确认发布这些信息的网页没有被第三方篡改呢？在这样的情况下就可以使用数字签名，即该组织可以对警告信息的文件施加数字签名，这样世界上的所有人就都可以验证警告信息的发布者是否合法。

(2) 软件下载

我们经常会从网上下载软件，我们需要判断所下载的软件是否可以安全运行，因为下载的软件有可能被主动攻击者篡改，从而执行一些恶意的操作。为了防止出现这样的问题，软件的作者可以对软件加上数字签名，而我们只要在下载之后验证数字签名，就可以识别出软件是否遭到了主动攻击者的篡改。

(3) 公钥证书

在验证数字签名时我们需要合法的公钥，那么怎么才能知道自己得到的公钥是否合法呢？可以将公钥当作消息，对它加上数字签名。像这样对公钥施加数字签名所得到的就是公钥证书。

(4) SSL/TLS

SSL/TLS 在认证服务器身份是否合法时会使用服务器证书，它就是加上了数字签名的服务器公钥。

6.1.3.4. 证书

1. 什么是证书

公钥证书，通常简称为证书，是一种数字签名的声明，它将公钥的值绑定到持有对应私钥的个人、设备或服务的身份。大多数普通用途的证书基于 X.509v3 证书标准。通常，证书包含以下信息：

- 主体的公钥值
- 主体标识符信息

- 有效期
- 颁发者标识符信息
- 颁发者的数字签名，用来证实主体的公钥和主体的标识符信息之间绑定关系的有效性

2. 证书使用方法

证书通常用来为实现安全的信息交换建立身份并创建信任，所以证书颁发机构(CA)可以把证书颁发给人员、设备和计算机上运行的服务。

某些情况下，计算机必须能够在高度信任涉及交易的其他设备、服务或个人的身份的情况下进行信息交换。某些情况下，人们需要在高度信任涉及交易的其他设备、服务或个人的身份的情况下进行信息交换。运行在计算机上的应用程序和服务也频繁地需要确认它们正在访问的信息来自可信任的信息源。

当两个实体试图建立身份和信任时，如果两个实体都信任相同的证书颁发机构，就能够在它们之间实现身份和信任的结合。一旦证书主体已呈现由受信任的CA所颁发的证书，那么，通过将证书主体的证书存储在它自己的证书存储区中，并且使用包含在证书中的公钥来加密会话密钥以便所有与证书主体随后进行的通讯都是安全的，试图建立信任的实体就可以继续进行信息交换。

3. 证书应用

(1) 在组织中的证书应用

很多组织安装有自己的证书颁发机构，并将证书颁发给内部的设备、服务和雇员，以创建更安全的计算环境。当雇员利用虚拟专用网络(VPN)从家里登录到组

织的网络时，VPN 服务器可以提供服务器证书以建立起自己的身份。因为公司的根颁发机构被信任，而公司根证书颁发机构颁发了 VPN 服务器的证书，所以，客户端计算机可以使用该连接，并且雇员知道其计算机实际上连接到组织的 VPN 服务器。

在数据可以经过 VPN 连接进行交换之前，VPN 服务器还必须能够验证 VPN 客户端的身份。或者通过交换计算机证书发生计算机级别的身份验证，或者通过使用点对点协议(PPP)身份验证方法，发生用户级别的身份验证。对于 L2TP/IPSec 连接，客户端和服务端双方均需要计算机证书。

客户端计算机证书可以服务于多个目的，这些目的大多数是基于身份验证的，这就允许客户端使用很多组织的资源，而不需要为每个资源分别准备证书。

VPN 服务器证书还可能服务于多个目的。相同的证书可能各种目的：确认电子邮件服务器、Web 服务器或者应用程序服务器的身份。颁发证书的证书颁发机构决定每个证书的用途数目。

(2) 颁发给个人的证书

个人可以向商业证书颁发机构购买证书，以便发送经过安全加密或数字签名以证明真实性的个人电子邮件。

一旦购买了证书并且用它来数字签名电子邮件，则邮件收件人就可以确认邮件在传输过程中没有发生改变，并且邮件来自于发送者，当然，先要假设邮件收件人信任向发送者颁发证书的证书颁发机构。

6.1.4. 密钥管理

密钥的安全是保证密码算法安全的基础。如何对密钥进行安全管理是密码产品、密码应用的设计开发人员关注的重点，也往往是不了解或刚涉入密码领域的人所忽视的一项重要内容。

6.1.4.1. 密钥全生命周期管理

密钥生命周期指的是密钥从生成到销毁的时间跨度,不同的密钥有不同的生命周期:签名密钥对可能有数年的生命周期,而一些临时密钥的生命周期为单次会话,使用完毕后立即销毁。一般而言,使用频率越高的密钥要求其生命周期尽量短。单个密钥的生命周期也不是固定的,如果密钥泄露,其生命周期应立即终止并销毁密钥。此外,有些与安全相关的敏感参数也应该视同密钥进行安全防护,包括但不限于用户口令、密钥生成和密码计算过程中使用的随机数或中间结果。

信息系统中的密钥在其生命周期内涉及到生成、存储、导入和导出、分发、使用、备份和恢复、归档、销毁等环节,以下具体介绍每个环节。

1. 密钥生成

密钥生成是密钥生命周期的起点,所有密钥都应当直接或间接地根据随机数生成。密钥生成的方式包括利用随机数直接生成、通过密钥派生函数生成。其中,后一种方式被认为是随机数间接生成,因为派生函数使用的主密钥、共享秘密信息的生成都与随机数相关。无论采用何种生成方式,密钥都应在密码产品内部产生。

2. 密钥存储

为了保证密钥存储安全,可以将密钥存储在核准的密码产品中,或者在对密钥进行保密性和完整性保护后,存储在通用存储设备或系统中。需要指出的是,并非所有密钥都需要存储,一些临时密钥或一次一密的密钥在使用完就要立即进行销毁。

3. 密钥导入导出

密钥的导入和导出主要指密钥在密码产品中的进出,既可以在同一个密码产品中进行密钥的导入和导出,也可以将密钥从一个密码产品导出后再导入到另一个密码产品中。为了保证密钥的安全性,密钥一般不能明文导出到密码产品外部。安全的密钥导入和导出方式包括加密传输和知识拆分。

(1) 加密传输

利用加密算法进行密钥的导入和导出是最简单和高效的方法。对称加密技术和非对称加密技术都可以完成密钥的导入和导出,但前提是通信双方需要预先共享一个密钥加密密钥或获取被导入方的公钥。同时,为了保证密钥的完整性,在密钥的导入和导出过程中,需要加入完整性保护和校验机制。利用非对称加密技术完成的密钥加密一般称为数字信封。

(2) 知识拆分

知识拆分是指将密钥拆分为几个独立的密钥分量,导出到密码产品外部。导入时,每个密钥分量单独导入,最终在密码产品内部进行合成。

4. 密钥分发

密钥分发主要用于不同密码产品间的密钥共享。根据分发方法，密钥分发主要分为人工分发和自动分发。这两者的主要区别在于人工分发方式需要人工参与，在线下通过面对面等方式完成密钥的安全分发，而自动的分发方式一般借助密码技术在线自动完成密钥分发。

(1) 人工分发

人工分发密钥指的是利用加密传输、知识拆分等手段通过人工将密钥从一个密码产品分发到其他产品中，实现密钥共享。人工分发的效率较低，只适用于少量密钥的分发，一般用于根密钥的分发。

(2) 自动分发

对称密钥和公钥加密密钥对的私钥可以通过数字信封、对称密钥加密等方式进行自动加密分发。自动分发的安全性主要通过密码技术本身来保证。

5. 密钥使用

密钥一般只能在核准的密码产品内部使用。用于核准的密码算法的密钥，不能再被非核准的密码算法使用，因为这些算法可能导致密钥泄露。特别是，不同类型的密钥不能混用，一个密钥不能用于不同用途，这主要有以下几个原因。

(1) 将一个密钥用于不同的用途，可能会降低密钥的安全性。

(2) 不同用途的密钥对密钥的要求互不相同。比如，加密密钥对可能会将其私钥归档以解密历史数据，而签名密钥对的私钥在其生命周期结束时应当立即销毁；如果一个密钥对同时用作加密和签名，将会产生矛盾。

(3) 限制密钥的用途可以降低密钥泄露时可能造成的损害。

6. 密钥备份和恢复

密钥备份的主要目的是保护密钥的可用性,作为密钥存储的补充以防止密钥的意外损坏。密钥备份与密钥存储非常类似,只不过备份的密钥处于不激活状态,只有完成恢复后才可以激活。密钥备份需要保护备份密钥的保密性、完整性及其与拥有者身份和其他信息的关联关系。

密钥备份时一般将备份的密钥存储在外部存储介质中,需要有安全机制保证仅有密钥拥有者才能恢复出密钥明文。密钥备份或恢复时应进行记录,并生成审计信息;审计信息应包括备份或恢复的主体、备份或恢复的时间等。

7. 密钥归档

密钥在其生命周期结束时,应当进行销毁。但是出于解密历史数据和验证历史签名的需要,有些不在生命周期内的密钥可能需要持续保存,需要注意的是签名密钥对的私钥不应进行归档。

密钥归档与密钥备份在形式上类似,主要区别在于密钥归档是在密钥的生命周期之外对密钥进行保存,在现有系统中该密钥已经不再使用;而密钥备份则针对仍在生命周期内的密钥。密钥归档时,也应当继续对这些密钥提供安全保护,以保证历史加密数据的安全性。密钥归档时应进行记录,并生成审计信息,审计信息应包括归档的密钥和归档时间等。

8. 密钥销毁

密钥的销毁是密钥生命周期的终点。密钥生命周期结束后,要对原始密钥进行销毁,并根据情况重新生成密钥,完成密钥更换。密钥销毁主要有两种情况。

- (1) 正常销毁：密钥在设计的使用截止时间到达时自动进行销毁，比如，临时密钥在使用完毕时应当立即销毁。
- (2) 应急销毁：密钥在已经泄露或存在泄露风险时进行的密钥销毁。对于存储在密码产品中的密钥，一般配备了紧急情况下自动销毁密钥的机制；当密钥所有者发现密钥存在泄露风险时，可能需要手动提前终止密钥的生命周期，进行密钥销毁。

6.1.4.2. 对称密钥管理

密钥管理因所使用的密码体制不同，管理方式也有很大区别。对称密码在一些特殊系统中应用广泛，如门禁系统、金融系统等。在门禁系统中，GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》规定了基于对称密钥体系的密钥分散过程。一般来说，首先通过门禁后台管理系统使用密钥管理子系统的密码设备生成门禁系统根密钥，然后将根密钥安全导入安全模块。在门禁卡发卡时，通过后台管理系统使用对称加密算法对系统根密钥进行密钥分散，实现一卡一密，即为每个卡片生成唯一卡片密钥。具体而言，可以利用根密钥对门禁卡的唯一标识（UID）以及用于密码分散的特定发行信息进行加密，获得卡片的唯一对称密钥，并将对称密钥安全下载到门禁卡中，实现门禁系统中对称密钥的分散。

在金融系统中，对称密钥管理标准有美国国家标准 ANSI X9.17《金融机构密钥管理（零售）》，这个标准为用于加密密钥的保护和交换规定了统一的处理方式，不仅适用于金融机构间的互操作，而且也可保证金融机构和大宗用户间的互

操作。我国关于对称密钥管理相关的标准有 GB/T 17901.1-1999《信息技术安全技术 密钥管理 第 1 部分：框架》，针对金融系统发布了国家标准 GB/T 27909.2-2011《银行业务密钥管理（零售）第 2 部分：对称密码及其密钥管理和生命周期》。

6.1.4.3. 公钥基础设施

公钥基础设施（PKI）是基于公钥密码技术实施的具有普适性的基础设施，可用于提供信息的保密性、信息来源的真实性、数据的完整性和行为的不可否认性等安全服务。

PKI 主要解决公钥属于谁的问题。需要强调的是，这里所说的公钥属于谁，实际上是指谁拥有与该公钥配对的私钥，而不是简单的公钥持有。确认公钥属于谁是希望确认谁拥有对应的私钥。

目前，我国制定的 GM/T0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》等系列标准对我国公众服务的数字证书认证系统的设计、建设、检测、运行及管理进行了规范。

1. PKI 系统组件

PKI 系统包括以下几类组件。

- (1) 证书认证机构（CA）。具有自己的公私钥对，负责为其他人签发证书，用自己的密钥来证实用户的公钥信息。一个 PKI 系统中可能会有多级 CA，包括根 CA 和各级子 CA。

- (2) 证书持有者。证书持有者拥有自己的证书和与证书中公钥匹配的私钥。证书持有者的身份信息和对应的公钥会出现在证书中，也称为用户。
- (3) 依赖方。一般将 PKI 应用过程中使用其他人的证书来实现安全功能（保密性、身份鉴别等）的通信实体称为依赖方，或者证书依赖方。
- (4) 证书注册机构（RA）。作为 CA 与申请者的交互接口，专门负责各种信息的检查和管理。只有在对申请者的各种检查通过之后，RA 才会将信息发送给 CA，要求 CA 签发证书。
- (5) 资料库。用于实现证书分发，负责存储所有的证书，供依赖方下载。
- (6) 证书撤销列表（CRL）。包含了当前所有被撤销证书的标识，验证者根据最新的 CRL 就能够判断证书是否被撤销。
- (7) 在线证书状态协议（OCSP）。一种实时检查证书撤销状态的协议标准。该协议是一种“请求-响应”协议，证书验证者向 OCSP 服务器查询某一张特定证书是否被撤销，服务器返回的响应消息表明该证书的撤销状态。OCSP 和 CRL 都是为了解决证书撤销状态查询的问题，相比较而言，OCSP 的实时性更高，部署起来也相对更复杂一些。
- (8) 轻量目录访问协议（LDAP）。一种开放的应用协议，提供访问控制和维护分布式信息的目录信息。CA 通过把新签发的证书与证书撤销链送到 LDAP 目录服务器，供用户查询、下载。
- (9) 密钥管理系统。为 PKI 系统中其他实体提供专门的密钥服务，包括生成、备份、恢复、托管等多种功能。

2. 数字证书结构

数字证书也称公钥证书，在证书中包含公钥持有者信息、公开密钥、有效期、扩展信息以及由 CA 对这些信息进行的数字签名。PKI 通过数字证书解决密钥归属问题。在 PKI 中，CA 也具有自己的公私钥对，对每一个“公钥证明的数据结构”进行数字签名，实现了公钥获得的数据起源鉴别、数据完整性和不可否认性。由于证书上带有 CA 的数字签名，用户可以在不可靠的介质上存储证书而不必担心被篡改，可以离线验证和使用，不必每一次使用都向资料库查询。

我国数字证书结构和格式遵循 GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》标准，标准中采用 GB/T 16262 系列标准的特定编码规则对证书项中的各项信息进行编码，组成特定的证书数据结构。ASN.1DER 编码是关于每个元素的标记、长度和值的编码系统。

3. 数字证书生命周期

证书的生命周期从证书的起始时间开始进入有效状态，在有效状态下的证书可以进行各种操作，生命周期的结束是当前时间进入了数字证书的失效日期或是数字证书被撤销，表明数字证书进入无效阶段。

4. 双证书体系

公钥密码的密钥既可以用于加密应用，又可以用于签名应用。然而，一方面，监管和用户自身的密钥恢复需求要求私钥在用户之外得到备份；另一方面，数字签名应用的私钥不能在用户之外再有备份。作为同时满足加密和签名两方面看似矛盾的需求解决方案，能够区分签名证书和加密证书的“双证书体系”得以引入，目前我国 PKI 系统采用的就是双证书体系。

6.1.5. 密码价值

6.1.5.1. 机密性

信息保密性保护的目的是避免信息泄露或暴露给未授权的实体。实现保密性保护有三种基本方法：一是访问控制的方法，防止敌手访问敏感信息；二是信息隐藏的方法，避免敌手发现敏感信息的存在；三是信息加密的方法，允许敌手观测到信息的表示，但是无法从表示中得到原始信息的内容或提炼出有用的信息。加密是数据通信和数据存储中实现保密性保护的一种主要机制，保密性保护也是密码技术最初的目标。

对于加密机制的应用，需要考虑密码体制的选取、算法的选择、工作模式、填充需要、初始化需要等因素。公钥密码技术和对称密码技术都可以用来实现加密机制，实现保密性保护。一般来说，公钥密码技术加密和解密方式灵活，但是计算成本高，主要应用于信息量不大、分享方式复杂的信息保密性保护，如密钥的协商或加密传输，大量信息传输或存储的保密性保护主要通过对称密码技术完成。公钥密码技术可以为对称密码应用提供密钥协商或安全传输的支撑。

6.1.5.2. 完整性

数据完整性保护的目的在于保护信息免受非授权实体的篡改或替代。数据完整性的破坏包括有意或者无意的损坏。数据完整性保护也有两种基本方法：一是访问控制方法，限制非授权实体修改被保护的数据；二是损坏—检测方法，这种方法无法避免数据损坏，但能确保这些损坏能够被检测出来，并能够被纠正或报

警。一般通过消息鉴别码或数字签名机制来实现完整性保护。在特殊应用中，在确保杂凑值无法被修改时，也可以单纯采用杂凑算法保护数据的完整性。下面主要介绍利用 MAC 和数字签名机制实现完整性保护的方法。

1. 消息鉴别码实现完整性

对称密码和杂凑算法都可用于消息鉴别码的生成。基于对称密码算法生成消息鉴别码时，一般对消息使用 CBC 模式进行加密，取密文的最后一个分组作为消息鉴别码。但需要注意的是，使用 CBC 模式生成 MAC 时，不能使用初始向量，而且消息长度需要双方预先约定。利用杂凑算法生成消息鉴别码是应用中经常采用的方式，相应的技术称为 HMAC。MAC 往往以消息标签的形式存在。消息发送者针对所发送的消息生成一个 MAC 作为消息标签，并将该标签和消息传输给接收者；消息接收者在将消息作为真实消息接收之前，通过共享的密钥和接收到的消息重新计算 MAC，验证计算出的 MAC 是否和接收到的 MAC 一致，如果二者一致则认为接收到的消息是完整的。

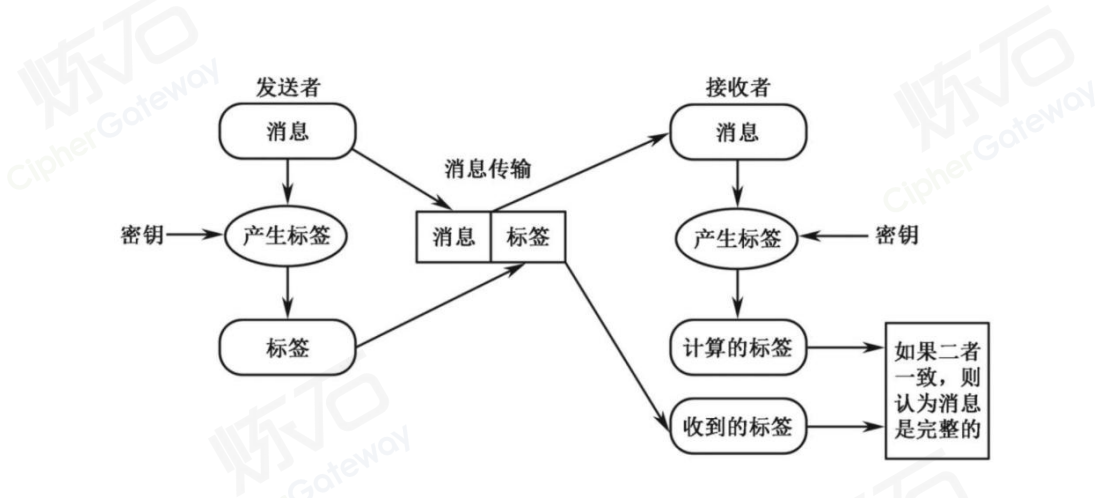


图 123 基于 MAC 的消息完整性保护过程

2. 数字签名实现完整性

数字签名也可以看作是标签的一种。基于对称密码或者杂凑算法的完整性保护机制能够确保接收者接收消息之前的消息完整性,但是不能防止接收者对消息的伪造;基于公钥密码技术的数字签名不仅可以防止敌手对消息进行篡改,还能防止接收者对消息进行伪造,即同时实现消息发送行为的不可否认性。

消息发送者使用私钥对发送的信息进行签名,并将签名结果作为标签,连同消息一起发送给接收者;接收者用公钥对签名信息进行验证,即利用接收到的消息及标签,以及发送方的公钥来验证接收到的消息的完整性。为了提升效率和安全性,方案还引入了杂凑函数,先对要签名的消息进行压缩,然后对压缩后的消息摘要进行签名产生标签。由于杂凑函数的引入,签名的对象变成消息摘要,而不是消息本身,从而减少了签名计算过程的计算量。

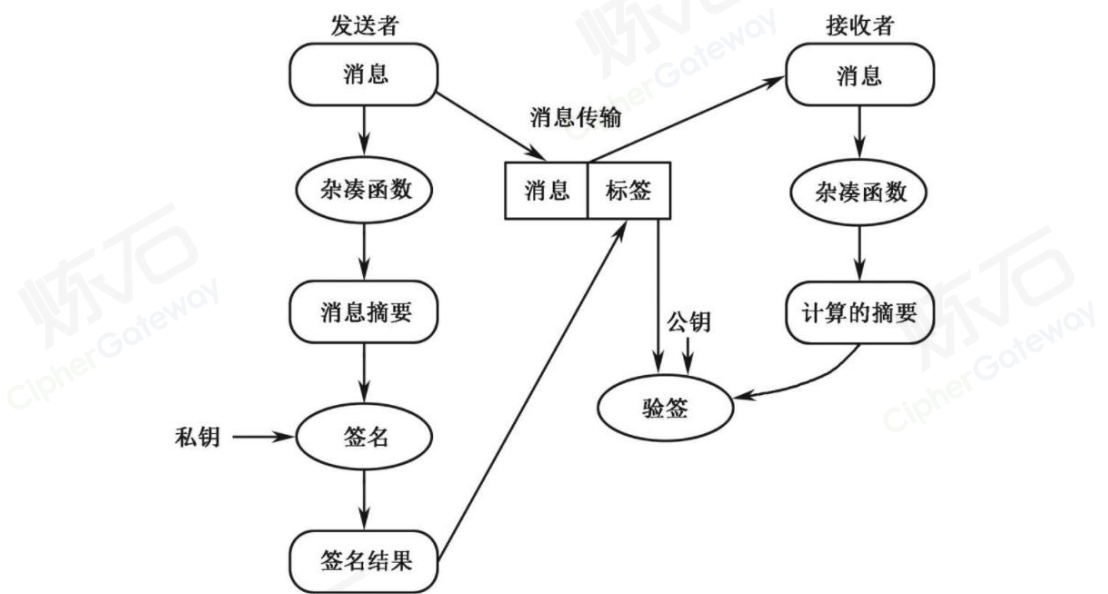


图 124 基于数字签名的消息完整性保护流程

6.1.5.3. 真实性

实现信息来源真实性的核心是鉴别。使用密码技术可以安全地实现对实体身份的鉴别。常用的鉴别方式包括：基于对称密码、公钥密码等密码技术的鉴别，基于静态口令的鉴别，基于动态口令的鉴别，以及基于生物特征的鉴别。后面三种鉴别方式虽然不是直接基于密码技术进行鉴别的，但在鉴别过程中仍需密码技术提供保护或支撑。

1. 基于密码技术的鉴别机制

基于密码技术鉴别机制的基本原理是：基于声称者知道某一秘密密钥这一事实，实现验证者对声称者身份的鉴别。对称密码技术和公钥密码技术都可用于鉴别机制的实现。这里给出一个基于密码技术鉴别的框架，如图 125 所示。使用对称密码技术和公钥密码技术进行鉴别都可以用该框架进行描述。

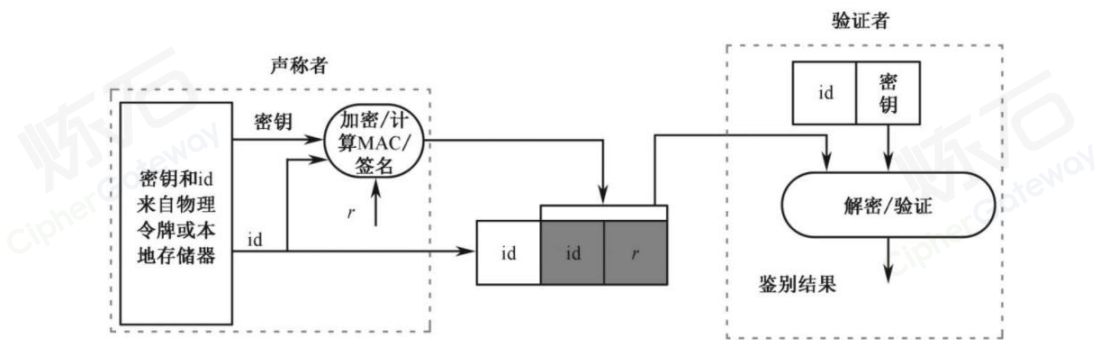


图 125 基于密码的鉴别方案的基本框架

基于对称密码技术的最简单的鉴别方法是声称者和验证者共享一个对称密钥。声称者用该密钥加密某一消息或计算该消息的 MAC。如果验证者能够成功解密消息，或者验证杂凑值是正确的，那么验证者相信消息来自声称者。被加密或

被杂凑的消息内容通常是一个非重复的值，以抵抗重放攻击，也可以使用“挑战—响应”机制来抵抗重放攻击。

2. 基于静态口令的鉴别机制

静态口令或者个人识别码（PIN）是最常用的鉴别信息之一，也是很多人口中的“密码”。直接使用口令进行鉴别有许多脆弱点，最严重的是外部泄露和口令猜测，以及窃听、重放攻击等。用密码技术可以有效提升口令鉴别过程的安全性。在口令传输过程中，可以采用对称加密、杂凑算法、公钥加密等方式保证口令的安全性。

3. 基于动态口令的鉴别机制

动态口令的使用主要用于抵抗重放攻击。在基于动态口令的鉴别方案中，用户每次使用的口令都是不同的。通常情况下，声称者和验证者共同使用一个初始状态同步的随机序列发生器，或者维持同步时钟。具体来说，声称者拥有一个存储秘密值的动态令牌，动态令牌采用密码算法，将秘密值、时间戳和其他一些信息作为输入，计算动态口令信息。由于声称者和验证者维持相同口令序列发生器，并保持同步，所以验证者能够产生正确的口令信息，从而验证声称者的身份。时间戳或者计数值的引入使得动态口令只有一次有效。我国密码行业标准 GM/T 0021-2012《动态口令密码应用技术规范》规定了动态口令系统中密码技术的应用要求。

4. 基于生物特征的鉴别机制

当对一个自然人实体进行鉴别时，一些较为稳定的生物特征可以作为鉴别信息，包括指纹、声音、虹膜、人脸等。生物特征识别技术在本质上与口令类似，

但是因为生物特征与自然人实体的不可分离性及信息量大的特点，所以，基于生物特征的鉴别机制在一定程度上避免了口令猜测、外部泄露等攻击。但是，与传统的静态口令鉴别机制面临的问题相同，基于生物特征的鉴别机制也容易受到窃听和重放攻击。因此，基于生物特征的鉴别机制一般不直接用于远程鉴别，而只用于设备对自然人的鉴别，身份验证通过后，设备再使用密码技术与应用服务器进行安全交互。

6.1.5.4. 不可否认性

使用不可否认功能，虽然不能防止通信参与方否认通信交换行为的发生，但是能够在产生纠纷时提供可信证据，有利于纠纷解决。网络环境中的不可否认可以分为起源的不可否认和传递的不可否认，主要通过数字签名技术来实现。

1. 起源的不可否认

起源的不可否认关系到某一特定方是否产生了特定数据的证据。产生证据的主体是发起者，在某些场景下也可以有可信第三方的参与。起源不可认证据要把各种信息片段用无可辩驳的方式连接起来，这些信息至少包括发起者的身份和数据的精确值。

2. 传递的不可否认

传递的不可否认是关于某一特定接收者接收到特定数据的证据。在这种情形下，产生证据的主体是接收者，在某些场景下也可以有可信第三方参与，证据验证者是发起者。传递不可否认将各种信息连接起来，形成证据。这些信息至少包括接收者的身份和数据的精确值。

6.2. 密码相关标准

6.2.1. 国家标准

序号	标准号	标准名称	发布日期	实施日期
1	GB/T 15843.1-2017	信息技术 安全技术 实体鉴别 第 1 部分：总则	2017/12/29	2018/7/1
2	GB/T 15843.2-2017	信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的 机制	2017/12/29	2018/7/1
3	GB/T 15843.3-2016	信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的 机制	2016/4/25	2016/11/1
4	GB/T 15843.4-2008	信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的 机制	2008/6/19	2008/11/1
5	GB/T 15843.5-2005	信息技术 安全技术 实体鉴别 第 5 部分：使用零知识技术的机 制	2005/4/19	2005/10/1
6	GB/T 15843.6-2018	信息技术 安全技术 实体鉴别 第 6 部分：采用人工数据传递的 机制	2018/9/17	2019/4/1

7	GB/T 15851.3-2018	信息技术 安全技术 带消息恢复的数字签名方案 第3部分：基于离散对数的机制	2018/12/28	2019/7/1
8	GB/T 15852.1-2020	信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制	2020/12/14	2021/7/1
9	GB/T 15852.2-2012	信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制	2012/12/31	2013/6/1
10	GB/T 15852.3-2019	信息技术 安全技术 消息鉴别码 第3部分：采用泛杂凑函数的机制	2019/8/30	2020/3/1
11	GB/T 17710-2008	信息技术 安全技术 校验字符系统	2008/7/16	2008/12/1
12	GB/T 17901.1-2020	信息技术 安全技术 密钥管理 第1部分：框架	2020/3/6	2020/10/1
13	GB/T 17901.3-2021	信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制	2021/3/9	2021/10/1
14	GB/T 17902.1-1999	信息技术 安全技术 带附录的数字签名 第1部分:概述	1999/11/11	2000/5/1

15	GB/T 17902.2-2005	信息技术 安全技术 带附录的 数字签名 第2部分:基于身份的 机制	2005/4/19	2005/10/1
16	GB/T 17902.3-2005	信息技术 安全技术 带附录的 数字签名 第3部分:基于证书的 机制	2005/4/19	2005/10/1
17	GB/T 17903.1-2008	信息技术 安全技术 抗抵赖 第 1部分:概述	2008/6/26	2008/11/1
18	GB/T 17903.2-2008	信息技术 安全技术 抗抵赖 第 2部分:采用对称技术的机制	2008/6/26	2008/11/1
19	GB/T 17903.3-2008	信息技术 安全技术 抗抵赖 第 3部分:采用非对称技术的机制	2008/7/2	2008/12/1
20	GB/T 17964-2008	信息安全技术 分组密码算法的 工作模式	2008/6/26	2008/11/1
21	GB/T 18018-2019	信息安全技术 路由器安全技术 要求	2019/8/30	2020/3/1
22	GB/T 18238.1-2000	信息技术 安全技术 散列函数 第1部分:概述	2000/10/17	2001/8/1
23	GB/T 18238.2-2002	信息技术 安全技术 散列函数 第2部分:采用n位块密码的散列 函数	2002/7/18	2002/12/1

24	GB/T 18238.3-2002	信息技术 安全技术 散列函数 第 3 部分:专用散列函数	2002/7/18	2002/12/1
25	GB/T 18336.1-2015	信息技术 安全技术 信息技术 安全评估准则 第 1 部分:简介 和一般模型	2015/5/15	2016/1/1
26	GB/T 18336.2-2015	信息技术 安全技术 信息技术 安全评估准则 第 2 部分:安全 功能组件	2015/5/15	2016/1/1
27	GB/T 18336.3-2015	信息技术 安全技术 信息技术 安全评估准则 第 3 部分:安全 保障组件	2015/5/15	2016/1/1
28	GB/T 19668.4-2017	信息技术服务 监理 第 4 部分: 信息安全监理规范	2017/7/31	2018/2/1
29	GB/T 19713-2005	信息技术 安全技术 公钥基础 设施 在线证书状态协议	2005/4/19	2005/10/1
30	GB/T 19714-2005	信息技术 安全技术 公钥基础 设施 证书管理协议	2005/4/19	2005/10/1
31	GB/T 19771-2005	信息技术 安全技术 公钥基础 设施 PKI 组件最小互操作规范	2005/5/25	2005/12/1
32	GB/T 20008-2005	信息安全技术 操作系统安全评 估准则	2005/11/11	2006/5/1

33	GB/T 20009-2019	信息安全技术 数据库管理系统 安全评估准则	2019/8/30	2020/3/1
34	GB/T 20011-2005	信息安全技术 路由器安全评估 准则	2005/11/11	2006/5/1
35	GB/T 20261-2020	信息安全技术 系统安全工程 能力成熟度模型	2020/11/19	2021/6/1
36	GB/T 20269-2006	信息安全技术 信息系统安全管 理要求	2006/5/31	2006/12/1
37	GB/T 20270-2006	信息安全技术 网络基础安全技 术要求	2006/5/31	2006/12/1
38	GB/T 20271-2006	信息安全技术 信息系统通用安 全技术要求	2006/5/31	2006/12/1
39	GB/T 20272-2019	信息安全技术 操作系统安全技 术要求	2019/8/30	2020/3/1
40	GB/T 20273-2019	信息安全技术 数据库管理系统 安全技术要求	2019/8/30	2020/3/1
41	GB/T 20274.1-2006	信息安全技术 信息系统安全保 障评估框架 第一部分：简介和 一般模型	2006/5/31	2006/12/1
42	GB/T 20274.2-2008	信息安全技术 信息系统安全保 障评估框架 第2部分：技术保	2008/7/18	2008/12/1

		障		
43	GB/T 20274.3-2008	信息安全技术 信息系统安全保 障评估框架 第 3 部分：管理保 障	2008/7/18	2008/12/1
44	GB/T 20274.4-2008	信息安全技术 信息系统安全保 障评估框架 第 4 部分：工程保 障	2008/7/18	2008/12/1
45	GB/T 20275-2013	信息安全技术 网络入侵检测系 统技术要求和测试评价方法	2013/12/31	2014/7/15
46	GB/T 20276-2016	信息安全技术 具有中央处理器 的 IC 卡嵌入式软件安全技术要 求	2016/8/29	2017/3/1
47	GB/T 20277-2015	信息安全技术 网络和终端隔离 产品测试评价方法	2015/5/15	2016/1/1
48	GB/T 20278-2013	信息安全技术 网络脆弱性扫描 产品安全技术要求	2013/12/31	2014/7/15
49	GB/T 20279-2015	信息安全技术 网络和终端隔离 产品安全技术要求	2015/5/15	2016/1/1
50	GB/T 20280-2006	信息安全技术 网络脆弱性扫描 产品测试评价方法	2006/5/31	2006/12/1
51	GB/T 20281-2020	信息安全技术 防火墙安全技术	2020/4/28	2020/11/1

		要求和测试评价方法		
52	GB/T 20282-2006	信息安全技术 信息系统安全工程管理要求	2006/5/31	2006/12/1
53	GB/T 20283-2020	信息安全技术 保护轮廓和安全目标的产生指南	2020/9/29	2021/4/1
54	GB/T 20518-2018	信息安全技术 公钥基础设施数字证书格式	2018/6/7	2019/1/1
55	GB/T 20520-2006	信息安全技术 公钥基础设施时间戳规范	2006/8/30	2007/2/1
56	GB/T 20945-2013	信息安全技术 信息系统安全审计产品技术要求和测试评价方法	2013/12/31	2014/7/15
57	GB/T 20979-2019	信息安全技术 虹膜识别系统技术要求	2019/8/30	2020/3/1
58	GB/T 20984-2007	信息安全技术 信息安全风险评估规范	2007/6/14	2007/11/1
59	GB/T 20985.1-2017	信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理	2017/12/29	2018/7/1
60	GB/T 20985.2-2020	信息技术 安全技术 信息安全事件管理 第2部分：事件响	2020/12/14	2021/7/1

		应规划和准备指南		
61	GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范	2007/6/14	2007/11/1
62	GB/T 21050-2019	信息安全技术 网络交换机安全技术要求	2019/8/30	2020/3/1
63	GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求	2007/8/23	2008/1/1
64	GB/T 21053-2007	信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求	2007/8/23	2008/1/1
65	GB/T 21054-2007	信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则	2007/8/23	2008/1/1
66	GB/T 22080-2016	信息技术 安全技术 信息安全管理体系 要求	2016/8/29	2017/3/1
67	GB/T 22081-2016	信息技术 安全技术 信息安全控制实践指南	2016/8/29	2017/3/1
68	GB/T 22186-2016	信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求	2016/8/29	2017/3/1
69	GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求	2019/5/10	2019/12/1
70	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南	2020/4/28	2020/11/1

71	GB/T 24363-2009	信息安全技术 信息安全应急响应计划规范	2009/9/30	2009/12/1
72	GB/T 25056-2018	信息安全技术 证书认证系统密码及其相关安全技术规范	2018/6/7	2019/1/1
73	GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南	2019/8/30	2020/3/1
74	GB/T 25061-2020	信息安全技术 XML 数字签名语法与处理规范	2020/11/19	2021/6/1
75	GB/T 25062-2010	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范	2010/9/2	2011/2/1
76	GB/T 25064-2010	信息安全技术 公钥基础设施电子签名格式规范	2010/9/2	2011/2/1
77	GB/T 25065-2010	信息安全技术 公钥基础设施签名生成应用程序的安全要求	2010/9/2	2011/2/1
78	GB/T 25066-2020	信息安全技术 信息安全产品类别与代码	2020/4/28	2020/11/1
79	GB/T 25067-2020	信息技术 安全技术 信息安全管理体系审核和认证机构要求	2020/4/28	2020/11/1
80	GB/T 25068.1-2020	信息技术 安全技术 网络安全第 1 部分：综述和概念	2020/11/19	2021/6/1

81	GB/T 25068.2-2020	信息技术 安全技术 网络安全 第 2 部分：网络安全设计和实现指南	2020/11/19	2021/6/1
82	GB/T 25068.3-2010	信息技术 安全技术 IT 网络安全 第 3 部分：使用安全网关的网间通信安全保护	2010/9/2	2011/2/1
83	GB/T 25068.4-2010	信息技术 安全技术 IT 网络安全 第 4 部分：远程接入的安全保护	2010/9/2	2011/2/1
84	GB/T 25068.5-2021	信息技术 安全技术 网络安全 第 5 部分：使用虚拟专用网的跨网通信安全保护	2021/3/9	2021/10/1
85	GB/T 25069-2010	信息安全技术 术语	2010/9/2	2011/2/1
86	GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求	2019/5/10	2019/12/1
87	GB/T 26855-2011	信息安全技术 公钥基础设施证书策略与认证业务声明框架	2011/7/29	2011/11/1
88	GB/T 28447-2012	信息安全技术 电子认证服务机构运营管理规范	2012/6/29	2012/10/1
89	GB/T 28448-2019	信息安全技术 网络安全等级保护测评要求	2019/5/10	2019/12/1

90	GB/T 28449-2018	信息安全技术 网络安全等级保护测评过程指南	2018/12/28	2019/7/1
91	GB/T 28450-2020	信息技术 安全技术 信息安全管理体系审核指南	2020/12/14	2021/7/1
92	GB/T 28451-2012	信息安全技术 网络型入侵防御产品技术要求和测试评价方法	2012/6/29	2012/10/1
93	GB/T 28452-2012	信息安全技术 应用软件系统通用安全技术要求	2012/6/29	2012/10/1
94	GB/T 28453-2012	信息安全技术 信息系统安全管理评估要求	2012/6/29	2012/10/1
95	GB/T 28454-2020	信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作	2020/4/28	2020/11/1
96	GB/T 28455-2012	信息安全技术 引入可信第三方的实体鉴别及接入架构规范	2012/6/29	2012/10/1
97	GB/T 28458-2020	信息安全技术 网络安全漏洞标识与描述规范	2020/11/19	2021/6/1
98	GB/T 29240-2012	信息安全技术 终端计算机通用安全技术要求与测试评价方法	2012/12/31	2013/6/1
99	GB/T 29241-2012	信息安全技术 公钥基础设施PKI 互操作性评估准则	2012/12/31	2013/6/1

100	GB/T 29242-2012	信息安全技术 鉴别与授权 安全断言标记语言	2012/12/31	2013/6/1
101	GB/T 29243-2012	信息安全技术 数字证书代理认证路径构造和代理验证规范	2012/12/31	2013/6/1
102	GB/T 29244-2012	信息安全技术 办公设备基本安全要求	2012/12/31	2013/6/1
103	GB/T 29245-2012	信息安全技术 政府部门信息安全管理基本要求	2012/12/31	2013/6/1
104	GB/T 29246-2017	信息技术 安全技术 信息安全管理体系 概述和词汇	2017/12/29	2018/7/1
105	GB/T 29765-2013	信息安全技术 数据备份与恢复产品技术要求与测试评价方法	2013/9/18	2014/5/1
106	GB/T 29766-2013	信息安全技术 网站数据恢复产品技术要求与测试评价方法	2013/9/18	2014/5/1
107	GB/T 29767-2013	信息安全技术 公钥基础设施桥 CA 体系证书分级规范	2013/9/18	2014/5/1
108	GB/T 29827-2013	信息安全技术 可信计算规范 可信平台主板功能接口	2013/11/12	2014/2/1
109	GB/T 29828-2013	信息安全技术 可信计算规范 可信连接架构	2013/11/12	2014/2/1
110	GB/T 29829-2013	信息安全技术 可信计算密码支	2013/11/12	2014/2/1

		撑平台功能与接口规范		
111	GB/T 30269.601-2016	信息技术 传感器网络 第 601 部分：信息安全：通用技术规范	2016/4/25	2016/8/1
112	GB/T 30269.602-2017	信息技术 传感器网络 第 602 部分：信息安全：低速率无线传感器网络层和应用支持子层安全规范	2017/12/29	2017/12/29
113	GB/T 30270-2013	信息技术 安全技术 信息技术安全性评估方法	2013/12/31	2014/7/15
114	GB/T 30271-2013	信息安全技术 信息安全服务能力评估准则	2013/12/31	2014/7/15
115	GB/T 30272-2013	信息安全技术 公钥基础设施标准一致性测试评价指南	2013/12/31	2014/7/15
116	GB/T 30273-2013	信息安全技术 信息系统安全保障通用评估指南	2013/12/31	2014/7/15
117	GB/T 30275-2013	信息安全技术 鉴别与授权 认证中间件框架与接口规范	2013/12/31	2014/7/15
118	GB/T 30276-2020	信息安全技术 网络安全漏洞管理规范	2020/11/19	2021/6/1
119	GB/T 30278-2013	信息安全技术 政务计算机终端核心配置规范	2013/12/31	2014/7/15

120	GB/T 30279-2020	信息安全技术 网络安全漏洞分类分级指南	2020/11/19	2021/6/1
121	GB/T 30280-2013	信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言	2013/12/31	2014/7/15
122	GB/T 30281-2013	信息安全技术 鉴别与授权 可扩展访问控制标记语言	2013/12/31	2014/7/15
123	GB/T 30282-2013	信息安全技术 反垃圾邮件产品技术要求和测试评价方法	2013/12/31	2014/7/15
124	GB/T 30283-2013	信息安全技术 信息安全服务分类	2013/12/31	2014/7/15
125	GB/T 30284-2020	信息安全技术 移动通信智能终端操作系统安全技术要求	2020/4/28	2020/11/1
126	GB/T 30285-2013	信息安全技术 灾难恢复中心建设与运维管理规范	2013/12/31	2014/7/15
127	GB/T 31167-2014	信息安全技术 云计算服务安全指南	2014/9/3	2015/4/1
128	GB/T 31168-2014	信息安全技术 云计算服务安全能力要求	2014/9/3	2015/4/1
129	GB/T 31495.1-2015	信息安全技术 信息安全保障指标体系及评价方法 第1部分：	2015/5/15	2016/1/1

		概念和模型		
130	GB/T 31495.2-2015	信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系	2015/5/15	2016/1/1
131	GB/T 31495.3-2015	信息安全技术 信息安全保障指标体系及评价方法 第3部分：实施指南	2015/5/15	2016/1/1
132	GB/T 31496-2015	信息技术 安全技术 信息安全管理体系实施指南	2015/5/15	2016/1/1
133	GB/T 31497-2015	信息技术 安全技术 信息安全管理体系 测量	2015/5/15	2016/1/1
134	GB/T 31499-2015	信息安全技术 统一威胁管理产品技术要求和测试评价方法	2015/5/15	2016/1/1
135	GB/T 31500-2015	信息安全技术 存储介质数据恢复服务要求	2015/5/15	2016/1/1
136	GB/T 31501-2015	信息安全技术 鉴别与授权 授权应用程序判定接口规范	2015/5/15	2016/1/1
137	GB/T 31502-2015	信息安全技术 电子支付系统安全保护框架	2015/5/15	2016/1/1
138	GB/T 31503-2015	信息安全技术 电子文档加密与签名消息语法	2015/5/15	2016/1/1

139	GB/T 31504-2015	信息安全技术 鉴别与授权 数字身份信息服务框架规范	2015/5/15	2016/1/1
140	GB/T 31506-2015	信息安全技术 政府门户网站系统安全技术指南	2015/5/15	2016/1/1
141	GB/T 31507-2015	信息安全技术 智能卡通用安全检测指南	2015/5/15	2016/1/1
142	GB/T 31508-2015	信息安全技术 公钥基础设施 数字证书策略分类分级规范	2015/5/15	2016/1/1
143	GB/T 31509-2015	信息安全技术 信息安全风险评估实施指南	2015/5/15	2016/1/1
144	GB/T 31722-2015	信息技术 安全技术 信息安全风险管理	2015/6/2	2016/2/1
145	GB/T 32213-2015	信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范	2015/12/10	2016/8/1
146	GB/T 32905-2016	信息安全技术 SM3 密码杂凑算法	2016/8/29	2017/3/1
147	GB/T 32907-2016	信息安全技术 SM4 分组密码算法	2016/8/29	2017/3/1
148	GB/T 32914-2016	信息安全技术 信息安全服务提供方管理要求	2016/8/29	2017/3/1
149	GB/T 32915-2016	信息安全技术 二元序列随机性	2016/8/29	2017/3/1

		检测方法		
150	GB/T 32918.1-2016	信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则	2016/8/29	2017/3/1
151	GB/T 32918.2-2016	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	2016/8/29	2017/3/1
152	GB/T 32918.3-2016	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	2016/8/29	2017/3/1
153	GB/T 32918.4-2016	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	2016/8/29	2017/3/1
154	GB/T 32918.5-2017	信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义	2017/5/12	2017/12/1
155	GB/T 32919-2016	信息安全技术 工业控制系统安全控制应用指南	2016/8/29	2017/3/1
156	GB/T 32920-2016	信息技术 安全技术 行业间和组织间通信的信息安全管理	2016/8/29	2017/3/1
157	GB/T 32921-2016	信息安全技术 信息技术产品供应方行为安全准则	2016/8/29	2017/3/1

158	GB/T 32922-2016	信息安全技术 IPsec VPN 安全接入基本要求与实施指南	2016/8/29	2017/3/1
159	GB/T 32923-2016	信息技术 安全技术 信息安全治理	2016/8/29	2017/3/1
160	GB/T 32924-2016	信息安全技术 网络安全预警指南	2016/8/29	2017/3/1
161	GB/T 32925-2016	信息安全技术 政府联网计算机终端安全管理基本要求	2016/8/29	2017/3/1
162	GB/T 32926-2016	信息安全技术 政府部门信息技术服务外包信息安全管理规范	2016/8/29	2017/3/1
163	GB/T 32927-2016	信息安全技术 移动智能终端安全架构	2016/8/29	2017/3/1
164	GB/T 33131-2016	信息安全技术 基于 IPsec 的 IP 存储网络安全技术要求	2016/10/13	2017/5/1
165	GB/T 33132-2016	信息安全技术 信息安全风险处理实施指南	2016/10/13	2017/5/1
166	GB/T 33133.1-2016	信息安全技术 祖冲之序列密码算法 第 1 部分：算法描述	2016/10/13	2017/5/1
167	GB/T 33134-2016	信息安全技术 公共域名服务系统安全要求	2016/10/13	2017/5/1
168	GB/T 33560-2017	信息安全技术 密码应用标识规	2017/5/12	2017/12/1

		范		
169	GB/T 33562-2017	信息安全技术 安全域名系统实施指南	2017/5/12	2017/12/1
170	GB/T 33563-2017	信息安全技术 无线局域网客户端安全技术要求（评估保障级 2 级增强）	2017/5/12	2017/12/1
171	GB/T 33565-2017	信息安全技术 无线局域网接入系统安全技术要求（评估保障级 2 级增强）	2017/5/12	2017/12/1
172	GB/T 34095-2017	信息安全技术 用于电子支付的基于近距离无线通信的移动终端安全技术要求	2017/7/31	2018/2/1
173	GB/T 34942-2017	信息安全技术 云计算服务安全能力评估方法	2017/11/1	2018/5/1
174	GB/T 34953.1-2017	信息技术 安全技术 匿名实体鉴别 第 1 部分：总则	2017/11/1	2018/5/1
175	GB/T 34953.2-2018	信息技术 安全技术 匿名实体鉴别 第 2 部分：基于群组公钥签名的机制	2018/9/17	2019/4/1
176	GB/T 34953.4-2020	信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的	2020/4/28	2020/11/1

		机制		
177	GB/T 34975-2017	信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法	2017/11/1	2018/5/1
178	GB/T 34976-2017	信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法	2017/11/1	2018/5/1
179	GB/T 34977-2017	信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法	2017/11/1	2018/5/1
180	GB/T 34978-2017	信息安全技术 移动智能终端个人信息保护技术要求	2017/11/1	2018/5/1
181	GB/T 34990-2017	信息安全技术 信息系统安全管理平台技术要求和测试评价方法	2017/11/1	2018/5/1
182	GB/T 35101-2017	信息安全技术 智能卡读写机具安全技术要求（EAL4 增强）	2017/11/1	2018/5/1
183	GB/T 35273-2020	信息安全技术 个人信息安全规范	2020/3/6	2020/10/1
184	GB/T 35274-2017	信息安全技术 大数据服务安全能力要求	2017/12/29	2018/7/1

185	GB/T 35275-2017	信息安全技术 SM2 密码算法加 密签名消息语法规范	2017/12/29	2018/7/1
186	GB/T 35276-2017	信息安全技术 SM2 密码算法使 用规范	2017/12/29	2018/7/1
187	GB/T 35277-2017	信息安全技术 防病毒网关安全 技术要求和测试评价方法	2017/12/29	2018/7/1
188	GB/T 35278-2017	信息安全技术 移动终端安全保 护技术要求	2017/12/29	2018/7/1
189	GB/T 35279-2017	信息安全技术 云计算安全参考 架构	2017/12/29	2018/7/1
190	GB/T 35280-2017	信息安全技术 信息技术产品安 全检测机构条件和行为准则	2017/12/29	2018/7/1
191	GB/T 35281-2017	信息安全技术 移动互联网应用 服务器安全技术要求	2017/12/29	2018/7/1
192	GB/T 35282-2017	信息安全技术 电子政务移动办 公系统安全技术规范	2017/12/29	2018/7/1
193	GB/T 35283-2017	信息安全技术 计算机终端核心 配置基线结构规范	2017/12/29	2018/7/1
194	GB/T 35284-2017	信息安全技术 网站身份和系统 安全要求与评估方法	2017/12/29	2018/7/1
195	GB/T 35285-2017	信息安全技术 公钥基础设施	2017/12/29	2018/7/1

		基于数字证书的可靠电子签名 生成及验证技术要求		
196	GB/T 35286-2017	信息安全技术 低速无线个域网 空口安全测试规范	2017/12/29	2018/7/1
197	GB/T 35287-2017	信息安全技术 网站可信标识技 术指南	2017/12/29	2018/7/1
198	GB/T 35288-2017	信息安全技术 电子认证服务机 构从业人员岗位技能规范	2017/12/29	2018/7/1
199	GB/T 35289-2017	信息安全技术 电子认证服务机 构服务质量规范	2017/12/29	2018/7/1
200	GB/T 35290-2017	信息安全技术 射频识别（RFID） 系统通用安全技术要求	2017/12/29	2018/7/1
201	GB/T 35291-2017	信息安全技术 智能密码钥匙应 用接口规范	2017/12/29	2018/7/1
202	GB/T 35317-2017	公安物联网系统信息安全等级 保护要求	2017/12/29	2017/12/29
203	GB/T 36322-2018	信息安全技术 密码设备应用接 口规范	2018/6/7	2019/1/1
204	GB/T 36323-2018	信息安全技术 工业控制系统安 全管理基本要求	2018/6/7	2019/1/1
205	GB/T 36324-2018	信息安全技术 工业控制系统信	2018/6/7	2019/1/1

		息安全分级规范		
206	GB/T 36466-2018	信息安全技术 工业控制系统风险评估实施指南	2018/6/7	2019/1/1
207	GB/T 36470-2018	信息安全技术 工业控制系统现场测控设备通用安全功能要求	2018/6/7	2019/1/1
208	GB/T 36618-2018	信息安全技术 金融信息服务安全规范	2018/9/17	2019/4/1
209	GB/T 36619-2018	信息安全技术 政务和公益机构域名命名规范	2018/9/17	2019/4/1
210	GB/T 36624-2018	信息技术 安全技术 可鉴别的加密机制	2018/9/17	2019/4/1
211	GB/T 36626-2018	信息安全技术 信息系统安全运维管理指南	2018/9/17	2019/4/1
212	GB/T 36627-2018	信息安全技术 网络安全等级保护测试评估技术指南	2018/9/17	2019/4/1
213	GB/T 36629.1-2018	信息安全技术 公民网络电子身份标识安全技术要求 第1部分：读写机具安全技术要求	2018/10/10	2019/5/1
214	GB/T 36629.2-2018	信息安全技术 公民网络电子身份标识安全技术要求 第2部分：载体安全技术要求	2018/10/10	2019/5/1

215	GB/T 36629.3-2018	信息安全技术 公民网络电子身份标识安全技术要求 第3部分：验证服务消息及其处理规则	2018/12/28	2019/7/1
216	GB/T 36630.1-2018	信息安全技术 信息技术产品安全可控评价指标 第1部分：总则	2018/9/17	2019/4/1
217	GB/T 36630.2-2018	信息安全技术 信息技术产品安全可控评价指标 第2部分：中央处理器	2018/9/17	2019/4/1
218	GB/T 36630.3-2018	信息安全技术 信息技术产品安全可控评价指标 第3部分：操作系统	2018/9/17	2019/4/1
219	GB/T 36630.4-2018	信息安全技术 信息技术产品安全可控评价指标 第4部分：办公套件	2018/9/17	2019/4/1
220	GB/T 36630.5-2018	信息安全技术 信息技术产品安全可控评价指标 第5部分：通用计算机	2018/9/17	2019/4/1
221	GB/T 36631-2018	信息安全技术 时间戳策略和时间戳业务操作规则	2018/9/17	2019/4/1
222	GB/T 36632-2018	信息安全技术 公民网络电子身	2018/10/10	2019/5/1

		份标识格式规范		
223	GB/T 36633-2018	信息安全技术 网络用户身份鉴别技术指南	2018/9/17	2019/4/1
224	GB/T 36635-2018	信息安全技术 网络安全监测基本要求与实施指南	2018/9/17	2019/4/1
225	GB/T 36637-2018	信息安全技术 ICT 供应链安全风险管理体系指南	2018/10/10	2019/5/1
226	GB/T 36639-2018	信息安全技术 可信计算规范 服务器可信支撑平台	2018/9/17	2019/4/1
227	GB/T 36643-2018	信息安全技术 网络安全威胁信息格式规范	2018/10/10	2019/5/1
228	GB/T 36644-2018	信息安全技术 数字签名应用安全证明获取方法	2018/9/17	2019/4/1
229	GB/T 36651-2018	信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架	2018/10/10	2019/5/1
230	GB/T 36950-2018	信息安全技术 智能卡安全技术要求（EAL4+）	2018/12/28	2019/7/1
231	GB/T 36951-2018	信息安全技术 物联网感知终端应用安全技术要求	2018/12/28	2019/7/1
232	GB/T 36957-2018	信息安全技术 灾难恢复服务要	2018/12/28	2019/7/1

		求		
233	GB/T 36958-2018	信息安全技术 网络安全等级保护安全管理中心技术要求	2018/12/28	2019/7/1
234	GB/T 36959-2018	信息安全技术 网络安全等级保护测评机构能力要求和评估规范	2018/12/28	2019/7/1
235	GB/T 36960-2018	信息安全技术 鉴别与授权 访问控制中间件框架与接口	2018/12/28	2019/7/1
236	GB/T 36968-2018	信息安全技术 IPSec VPN 技术规范	2018/12/28	2019/7/1
237	GB/T 37002-2018	信息安全技术 电子邮件系统安全技术要求	2018/12/28	2019/7/1
238	GB/T 37024-2018	信息安全技术 物联网感知层网络安全安全技术要求	2018/12/28	2019/7/1
239	GB/T 37025-2018	信息安全技术 物联网数据传输安全技术要求	2018/12/28	2019/7/1
240	GB/T 37027-2018	信息安全技术 网络攻击定义及描述规范	2018/12/28	2019/7/1
241	GB/T 37033.1-2018	信息安全技术 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别	2018/12/28	2019/7/1

242	GB/T 37033.2-2018	信息安全技术 射频识别系统密码应用技术要求 第2部分：电子标签与读写器及其通信密码应用技术要求	2018/12/28	2019/7/1
243	GB/T 37033.3-2018	信息安全技术 射频识别系统密码应用技术要求 第3部分：密钥管理技术要求	2018/12/28	2019/7/1
244	GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求	2018/12/28	2019/7/1
245	GB/T 37046-2018	信息安全技术 灾难恢复服务能力评估准则	2018/12/28	2019/7/1
246	GB/T 37076-2018	信息安全技术 指纹识别系统技术要求	2018/12/28	2019/7/1
247	GB/T 37090-2018	信息安全技术 病毒防治产品安全技术要求和测试评价方法	2018/12/28	2019/7/1
248	GB/T 37091-2018	信息安全技术 安全办公U盘安全技术要求	2018/12/28	2019/7/1
249	GB/T 37092-2018	信息安全技术 密码模块安全要求	2018/12/28	2019/7/1
250	GB/T 37093-2018	信息安全技术 物联网感知层接入通信网的安全要求	2018/12/28	2019/7/1

251	GB/T 37094-2018	信息安全技术 办公信息系统安全管理要求	2018/12/28	2019/7/1
252	GB/T 37095-2018	信息安全技术 办公信息系统安全基本技术要求	2018/12/28	2019/7/1
253	GB/T 37096-2018	信息安全技术 办公信息系统安全测试规范	2018/12/28	2019/7/1
254	GB/T 37931-2019	信息安全技术 Web 应用安全检测系统安全技术要求和测试评价方法	2019/8/30	2020/3/1
255	GB/T 37932-2019	信息安全技术 数据交易服务安全要求	2019/8/30	2020/3/1
256	GB/T 37933-2019	信息安全技术 工业控制系统专用防火墙技术要求	2019/8/30	2020/3/1
257	GB/T 37934-2019	信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求	2019/8/30	2020/3/1
258	GB/T 37935-2019	信息安全技术 可信计算规范 可信软件基	2019/8/30	2020/3/1
259	GB/T 37939-2019	信息安全技术 网络存储安全技术要求	2019/8/30	2020/3/1
260	GB/T 37941-2019	信息安全技术 工业控制系统网	2019/8/30	2020/3/1

		络审计产品安全技术要求		
261	GB/T 37950-2019	信息安全技术 桌面云安全技术要求	2019/8/30	2020/3/1
262	GB/T 37952-2019	信息安全技术 移动终端安全管理平台技术要求	2019/8/30	2020/3/1
263	GB/T 37953-2019	信息安全技术 工业控制网络监测安全技术要求及测试评价方法	2019/8/30	2020/3/1
264	GB/T 37954-2019	信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法	2019/8/30	2020/3/1
265	GB/T 37955-2019	信息安全技术 数控网络安全技术要求	2019/8/30	2020/3/1
266	GB/T 37956-2019	信息安全技术 网站安全云防护平台技术要求	2019/8/30	2020/3/1
267	GB/T 37962-2019	信息安全技术 工业控制系统产品信息安全通用评估准则	2019/8/30	2020/3/1
268	GB/T 37964-2019	信息安全技术 个人信息去标识化指南	2019/8/30	2020/3/1
269	GB/T 37971-2019	信息安全技术 智慧城市安全体系框架	2019/8/30	2020/3/1

270	GB/T 37972-2019	信息安全技术 云计算服务运行 监管框架	2019/8/30	2020/3/1
271	GB/T 37973-2019	信息安全技术 大数据安全管理 指南	2019/8/30	2020/3/1
272	GB/T 37980-2019	信息安全技术 工业控制系统安 全检查指南	2019/8/30	2020/3/1
273	GB/T 37988-2019	信息安全技术 数据安全能力成 熟度模型	2019/8/30	2020/3/1
274	GB/T 38249-2019	信息安全技术 政府网站云计算 服务安全指南	2019/10/18	2020/5/1
275	GB/T 38540-2020	信息安全技术 安全电子签章密 码技术规范	2020/3/6	2020/10/1
276	GB/T 38541-2020	信息安全技术 电子文件密码应 用指南	2020/3/6	2020/10/1
277	GB/T 38542-2020	信息安全技术 基于生物特征识 别的移动智能终端身份鉴别技 术框架	2020/3/6	2020/10/1
278	GB/T 38556-2020	信息安全技术 动态口令密码应 用技术规范	2020/3/6	2020/10/1
279	GB/T 38558-2020	信息安全技术 办公设备安全测 试方法	2020/3/6	2020/10/1

280	GB/T 38561-2020	信息安全技术 网络安全管理支撑系统技术要求	2020/3/6	2020/10/1
281	GB/T 38625-2020	信息安全技术 密码模块安全检测要求	2020/4/28	2020/11/1
282	GB/T 38626-2020	信息安全技术 智能联网设备口令保护指南	2020/4/28	2020/11/1
283	GB/T 38628-2020	信息安全技术 汽车电子系统网络安全指南	2020/4/28	2020/11/1
284	GB/T 38629-2020	信息安全技术 签名验签服务器技术规范	2020/4/28	2020/11/1
285	GB/T 38631-2020	信息技术 安全技术 GB/T 22080 具体行业应用 要求	2020/4/28	2020/11/1
286	GB/T 38632-2020	信息安全技术 智能音视频采集设备应用安全要求	2020/4/28	2020/11/1
287	GB/T 38635.1-2020	信息安全技术 SM9 标识密码算法 第 1 部分：总则	2020/4/28	2020/11/1
288	GB/T 38635.2-2020	信息安全技术 SM9 标识密码算法 第 2 部分：算法	2020/4/28	2020/11/1
289	GB/T 38636-2020	信息安全技术 传输层密码协议 (TLCP)	2020/4/28	2020/11/1
290	GB/T 38638-2020	信息安全技术 可信计算 可信	2020/4/28	2020/11/1

		计算体系结构		
291	GB/T 38644-2020	信息安全技术 可信计算 可信连接测试方法	2020/4/28	2020/11/1
292	GB/T 38645-2020	信息安全技术 网络安全事件应急演练指南	2020/4/28	2020/11/1
293	GB/T 38646-2020	信息安全技术 移动签名服务技术要求	2020/4/28	2020/11/1
294	GB/T 38647.1-2020	信息技术 安全技术 匿名数字签名 第1部分：总则	2020/4/28	2020/11/1
295	GB/T 38647.2-2020	信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制	2020/4/28	2020/11/1
296	GB/T 38648-2020	信息安全技术 蓝牙安全指南	2020/4/28	2020/11/1
297	GB/T 38671-2020	信息安全技术 远程人脸识别系统技术要求	2020/4/28	2020/11/1
298	GB/T 38674-2020	信息安全技术 应用软件安全编程指南	2020/4/28	2020/11/1
299	GB/T 39205-2020	信息安全技术 轻量级鉴别与访问控制机制	2020/10/11	2021/5/1
300	GB/T 39276-2020	信息安全技术 网络产品和服务安全通用要求	2020/11/19	2021/6/1

301	GB/T 39335-2020	信息安全技术 个人信息安全影响评估指南	2020/11/19	2021/6/1
302	GB/T 39412-2020	信息安全技术 代码安全审计规范	2020/11/19	2021/6/1
303	GB/T 39477-2020	信息安全技术 政务信息共享数据安全技术要求	2020/11/19	2021/6/1
304	GB/T 39680-2020	信息安全技术 服务器安全技术要求和测评准则	2020/12/14	2021/7/1
305	GB/T 39720-2020	信息安全技术 移动智能终端安全技术要求及测试评价方法	2020/12/14	2021/7/1
306	GB/T 39725-2020	信息安全技术 健康医疗数据安全指南	2020/12/14	2021/7/1
307	GB/T 39786-2021	信息安全技术 信息系统密码应用基本要求	2021/3/9	2021/10/1
308	GB/T 40018-2021	信息安全技术 基于多信道的证书申请和应用协议	2021/4/30	2021/11/1

参考 <http://openstd.samr.gov.cn>

6.2.2. 行业标准

序号	行标号	标准名称	发布	实施
1	GM/T 0001.1-2012	祖冲之序列密码算法：第 1 部分： 算法描述	20120321	20120321
2	GM/T 0001.2-2012	祖冲之序列密码算法：第 2 部分： 基于祖冲之算法的机密性算法	20120321	20120321
3	GM/T 0001.3-2012	祖冲之序列密码算法：第 3 部分： 基于祖冲之算法的完整性算法	20120321	20120321
4	GM/T 0002-2012	SM4 分组密码算法	20120321	20120321
5	GM/T 0003.1-2012	SM2 椭圆曲线公钥密码算法第 1 部 分：总则	20120321	20120321
6	GM/T 0003.2-2012	SM2 椭圆曲线公钥密码算法第 2 部 分：数字签名算法	20120321	20120321
7	GM/T 0003.3-2012	SM2 椭圆曲线公钥密码算法第 3 部 分：密钥交换协议	20120321	20120321
8	GM/T 0003.4-2012	SM2 椭圆曲线公钥密码算法第 4 部 分：公钥加密算法	20120321	20120321
9	GM/T 0003.5-2012	SM2 椭圆曲线公钥密码算法第 5 部 分：参数定义	20120321	20120321
10	GM/T 0004-2012	SM3 密码杂凑算法	20120321	20120321

11	GM/T 0005-2012	随机性检测规范	20120321	20120321
12	GM/T 0006-2012	密码应用标识规范	20120321	20120321
13	GM/T 0008-2012	安全芯片密码检测准则	20121122	20121122
14	GM/T 0009-2012	SM2 密码算法使用规范	20121122	20121122
15	GM/T 0010-2012	SM2 密码算法加密签名消息语法规范	20121122	20121122
16	GM/T 0011-2012	可信计算 可信密码支撑平台功能与接口规范	20121122	20121122
17	GM/T 0012-2012	可信计算 可信密码模块接口规范	20121122	20121122
18	GM/T 0012-2020	可信计算 可信密码模块接口规范	20201228	20210701
19	GM/T 0013-2012	可信计算 可信密码模块接口符合性测试规范	20121122	20121122
20	GM/T 0014-2012	数字证书认证系统密码协议规范	20121122	20121122
21	GM/T 0015-2012	基于 SM2 密码算法的数字证书格式规范	20121122	20121122
22	GM/T 0016-2012	智能密码钥匙密码应用接口规范	20121122	20121122
23	GM/T 0017-2012	智能密码钥匙密码应用接口数据格式规范	20121122	20121122
24	GM/T 0018-2012	密码设备应用接口规范	20121122	20121122
25	GM/T 0019-2012	通用密码服务接口规范	20121122	20121122
26	GM/T 0020-2012	证书应用综合服务接口规范	20121122	20121122

27	GM/T 0021-2012	动态口令密码应用技术规范	20121122	20121122
28	GM/T 0022-2014	IPSec VPN 技术规范	20140213	20140213
29	GM/T 0023-2014	IPSec VPN 网关产品规范	20140213	20140213
30	GM/T 0024-2014	SSL VPN 技术规范	20140213	20140213
31	GM/T 0025-2014	SSL VPN 网关产品规范	20140213	20140213
32	GM/T 0026-2014	安全认证网关产品规范	20140213	20140213
33	GM/T 0027-2014	智能密码钥匙技术规范	20140213	20140213
34	GM/T 0028-2014	密码模块安全技术要求	20140213	20140213
35	GM/T 0029-2014	签名验签服务器技术规范	20140213	20140213
36	GM/T 0030-2014	服务器密码机技术规范	20140213	20140213
37	GM/T 0031-2014	安全电子签章密码技术规范	20140213	20140213
38	GM/T 0032-2014	基于角色的授权与访问控制技术规 范	20140213	20140213
39	GM/T 0033-2014	时间戳接口规范	20140213	20140213
40	GM/T 0034-2014	基于 SM2 密码算法的证书认证系统 密码及其相关安全技术规范	20140213	20140214
41	GM/T 0035.1-2014	射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安 全级别	20140213	20140213
42	GM/T 0035.2-2014	射频识别系统密码应用技术要求 第 2 部分：电子标签芯片密码应用	20140213	20140213

		技术要求		
43	GM/T 0035.3-2014	射频识别系统密码应用技术要求 第 3 部分：读写器密码应用技术要求	20140213	20140213
44	GM/T 0035.4-2014	射频识别系统密码应用技术要求 第 4 部分：电子标签与读写器通信密码应用技术要求	20140213	20140213
45	GM/T 0035.5-2014	射频识别系统密码应用技术要求 第 5 部分：密钥管理技术要求	20140213	20140213
46	GM/T 0036-2014	采用非接触卡的门禁系统密码应用技术指南	20140213	20140213
47	GM/T 0037-2014	证书认证系统检测规范	20140213	20140213
48	GM/T 0038-2014	证书认证密钥管理系统检测规范	20140213	20140213
49	GM/T 0039-2015	密码模块安全检测要求	20150401	20150401
50	GM/T 0040-2015	射频识别标签模块密码检测准则	20150401	20150401
51	GM/T 0041-2015	智能 IC 卡密码检测规范	20150401	20150401
52	GM/T 0042-2015	三元对等密码安全协议测试规范	20150401	20150401
53	GM/T 0043-2015	数字证书互操作检测规范	20150401	20150401
54	GM/T 0044.1-2016	SM9 标识密码算法 第 1 部分：总则	20160328	20160328
55	GM/T 0044.2-2016	SM9 标识密码算法 第 2 部分：数字签名算法	20160328	20160328

56	GM/T 0044.3-2016	SM9 标识密码算法 第3部分：密钥 交换协议	20160328	20160328
57	GM/T 0044.4-2016	SM9 标识密码算法 第4部分：密钥 封装机制和公钥加密算法	20160328	20160328
58	GM/T 0044.5-2016	SM9 标识密码算法 第5部分：参数 定义	20160328	20160328
59	GM/T 0045-2016	金融数据密码机技术规范	20160328	20160328
60	GM/T 0046-2016	金融数据密码机检测规范	20161223	20161223
61	GM/T 0047-2016	安全电子签章密码检测规范	20161223	20161223
62	GM/T 0048-2016	智能密码钥匙密码检测规范	20161223	20161223
63	GM/T 0049-2016	密码键盘密码检测规范	20161223	20161223
64	GM/T 0050-2016	密码设备管理 设备管理技术规范	20161223	20161223
65	GM/T 0051-2016	密码设备管理 对称密钥管理技术 规范	20161223	20161223
66	GM/T 0052-2016	密码设备管理 VPN 设备监察管理规 范	20161223	20161223
67	GM/T 0053-2016	密码设备管理 远程监控与合规性 检验接口数据规范	20161223	20161223
68	GM/T 0054-2018	信息系统密码应用基本要求	20180208	20180208
69	GM/T 0055-2018	电子文件密码应用技术规范（报批 稿）	20180502	20180502

70	GM/T 0056-2018	多应用载体密码应用接口规范（报批稿）	20180502	20180502
71	GM/T 0057-2018	基于 IBC 技术的身份鉴别规范（报批稿）	20180502	20180502
72	GM/T 0058-2018	可信计算TCM服务模块接口规范(报批稿)	20180502	20180502
73	GM/T 0059-2018	服务器密码机检测规范（报批稿）	20180502	20180502
74	GM/T 0060-2018	签名验服务器检测规范（报批稿）	20180502	20180502
75	GM/T 0061-2018	动态口令密码应用检测规范（报批稿）	20180502	20180502
76	GM/T 0062-2018	密码产品随机数检测要求（报批稿）	20180502	20180502
77	GM/T 0063-2018	智能密码钥匙密码应用接口检测规范	20180918	20180918
78	GM/T 0064-2018	限域通信（RCC）密码检测要求	20180918	20180918
79	GM/T 0065-2019	商用密码产品生产和保障能力建设规范	20190712	20190712
80	GM/T 0066-2019	商用密码产品生产和保障能力建设实施指南	20190712	20190712
81	GM/T 0067-2019	基于数字证书的身份鉴别接口规范	20190712	20190712
82	GM/T 0068-2019	开放的第三方资源授权协议框架	20190712	20190712
83	GM/T 0069-2019	开放的身份鉴别框架	20190712	20190712

84	GM/T 0070-2019	电子保单密码应用技术要求	20190712	20190712
85	GM/T 0071-2019	电子文件密码应用指南	20190712	20190712
86	GM/T 0072-2019	远程移动支付密码应用技术要求	20190712	20190712
87	GM/T 0073-2019	手机银行信息系统密码应用技术要求	20190712	20190712
88	GM/T 0074-2019	网上银行密码应用技术要求	20190712	20190712
89	GM/T 0075-2019	银行信贷信息系统密码应用技术要求	20190712	20190712
90	GM/T 0076-2019	银行卡信息系统密码应用技术要求	20190712	20190712
91	GM/T 0077-2019	银行核心信息系统密码应用技术要求	20190712	20190712
92	GM/T 0078-2020	密码随机数生成模块设计指南	20201228	20210701
93	GM/T 0079-2020	可信计算平台直接匿名证明规范	20201228	20210701
94	GM/T 0080-2020	SM9 密码算法使用规范	20201228	20210701
95	GM/T 0081-2020	SM9 密码算法加密签名消息语法规范	20201228	20210701
96	GM/T 0082-2020	可信密码模块保护轮廓	20201228	20210701
97	GM/T 0083-2020	密码模块非入侵式攻击缓解技术指南	20201228	20210701
98	GM/T 0084-2020	密码模块物理攻击缓解技术指南	20201228	20210701
99	GM/T 0085-2020	基于 SM9 标识密码算法的技术体系	20201228	20210701

		框架		
100	GM/T 0086-2020	基于 SM9 标识密码算法的密钥管理系统技术规范	20201228	20210701
101	GM/T 0087-2020	浏览器密码应用接口规范	20201228	20210701
102	GM/T 0088-2020	云服务器密码机管理接口规范	20201228	20210701
103	GM/T 0089-2020	简单证书注册协议规范	20201228	20210701
119	GM/T 0090-2020	标识密码应用标识格式规范	20201228	20210701
104	GM/T 0091-2020	基于口令的密钥派生规范	20201228	20210701
105	GM/T 0092-2020	基于 SM2 算法的证书申请语法规则	20201228	20210701
106	GM/T 0093-2020	证书与密钥交换格式规范	20201228	20210701
107	GM/T 0094-2020	公钥密码应用技术体系框架规范	20201228	20210701
108	GM/T 0095-2020	电子招投标密码应用技术要求	20201228	20210701
109	GM/T 0096-2020	射频识别防伪系统密码应用指南	20201228	20210701
110	GM/T 0097-2020	射频识别电子标签统一名称解析服务安全技术规范	20201228	20210701
111	GM/T 0098-2020	基于 IP 网络的加密语音通信密码技术规范	20201228	20210701
112	GM/T 0099-2020	开放式版式文档密码应用技术规范	20201228	20210701
113	GM/T 0100-2020	人工确权型数字签名密码应用技术要求	20201228	20210701
114	GM/T 0101-2020	近场通信密码安全协议检测规范	20201228	20210701

115	GM/T 0102-2020	密码设备应用接口符合性检测规范	20201228	20210701
118	GM/Z 4001-2013	密码术语	20130620	20130620
116	GM/Y 5001-2021	密码标准使用指南	20210801	20210801
117	GM/Y 5002-2018	云计算身份鉴别服务密码标准体系	20180601	20180601

参考 <http://www.gmbz.org.cn>

参考文献

- [1] 中国政府网.“十四五”数字经济发展规划.
[EB/OL].http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm
- [2] 新华网.绍兴首例“大数据杀熟”案成功维权[EB/OL].
http://www.zj.xinhuanet.com/2021-07/08/c_1127635869.htm
- [3] 北京市海淀区人民法院.腾讯科技（深圳）有限公司与北京某借公司等一审民事判决书[EB/OL].（2018）京 0108 民初 17738 号
<https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=42b24563187a431ba7e5ab0d003b2e66>
- [4] 北京市海淀区人民法院.腾讯科技（深圳）有限公司与北京某借公司等商标权属、侵权纠纷二审民事判决书[EB/OL].（2018）京 73 民终 2187 号.
[EB/OL]<https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=8b6f5cc22c1943b59914ab1b0040cbe7>
- [5] 中华新闻网.京东 12G 用户数据泄漏！官方：确实存在已修复
[EB/OL].<http://news.sohu.com/20161211/n475529281.shtml>
- [6] 人民日报.“20 万孩童信息被售案”告破抓获 4 名嫌疑人
[EB/OL].http://www.xinhuanet.com/politics/2016-05/06/c_128961444.htm
- [7] 人民网.某论坛被曝泄露用户数据
[EB/OL].<http://it.people.com.cn/n/2015/0106/c1009-26330019.html>
- [8] 观察者网.乌云漏洞报告某易用户数据库疑似泄露
[EB/OL].https://www.sohu.com/a/36512959_115479
- [9] 亿欧智库.圆通 40 万用户信息泄露背后

[EB/OL].<https://xueqiu.com/2766276381/165113805>.

- [10] 腾讯网.257 万条公民银行个人信息被泄露银行行长卖账号
.<https://news.qq.com/a/20161017/002075.htm>
- [11] 新浪综合.广西移动人为造成重大故障 80 万移动用户手机失联
[EB/OL].<http://news.idcquan.com/news/125899.shtml>.
- [12] 浙江省绍兴市越城区人民法院.“某智华胜”涉嫌非法窃取用户信息 30 亿条
[EB/OL].(2019)浙 0602 刑初 1143
号.[https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=b125d8d9e8914a81abc1ab2c009b6dcd)
[docId=b125d8d9e8914a81abc1ab2c009b6dcd](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=b125d8d9e8914a81abc1ab2c009b6dcd).
- [13] 央视网.客户信息被泄露中信银行被银保监会罚款 450 万元[EB/OL].
<https://m.gmw.cn/baijia/2021-03/19/1302176444.html>
- [14] 河南省高级人民法院.中国建设银行股份有限公司汝阳支行、顾三斗储蓄存款
合同纠纷再审审查与审判监督民事裁定书[EB/OL].(2019)豫民申 6252
号.[https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=51a3eaea8a7c427eaf3aaafe0095305e)
[docId=51a3eaea8a7c427eaf3aaafe0095305e](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=51a3eaea8a7c427eaf3aaafe0095305e).
- [15] 河南省高级人民法院.中国建设银行股份有限公司汝阳支行、顾三斗储蓄存款
合同纠纷二审民事判决书.(2019)豫 03 民终 1928
号.[EB/OL].[https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/in](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=d79ec7c6d77541e0afccac93008df3fe)
[dex.html?docId=d79ec7c6d77541e0afccac93008df3fe](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=d79ec7c6d77541e0afccac93008df3fe).
- [16] 河北省涿州市人民法院.非法获取公民的电话信息 10 万多条一审
[EB/OL].(2020)冀 0681 刑初 507
号.[https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=6d01197ce72a4645aaabaced001be2e8)
[docId=6d01197ce72a4645aaabaced001be2e8](https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=6d01197ce72a4645aaabaced001be2e8).
- [17] 齐鲁晚报.青岛胶州 6685 人就诊名单被泄露警方回应[EB/OL].

<http://yuqing.people.com.cn/n1/2020/0416/c209043-31676483.html>.

- [18] 新浪财经.邯郸丛台区政府网站再度泄露个人隐私,区长回应后网页已撤下 [EB/OL].<https://baijiahao.baidu.com/s?id=1709513616936410568&wfr=spider&for=pc>.
- [19] 赛迪研究院网络安全研究所,赛迪区块链研究院.《2020-2021 中国商用密码产业发展报告》[N].2021.5
- [20] 杨斌. IBC 和 PKI 组合应用研究[D]. 解放军信息工程大学电子技术学院, 2009.
- [21] Wenbo Mao. 现代密码学理论与实践[M]. 王继林,伍前红等译. 北京:电子工业出版社. 2004
- [22] 林璟铨,马原,荆继武,王琼霄,雷灵光,蔡权伟,王雷.适用于云计算的基于 SM2 算法的签名及解密方法和系统[P].中国, CN104243456A,2014.
- [23] 王卫红, 李晓明 计算机网络与互联网[M] 北京 机械工业出版社,2009
- [24] 李涛著. 网络安全概论[M] 北京: 电子工业出版社,2004.
- [25] 李学锋,陈丹.基于 SSL 的 VPN 关键技术的应用研究 2008
- [26] 高小鹏,陈雷,龙翔.计算机工程 2004 年 12 月 Vol.30 No.23 同步链路密码机中的流量控制技术
- [27] 朱效农 DDN 专网链路加密新探索
- [28] 龙桂鲁 牛鹏皓 北京科技报/2020 年/11 月/2 日/第 012 版 量子通信:能发现窃听的通信
- [29] 任晶雯 孙宇清 基于关联规则挖掘的背景知识攻击及隐私保护研究
- [30] 宋健,许国艳, 仝荣朋 计算机应用 2016 基于差分隐私的数据匿名化隐私保护方法
- [31] 刘艮,蒋天发.同态加密技术及其在物联网中的应用研究[J].信息网络安全,2011(5)
- [32] LiZhi,ZhuXinglei,LianYong, etal. Constructingsecure content dependent watermarking scheme using homomorphic encryption [C] // Proc of the 2007

IEEE Int Conf on Multimedia and Exposition (ICME2007). Piscataway, NJ: IEEE, 2007

- [33] 刘明洁 王安 计算机研究与发展 2014, 51 (12) 全同态加密研究动态及其应用概述
- [34] 苏冠通 徐茂桐 《信息通信技术与政策》2019 年 5 月第 5 期 安全多方计算技术与应用综述
- [35] 张艳硕 李泽昊 北京电子科技学院学报 2020 年 12 月 第 28 卷 第 4 期零知识证明的分层次案例化教学设计
- [36] 王瑞锦, 唐榆程, 裴锡凯, 郭上铜 张凤荔 计算机科学 Vol.48,No.11A, Nov.2021 基于轻量级同态加密和零知识证明的区块链隐私保护方案
- [37] 张玉清,王晓菲,刘雪峰,刘玲.云计算环境安全综述[J].软件学报,2016,27(06):1328-1348.DOI:10.13328/j.cnki.jos.005004.
- [38]张兴兰,刘祥.安全高效的可验证大型线性方程组求解外包计算方案[J].网络与信息安全学报,2017,3(06):1-7.
- [39] 冯登国,刘敬彬,秦宇,冯伟.创新发展中的可信计算理论与技术[J].中国科学:信息科学,2020,50(08):1127-1147.
- [40] 杜玲. 面向多媒体认证的数字水印技术研究[D].天津大学,2016.
- [41] 夏文财.数字水印简介[J].科教导刊:电子版,2017(10):1.
- [42] 郑美玲,陈瀚,俞洪水,朱健萍.电子签章系统中 PKI 与数字水印技术[J].科学技术创新,2021(30):101-103.
- [43] 师立华. 档案管理中电子文件防篡改技术的应用及启示[J].管理学家,2021(7):81-83.
- [44] 章睿. 基于可信计算技术的隐私保护研究[D].北京交通大学,2011.
- [45] 中科三方.《为什么要求做“密评”？》[N].2021.6.23
- [46] 夏鲁宁,马原,郑昉昱.《深度解读密评新国标 GB/T 39786-2021》[N].2021.4
- [47] 山志.《关基、等保与密评的关系》[N].2020.9.9

- [48] GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》，国家标准化管理委员会，2021年3月发布
- [49] 《信息系统密码应用测评要求》，中国密码学会密评联委会,2020年12月发布
- [50] 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》国家标准化管理委员会，2020年3月发布
- [51] 《信息系统密码应用测评过程指南》，中国密码学会密评联委会,2020年12月发布
- [52] 《信息系统密码应用高风险判定指引》，中国密码学会密评联委会,2021年12月发布
- [53] 《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,2021年12月发布
- [54] GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》，国家标准化管理委员会，2019年5月发布
- [55] 《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,2020年12月发布
- [56] 霍伟,郭启全,马原.商用密码应用与安全性评估[M].电子工业出版社.2020.4
- [57] [日]结城浩 著,周自恒 译.图解密码技术:第3版[M]..北京:人民邮电出版社.2016.6
- [58] 刘建华主编,孙韩林副主编.物联网安全[M].中国铁道出版社,2013.09

作者介绍

炼石网络是一家数据安全技术创新厂商，先后获得安天、国科嘉和、腾讯等投资。炼石提倡“以数据为中心的新安全理念”，核心自研产品是 CASB 数据安全平台，该产品夺得第七届互联网安全大会(ISC 2019)首届“创新独角兽沙盒大赛”总冠军。技术特色是免开发改造应用的数据保护、高性能国产密码和去标识化技术，为政府、金融、运营商、交通、教医旅等用户提供个人信息保护、商业秘密保护、国密合规改造。面向《密码法》《数据安全法》《个人信息保护法》等法律法规，企业重要数据与个人信息亟待提升防护水平与合规改造。炼石基于面向切面数据安全技术，构建高覆盖率的安全增强点组合，融合识别、加密、去标识化、检测/响应、追溯等能力，有效保护结构化与非结构化数据，打造免开发改造的应用级数据安全防护，实现分布式保护、集中式管控，可应用在数据存储、使用、加工、传输、提供等生命周期。炼石方案可在不影响业务的前提下敏捷实施上线，将安全与业务在技术上解耦、但又在能力上融合交织，实现主体到应用内用户、客体到字段级的防护，打造实战化数据安全防护体系。欢迎感兴趣的合作伙伴，随时和我们联系，共同掘金“数据安全市场”。



让数据开发利用更安全



www.ciphergateway.com

support@ciphergateway.com

400-819-0181