atsec Information Security
Tel: +86-10-53056681
Fax: +86-10-53056678
www.atsec.com

下一代密码模块安全标准探讨

艾特赛克（北京）信息技术有限公司　李迪

1　背景

作为全球范围认可程度最高的密码模块安全标准，从 2001 年颁布算起，FIPS 140-2 已经走过了 17 年的时光，通过 FIPS 140-2 认证的密码产品已达 3336 款（截至 2018 年 12 月 3 日），参与厂商超过 600 家，其中国内厂商如华为、握奇数据、三未信安、海康威视等也都有多款且不同类型的产品均通过了 atsec 的测评且获得了 FIPS 140-2 证书。

然而就是在这 17 年间，IT 业界的新技术、新标准层出不穷，如大数据、云计算、物联网、AI 等，而密码模块的使用也已经不局限于银行、电信等传统领域，而是广泛的拓展到了智能设备、互联网、移动应用等，并且和大众的日常生活息息相关。这也就导致了密码模块产业内对出台下一代标准的呼声越来越高，并且对下一代密码模块安全标准的要求也有所提高，比如：

- 从美国体系下分离出来，变成国际认可标准用以切合各国实际要求
- 易于变更的流程，可以及时反映出业界的新技术和新思想
- 移除旧的不能贴合实际的标准要求
- 针对新类型产品，提供更易于实现以及用户友好的机制

2　新标准的发展

由美国美国国家标准研究院（NIST）和加拿大通信安全局（CSE）联合成立的密码模块认证计划组织（CMVP）在 2005 年开始着手制定下一代密码模块安全标准，然而最终由于该标准草案收到大量的无法解决的公众意见而始终未能定稿，并且在 2006 年 ISO/IEC 19790 草案出台后正式被废弃。在之后几年中，ISO/IEC 19790 经历了数次改版，CMVP 也在计划将其作为 FIPS 140-2 的下一代标准。一旦获批，意味着美国和加拿大将直接使用 ISO/IEC 19790 作为下一代密码模块安全标准，而 NIST 计划分配 FIPS 140-3 作为该标准代号。下图是 ISO/IEC 19790 标准制定进展：

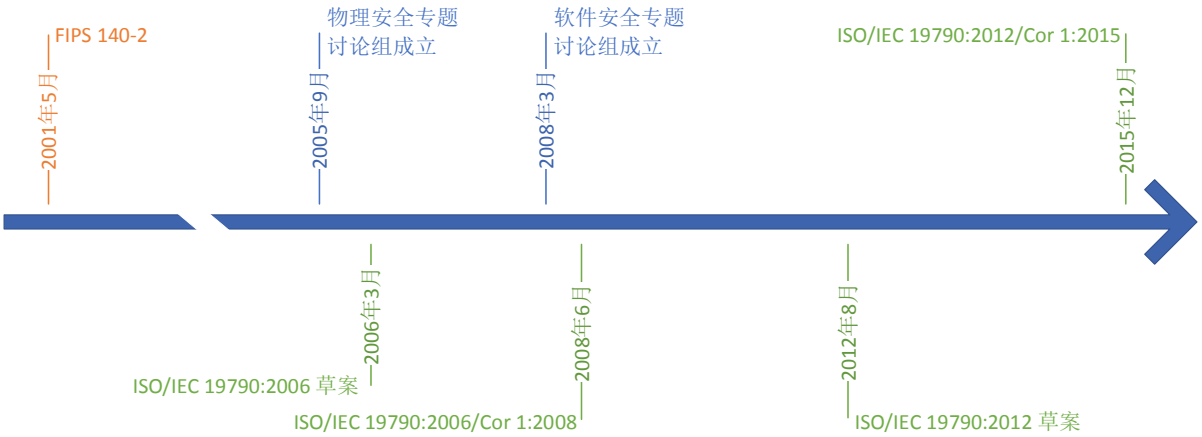

图 1： ISO/IEC 19790 发展进程

可以看到，目前新一代密码模块检测标准是 2015 年底修订的版本“ISO/IEC 19790:2012/Cor 1:2015”，下文均以 ISO/IEC 19790 指代最新的标准版本。

3 新标准与 FIPS 140-2 的比较

作为依托于美国联邦背景的 FIPS 140-2 标准，在其标准主框架之外，其强制使用部分美国本土的标准，比如在附录 A 中引用了 FIPS 197 AES 对称密码算法、FIPS 186-4 数字签名非对称算法、FIPS 180-4 散列算法等，并在标准配套的实施指南（Implementation Guide）中强制使用许多美国国家标准研究院（NIST）的特别出版物，比如 NIST SP800-56A 基于离散对数方式的会话密钥建立体系等，如下图所示：

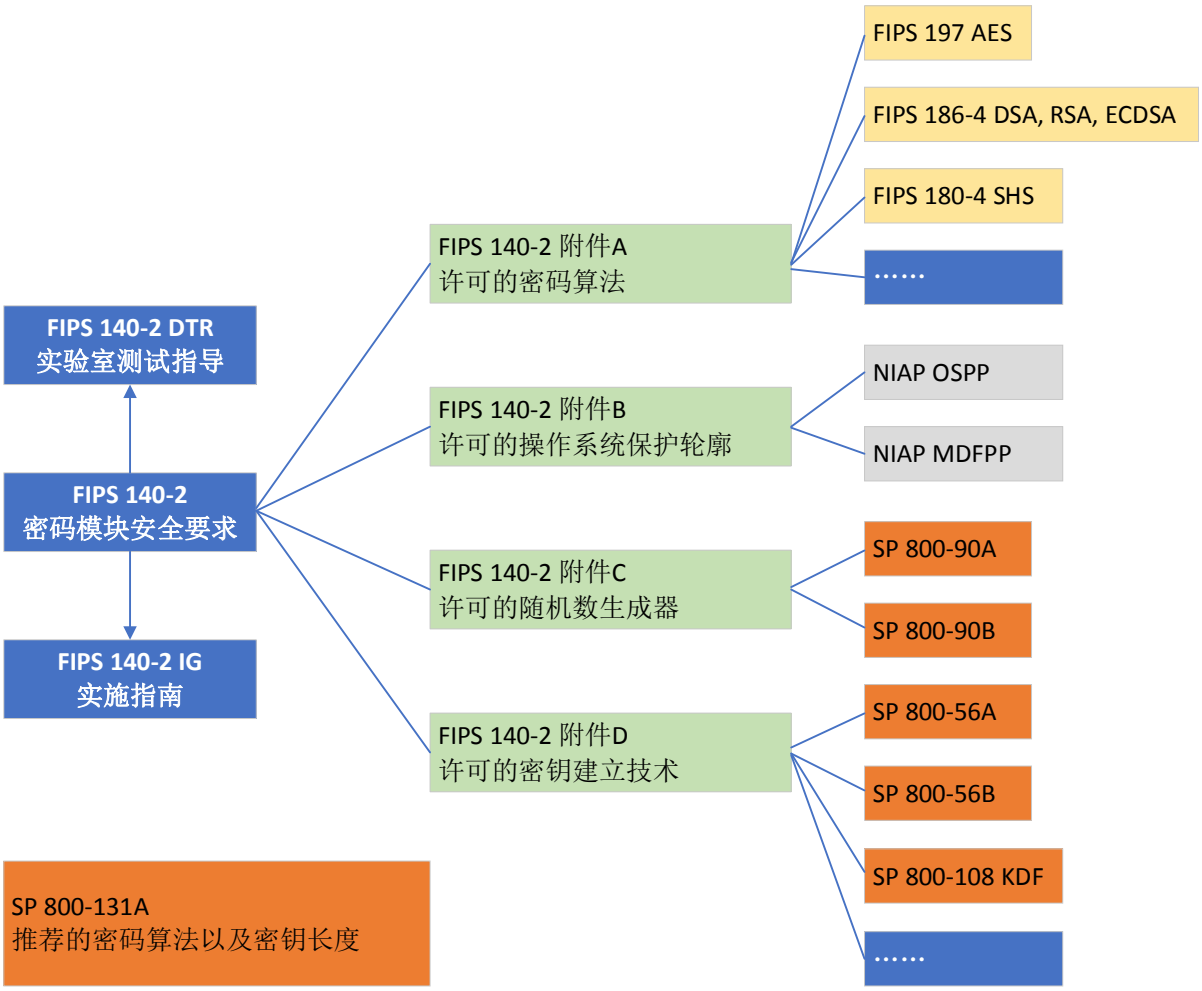

图 2：FIPS 140-2 标准以及相关支撑文档体系

这些强制引用的文档导致 FIPS 140-2 标准在很多国家无法落地实施。而作为国际标准 ISO/IEC 19790，各国可以依托于自身体系进行密码算法或是其他密码相关功能的选择，比如我国就可以要求在商用密码领域使用 SM2、SM3、SM4 分别作为非对称密码算法、散列算法以及对称密码算法，使用 GM/T 0003.3 作为密钥交换协议等，这样就可以在充分利用成熟的国际标准作为密码模块检测框架的同时，保持我国自身密码体系的独特性与创新性。ISO/IEC 19790 及其相关国际标准体系图如下，其中 ISO/IEC 24759 可被视为国际标准版本的 FIPS 140-2 DTR：

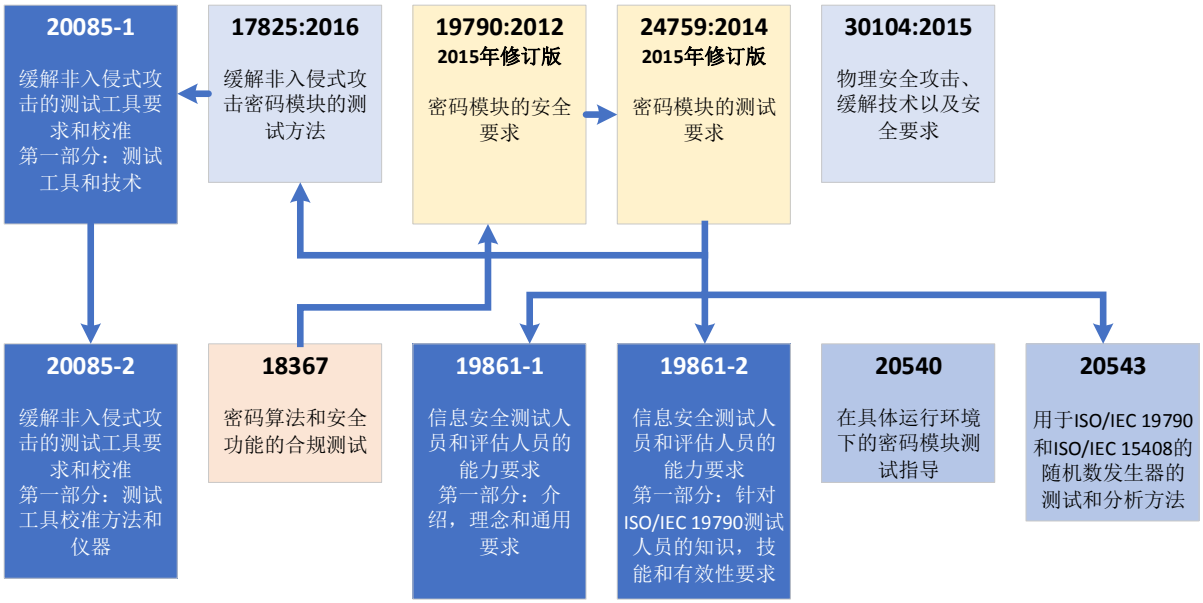

图 3：ISO/IEC 19790 以及相关支撑文档体系

在 ISO/IEC 19790 演进的过程中，分别成立了两个独立的讨论组，一个关注在物理安全层面，一个关注在软件安全层面。其中物理安全专题讨论组重点关注在：

- 非侵入性测试要求，主要针对侧信道攻击（Side Channel Attack）
- 针对安全等级三级的环境失效保护（EFP）/环境失效检测（EFT）要求
- 针对安全等级四级的环境失效保护（EFP）要求
- 针对安全等级四级的错误注入攻击（Fault Induction Attack）的缓解

软件安全专题讨论组重点关注在：

- 针对软件安全的特有章节
- 针对软件模块的边界定义
- 移除了针对安全等级二级软件模块的通用评估准则（CC）要求
- 移除了针对安全等级三级和四级的运行环境要求

限于篇幅，本文不展开详细解释。对具体内容感兴趣的读者可参考 ISO/IEC 19790 标准的对应条目要求。

下面我们会对 FIPS 140-2 和 ISO/IEC 19790 标准进行比对：

FIPS 140-2	ISO/IEC 19790
1. 密码模块规格	1. 密码模块规格
2. 密码模块接口	2. 密码模块接口
3. 角色、服务和鉴别	3. 角色、服务和鉴别

4. 有限状态模型	4. 软件/固件安全
5. 物理安全	5. 运行环境
6. 运行环境	6. 物理安全
7. 密钥管理	7. 非入侵式安全
8. 电磁兼容要求	8. 敏感安全参数管理
9. 自测试	9. 自测试
10. 设计保障	10. 生命周期保障
11. 对其他攻击的缓解	11. 对其他攻击的缓解
附录 C. 安全策略	附件 A. 文档要求
附件 A. 许可的安全功能	附件 B. 密码模块安全策略
附件 B. 许可的操作系统保护轮廓	附件 C. 许可的安全功能
附件 C. 许可的随机数生成器	附件 D. 许可的敏感安全参数生成和建立
附件 D. 许可的密钥建立技术	附件 E. 许可的鉴别机制
	附件 F. 许可的非入侵式攻击缓解测试指标

表 1：FIPS 140-2 与 ISO/IEC 19790 的比较

如上表所示，与现行的 FIPS 140-2 标准相比，ISO/IEC 19790 基本上继承了目前的框架体系，仍然具备 4 个安全等级，删除了对电磁兼容的要求，将“密钥管理”和“设计保障”扩展为“敏感安全参数管理”和“生命周期保障”，并在“生命周期保障”中融入了“有限状态模型”的要求，额外增加了“软件/固件安全”和“非入侵式安全”。下文会按照章节列举 ISO/IEC 19790 变更或新增的要求点。

3.1 密码模块规格

在现有的许可模式和非许可模式之间，ISO/IEC 19790 中加入了降级模式。当一个密码模块从错误状态退出后就会自动运行于降级模式，在该模式下只能对外提供状态信息，且导致之前进入错误状态的功能需要被隔离出来。在降级模式中第一次执行任何密码算法之前，需要先针对该算法进行自测试，同时，如果密码模块使用到被隔离的功能或算法时，需要通过标记显示出来。只有当模块通过了所有的运行前自测试和条件自测试后才可以脱离降级模式，如果运行前自测试失败，则密码模块不能进入降级模式。

3.2 密码模块接口

在现有的四个逻辑接口（数据输入、数据输出、控制输入、状态输出）之外，ISO/IEC 19790 定义了第五个接口：控制输出。所有用于控制密码模块运行的输出命令、信号及控制数据（例如，对另一个模块的控制命令）应通过“控制输出”接口输出。当密码模块处于错误状态时，应禁止通过“控制输出”接口的控制输出，除非在安全策略文档中规定了例外情况。

3.3 角色、服务和鉴别

ISO/IEC 19790 定义了密码模块至少应该具有密码主管角色，而用户角色不是必须具备的。

同时，密码模块至少要提供如下的服务：

- 显示密码模块的版本，输出密码模块的名称或模块标识符以及版本信息，同时这些信息与模块的确认记录相关联。
- 显示当前状态
- 执行自测试
- 执行许可的安全功能
- 执行置零

在 FIPS 140-2 的要求之外，ISO/IEC 19790 额外定义了“自启动密码服务能力”，指的是无需外界操作员请求，模块就能够执行密码操作和其他核准的安全功能或敏感安全参数管理技术。该能力要求由密码主管进行配置，需要两个内部独立操作来激活该能力，同时其激活状态需要由状态指示给出。

另外，身份鉴别强度的对应要求需要通过密码模块自身实现，而不能依赖于策略文档或是外部的安全规则，比如密码长度、复杂度等。同时，为了提供更高强度的身份鉴别机制，针对安全等级四级的密码模块，ISO/IEC 19790 要求必须提供多因素认证机制。

3.4 软件/固件安全

本条目为 ISO/IEC 19790 新增要求，只适用于软件/固件模块，或混合模块。

针对安全等级二级的密码模块，必须使用许可的数字签名算法或是带密钥的消息鉴别码作为完整性测试机制；针对安全等级三级或四级的密码模块，则只能使用许可的数字签名算法作为完整性测试机制。

3.5 运行环境

针对安全等级二级的软件模块，操作系统不再受到通用评估准则要求的限制，而是需要满足 ISO/IEC 19790 中所列出的针对操作系统访问控制、审计等功能的一系列限制。

3.6 物理安全

在 FIPS 140-2 的物理安全基础之上，ISO/IEC 19790 明确允许模块使用符合标准要求的半透明的外壳。

针对安全等级三级的密码模块，则要求必须具备环境失效保护机制，或者至少通过环境失效测试；而针对安全等级四级的密码模块，标准明确规定必须实施环境失效保护机制。

3.7 非入侵式安全

本条目为 ISO/IEC 19790 新增要求，适用于硬件模块、固件模块或固件混合模块，运行在可修改操作环境的软件模块可以由厂家或实验室决定是否测试本条目。

针对安全等级一级或二级的密码模块，需要通过体系文件阐明用于密码模块是如何免受附件 F 中的所有非入侵式技术攻击的。

针对安全等级三级或四级的密码模块，实验室需要针对模块进行测试，以确保模块实现了缓解附件 F 中列出的非入侵式攻击的机制。

最新的 ISO/IEC 19790 标准中尚未对“附件 F：许可的非入侵式攻击缓解测试指标”进行具体的定义。

3.8 敏感安全参数管理

ISO/IEC 19790 中定义的敏感安全参数（Sensitive Security Parameter）包含了关键安全参数（Critical Security Parameter）以及公开安全参数（Public Security Parameter）。

针对安全等级二级以上的密码模块，不能通过规定的程序执行（如磁盘格式化）对敏感安全参数进行置零，而是必须有模块自身实现置零的机制，例如使用全 0 或全 1 或随机数据覆盖，但是不能使用另一个未受保护的敏感安全参数来覆盖当前需要置零的敏感安全参数。

3.9 自测试

自测试在 ISO/IEC 19790 中分为两类：

- 运行前自测试，包括软件/固件完整性测试、旁路测试、关键功能测试
- 条件自测试，包括密码算法条件自测试、密钥对一致性测试、软件/固件加载测试、手动输入测试、旁路测试、关键功能测试、周期测试

无论运行在许可模式还是非许可模式下，密码模块都需要执行自测试。

针对安全等级三级或四级的密码模块，授权管理员可以访问模块的错误日志。该错误日志至少应提供最近的错误事件，例如某一个自测试项目失败。同时，密码模块需要在定义的时间周期内，无需外部的输入或控制而自动重复执行运行前或条件自测试。

完整性测试需要覆盖密码模块的所有软件/固件部分。用于完整性测试所使用的密码算法应先通过密码算法条件自测试。针对不包含软件或固件的纯粹硬件模块来说，应至少实现一个密码算法条件自测试作为运行前自测试。

ISO/IEC 19790 与 FIPS 140-2 的不同之处还在于，密码算法自测试从上电自测试变成了条件自测试，同时也不局限于已知答案测试，而是可以使用对比测试或错误检测测试来替代。

另外需要注意的是，FIPS 140-2 中所定义的连续随机数生成器测试（Continuous Random Number Generator Test）不再适用。

3.10 生命周期保障

ISO/IEC 19790 对密码模块的厂商测试提出了要求，厂商需要独立于实验室之外对密码模块进行测试，但是标准本身并没有提及哪些测试必须要由厂商来执行。

有限状态模型在 FIPS 140-2 已有的要求之上扩展了更多的必要状态，目前密码模块所需要具备的状态至少包括：

- 电源开启/关闭状态
- 初始化状态
- 密码主管状态
- 关键安全参数（CSP）输入状态
- 用户状态（若实现了用户角色）
- 许可运行状态
- 自测试状态
- 错误状态

另外，从其他角色转换为密码主管角色在 ISO/IEC 19790 标准中被严格禁止。

针对生命周期终止的密码模块，应当有体系文件文档阐明安全清理或是安全销毁模块的流程。

3.11 对其他攻击的缓解

针对安全等级一级、二级或三级的密码模块，如果该模块有专门的设计用来缓解标准中未定义的攻击技术，则需要提供体系文件阐明如何缓解该攻击的。

针对安全等级四级的密码模块，如果声明了能够缓解某些攻击，则需要详细说明缓解攻击的方法，并且提供测试该缓解技术有效性的证据。

4 后记

目前我国在密码模块安全要求标准的制定上仍然处于跟随状态，现行的 GM/T 0028-2014 参考 FIPS 140-2 编写，升级版本的 GB/T 37092-2018 参考 ISO/IEC 19790 编写，已经进入发布流程。目前“信息安全技术 密码模块安全检测要求”正在编写中，而针对图 3 中列出的其他诸多关键支撑文档仍然缺失。

由于标准的发布和实施与国际密码技术产业存在一定的滞后，国内实验室对如何使用这些标准对密码模块进行检测也仍有较大的疑问。作为国际知名的密码模块检测实验室，atsec 希望能携手国内同行，共同提升国内密码模块检测水平，为商用密码行业的发展贡献自身的力量。