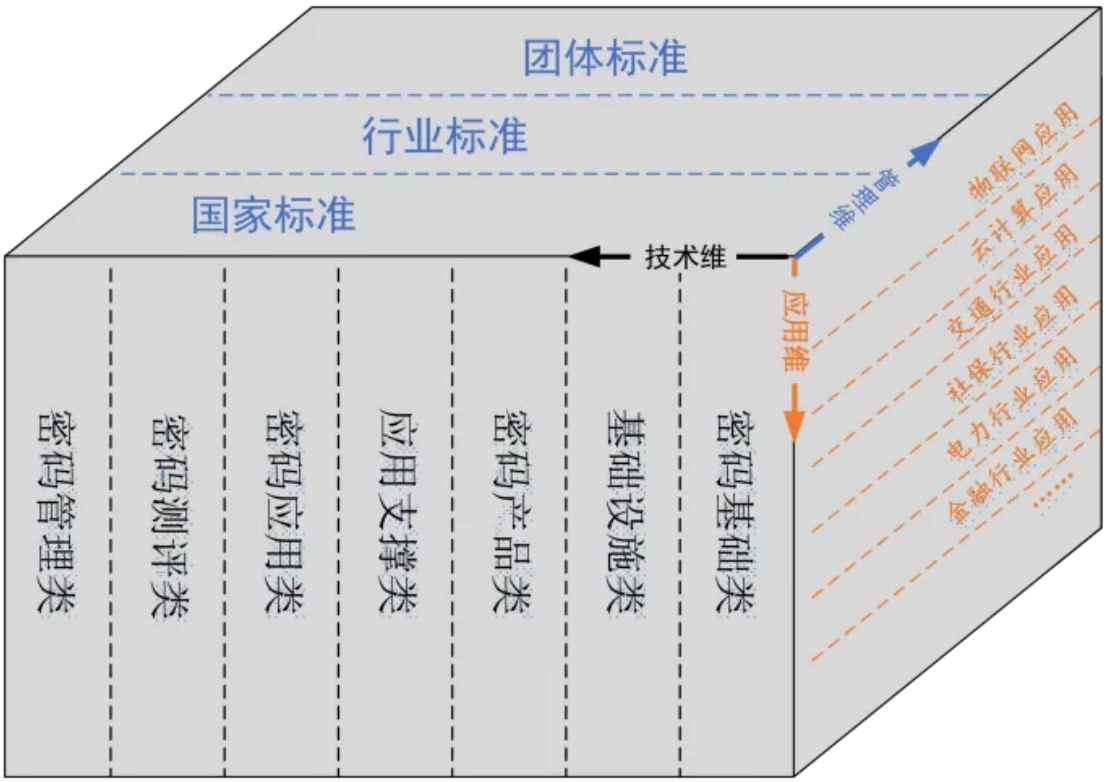
密码体系

我国商用密码标准体系框架分为管理维、技术维、应用维，体系框架图如下所示。



行业标准由国家密码管理局归口管理，团体标准由密码领域学会、行业协会等社会组织协调相关市场主体共同制定以满足市场和创新需要。

商用密码标准体系的详细内容可参考密码行业标准化技术委员会网站（www.gmbz.org.cn）发布并年度更新的GM/Y 5001《密码标准使用指南》。

> 行业标准化技术委员会

网络安全等级和密码应用等级

GB/T 39786—2021中的密码应用等级与网络安全等级保护的级别存在对应关系。信息系统根据GB/T 22240—2020《信息安全技术 网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级，即等保定级为第一级的网络与信息系统应遵循GB/T 39786第一级密码应用基本要求，等保定级为第二级的网络与信息系统应遵循GB/T 39786第二级密码应用基本要求，以此类推。

密码鉴别要求

网络和通信安全、设备和计算安全、应用和数据安全三个层面身份

网络和通信安全层面针对的是建立网络通信链路的密码设备（如IPSec/SSL VPN）；设备和计算安全层面针对的是登录设备的管理员、用户等人员；应用和数据安全层面针对的是具体应用的用户。因此，需要根据信息系统密码应用需求，在不同层面实现身份鉴别机制，保证各层面鉴别对象身份的真实性。

密码国标文件

1、 GB/T 33133-2016 《信息安全技术 祖冲之序列密码算法》

2、 GB/T 32907-2016 《信息安全技术 SM4分组密码算法》

3、 GB/T 32918-2016 《信息安全技术 SM2椭圆曲线公钥密码算法》

4、 GB/T 32905-2016 《信息安全技术 SM3密码杂凑算法》

5、 GB 15843-2008 《信息技术 安全技术 实体鉴别 》

6、 GB/T 15852.1-2008 《信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制》

7、 GB/T 17903 《信息技术 安全技术 抗抵赖 》

8、 GB/T 16264.8-2005 《信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架》

9、 GB/T 16264.5-2008 《信息技术 开放系统互连 目录 第5部分：协议规范》

10、 GB/T 18238-2016《信息技术 安全技术 散列函数》

11、 GB/T 17964-2008 《信息安全技术 分组密码算法的工作模式》

12、 GB/T 17902-2017 《信息技术 安全技术 带附录的数字签名 》

13、 GB/T 15851-1995 《信息技术 安全技术 带消息恢复的数字签名方案》

14、 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》

15、 GB/T 33560-2017 《信息安全技术 密码应用标识规范》

16、 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》

17、 GB/T 35276-2017 《信息安全技术 SM2密码算法使用规范》

18、 GB/T 19714-2005 《信息技术 安全技术 公钥基础设施 证书管理协议》

19、 GB/T 25056-2010 《信息安全技术 证书认证系统密码及其相关安全技术规范》

20、 GB/T 20518-2006 《信息安全技术 公共基础设施 数字证书格式》

21、 GB/T 20519-2006 《信息安全技术 公钥基础设施 特定权限管理中心技术规范》

22、 GB/T 20520-2006 《信息安全技术 公钥基础设施 时间戳规范》

23、 GB/T 21053-2007 《信息安全技术 PKI系统安全等级保护技术要求》

24、 GB/T 21054-2007 《信息安全技术 PKI系统安全等级保护评估准则 》

25、 GB/T 17913-2005 《信息技术 安全技术 公钥基础设施 在线证书状态协议》

26、 GB/T 25061-2010 《信息安全技术 公钥基础设施 XML数字签名语法与处理规范》

27、 GB/T 25064-2010 《信息安全技术 公钥基础设施 电子签名格式规范》

28、 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》

29、 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》

30、 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》

31、 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》

32、 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》

33、 GB/T30275-2013 《信息安全技术 鉴别与授权 认证中间件框架与接口规范》

34、 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》

35、 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》

36、 GB/T35285-2017 《信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求》

37、 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》

38、 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》

39、 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》

40、 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》

41、 GB/T 29829-2015 《信息安全技术 可信计算密码支撑平台功能与接口规范》

42、 GB/T 35291-2017 《信息安全技术 智能密码钥匙应用接口规范》

43、 GB/T 17901-1999 《信息技术 安全技术 密钥管理》

44、 GB/T 32915-2016 《信息安全技术 二元序列随机性检测方法》

密码策略

主题	描述
强制实施密码历史记录	介绍 **强制执行密码历史记录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最长密码使用期限	介绍 **最长密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最短密码使用期限	介绍 **最短密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最短密码长度	介绍 **最小密码长度** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
密码必须符合复杂性要求	介绍 **密码必须满足复杂性要求** 安全策略设置的最佳做法、位置、值和安全注意事项。
用可还原的加密来存储密码	介绍 **使用可逆加密** 安全策略设置存储密码的最佳做法、位置、值和安全注意事项。

> 安全策略设置 (Windows 10) - Windows security | Microsoft Learn

服务器类型或组策略对象 (GPO)	默认值
默认域策略	42 天
默认域控制器策略	未定义
独立服务器默认设置	42 天
域控制器有效的默认设置	42 天
成员服务器有效的默认设置	42 天
客户端计算机上的有效 GPO 默认设置	42 天

服务器类型或组策略对象 (GPO)	默认值
默认域策略	七个字符
默认域控制器策略	未定义
独立服务器默认设置	零个字符
域控制器有效默认设置	七个字符
成员服务器有效默认设置	七个字符
客户端计算机上有效的 GPO 默认设置	零个字符

1. 密码不能包含用户的 samAccountName (帐户名称) 值或整个 displayName (Full Name 值) 。 这两个检查不区分大小写。

   将完全检查 samAccountName，只是为了确定它是否是密码的一部分。 如果 samAccountName 的长度少于三个字符，则跳过此检查。 displayName 针对分隔符进行分析：逗号、句点、短划线或连字符、下划线、空格、井号和制表符。 如果找到这些分隔符中的任何一个，则将拆分 displayName，并且所有已分析部分 (令牌) 确认不包含在密码中。 将忽略短于三个字符的标记，并且不会检查令牌的子字符串。 例如，名称“Erin M. Hagens”拆分为三个标记：“Erin”、“M”和“Hagens”。 由于第二个标记只有一个字符长，因此将被忽略。 因此，此用户不能将密码包含“erin”或“hagens”作为密码中的任何一个子字符串。

2. 密码包含以下三个类别中的字符：
   - 欧洲语言的大写字母 (A 到 Z，带有音调符号、希腊语和西里尔文字符)
   - 欧洲语言的小写字母 (到 z，sharp-s，带有音调符号、希腊语和西里尔字符)
   - (0 到 9)
   -) (特殊字符的非字母数字字符： (~！ @#$%^&*_-+='|\ () {}[]：;“'<>,.?/) 欧元或英镑等货币符号不计入此策略设置的特殊字符。
   - 分类为字母字符但不是大写或小写的任何 Unicode 字符。 此组包含来自亚洲语言的 Unicode 字符。

Google

符合密码的相关要求

密码可以是字母、数字和符号（仅限 ASCII 标准字符）的任意组合。不支持重音符号和带重音符号的字符。

不能使用存在下列情况的密码：

- 安全系数特别低。例如：“password123”
- 您曾在自己的帐号中使用过
- 以空格开头或结尾