GM/Y 5006-2024

信息系统密钥生命周期选取研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘要

密码技术作为网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是保障网络空间安全的关键技术。密钥的安全则是密码技术正常发挥其预期作用的基础。

本研究报告首先对本报告的编制背景、意义进行了介绍，其次对国内外的相关研究现状进行调研分析；然后研究报告对于目前商用密码算法标准体系中所涉及的密钥种类进行分析；最后给出了各类密钥的推荐生命周期长度。

关键词：密钥管理、密钥更新、密钥生命周期长度

目录

前言

《信息系统密钥生命周期选取指南》项目是密标委根据国家密码管理局批准的《2020 年密码行业标准制/修订计划》下达的标准研究任务，项目所属工作组为基础工作组。中国科学院信息工程研究所作为牵头单位，成立相应的编制工作组，组织完成该标准的编制工作。

本研究报告主要用于指导信息系统密码应用中的密钥生命周期的选取，确保信息系统中密钥在长期使用周期内的安全，也可以作为商用密码应用安全性评估中密钥管理评估环节的重要参考。

本报告起草单位：中国科学院信息工程研究所、中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、深圳市纽创信安科技开发有限公司、鼎铉商用密码测评技术(深圳)有限公司、智巡密码（上海）检测技术有限公司、国家信息技术安全研究中心、财付通支付科技有限公司

本报告主要起草人员：郑昉昱、林璟锵、马原、贾世杰、陈天宇、吕娜、李向锋、傅大鹏、邹超、刘硕、刘军荣、韩玮、吴冬宇、范佳奇、何畅、吴怡。

信息系统密钥生命周期选取研究

1. 概述

1.1. 背景

我国密码算法体系基本形成，椭圆曲线公钥密码算法SM2、密码杂凑算法SM3、分组密码算法SM4、序列密码算法ZUC、标识密码算法SM9等发布实施，标志着我国商用密码算法体系已基本形成；密码标准体系日益完善，覆盖了密码算法、产品、技术、检测、应用等各个方面；算法国际标准化工作取得重大突破，ZUC 算法成为4G国际标准，SM2、SM3、SM4、SM9成为ISO/IEC国际标准；在应用推进方面，国家专门成立了协调推进机构，商用密码已经在金融、教育、社保、交通、通信、能源、公共安全、国防工业等重要领域得到广泛应用。以上这些都表明着我国商用密码在法治化、规范化基础上，逐步向科学化、体系化方向迈进。

除了要使用合规、安全的密码算法之外，为了前向/后向安全、考虑到可能发生的安全事件，信息系统中的密钥需要定期更换，所以密码保障系统需要支持自动或者手动方式的密钥更新功能。NIST SP 800-57 给出了各种应用场景推荐使用的密码算法安全强度和密钥更新周期，包括数据传输、数据存储、数字签名、鉴别、授权、密钥传输和封装、密钥协商、随机数等不同应用场景。但是目前国内缺少相应的标准规范，没有统一、科学的密钥生命周期要求，在某些信息系统中，一些密钥长期使用不进行更换，带来了潜在的密钥泄露风险，将严重影响信息系统密码应用的安全性。

本项目主要研究信息系统密码应用中的密钥生命周期的选取，可以作为商用密码应用安全性评估中密钥管理评估环节的重要参考。

1.2. 引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 15852.1 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
- GB/T 15852.2 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
- GB/T 15843.2 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 15843.3 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
- GB/T 15843.4 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
- GB/T 32905 信息安全技术 SM3密码杂凑算法
- GB/T 32907 信息安全技术 SM4分组密码算法
- GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法
- GB/T 36624 信息技术 安全技术 可鉴别的加密模式

- GB/T 37092 信息安全技术 密码模块安全要求
- GB/T 38635 信息安全技术 SM9标识密码算法
- GB/T 39786 信息安全技术 信息系统密码应用基本要求
- GM/Z 4001 密码术语

2. 国内外研究现状

本章节主要介绍密钥生命周期长度选取相关的国内外研究现状。国际上，NIST SP 800-57为不同类型的密钥提出了比较完备的密钥生命周期长度选取指南；而我国的信息系统密码应用标准GM/T 0054和一些密码产品（如VPN产品等）的标准规范也给出了对密钥更新的要求。

2.1 NIST SP 800-57

NIST SP 800-57 全名为 *Recommendation for Key Management*，面向的读者包括系统或应用程序所有者和管理者、密码模块开发人员、密码开发人员以及系统，共分为 3 部分：

- 第 1 部分（General）包含基本的密钥管理指南。它主要为开发人员和系统管理员提供与密钥管理相关的“最佳实践”，包括：
  1) 定义了密码技术可以提供的安全服务；
  2) 提供了密码算法相关的背景知识；
  3) 对密钥和其他密钥相关信息对密钥进行分类，并给出了不同类型的密钥所需的保护方式；
  4) 标识密钥在其生命周期内可能存在的状态；
  5) 确定密钥管理中涉及的功能；
  6) 讨论各种密钥管理问题，包括密钥用法、密码生命周期长度、域参数验证、公钥验证、密钥库管理、可审计性、生存性以及密码算法和密钥大小选择指南。
- 第 2 部分（*Best Practices for Key Management Organizations*）提供了框架和一般指导，以满足美国联邦政府对密钥管理制度的法定和政策要求。
- 第 3 部分（*Application-Specific Key Management Guidance*）用于解决与当前现有应用相关的密钥管理问题。

与本研究报告最为相关的部分是 5.1 小节“密钥类型和其他信息”（*Key Types and Other Information*）以及 5.3 小节“密钥生命周期”（*Cryptoperiods*）和 5.6 小节“密钥算法和密钥长度选取指南”（*Guidance for Cryptographic Algorithm and Key-Size Selection*）

2.1.1 密钥类型

NIST SP 800-57 根据密钥的用途和所涉及的密码算法，将密钥分为 19 类，分别是：

- *Private signature key*：签名私钥是用于生成数字签名的长期非对称密钥对中的私钥。如果处理得当，签名私钥可用于提供源身份鉴别和完整性身份鉴别，并支持消息、文档或存储数据的不可否认性。
- *Public signature-verification key*：签名公钥是用于生成数字签名的长期非对称密钥对中的公钥，公钥算法使用该密钥来提供源身份鉴别和完整性身份鉴别，并为消息、文档或存储数据提供不可否认性服务。

- *Symmetric authentication key*：对称鉴别密钥与对称密钥算法一起使用，为通信会话、消息、文档或存储数据提供身份鉴别和完整性鉴别。注意，对于对称密钥算法的可鉴别加密模式（比如 GCM），鉴别和加密使用同一密钥。
- *Private authentication key*：私有身份鉴别密钥是非对称密钥对中的私钥，该密钥对与公钥算法一起使用，以在建立经过身份鉴别的通信会话或授权执行某些操作时，为实体提供身份保证（即身份鉴别）。
- *Public authentication key*：公共身份鉴别密钥是非对称密钥对中的公钥，该密钥对与公钥算法一起使用，以在建立经过身份鉴别的通信会话或授权执行某些操作时，为实体提供身份保证（即身份鉴别）。
- *Symmetric data-encryption key*：对称数据加密密钥与对称密钥算法一起用于对数据进行机密性保护（即加密明文数据）。同样的密钥也用于解除机密性保护（即，解密密文数据）。注意，对于对称密钥算法的鉴别加密操作模式（比如 GCM），源鉴别和加密使用同一个密钥。
- *Symmetric key-wrapping key*：对称密钥包装密钥（有时称为密钥加密密钥）配合对称密钥算法使用，用于加密其他密钥。用于加密密钥的密钥包装密钥也用于反向加密操作（即，解密密钥密文）。根据使用密钥的算法，密钥也可用于提供完整性保护。
- *Symmetric random number generation keys*：对称随机数生成密钥用于生成随机数或随机比特。
- *Symmetric master key/key-derivation key*：对称主密钥被对称加密方法用来派生其他对称密钥（例如数据加密密钥或密钥包装密钥）。主密钥也称为密钥派生密钥。
- *Private key-transport key*：密钥传输私钥是非对称密钥对中的私钥，用于解密被相应公钥加密的密钥。密钥传输密钥通常用于建立对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。
- *Public key-transport key*：密钥传输公钥是用于加密密钥的非对称对中的公钥。这些密钥用于建立对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。所建立密钥的密文形式可被存储下来以供稍后使用私钥传输密钥进行解密。
- *Symmetric key-agreement key*：对称密钥协商密钥用于使用对称密钥协商算法建立对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。
- *Private static key-agreement key*：静态密钥协商私钥是非对称密钥对中的长期私钥，该密钥对用于建立对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。
- *Public static key-agreement key*：静态密钥协商公钥是非对称密钥（公共）密钥对中的长期公共密钥，该密钥对用于建立对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。
- *Private ephemeral key-agreement key*：临时密钥协议私钥是非对称密钥对中的短期私钥，这些密钥对仅用于建立一个或多个对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。
- *Public ephemeral key-agreement key*：临时密钥协商公钥是非对称密钥对中的短期公钥，在单个密钥建立事务中用于建立一个或多个对称密钥（例如密钥包装密钥、数据加密密钥或 MAC 密钥）和（可选的）其他密钥材料（例如初始向量）。

- *Symmetric authorization key*：对称授权密钥用于使用对称加密方法向实体提供权限。负责监视和授予访问权限的实体以及寻求访问资源的实体都持有授权密钥。
- *Private authorization key*：私密授权密钥是非对称密钥对中的私钥，该密钥对用于证明所有者的权限（例如使用数字签名）。
- *Public authorization key*：公共授权密钥是非对称密钥对中的公钥，用于验证持有相应私密授权密钥的实体的权限。

2.1.2 密钥生命周期长度

NIST SP 800-57 中，密钥生命周期是指特定密钥被合法实体授权使用或给定系统的密钥生效的时间跨度。合适的密钥生命周期应能够：

- 限制可用于密码分析的信息量（例如用密钥加密的明文和密文对的数量）；
- 限制单个密钥泄露导致的数据曝光量；
- 限制特定算法的使用（例如，将其限制在该算法的预估有效寿命内）；
- 限制敌手尝试穿透物理、程序和逻辑访问机制等密钥保护措施的可用时间；
- 在密钥被无意中泄露给未授权实体后，限制信息可能被破解的时间窗口；
- 限制计算密集型密码分析的可用时间。

密钥生命周期被定义为任意时间段，或者由密钥保护的最大数据量来确定。如果密钥被泄露，其剩余的密钥生命周期将不再生效。

（1） 影响密钥生命周期长度的因素

影响密钥生命周期长度的因素主要包括：

- 密码机制的强度（例如算法、密钥长度、分组大小和操作模式）；
- 机制的具体实现（例如 FIPS 140 中第 4 级的实现或个人计算机上的软件实现）；
- 操作环境（例如安全的访问受限设施、开放式办公环境或公众可访问的终端）；
- 人员流动（例如系统管理员和 CA 系统人员的流动）；
- 数据流量或事务数；
- 数据的安全周期；
- 算法使用所需的限制（例如避免一次性操作被重复执行所需的最大调用次数）；
- 安全功能（例如数据加密、数字签名、密钥派生或密钥保护）；
- 密钥更新的方法（例如键盘输入、使用人工无法直接访问密钥的密钥加载设备载入、或 PKI 内的远程载入）；
- 使用的密钥更新或派生过程；
- 网络中共享公有密钥的节点数；
- 密钥的副本数及其分发方法；
- 敌手对信息的威胁（例如其可用于发起攻击的技术实力和财力资源）；
- 新的破坏性技术（如量子计算机）对信息的威胁。

一般来说，短的密钥生命周期可以增强安全性。例如，如果敌手拥有的单个密钥加密的信息量有限，则针对该加密算法的密码分析可能不太容易成功。另一方面，鉴于手动密钥分发方法易受人为错误和脆弱性影响，频繁的密钥变更反而会增加密钥泄露的风险。在这些情况下，特别是在硬件中使用非常强的加密技术时，使用较少的、控制良好的手动密钥分发比使用更频繁的、控制较差的手动密钥分发更为谨慎。

在采用足够强度密码算法时，物理访问控制、逻辑访问控制和过程控制等因素对密钥生命周期选择的影响往往超过算法和密钥大小等因素。面对核准的算法、操作模式和密钥大小的情况，对手通过渗透或破坏系统来访问密钥所花费的时间和资源要比发起和执行密码攻击少很多。

用于保护通信数据机密性的密钥通常比用于保护存储数据的密钥具有更短的密钥生命周期。对于存储的数据，密钥生命周期通常更长，因为生成新密钥和重新加密所有数据的开销可能非常繁重。

在某些情况下，更换密钥的成本非常高。例如对非常大的数据库或分布式数据库进行解密和重新加密，以及撤销和替换海量密钥（例如在地理上和组织上散布着非常多的密钥持有者）。在这种情况下，使用更长的密钥生命周期和更强的安全措施可能更合理（例如耗费巨大且不方便的物理、程序和逻辑访问控制，以及使用强大的密码机制来支持更长的密钥生命周期，即便这可能导致显著的额外开销）。

（2） 非对称密钥对的生命周期长度选择

对非对称密钥对而言，其公私钥都有自己的密钥生命周期。密钥对中的一个密钥用于实施密码技术保护（例如创建数字签名），其密钥生命周期称为“发起者使用周期”。密钥对中的另一个密钥用于处理受保护的信息（例如验证数字签名）；它的密钥生命周期称为“接收者使用周期”。密钥对的发起者和接收者的使用周期通常同时开始，但接收者的使用周期可能会超出发起者的使用周期。例如：

- 数字签名密钥对中，签名私钥对数据进行签名，因此其密钥生命周期被认为是发起者使用周期。签名公钥用于验证数字签名；其密钥生命周期被视为接收者使用期。
- 对用于生成数字签名并将其作为源头证明的签名私钥（即，用于来源鉴别）而言，发起者使用周期（即，私钥可用于生成签名的期限）通常短于接收者使用周期（即，可由签名公钥验证签名的期限）。在这种情况下，私钥只在一段固定的时间内使用，之后密钥所有者应销毁私钥，而公钥则可以保留更长的时间，用来验证签名。
- 用于对挑战信息进行签名的源鉴别私钥的密钥生命周期基本上与相应公钥（即，源鉴别公钥）的密钥生命周期相同。也就是说，当私钥不再用于签名挑战时，就不再需要公钥。在这种情况下，发起者和接收者的使用周期是相同的
- 对于密钥传输密钥，公钥用于应用保护（即加密数据），因此其密钥生命周期将被视为发起者使用周期；而私钥用于解密加密数据，因此其密钥生命周期将被视为接收者使用周期。发起者使用周期（即，公钥可用于加密的周期）通常短于接收者使用周期（即，加密信息可被解密的周期）。
- 对于密钥协商算法，密钥对中两个密钥的密钥生命周期通常相同。

如果通过证书中签发公钥，则由证书中的 notBefore 和 notAfter 字段标明有效期。证书可以重新签发（即，可以签发一个新证书，拥有新的有效期，但保持原有公钥）。同一公钥的原始证书和所有后续更新的证书的有效期所涵盖的有效期范围不得超过用于实施密码技术保护的密钥（即具有发起者使用期的密钥）的密钥生命周期的开始和结束日期。

（3） 对称密钥使用周期和密钥生命周期

对于对称密钥，单个密钥同时被用于保护（例如，对数据加密或计算 MAC）和处理受保护信息（例如，解密密文数据或验证 MAC）。可以对数据进行加密保护的时间段称为发起者使用期，处理受保护信息的时间段则称为接收者使用期。在发起者使用期结束后，不得使用对称密钥提供保护。接收者的使用期限可能会超过发起者使用周期。也就是说，在发起者使用周期结束后一段时期内，被保护的数据仍可以被接收者处理。但是，在许多情况下，发起者和接收者的使用周期是相同的。对称密钥的总“密钥生命周期”是从发起者使用周期开始到接收者使用周期结束的时间段，尽管发起者使用周期历来都被用作密钥的密钥生命周期。

注意，在某些情况下，预先设定的密钥生命周期可能不足以保证受保护数据的安全寿命。如果所需的安全期限超过密钥生命周期，则可能需要使用新密钥重新应用保护。

对称密钥的密钥生命周期示例如下：

- 当对称密钥仅用于保护通信安全时，从发起者应用保护到接收者处理的时间段可以忽略不计。在这种情况下，密钥在整个密钥生命周期（即，发起者使用周期和接收者使用周期相同）内可被授权用于任一目的。
- 当使用对称密钥保护存储的信息时，发起者的使用期限（发起者对存储的信息应用加密保护时）可能比接收者的使用期限（处理存储的信息时）早得多。在这种情况下，密钥生命周期从授权使用密钥应用保护的初始时间开始，并以授权使用该密钥进行数据处理的最新时间结束。一般来说，接收者对所存储信息的使用周期将在发起者使用周期之后继续，以便所存储的信息可以在稍后的时间被鉴别或解密。
- 当使用对称密钥来保护存储的信息时，接收者的使用期可能会在发起人的使用期开始之后开始。例如，信息可以在进入某些存储介质上之前被加密。在稍后的某个时间，可以将密钥分发下去以便解密和恢复信息。

（4） 推荐密钥生命周期长度

密钥类型、使用环境和数据特征可能影响给定密钥所需的密钥生命周期。下面提供了各种密钥类型的建议密钥生命周期。注意，建议的密钥生命周期只是粗略的数量级；根据使用密钥的应用程序和环境，可能需要更长或更短的密钥生命周期。然而，当分配比下文建议的更长的密钥生命周期时，应认真考虑可能带来的风险。大多数推荐的密钥生命周期都是基于对最高运行效率的期望和对使用环境最低标准的假设得出的（参见 FIPS 140 和 SP 800-37）。

1） *Private signature key:*

a) 类型考虑：一般来说，签名私钥的密钥生命周期可能短于相应的签名公钥的密钥生命周期。当 CA 签发相应的公钥时，签名私钥的密钥生命周期将在最后一个为公钥颁发的证书的 notAfter 日期时来临时结束。

b) 密钥生命周期：考虑到使用核准的算法和密钥长度，以及密钥存储和使用环境的安全性将随着密钥提供完整性保护的过程的敏感性和/或关键性的增加而增加的预期，建议最大密钥生命周期约为一到三年。签名私钥应在其密钥生命周期结束时销毁。

2） *Public signature-verification key:*

a) 类型考虑：一般来说，签名公钥的密钥生命周期可能比相应的签名私钥的密钥生命周期长。实际上，密钥生命周期是需要验证该签名私钥产生的任何签名的时间段。长的签名公钥密钥生命周期（比签名私钥的密钥生命周期长）带来安全风险相对最小。

b) 密钥生命周期：密钥生命周期可能长达数年。然而，由于保护机制长期暴露在恶意攻击下，签名的可靠性也会随着时间的推移而降低。也就是说，对于任何给定的算法和密钥大小，（数字签名）面对密码分析的脆弱性都会随着时间的推移而增加。尽管选择最强大的算法和较大的密钥长度可以最大限度地减少这种脆弱性，但这样对于私钥的安全性并不会提升，因为私钥面临的往往是针对物理、程序和逻辑访问控制等机制的攻击。一些系统使用密码学时间戳函数在每个签名消息上附加不可伪造的时间戳，即便签名私钥的密钥生命周期已经过时，也可以使用相应的签名公钥来验证其时间戳在签名私钥的密钥生命周期内的消息上的签名。在这种情况下，靠密码学时间戳函数来

保证消息签名是在签名私钥的发起者使用期间内产生的。

3） *Symmetric authentication key:*

a) 类型考虑：对称鉴别密钥的密钥生命周期取决于被保护信息类型的敏感度以及密钥和相关算法提供的保护类型。对于非常敏感的信息，身份验证密钥可能需要被受保护信息的独享。对于不太敏感的信息，适当的加密周期可以超出密钥的单次使用。对称鉴别密钥的发起者使用周期适用于在对信息应用原始加密保护时使用该密钥（例如，计算 MAC）；在发起人使用周期结束后，不得使用该密钥对已经计算过 MAC 的信息生成新的 MAC。然而，在发起人使用期之后，密钥可能需要继续保持有效（即，接收者使用周期可能延伸到发起者使用周期之后），用于验证受保护数据上的 MAC。接收者使用周期是需要验证在发起者使用期内生成的 MAC 的时间段。注意，如果 MAC 密钥被泄露，则对手可能修改消息，然后重新计算 MAC。

b) 密钥生命周期：在使用了核准的算法和密钥长度后，如果希望密钥存储和使用环境的安全性随着密钥提供完整性保护的过程的敏感性和/或关键性的增加而增加，那我们建议发起者使用周期不超过两年，并且建议接收者使用期限不超过发起者使用周期结束后的三年。

4） *Private authentication key:*

a) 类型考虑：可以多次使用身份鉴别私钥来确保数据完整性和身份鉴别。在大多数情况下，鉴别私钥的密钥生命周期与相应公钥的密钥生命周期相同。

b) 密钥生命周期：身份鉴别私钥的密钥生命期长度不超过一年或两年，这取决于其使用环境和已鉴别信息的敏感性/关键性。

5） *Public authentication key:*

a) 类型考虑：在大多数情况下，身份鉴别公钥的密钥生命周期与相应身份鉴别私钥的密钥生命周期相同。密钥生命周期实际上是需要鉴别由相应的鉴别私钥保护的信息发起者身份（即，需要鉴别身份）的时间段。

b) 密钥生命周期：身份鉴别公钥的适当密钥生命周期不超过一年或两年，这取决于其使用环境和已鉴别信息的敏感性/关键性。

6） *Symmetric data-encryption key:*

a) 类型考虑：对称数据加密密钥用于保护存储的数据、消息或通信会话。鉴于数据泄露的严重后果，用于在短时间内加密大量数据（例如用于链路加密）的数据加密密钥的发起者使用周期应相对较短。随着时间的推移，用于加密少量数据的加密密钥可能会有较长的发起者使用周期。对称数据加密密钥的发起者使用周期适用于使用该密钥加密信息。在发起人使用周期内，可以使用数据加密密钥对数据进行加密；超过此期间的话，密钥不得用于数据加密，但可以用于解密已经加密的受保护数据（即，接收者使用周期可能需要延长到发起者使用周期之外）。

b) 密钥生命周期：建议在短时间内加密大量数据（例如链接加密）的发起者使用周期为一天或一周。用于加密较小数据量的加密密钥的发起者使用周期可能长达两年。建议接收者使用周期不超过发起者使用期限结束后的三年。在用于加密单个消息或单个通信会话的对称数据加密密钥的情况下，受保护数据的生存期可以是数月或数年，因为加密的消息可以被存储以供以后读取。如果数据以加密的形式保存，则需要保存对称数据加密密钥，直到该数据在新密钥下重新加密或销毁。请注意，随着时间的推移，对数据保密性的信心会降低。

7） *Symmetric key-wrapping key:*

a) 类型考虑：用于在短时间内包装（即加密和完整性保护）大量密钥的对称密钥包装密钥的发起者使用周期应相对较短。如果包装了少量密钥，则密钥包装密钥的发起者使用周期可以长一些。对称密钥包装密钥的发起者使用周期适用于在为密钥提供密钥包装保护时使用该密钥；不得使用已超出发起者使用周期的密钥包装密钥执行包装操作。然而，在发起者使用周期结束后，密钥包装密钥仍可能被用于（即，接收者使用周期可能需要延伸到发起者使用周期之外）展开受保护的密钥（即，解密和验证包装密钥的完整性）；接收者使用周期是在密钥包装密钥的发起者使用周期内可能需要展开密钥包装的时间段。一些对称密钥包装密钥仅用于单个消息或通信会话。在使用这些非常短期的密钥包装密钥时，适当的密钥生命周期（即，包括发起者和接收者使用周期）就是单次通信会话。假设包装的密钥不会以其包装的形式保留，因此密钥包装密钥的发起者使用周期和接收者使用周期是相同的。在其他情况下，可以保留密钥包装密钥，以便稍后可以恢复由其加密的文件或消息。在这种情况下，接收者使用周期可以远长于发起者使用周期，密钥生命周期可能持续数年。

b) 密钥生命周期：用于在短时间内包装大量密钥的对称密钥包装密钥的建议发起方使用期限大约为一天或一周。如果要在密钥包装密钥下包装数量相对较少的密钥，则密钥包装密钥的发起人使用期限可能长达两年。在密钥包装密钥仅用于单个消息或通信会话的情况下，密钥生命周期将限于单个通信会话。建议接受者的使用期限不超过发起者使用期限结束后的三年。

8） *Symmetric RBG keys:*

a) 类型考虑：对称 RBG 密钥用于确定性随机比特生成函数。该密钥的变更（例如，在重新做种期间）由 SP 800-90 中核准的 RBG 控制。密钥生命周期仅包括发起者使用周期。

b) 密钥生命周期：假设使用了核准的 RBG，则对称 RBG 密钥的最大密钥生命周期取决于 RBG 的设计（参见 SP 800-90）。

9） *Symmetric master key/key-derivation key:*

a) 类型考虑：对称主密钥（也称为密钥派生密钥）可多次用于使用（单向）密钥派生函数或方法派生其他密钥。因此，密钥生命周期只包含此密钥类型的发起者使用周期。合适的密钥生命周期取决于从主密钥派生的密钥的性质和用途。从主密钥派生的子密钥的密钥生命周期可以相对较短（例如单次使用、通信会话或事务）。或者，主密钥可以在更长的时间段内被使用，以导出（或重新导出）用于相同或不同目的的多个密钥。派生密钥的密钥生命周期取决于它们的用途（例如作为对称数据加密或完整性鉴别密钥）。

b) 密钥生命周期：对称主密钥的适当密钥生命周期可以是一年，这取决于其使用环境、派生密钥保护的信息的敏感性/关键性以及从主密钥派生的密钥数目。

10） *Private key-transport key:*

a) 类型考虑：传输私钥可以多次用于解密密钥。由于可能需要在密钥被加密以进行传输之后的某个时刻对密钥进行解密，传输私钥的密钥生命周期可能长于相应公钥的密钥生命周期。私钥的密钥生命周期是由相应公钥加密的任何密钥需要解密的时间段。

b) 密钥周期：给定条件 1）使用了核准的算法和密钥大小，2）在相应传输公

钥下加密的密钥可以保护的信息量，以及 3）期望密钥存储和使用环境的安全性将随着密钥提供保护的过程的敏感度和/或关键性的增加而增加，建议传输私钥的密钥生命周期不超过两年。在接收到的消息稍后被存储和解密的某些应用（例如电子邮件）中，传输私钥的密钥生命周期可能超过传输公钥的密钥生命周期。

11） *Public key-transport key:*

a) 类型考虑：传输公钥的密钥生命周期是指其可用于加密将要传输的密钥的时间段。如果公钥是由 CA 签发的，则公钥的密钥生命周期在最后一个为公钥颁发的证书到期时结束。传输公钥可以公开。如同在关于传输私钥的讨论中所说的，由于在密钥被加密以进行传输之后还需要被解密出来，传输公钥的密钥生命周期可能短于相应私钥的密钥生命周期。

b) 密钥生命周期：基于对相应私钥密钥生命周期的假设，建议密钥生命周期不超过一年或两年。

12） *Symmetric key-agreement key:*

a) 类型考虑：对称密钥协商密钥可以多次使用。对称密钥协商密钥的密钥生命周期取决于 1）环境安全因素，2）所建立密钥的性质（如类型和格式）和数量，以及 3）所采用的密钥协商算法和协议的细节。注意，对称密钥协协商钥可用于建立对称密钥（例如对称数据加密密钥）或其他密钥材料（例如初始向量）。

b) 密钥生命周期：假设使用对称密钥协商密钥的密码应用满足 1）采用了核准的算法和密钥方案，2）密码设备满足 FIPS 140 的技术要求，3）已根据 FIPS 199 确定风险等级，则密钥的适当密钥生命周期不超过一年或者两年。在某些应用程序（例如电子邮件）中，接收到的消息随后会被存储和解密，则密钥的接收者使用周期可以超过发起者使用周期。

13） *Private static key-agreement key:*

a) 类型考虑：可以多次使用静态（即长期）密钥协商私钥。如果相应公钥是由 CA 签发的，当为其颁发的最后一个证书失效时，静态密钥协商私钥的密钥生命周期也随之结束。与对称密钥协商密钥一样，该密钥的密钥生命周期取决于 1）环境安全因素，2）已建立密钥的性质（例如类型和格式）和数量，以及 3）所采用的密钥协商算法和协议的细节。注意，静态密钥协商私钥可用于建立对称密钥（例如密钥包装密钥）或其他密钥材料。

b) 密钥生命周期：假设使用私有静态密钥协商密钥的密码应用满足 1）采用了核准的算法和密钥方案，2）密码设备满足 FIPS 140 的技术要求，3）已根据 FIPS 199 确定风险等级，则密钥的适当密钥生命周期不超过一年或两年。虽然静态密钥协商私钥和静态密钥协商公钥的密钥生命周期通常相同，但是在接收到的消息随后被存储和解密的某些应用（例如电子邮件）中，静态密钥协商私钥的密钥生命周期可以超过相应静态密钥协商公钥的密钥生命周期。

14） *Public static key-agreement key:*

a) 类型考虑：静态（即长期）密钥协商公钥的密钥生命周期通常与对应的静态密钥协商私钥的密钥生命周期相同。

b) 密钥生命周期：静态密钥协商公钥的密钥生命周期可以是一年或两年。

15） *Private ephemeral key-agreement key:*

a) 类型考虑：临时（即短期）密钥协商私钥是非对称密钥对中的私钥元素，该

密钥对在一次事务中用于建立一个或多个密钥。临时密钥协商私钥可用于建立对称密钥（例如密钥包装密钥）或其他密钥材料。

b) 密钥生命周期：临时密钥协商私钥用于单次密钥协商事务。然而，在一次事务（广播）期间，可以多次使用临时私钥来与多方建立同一对称密钥。临时密钥协商密钥的密钥生命周期是单次密钥协商事务的持续时间。

16） *Public ephemeral key-agreement key:*

a) 类型考虑：临时（即短期）密钥协商公钥是非对称密钥对中的公钥元素，该密钥对仅限一次性使用，用于建立一个或多个密钥。

b) 密钥生命周期：临时密钥协商公钥用于单次密钥协议事务。临时密钥协商公钥的密钥生命周期在生成共享密钥后立即结束。注意，在某些情况下，对于密钥协商事务而言，每名参与者的临时密钥协商公钥的密钥生命周期可能并不相同。例如，考虑一个加密的电子邮件应用程序，其中邮件发送者生成一个临时密钥协商密钥对，然后使用该密钥对生成一个用于加密电子邮件内容的加密密钥对，对于发送方，公钥的密钥生命周期在生成共享密钥并导出加密密钥时结束，然而，对于加密电子邮件的接收者，在生成共享密钥并确定解密密钥之前，临时公钥的密钥生命周期不会结束；如果在收到电子邮件时没有立即处理该电子邮件（例如电子邮件发送一周后才被解密），那么在使用临时公钥产生共享秘密前，该公钥的密钥生命周期都不会结束（从接收方的角度来看）。

17） *Symmetric authorization key:*

a) 类型考虑：根据受保护的资源和被授权访问的实体的角色，对称授权密钥可以在较长时间内使用。对于此密钥类型，发起者使用周期和接收者使用周期是相同的。确定对称授权密钥的密钥生命周期时，主要考虑因素包括密钥的健壮性、加密方法的充分性以及密钥保护机制和过程的充分性。

b) 密钥生命周期：假设使用了核准的算法和密钥大小，并且希望密钥存储和使用环境的安全性随着授权过程的敏感性和关键性的增加而增加，则建议密钥生命周期不超过两年。

18） *Private authorization key:*

a) 类型考虑：根据受保护的资源和被授权访问的实体的角色，私人授权密钥可能会被长时间使用。确定授权私钥的密钥生命周期时，主要考虑因素包括密钥的健壮性、加密方法的充分性以及密钥保护机制和过程的充分性。授权私钥与其对应公钥的密钥生命周期应相同。

b) 密钥生命周期：假设使用了核准的算法和密钥大小，并希望密钥存储和使用环境的安全性随着授权过程的敏感性和重要性的增加而增加，建议授权私钥的密钥生命周期不超过两年。

19） *Public authorization key:*

a) 类型考虑：授权公钥是非对称密钥对中的公共元素，用于验证拥有相应私钥的实体的权限。

b) 密钥生命周期：授权公钥的密钥生命周期应与授权私钥的密钥生命周期相同，建议不超过两年。

表 1 总结了每种密钥类型的推荐密钥生命周期。根据使用密钥的应用程序和环境，实际的密钥生命期可能稍有出入。然而，当采用比推荐值的更长的密钥生命周期时，应认真考虑可能带来的风险。

表 1　每种密钥类型的推荐密钥生命周期

密钥类型	密钥生命周期	
	发起者使用周期 Originator-Usage Period (OUP)	接收者使用周期 Recipient-Usage Period
1. Private Signature Key	1 到 3 年	-
2. Public Signature-Verification Key	若干年(取决于密钥长度)	
3. Symmetric Authentication Key	≤2 年	≤OUP + 3 年
4. Private Authentication Key	1 到 2 年	
5. Public Authentication Key	1 到 2 年	
6. Symmetric Data Encryption Keys	≤2 年	≤ OUP + 3 年
7. Symmetric Key-Wrapping Key	≤2 年	≤ OUP + 3 年
8. Symmetric RBG Keys	详见 SP 800-90	-
9. Symmetric Master Key/Key Derivation Key	约 1 年	-
10. Private Key Transport Key	≤2 年	
11. Public Key Transport Key	1 到 2 年	
12. Symmetric Key Agreement Key	1 到 2 年	
13. Private Static Key Agreement Key	1 到 2 年	
14. Public Static Key Agreement Key	1 到 2 年	
15. Private Ephemeral Key Agreement Key	一次密钥协商	
16. Public Ephemeral Key Agreement Key	一次密钥协商	
17. Symmetric Authorization Key	≤2 年	
18. Private Authorization Key	≤2 年	
19. Public Authorization Key	≤2 年	

2.1.3　密钥算法和密钥长度选取指南

密码算法安全强度是指破解密码算法所需的计算量大小，它的单位是位（bit）：*n*位的安全强度，表示攻破该密码算法需要2^n次计算。按照目前的技术发展水平，80位安全强度及以下的密码算法（例如RSA-1024算法）是不安全的，112位安全强度的密码算法（例如RSA-2048算法）在2030年后是不安全的。

密码算法的安全强度并不等于密钥长度。一般来说，对称密码算法的安全强度与密钥长度相当，公钥密码算法的安全强度显著小于密钥长度。例如，RSA 算法密钥包括两个大素数因子，密钥空间并不等于密钥长度确定的全部取值空间。同时，由于密码算法的各种破解方法，也会导致安全强度小于密钥长度。例如，3Key-TDEA（3-Key Triple Data Encryption Algorithm，三个不同密钥的三重数据加密算法）的密钥长度是 168 位，但是由于中间相遇攻击，安全强度只有 112 位；2Key-TDEA（2-Key Triple Data Encryption Algorithm，两个不同密钥的三重数据加密算法）的密钥长度是 112 位，安全强度只有 80 位；由于各种大整数分解方法，RSA-1024、RSA-2048 算法的安全强度分别只有 80、112 位；基于 256 位素域的 SM2 算法的安全强度只有 128 位。对称密码算法和公钥密码算法、密码杂凑算法的安全强度分别如表 2、表 3 所示。

表 2 对称密码算法和公钥密码算法的安全强度

安全强度	对称密码算法	FFC (DSA, DH, MQV)	IFC (RSA)	ECC (ECDSA, EdDSA, DH, MQV)
≤ 80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

表 3 密码杂凑算法的安全强度

安全强度	数字签名算法等依赖抗碰撞的应用	HMAC, KMAC, KDF，随机数生成
≤ 80	SHA-1	/
112	SHA-224, SHA-512/224, SHA3-224	/
128	SHA-256, SHA-512/256, SHA3-256	SHA-1, KMAC128
192	SHA-384, SHA3-384	SHA-224, SHA-512/224, SHA3-224
≥ 256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512, KMAC256

2.2 NIST SP 800-67rev2

NIST 于 2012 年 1 月发布了 SP 800-67rev1。SP 800-67rev1 增加了一项要求，要求用户在同一个 3Key-TDEA（也就是 3 个不同密钥的 3DES）密钥下，不能加密超过 2^{32} 个 64 比特数据块。根据 SP 800-67rev1，NIST 于 2017 年 7 月 11 日在计算机安全部门的网站上发布了一份文件[1]，该文件解释了对使用相同密钥的三重 DES 加密数量进行限制的理由，其理由主要是 DES 本身相对较小的分组长度（64 比特）导致可能存在的密文碰撞的几率较大（约为 2^{-32}），平均加密 $2^{32}\times$64 比特=32GB 数据就有可能发生密文碰撞，这对于现有应用是存在风险的。

在 2017 年 11 月，NIST 发布了 SP 800-67rev2，进一步收紧了这一限制。根据 SP 800-67rev2，一个密钥不得用于加密超过 2^{20} 个 64 比特数据块（即 8MB）。此版本的 SP 800-67 标准包含在 2020 年 3 月发布的 SP 800-140C 中，也就是著名的 FIPS 140 标准的附录 C“核准的安全功能”。

[1] https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea

目前，针对 AES、SM4 等 128 比特分组长度的密码算法并无此强制要求，主要是其密文碰撞的几率相对较低（约为 2^{-64}），平均加密 $2^{64}\times128$ 比特=2560 亿 GB 的数据，这在实际应用中几乎不可能达到。

2.3 国外主要厂商的生命周期推荐

在 2019 年举办的第 48 届 CA/Browser 论坛上，就有研究人员提出将浏览器根证书有效期缩短为 398 天（一年零一个月），但该提议在不记名投票中遭到了广大 CA 机构的反对，未能通过。然而，在 2020 年的论坛中，苹果公司单方面宣布了新的根证书嵌入策略，新策略于 2020 年 9 月 1 日开始施行，届时，iOS 系统和 Safari 浏览器将不再信任有效期超过 398 天的 TLS/SSL 证书（包括根证书）。

针对网站证书，欧盟网络安全局（European Union Agency for Cybersecurity, ENISA）在报告《Qualified Website Authentication Certificates》中提出了六条策略和十二项推荐做法，报告成功推出了合格网站认证证书（QWAC，Qualified Website Authentication Certificates）的概念，并广为欧洲各机构所接受。在著名 CA 机构 QuoVadis 在其证书策略中明确规定了各种证书使用期限，根 CA 证书为 30 年，下级签发机构证书为 10 到 15 年，商用 SSL 证书为 3 年，扩展验证 SSL 证书为 2 年。

相对传统证书场景而言，IoT 设备具有数量规模大、安全性低，理应更频繁地更新证书和密钥，但 IoT 设备更换证书的成本更高，安全风险也更大，需要视具体情况选择合适的证书方案。EuroSmart 联盟所选取的一系列 IoT 证书方案[2]中，证书有效期从 1 到 5 年不等，也有部分方案甚至允许使用无限期证书。

2.4 GM/T 0054（GB/T 39786）

GM/T 0054-2018《信息系统密码应用基本要求》在“密钥管理”章节主要约束了密钥生命周期内各个环节的安全要求，但缺少对于密钥生命周期长度的要求，仅要求“应按照密钥更换周期要求更换密钥”。该标准对应国标版本 GB/T 39786《信息安全技术 信息系统密码应用基本要求》则仅提出了要求建立密钥管理制度等要求，同样未对于密钥生命周期长度提出要求。

2.5 GM/T 0022 和 GM/T 0023

GM/T 0022《IPSec VPN 技术规范》（对应国标版本为 GB/T 36968《信息安全技术 IPSec VPN 技术规范》）中要求 IPSec VPN 产品应具有根据时间周期和报文流量两种条件进行工作密钥和会话密钥的更新功能，其中根据时间周期条件进行密钥更新为必备功能，根据报文流量条件进行密钥更新为可选功能；工作密钥的最大更新周期不大于 24 小时；会话密钥的最大更新周期不大于 1 小时；但是未对长期密钥（签名密钥对和加密密钥对）的更新周期进行约束

GM/T 0023《IPSec VPN 网关产品规范》对 IPSec VPN 网关产品提出了进一步的要求，要求：应具有根据时间周期和报文流量两种条件进行工作密钥和会话密钥的更新功能，其中根据时间周期条件进行密钥更新为必备功能，根据报文流量条件进行密钥更新为可选功能。工作密钥的最大更新周期不大于 24 小时。如果采用流量条件，最大更新流量不大于 $2^{10}\times2^{32}$ 字节。会话密钥的最大更新周期不大于 1 小时。如果采用流量条件，最大更新流量不大于 $2^{10}\times2^{32}$ 字节。

[2] https://www.eurosmart.com/wp-content/uploads/2020/02/2020-01-27-Eurosmart_IoT_Study_Report-v1.2.pdf

2.6 GM/T 0024 和 GM/T 0025

GM/T 0024《SSL VPN 技术规范》中要求工作密钥产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。但没有明确说明具体的更新周期。

GM/T 0025《SSL VPN 网关产品规范》要求 SSL VPN 网关产品应具有根据时间周期或报文流量进行工作密钥更新的功能。其中，根据时间周期进行更新为必备功能，根据报文流量进行更新为可选功能。根据时间周期进行更新的情况下，客户端-服务端模式最长时间不超过 8 小时，网关-网关模式最长时间不超过 1 小时。

2.7 GB/T 17901

GB/T 17901.1-2020《信息技术 安全技术 密钥管理 第 1 部分：框架》主要描述了密钥管理的一般概念，描述了密钥管理的一般模型、密钥管理的基本内容、两实体间密钥分发的概念模型、特定服务的提供者等内容，但并未对密钥生命周期的长度进行具体的要求。

GB/T 17901.1-2020《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》主要描述了利用非对称密码算法实现密钥协商、密钥传递的方法，同样未对并未对密钥生命周期的长度进行具体的要求。

3. 密钥类别分析

3.1 密码算法和数据安全保护

密码算法是密码技术的核心，各种基于密码技术的安全功能都需要密码算法的支持。密码技术可以实现数据机密性（data confidentiality）、数据完整性（data integrity）、消息起源鉴别（source authentication）、不可否认性（non-repudiation）等安全功能：

- 数据机密性是指保证数据不会泄露给非授权的个人、计算机等实体。利用密码算法的加密和解密操作，可以实现数据机密性。
- 数据完整性是指保证数据在传输、存储和处理过程中不会遭到非授权的篡改或破坏。利用消息鉴别码或数字签名算法可以实现数据完整性。密码杂凑算法只能防范不经意的传输错误，但不能防范攻击者恶意的篡改，除非它产生的消息摘要无法被修改。
- 消息起源鉴别是指保证消息来自于特定的个人、计算机等实体，且没有非授权的篡改或破坏。利用消息鉴别码或者数字签名算法，可以实现消息起源鉴别。
- 不可否认性是指实体不能否认自己曾经执行的操作或者行为，不可否认性也称为抗抵赖性。利用数字签名算法可以实现行为的不可否认性。

常用的密码算法包括密码杂凑算法、对称密码算法和公钥密码算法三类密码算法。

密码杂凑算法，或者称为密码杂凑函数，可以为任意长度的消息计算生成定长的消息摘要。密码杂凑算法的计算是单向的，从给定的消息摘要计算输入的消息在计算上是不可行的。输入消息的微小变化，会导致密码杂凑算法输出的巨大变化。密码杂凑算法的计算过程一般不需要密钥，但是它可以应用在多种带密钥的密码算法或者密码协议中。在数据安全保护中，密码杂凑算法可以：

① 作为消息鉴别码（Message Authentication Code，MAC）的基础函数，实现数据完整性和消息起源鉴别，例如带密钥的杂凑消息鉴别码（Keyed-Hash MAC，

HMAC）；

② 配合数字签名算法（例如SM2算法等），用于压缩消息、产生消息摘要。

对称密码算法，用于明密文数据的可逆变换，且变换和逆变换的密钥是相同的。明文到密文的变换，称为加密；密文到明文的变换，称为解密。加解密的秘密参数，称为密钥。对称密码算法中的“对称”是指加密密钥和解密密钥是相同的。在不知道密钥的情况下，从明文获得密文的有关信息、或者从密文获得明文的有关信息，在计算上是不可行的。在数据安全保护中，对称密码算法可以：

① 用于加解密数据，实现数据机密性保护；

② 用于构建消息鉴别码（MAC），实现数据完整性和消息起源鉴别，例如CBC-MAC（Cipher Block Chaining MAC，密文分组链接MAC）、CMAC（Cipher-based MAC，基于对称加密算法的MAC）等；

③ 使用专门的对称密码算法工作模式，在实现数据机密性的同时，提供MAC类似功能的数据完整性和消息起源鉴别，例如GCM（Galois/Counter Mode，伽罗瓦/计数器模式）和CCM（Counter with CBC-MAC，带CBC-MAC的计数器模式）。

公钥密码算法，也称为非对称密码算法。公钥密码算法，同样也可用于明密文数据的变换，且变换和逆变换的密钥是不同的，包括用于加密的公开密钥（简称公钥）和用于解密的私有密钥（简称私钥）。任何人都可以使用公钥来加密数据，拥有对应私钥的实体才可以解密，而且从公钥不能获得私钥的任何有关信息。除了公钥加密算法，公钥密码算法还包括数字签名算法。拥有私钥的实体可以对消息计算数字签名，任何人都可以使用公钥来验证数字签名的有效性。总的来说，在数据安全保护中，公钥密码算法可以：

① 直接用于加解密数据，实现数据机密性。由于公钥密码算法的计算效率低，此种用法非常少见；

② 用于计算数字签名和验证数字签名，实现数据完整性保护、消息起源鉴别和抗抵赖。

3.2 密钥管理

柯克霍夫斯原则（Kerckhoffs’s Principle）要求：即使密码系统的任何细节都是公开已知的，只要密钥没有泄露，它也应该是安全的。网络空间安全的密码学应用，也应该遵守柯克霍夫斯原则，使用公开的密码算法，通过密钥的管理和保护，实现安全功能。对于对称密码算法，加密和解密的密钥是相同的，密钥必须保证不泄露；对于公钥密码算法，用于加密和签名验证的公钥可以公开，用于解密和数字签名的私钥必须保证密钥不泄露。

密钥的安全性直接关系着密码系统的安全性。下面介绍在密钥生命周期中的重要环节、以及相关的密钥管理密码算法。最后总结各种密码算法实现过程中需要保护的密钥等敏感数据。

密钥除了作为密码算法的最重要参数参加密码计算外，还需要经历生成、建立、存储、销毁等环节。在各环节中，密钥的安全性都必须得到保障。

3.2.1 密钥生命周期的重要环节

密钥生命周期是指密钥从生成、使用到销毁等各环节组成的全过程。不同密钥的生命周期各不相同，时间跨度也不相同。比如，临时性的会话密钥，在通信会话结束后立即销毁，一般不涉及存储，使用的时间跨度也比较短。又比如，代表用户身份的数字签

名密钥，可以多次使用，使用的时间长，甚至可以是数年，需要考虑不使用时的存储安全。

密钥生命周期包括生成、建立、使用、存储、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。为了保证密钥不会被攻击者猜测，密钥取值应均匀地分布在密钥空间中，因此密钥应当直接或间接地根据随机数生成。密钥生成的主要方式包括随机数直接生成和通过密钥派生函数（KDF）生成两大类。密钥派生函数方式相当于是随机数间接生成，因为密钥派生函数输入的秘密值（如主密钥、密钥材料）都应该是随机的。

基于用户口令派生密钥也是一种常用的密钥生成方式：利用用户口令以及其它公开信息，使用密码杂凑算法等方法来计算密钥。用户口令派生密钥的密钥空间依赖于口令的复杂度，相比于密钥的预期复杂度（例如，SM4 算法的密钥空间为 2^{128}），口令只能提供有限的随机熵（例如，8 位数字口令的取值空间仅约等于 2^{27}），极大地降低了暴力搜索攻击的难度。

（2） 密钥建立

密钥建立是指在通信实体之间建立共享的密钥。密钥建立可以通过手动方式，例如采取面对面的方式人工传递密钥，依赖人与人之间的信任关系来实现密钥共享；密钥建立也可以通过密码技术来实现，利用密码技术实现的密钥建立方案包括密钥协商和密钥传输两大类：

① 密钥协商是指两个或多个实体相互通信、交互数据，协商生成共享密钥；

② 密钥传输是指将密钥从一个实体安全地发送到另一个实体，密钥由发送者加密并由接收者解密。

密钥协商和密钥传输的区别在于，密钥传输的密钥由发送者单方确定，而密钥协商的密钥由参与通信的多个实体共同确定。通常而言，密钥协商算法涉及不重复使用的随机数，可以提供更好的前向安全性（forward secrecy）；对于密钥传输，如果接收者的解密密钥泄露，则攻击者可以获得之前传输的密钥。但密钥协商要求通信多方必须同时在线，不适用于某些需要离线通信的场景（例如电子邮件），所以离线通信的场景往往使用密钥传输算法来进行密钥建立。

（3） 密钥使用

密钥使用是指在各种密码算法中，使用密钥来进行加密、解密、数字签名、签名验证等。密钥使用过程中，密钥一般不可避免地以明文形式存在，而且所涉及的敏感中间变量也是明文，因此，密钥需要在受控的环境下进行使用，防止恶意攻击者直接从计算过程中获取密钥明文。受控的密码计算环境构建可以有多种技术路线，在目前成熟的信息系统建设中，最为常见的一种做法是将密钥保存在物理隔离的密码模块中，通过隔离的计算环境和有效的物理保护来确保密钥不会泄露。但是密码软件实现往往缺乏这种物理隔离的条件，为其密钥安全带来了极大的挑战。

由于公钥的可以公开的特性，公钥不必担心泄露的风险，但是必须在使用前（如签名验证或者密钥协商过程）需要验证公钥的完整性和公钥来源的真实性。

（4） 密钥存储

对于长期使用的密钥，在密码设备掉电之后，密钥需要存储在非易失的存储介质中，且保证密钥存储的机密性和完整性。但并不是所有密钥都需要存储，临时性的会话密钥或者一次一密的密钥在使用后就立即销毁。密钥存储主要有两种方式：

① 存储在访问受限的存储区域或者存储介质中：有些密码设备带有访问受限的存储区域或者存储介质，专门用于密钥存储。这些区域有的部署了入侵检测或者

入侵响应机制，可防止非授权的访问或者在被非法访问时立即销毁密钥；有的则利用访问控制机制实现密钥存储的保护，将密钥存储在仅有特定的授权用户才能访问的存储位置。

② 加密存储在通用存储介质中：对于某些应用场景，由于密钥数量较大，只能将密钥存储在通用的外部存储介质（例如数据库系统）。在这种情况下，需要利用密码算法对密钥数据进行机密性和完整性保护后再进行存放。

（5） 密钥销毁

密钥销毁是密钥生命周期的终点。密钥生命周期结束后，应该销毁密钥，并根据需要重新生成密钥，完成密钥更新。密钥销毁时，应当销毁所有的密钥副本（但不包括归档备用的密钥副本）。密钥销毁主要有两种情况：

① 正常销毁：密钥到达设计的使用截止时间，自动销毁，避免密钥数据被攻击者恢复，例如临时密钥在使用完毕时应立即销毁。

② 应急销毁：存在泄露风险时的密钥销毁。有些高安全等级的密码系统带有入侵响应的密钥销毁机制。如果没有自动的应急销毁机制，当发现有密钥泄露风险时，需要手动提前终止密钥的生命周期，将密钥进行销毁。

3.2.2 密钥管理密码算法

密码算法不仅可以为应用系统提供数据机密性、数据完整性、消息起源鉴别、不可否认性等重要安全功能，同时也是密钥管理的基础工具。密钥管理密码算法不直接处理用户应用数据，而是用于处理密钥数据。根据用途，密钥管理密码算法可分为密钥生成算法（包括确定性随机数生成算法和密钥派生算法）和密钥建立算法（包括密钥传输算法和密钥协商算法）两大类。密钥管理密码算法需要在三大类密码算法的基础上进行搭建，如图 1 所示：

① 随机数生成算法：在确定性随机数生成器（Deterministic Random Bit Generator，DRBG）中，需要将密码杂凑算法或对称密码算法作为伪随机函数（Pseudo-Random Function，PRF）来产生随机比特。

② 密钥派生算法：在密钥派生函数（Key Derivation Function，KDF）中，需要将密码杂凑算法或对称密码算法作为伪随机函数（PRF）来产生随机比特。

③ 密钥传输算法：密钥传输时将密钥通过加密的方式从一方传输给另一方，加密技术就依赖于对称密码算法或公钥密码算法，但是由于所要加密的是密钥，密钥传输算法在使用模式上与用于加密数据时略有不同。

④ 密钥协商算法：密钥协商算法一般依赖公钥密码算法的数学问题，在不可信的网络中协商出共享密钥。当然，也可以基于对称密码算法和密码杂凑算法实现密钥协商，但是使用相对较少。

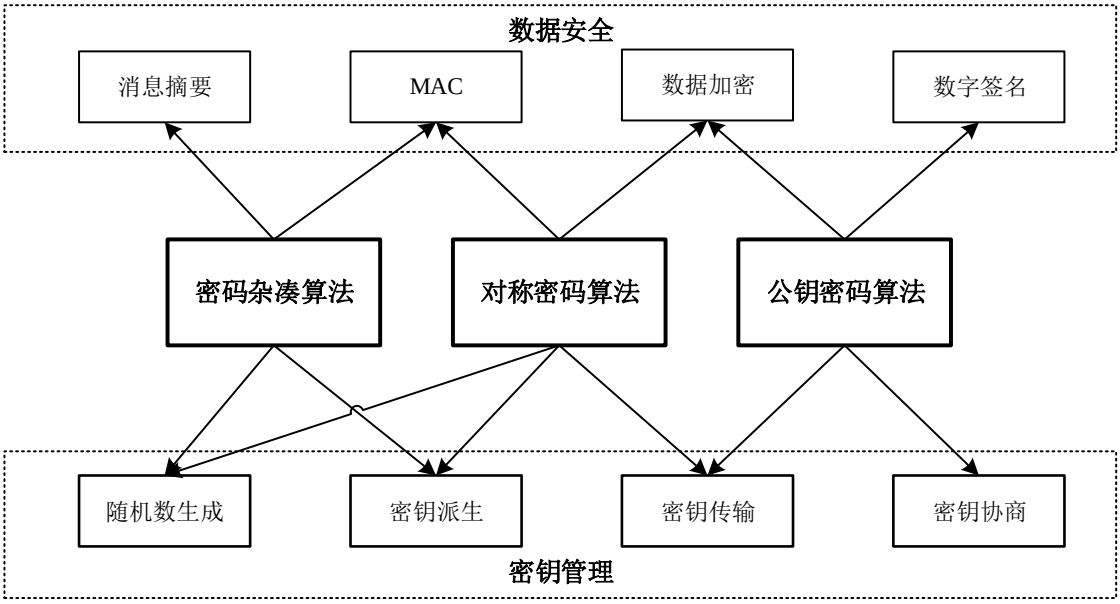

图 1 密码算法与数据安全、密钥管理

3.3 密钥安全

密钥的安全性直接关系到密码系统的安全性。除了密钥外，密码算法使用过程中各种影响安全性的敏感参数也应该视同密钥一样进行保护，包括但不限于：中间计算结果、密钥生成和密码计算过程中使用的随机数（例如 SM2 签名算法中使用的随机数和密钥协商过程生成的随机数）。

本节总结了各类算法涉及的、需要保护的变量。GM/T 0028 和 GB/T 37092 标准（*Security Requirement for Cryptographic Modules*）中将密码算法实现中需要防止非授权的访问、使用、泄露、修改和替换的数据项称为关键安全参数（critical security parameter），一般包括以下几类：

① 密钥：对称密钥和私钥。根据不同算法和用途，对称密钥包括对称加密密钥、MAC 密钥、密钥加密密钥等，私钥包括签名私钥、解密私钥、密钥协商私钥等。

② 与对称密钥、私钥相关的中间计算结果：加解密、签名、公钥解密、MAC 计算和验证、密钥协商等计算涉及的中间变量，包括算法执行的中间结果、上下文信息、预计算表等。通过这些中间计算结果，攻击者可以推算对称密钥和私钥、或者降低猜测对称密钥和私钥的难度。

③ 特定算法要求不能公开的变量：密码算法中明确要求不能公开的数据，例如 SM2 算法在签名过程中使用的随机值，DH 和 MQV 算法通信双方选取的随机值（可视为临时私钥），DRBG 算法的熵输入、种子、内部状态值等。

④ 密码算法产生的密钥和密钥材料：密钥管理密码算法生成或者保护的密钥或密钥材料，如 DRBG、KDF 生成的密钥和 DH、MQV 等协商获得的密钥（或密钥材料）。

除此之外，有些密码算法的相关数据可以公开，但是需要防止非授权的修改和替换。GB/T 37092 标准中这些数据项称为公开安全参数（public security parameter），一般包括以下几类：

① 公钥：公钥密码算法的公钥。根据不同的算法，公钥包括验签公钥、加密公钥、

密钥协商公钥等。

② 与公钥相关的中间计算结果：验签等计算涉及的中间变量；此外，密钥协商过程中的临时公钥也是可以公开的。但是，由于公钥加密过程涉及敏感的明文数据，因此一般公钥加密过程是需要保护的。

③ 密码算法的常量：密码算法的常量可以视为密码算法的一部分，是可以公开的，例如密码杂凑算法的内部状态初始值、对称密码算法的 S 盒等；

④ 域参数：在 SM2、SM9 等公钥密码算法中，需要双方事先确定一组域参数，并基于域参数实现密码算法。与密码算法常量类似，域参数也是可以公开的。

⑤ 特定算法可以公开的变量类：某些密码算法的一些变量需要以明文形式传递，而且这些变量泄露给非授权的实体不会导致安全性问题，常用的这类变量包括对称密码算法的 IV，迭代轮数，以及 DRBG 的补种计数器、nonce、个性化字符串等。

关键安全参数和公开安全参数统称为敏感安全参数（sensitive security parameter），本小节针对各个不同算法，对密码算法中需要保护的敏感安全参数进行说明。

3.3.1 密码杂凑算法的敏感安全参数

当密码杂凑算法用于计算杂凑值、消息摘要值时，输入消息以及整个计算过程不需要保密，所有计算过程可以完全公开，只需要保障计算过程不被非法篡改或破坏即可。

但是，当密码杂凑算法用作 HMAC 的组件时，由于涉及密钥数据，其安全要求完全不同。在 HMAC 计算过程中，MAC 密钥在与常量的异或、与消息的拼接后，输入密码杂凑算法；如果攻击者可以获取 HMAC 计算过程的中间计算结果，就能很容易地得到 MAC 密钥。因此，MAC 密钥以及 HMAC 计算过程中所有的中间计算结果都应当严格保密。

3.3.2 对称密码算法的敏感安全参数

对称密码算法的密钥可以分为进行加解密计算的加密密钥和进行 MAC 计算的 MAC 密钥。对于 GCM、CCM 等鉴别加密模式，单个密钥同时用于加解密计算和 MAC 计算。这些密钥都需要严格保密。

对于分组密码算法，一般会将密钥通过密钥编排（key schedule）扩展为轮密钥。密钥本身不直接参与运算，而是由轮密钥在分组密码算法的各轮计算中发挥作用。掌握了轮密钥，事实上也就掌握了密钥，可以轻易地进行数据的解密和 MAC 的生成，因此分组密码算法的轮密钥也是需要严格保密的。但是，分组密码算法的工作模式（如 CBC、CFB、OFB、GCM 等）涉及的 IV 值则可以公开，一般与密文一并发送，但是 IV 对于每个消息必须唯一（uniqueness），不能重用；CBC、CFB 的要求则更高，要求 IV 不可预测（unpredictable）。对于 CMAC，需要保护的变量与分组密码算法类似。

对于序列密码算法，密钥不直接用于对明文的加密，而是由密钥和 IV 计算内部状态，根据内部状态通过密钥流生成算法输出密钥流（也叫扩展密钥序列），然后将明文序列和密钥流进行异或。因此，序列密码算法的密钥、内部状态以及生成的密钥流都需要保密。与分组密码算法类似，IV 值可以公开，但要求 IV 不重复。

3.3.3 公钥密码算法的敏感安全参数

公钥密码算法中的密钥根据密钥用途可分为签名公私钥对、加密公私钥对等。其中私钥都需要保密，公钥可以公开。

相对应地，公钥密码算法的签名和加解密过程（公钥加密虽然只涉及公钥，但是待

加密的明文数据也需要保密）涉及的中间变量也要保密。值得一提的是，ECDSA 和 SM2 签名过程中使用的随机值 k 尤其需要保护，这是因为：

- 一旦随机值 k 被泄露，则 ECDSA 签名结果 $s=k^{-1}(e+dr)$ 和 SM2 签名结果 $s=(1+d)^{-1}(k-dr)=(1+d)^{-1}(k+r)-r$ 中除私钥 d 外所有的变量都是已知的，可以很容易计算出私钥。
- 更进一步地，k 不能重复使用，因为如果采用的随机值 k 是固定的，使用私钥 d 对消息摘要为 e_1 和 e_2 的两组消息进行 ECDSA 签名时，签名值分别为(r_1,s_1)和(r_2,s_2)，则有：(a) $r_{1=}$ r_2，(b) $s_1=k^{-1}(e_1+dr_1)$ 和 (c) $s_2=k^{-1}(e_2+dr_2)$。计算 (b)-(c)，有 $s_1-s_2=k^{-1}(e_1-e_2)$，即 $k^{-1}=(s_1-s_2)(e_1-e_2)^{-1}$，带入$(b)$中即可计算私钥：$d=[s_1(s_1-s_2)^{-1}(e_1-e_2)-e_1]r_1^{-1}$。SM2 也有类似攻击。

3.3.4 密钥管理密码算法的敏感安全参数

作为用于密钥管理的算法，密钥管理密码算法也有着自己需要保护的敏感安全参数。不同密钥管理密码算法的情况如下：

① 确定性随机数生成算法：

a) 对于 Hash_DRBG，熵输入、种子以及内部状态中的 C 和 V 都需要严格保密；对于 HMAC_DRBG 和 CTR_DRBG，熵输入、种子以及内部状态中的 Key 和 V 都需要严格保密。一旦这些变量被非法获取，则 DRBG 算法生成的随机数就是可预测的。

b) 用于生成种子的 nonce、个性化字符串、额外输入可以公开，因为种子的随机性主要由熵输入提供，这些可公开的输入起到类似于盐值（salt）的作用。每次初始化 DRBG 时，应输入不同的 nonce。

c) DBRG 生成的随机数需要根据用途进行保护。例如，如果随机数作为密钥使用则需要保密，如果作为 IV 则不必保密。

② 密钥派生函数：

a) KBKDF 的主密钥、密钥材料和派生出的密钥需要保密；用于派生密钥的附加信息（例如标签）则可以公开；

③ 对于密钥协商算法，DH、ECDH 等不提供鉴别功能的密钥协商算法和 MQV、ECMQV 等鉴别密钥协商算法需要保护的数据略有不同：

a) DH、ECDH 需要保护的是双方随机生成的随机值（即临时私钥），而临时私钥对应的临时公钥则可以公开；

b) MQV、ECMQV 不仅需要保护双方随机生成的随机值（即临时私钥），还需要保护自己持有的长期私钥；而长期公钥和临时公钥都可以公开；

c) 通信双方还需要确认有限域（对于 DH 和 MQV）和椭圆曲线（对于 ECDH 和 ECMQV）的域参数，域参数可以公开。

④ 密钥传输算法基于公钥加密算法或对称加密算法实现，因此密钥加密（key wrapping）需要保护的数据则与对称密码算法类似；密钥封装（key encapsulation）需要保护的数据与公钥密码算法类似。需要注意的是，由于密钥传输算法所保护的密钥也需要保护，因此利用公钥计算的密钥封装过程也要保密。

3.3.5 小结

表 4 结了各类密码算法及工作模式中涉及到的各类敏感安全参数。此外，需要说明的是，有些密码算法实现（包括密码杂凑计算、加解密、MAC、签名、验签等运算）为了支持分段输入，提供了初始化（initialize）、更新（update）、结束（finalization）等函

数，这就需要维持上下文信息保存的状态信息。对于加解密、MAC、签名运算，这些状态信息通常包括了密钥和密钥相关信息，因此这些状态信息也是需要严格保密的。

表 4　密钥算法与密钥

算法类型	密码算法	需要保密的变量			可公开的变量
		密钥	中间计算结果	算法产生的密钥和其它数据	
密码杂凑算法	HMAC	MAC 密钥	MAC 生成和验证过程	/	/
对称密码算法	分组密码算法	加解密密钥、MAC 密钥、扩展的轮密钥	加密和解密过程，MAC 生成和验证过程	/	IV（不能重用或不可预测）
	序列密码算法	加解密密钥，以及生成的密钥流	加解密过程	内部状态	IV（不能重用）
公钥密码算法	RSA	签名私钥、解密私钥	签名、加解密过程	/	验签公钥、加密公钥
	ECDSA	签名私钥	签名过程	签名计算中随机值 *k*（且不能重复使用）	域参数、验签公钥
	SM2	签名私钥、解密私钥	签名、加解密过程	签名计算中随机值 *k*（且不能重复使用）	域参数、验签公钥、加密公钥
密钥管理	DRBG	/	随机数生成的全过程，包括初始化、生成、补种等	熵输入、种子、内部状态的 Key、C 和 V，生成的随机数根据用途保护	nonce（不能重用）、个性化字符串、额外输入
	KBKDF	主密钥	密钥派生过程	派生出的密钥	标签、上下文等附加信息
	密钥封装	解密私钥	密钥封装和解封装过程	传输的密钥或密钥材料	加密公钥
	密钥加密	加解密密钥	密钥加解密过程	传输的密钥或密钥材料	/
	DH、ECDH	/	密钥协商过程	双方各自选定的随机值、协商出的密钥或密钥材料	域参数、临时公钥
	MQV、ECMQV	长期私钥	密钥协商过程		域参数、长期公钥和临时公钥

3.4　密钥类别分析

根据我国商用密码算法标准体系，参考 NIST SP 800-57，本报告将密钥分为以下三大类：

- 数据保护类密钥：这类密钥直接保护数据的机密性、完整性、消息来源真实性和行为的不可否认性；根据不同算法和不同功能，可以进一步分为：数据加密对称密钥、数据 MAC 对称密钥、数据加密公/私钥、数据签名公/私钥。
- 身份鉴别类密钥：主要在实体鉴别协议中，用于验证实体身份；与数据保护类不同的是，该类密钥虽然也对鉴别过程数据（比如挑战值、时间戳等）进行加密/签名等操作，但是目的并不是为了保护鉴别过程数据，而是为了验证对方是否持有相同/对应的密钥；根据不同的身份鉴别协议，可以进一步分为：身份鉴别对称密钥、身份鉴别公/私钥。
- 密钥管理类密钥：这类密钥主要用于密钥管理算法，实现随机数生成、密钥派

生、密钥建立等功能，根据不同的密钥管理功能，可以进一步分为：密钥派生密钥、密钥加密对称密钥、密钥封装公/私钥、密钥签名公/私钥、密钥协商对称密钥、密钥协商公/私钥。有些密钥的使用方法（如密钥加密对称密钥、密钥封装公/私钥、密钥签名公/私钥）与数据保护类密钥类似，区别在于保护的内容并不一致。

与 NIST SP 800-57 相比，如表 5 所示，主要变化如下：

- 删除了 *Symmetric/Private/Public authorization key*，该密钥与鉴别类密钥的区别难以明确界定；
- 删除了 *Private/Public ephemeral key-agreement key*，密钥协商过程中的随机值虽然需要进行保护，但是列为密钥容易产生歧义；
- 拆分 *Symmetric authentication key* 为数据 MAC 对称密钥和身份鉴别对称密钥，主要为了明确区分用于数据MAC保护的密钥和用于GB/T 15843实体鉴别协议中使用的密钥；
- 增加了数据加密公/私钥，由于 NIST 密码标准体系中一般不直接对数据进行公钥加密，而是采用数字信封的方式；但是为了考虑广泛性和通用性，本报告数据加密公/私钥；
- 增加了密钥派生公私钥对，主要用于支持 SM9 算法（GB/T 38635.2）中由系统签名/加密主密钥产生用户签名/加密密钥的过程；
- 增加了密钥签名公私钥，主要用于增加对 PKI 体系中的 CA 公/私钥的支持，该类密钥与一般用于数据/文件签名的签名公私钥存在明显不同的安全要求。

表 5 本报告和 NIST SP800-57 定义的密钥类型的区别

密钥大类	**本报告中的密钥类型**	**NIST SP800-57 对应的密钥类型**
数据保护类密钥	1.数据加密对称密钥	*Symmetric data-encryption key*
	2.数据 MAC 对称密钥	*Symmetric authentication key*
	3.数据加密公私钥对	N/A
	4.数据签名公私钥对	*Private signature key*
		Public signature-verification key
身份鉴别类密钥	5.身份鉴别对称密钥	*Symmetric authentication key*
	6.身份鉴别公私钥对	*Private authentication key*
		Public authentication key
密钥管理类密钥	7.随机数生成密钥	*Symmetric random number generation keys*
	8.密钥派生对称密钥	*Symmetric master key/key-derivation key*
	9.密钥派生公私钥对	N/A
	10.密钥加密对称密钥	*Symmetric key-wrapping*
	11.密钥封装公私钥对	*Private key-transport key*
		Public key-transport key
	12.密钥签名公私钥对	N/A
	13.密钥协商对称密钥	*Symmetric key-agreement key*
	14.密钥协商公私钥对	*Private static key-agreement key*
		Public static key-agreement key
NIST SP800-57 特有的密钥类型	N/A	*Symmetric/Private/Public authorization key*
		Private/Public ephemeral key-agreement key

3.4.1 数据保护类密钥

（1） 数据加密对称密钥

数据加密对称密钥是一种对称密钥，在对称密码算法中使用，用于对数据进行加密或解密，以保护数据的机密性。在GB/T 36624规定的可鉴别加密模式中使用的对称密钥，既是数据加密对称密钥，也是数据MAC对称密钥。

（2） 数据 MAC 对称密钥

数据MAC对称密钥是一种对称密钥，在对称密码算法中使用，用于计算消息的消息鉴别码，以保护数据源真实性鉴别和数据完整性保护。在GB/T 36624规定的可鉴别加密机制中使用的对称密钥，既是数据加密对称密钥，也是数据MAC对称密钥。

（3） 数据加密公私钥对

数据加密公私钥对是一对密钥，分别为数据加密私钥和数据加密公钥。

数据加密私钥在公钥密码算法（如GB/T 32918.4和GB/T 38635.2）中使用，对密文数据进行解密。

数据加密公钥在公钥密码算法（如GB/T 32918.4和GB/T 38635.2）中使用，对明文数据进行加密。

（4） 数据签名公私钥对

数据签名公私钥对是一对密钥，分别为数据签名私钥和数据签名公钥。

签名私钥用于数字签名算法（如GB/T 32918.2和GB/T 38635.2）中，提供数据完整性、数据来源真实性以及数据原发/接收行为不可否认性保护。

数据公钥用于数字签名算法（如GB/T 32918.2和GB/T 38635.2）中，提供对数据完整性、数据来源真实性以及数据原发/接收行为不可否认性的验证。

3.4.2 身份鉴别类密钥

（1） 身份鉴别对称密钥

身份鉴别对称密钥是一种对称密钥，在GB/T 15843.2和GB/T 15843.4中定义的实体鉴别协议中使用，用于对实体的身份进行鉴别。

（2） 身份鉴别公私钥对

身份鉴别公私钥对是一对密钥，分别为身份鉴别私钥和身份鉴别公钥。

身份鉴别私钥用于GB/T 15843.3中定义的实体鉴别协议中使用，通过对挑战值进行签名生成以产生身份鉴别信息（即响应值）。

身份鉴别公钥用于GB/T 15843.3中定义的实体鉴别协议中使用，通过对响应值进行签名验证以鉴别实体身份。

3.4.3 密钥管理类密钥

（1） 随机数生成密钥

随机数生成密钥是一种对称密钥，在确定性随机数发生器中使用，作为随机数种子用于生成随机数。

（2） 密钥派生对称密钥

密钥派生密钥是一种对称密钥，在密钥派生函数中使用，用于派生其他密钥。

（3） 密钥派生公私钥对

密钥派生密钥是一对密钥，在特定的密钥生成算法中使用（如GB/T 38635.2中由系统签名/加密主密钥产生用户签名/加密密钥的过程），用于派生其他密钥。

（4） 密钥加密对称密钥

密钥加密对称密钥是一种对称密钥，在对称密码算法中使用，以保护密钥的机密性、

完整性或来源真实性。若利用GB/T 36624规定的可鉴别加密模式进行密钥保护，则密钥加密对称密钥同时可以保护密钥的机密性、完整性和来源真实性。

（5） 密钥封装公私钥对

密钥封装公私钥对是一对密钥，分别为密钥封装私钥和密钥封装公钥。

密钥封装私钥在公钥加密算法（如GB/T 32918.4和GB/T 38635.2）中使用，以保护密钥的机密性和/或完整性。

密钥封装公钥在公钥加密算法（如GB/T 32918.4和GB/T 38635.2）中使用，以保护密钥的机密性和/或完整性。

（6） 密钥签名公私钥对

密钥签名公私钥对是一对密钥，分别为密钥签名私钥和密钥签名公钥。

密钥签名私钥在数字签名算法（如GB/T 32918.2和GB/T 38635.2）中使用，用于保护密钥的完整性和来源真实性。一种常见的密钥签名私钥是PKI体系中的CA私钥，CA利用自己的签名私钥对用户的数字证书进行签名，保证用户数字证书（及其包含的公钥）的完整性和来源真实性。相比于数据签名私钥，密钥签名私钥的使用频率较低，因此可以有更长的生命周期。

密钥签名公钥是一种非对称密钥，在数字签名算法（如 GB/T 32918.2 和 GB/T 38635.2）中使用，用于保护密钥的完整性和来源真实性。一种常见的密钥签名私钥是 PKI 体系中的 CA 公钥，CA 利用自己的签名私钥对用户的数字证书进行签名，其他人可以利用 CA 公钥验证用户数字证书（及其包含的公钥）的完整性和来源真实性。

（7） 密钥协商对称密钥

密钥协商对称密钥是一种对称密钥，也称为预共享密钥，在对称密码算法或密码杂凑算法中使用，用于协商密钥或密钥材料。

（8） 密钥协商公私钥对

密钥协商公私钥对是一对密钥，分别为密钥协商私钥和密钥协商公钥。

密钥协商私钥是一种非对称密钥，在密钥交换协议（如GB/T 32918.3和GB/T 38635.2）中使用，用于协商密钥或密钥材料。

4. 密钥生命周期选取推荐

本章将介绍一种分级分类的密钥生命周期选取推荐方法。请注意：本章给出的是一种框架性建议，所提出的密钥分级方法和不同等级的密钥生命周期长度推荐仅用于展示该框架，具体数值仅供参考。

4.1 总体原则

合适的密钥生命周期长度应能够：

- 限制可用于密码分析的信息量（如明/密文对的数量）；
- 限制单个密钥泄露可能导致的数据泄露量；
- 限制特定算法的使用（如将其限制在该算法的预估有效寿命内）；
- 限制敌手尝试破坏密钥保护措施的可用时间；
- 在密钥被无意中泄露给未授权实体后，限制数据安全可能被破坏的时间窗口；
- 限制计算密集型密码分析的可用时间。

密钥生命周期长度的选取应参考以下因素：

a） 密钥所处的环境：密钥所处的环境越安全，则密钥生命周期一般可以设置得越

长；

b） 所保护数据资产的敏感度：密钥保护的数据资产越敏感，则密钥生命周期一般可以设置得越短；

c） 密钥类型：由于密钥管理中存在的风险（如密钥在分发时可能存在的泄露风险），公私钥对的生命周期长度一般比对称密钥要长；

d） 密钥更新难度：某些情况下，密钥难以进行更新，或者更换密钥的成本超过了密钥本身保护数据资产的价值，则密钥的生命周期长度可以适当增长。

对于相对成熟、应用场景相对固定的密码产品（如VPN类产品、电子签章类产品），密钥生命周期可以在密码产品设计时进行确认，信息系统在使用时根据情况进行酌情调整。如果特定行业或领域已有标准规定密钥生命周期的，应优先参考相关标准选取密钥生命周期长度。

4.2 密钥分级

本研究报告将根据密钥所处的环境、所保护数据资产的敏感度将密钥为 5 级，分别为 A—E 级（A—E 级别逐步增加），级别越低，所保护数据资产的敏感度越高，密钥所处的环境安全性越低，意味着密钥生命周期长度也相应较低。具体分级方式如表 6 所示。

表 6 密钥分级表

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="4">所处环境</td></tr>
<tr><td>开放 [1]</td><td>相对安全 [2]</td><td>非常安全 [3]</td><td>具备资质的密钥管理服务商[4]</td></tr>
<tr><td rowspan="2">数据重要程度</td><td>重要</td><td>A</td><td>B</td><td>C</td><td rowspan="2">E</td></tr>
<tr><td>一般</td><td>B</td><td>C</td><td>D</td></tr>
<tr><td colspan="6">[1] 如：一般通用服务器
[2] 如：有一定防护能力的密码产品（如 GB/T 37092 安全一级或二级的密码产品）或具有较强的访问控制机制的运行环境
[3] 如：有较强防护能力的密码产品（如 GB/T 37092 安全三级或四级的密码产品）或具有很强的访问控制机制
[4] 如：具有电子认证服务使用密码许可证的电子认证服务商。这类服务商一般部署了非常全面的技术和管理手段以保护自身密钥的安全。</td></tr>
</table>

如果同一个密钥（或者构成同一个密钥的分量）保存在不同安全条件的环境下，在选取生命周期时，应遵循以下原则：

- 如果任意一个环境下的密钥本身、密钥副本或密钥分量的泄露、篡改等会影响密钥的安全性，则密钥级别应依据较低安全强度的环境而定。比如，用于用户身份鉴别的密钥同时存储在服务端满足 GB/T 37092 安全三级的服务器密码机和客户端满足 GB/T 37092 安全二级的智能密码钥匙中，则应根据客户端密钥存储环境（即智能密码钥匙）确定密钥级别。
- 此外，密钥级别需要根据密钥本身、密钥副本或密钥分量的保管方式、协议等，进行安全性分析后进行确定。比如密钥利用 Shamir 秘密分享方案将密钥分为 5 份，其中 3 份可以恢复密钥，5 份密钥分量中的 3 份存储在满足 GB/T 37092 安全三级的服务器密码机中，剩余的 2 份存储在满足 GB/T 37092 安全二级的智能密码钥匙中，考虑到恢复密钥时必须有一个保存在 GB/T 37092 安全三级的服务器密码机中的密钥参与，可以根据服务器密码机的环境安全程度确定密钥级别。

4.3 不同等级的密钥生命周期长度推荐

根据不同级别的密钥，密钥生命周期长度推荐如表 7 所示。

表 7 密钥生命周期长度推荐

密钥大类	密钥类型	密钥生命周期长度上限				
		A 类	B 类	C 类	D 类	E 类
数据保护类密钥	1.数据加密对称密钥	1个月或1TB数据	2年或2TB数据	3年或4TB数据	5年或8TB数据	8年或8TB数据
	2.数据 MAC 对称密钥	1个月或1TB数据	2年或2TB数据	3年或4TB数据	5年或8TB数据	8年或8TB数据
	3.数据加密公私钥对	2个月或1TB数据	2年或2TB数据	3年或4TB数据	5年或8TB数据	8年或8TB数据
	4.数据签名公私钥对	2个月或1000次签名	2年或8192次签名	3年或32768次签名	5年或65536次签名	8年或65536次签名
身份鉴别类密钥	5.身份鉴别对称密钥	3个月或1000次鉴别	3年或8192次鉴别	5年或32768次鉴别	8年或65536次鉴别	10年或65536次签名
	6.身份鉴别公私钥对	3个月或1000次鉴别	3年或8192次鉴别	5年或32768次鉴别	8年或65536次鉴别	10年或65536次签名
密钥管理类密钥	7.随机数生成密钥	参考具体的确定性随机数发生器算法				
	8.密钥派生密钥	3 个月或 1000 次派生	1 年或 8192 次派生	3 年或 32768 次派生	5 年或 65536 次派生	10 年或 65536 次派生
	9.密钥派生公私钥对	6 个月或 1000 次派生	3 年或 8192 次派生	5 年或 32768 次派生	10 年或 65536 次派生	20 年或 65536 次派生
	10.密钥加密对称密钥	3 个月或 1000 次加密	2 年或 8192 次加密	3 年或 32768 次加密	5 年或 65536 次加密	10 年或 65536 次加密
	11.密钥封装公私钥对	3 个月或 1000 次封装	2 年或 8192 次封装	5 年或 32768 次封装	10 年或 65536 次封装	20 年或 65536 次封装
	12.密钥签名公私钥对	6 个月或 1000 次签名	3 年或 8192 次签名	5 年或 32768 次签名	10 年或 65536 次签名	20 年或 65536 次签名
	13.密钥协商对称密钥	3 个月或 1000 次协商	2 年或 8192 次协商	3 年或 32768 次协商	5 年或 65536 次协商	10 年或 65536 次协商
	14.密钥协商公私钥对	6 个月或 1000 次协商	3 年或 8192 次协商	5 年或 32768 次协商	8 年或 65536 次协商	20 年或 65536 次协商

如表 7所示，信息系统在确定某个密钥的生命周期时，可以采用两种策略：

- 基于时间跨度的密钥生命周期长度：即设定某个密钥的最长使用寿命，当密钥使用超过所设定的时间跨度后，终止密钥生命周期；
- 基于使用次数的密钥生命周期长度：即限制密钥的使用次数，当密钥使用超过所设定的次数后，终止密钥生命周期。

密钥生命周期可以根据信息系统业务需要，基于时间跨度或基于使用次数进行确定。选取时，应遵循以下原则：

- 优先使用基于使用次数的策略；
- 在难以事前判断保护数据的量时，可以根据时间跨度来确定密钥的生命周期。
- 若事前可以大致估计单位时间内的所保护的数据量，可以参考相应级别的所保护的总数据量，计算出密钥可以使用的时间，取其与相应参考相应级别密钥的生命周期长度的较小值作为密钥生命周期。

4.4 影响密钥生命周期的其他因素

在具体设计密钥生命周期长度时，还应当根据以下因素对其进行调整，具体包括：

a） 密钥存在泄露风险：如果密钥已经泄露或者存在泄露风险时，需要提前结束密钥生命周期

b） 密钥管理人员的更替：密钥管理人员更替后，密钥生命周期长度应适当减少或直接终止该密钥的密钥生命周期；

c） 新型攻击技术（例如，量子计算机）的威胁：在新型攻击技术下，有些密码算法或者较短的密钥长度已不安全，密钥生命周期长度应适当减少或直接终止该密钥的密钥生命周期；

d） 密钥更新方式：如果密钥更新方式存在较高安全风险或所需成本过高，比如手动分发密钥的方法容易受人为错误的影响，则密钥生命周期长度可适当延长，但不得超过推荐值的2倍。

参考文献

[1] Elaine Barker. SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 – General [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2020

[2] National Institute of Standards and Technology. FIPS 180-4, Secure Hash Standard (SHS) [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2015

[3] National Institute of Standards and Technology. FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC) [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2008

[4] Morris Dworkin (NIST). SP 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2016

[5] Morris Dworkin (NIST). SP 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2007

[6] Morris Dworkin (NIST). SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2007

[7] Elaine Barker, Nicky Mouha (NIST). SP 800-67rev2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2017

[8] National Institute of Standards and Technology. FIPS 186-4, Digital Signature Standard (DSS) [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2009

[9] Elaine Barker (NIST), John Kelsey (NIST). SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2015

[10] Lily Chen (NIST). SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised) [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2009

[11] Meltem Sönmez Turan (NIST), Elaine Barker (NIST), William Burr (NIST), Lily Chen (NIST). SP 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2009

[12] Elaine Barker (NIST), Lily Chen (NIST), Allen Roginsky (NIST), Apostol Vassilev (NIST), Richard Davis (NSA). SP 800-56A Rev. 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2009

[13] Elaine Barker (NIST), Lily Chen (NIST), Allen Roginsky (NIST),

Apostol Vassilev (NIST), Richard Davis (NSA), Scott Simon (NSA). SP 800-56B Rev. 2, Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography [S]. Gaithersburg: National Institute of Standards and Technology (NIST), 2014

[14] 全国信息安全标准化技术委员会. GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法[S]. 北京：中国国家标准化管理委员会.

[15] 全国信息安全标准化技术委员会. GB/T 32907 信息安全技术 SM4 分组密码算法[S]. 北京：中国国家标准化管理委员会.

[16] 全国信息安全标准化技术委员会. GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法[S]. 北京：中国国家标准化管理委员会.

[17] 全国信息安全标准化技术委员会. GB/T 15843 信息技术 安全技术 实体鉴别[S]. 北京：中国国家标准化管理委员会.

[18] 全国信息安全标准化技术委员会. GB/T 36624 信息技术 安全技术 可鉴别的加密机制[S]. 北京：中国国家标准化管理委员会.

[19] 全国信息安全标准化技术委员会. GB/T 37092 信息安全技术 密码模块安全要求[S]. 北京：中国国家标准化管理委员会.