密码模块三级的重要性与实践

北京三未信安科技发展有限公司

高志权

CONTENTS

密码模块安全相关标准

FIPS PUB 140

~~FIPS PUB 140-1 Security Requirements for Cryptographic Modules, 1994~~
FIPS PUB 140-2 Security Requirements for Cryptographic Modules, 2002
Derived Test Requirements for FIPS PUB 140-2, 2011
FIPS PUB 140-3 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2019

01

ISO/IEC 19790:2012

ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules
ISO/IEC 24759:2017 Information technology -- Security techniques -- Test requirements for cryptographic modules

02

GM/T 0028-2014 | GM/T 37092-2018

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
GB/T 37092-2018 信息安全技术 密码模块安全要求

03

FIPS 140 版本演变

FIPS 140-1

1994年首次发布
1995年首个模块通过
2005年最后一个模块

FIPS 140-2

2001年发布
2002年修订
2003年首个模块通过

FIPS 140-3

2013年草案
2019年正式发布

适用于所有使用基于加密的安全系统来保护计算机和电信系统（包括语音系统）中敏感信息的联邦机构，如1996年“信息技术管理改革法”第104-106号公共法第5131节和 2002年联邦信息安全管理法，公法107-347。

CMVP是美国国家标准与技术研究院（NIST）与加拿大通信安全机构（CSEC）之间落实FIPS 140标准的联合计划，英国通信电子安全组（CESG）也建议使用经FIPS 140验证的加密模块。

FIPS 140-3 最新进展

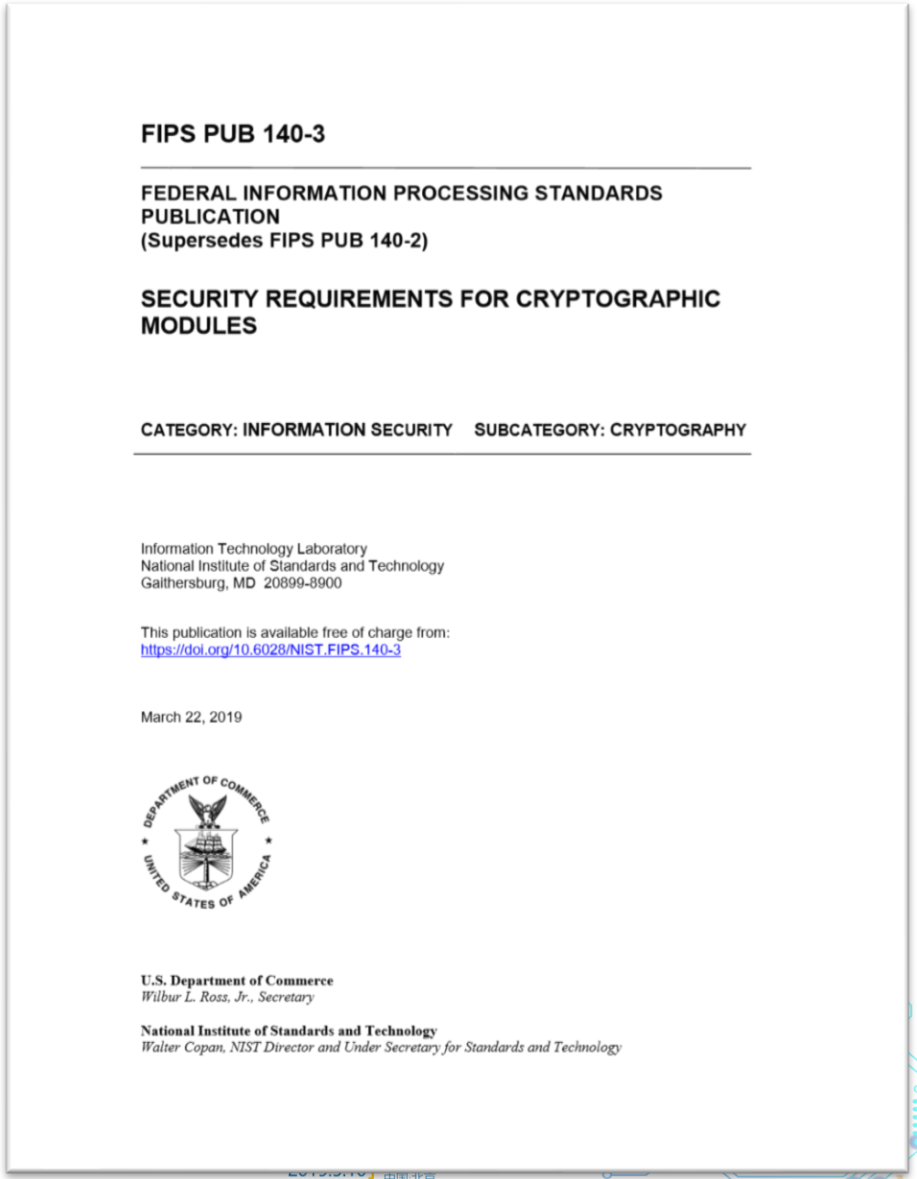
Approval and Issuance of FIPS 140-3

The 3rd version of FIPS 140 has been signed by the U.S. Commerce Secretary!

FIPS 140-3, "Security Requirements for Cryptographic Modules," was approved on March 22, 2019 and announced in the Federal Register on May 1, 2019.
FIPS 140-3 supersedes FIPS 140-2.

Key Dates:
- Takes Effect: 9/22/19
- New Testing Begins: 9/22/20
- 140-2 Sunset: 9/21/21
- 140-3 Mandated: 9/22/21

https://csrc.nist.gov/News/2019/approval-and-issuance-of-fips-140-3



FIPS PUB 140-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140-2)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: INFORMATION SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.140-3

March 22, 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary for Standards and Technology

FIPS 140-2

	Level1	Level2	Level3	Level4
密码模块规格	密码模块的说明、边界、认可的加密算法、认可的操作模式。密码模块的说明，包括所有硬件、软件与固件，安全策略的描述			
密码模块端口和接口	所需与可选的接口，所有的接口与所有的输入、输出数据的路径的说明。		对用于未保护的关键安全参数的数据连接端口，应当在逻辑或物理上与其他数据连接端口分开。	
角色、服务与鉴别	要求逻辑上分开的可选角色和服务。	基于角色或基于身份的操作员鉴别。	基于身份的操作员鉴别。	
有限状态模型	有限状态模型说明，要求的状态与可选的状态。状态转换图与状态转移说明。			
物理安全	产品级装置	锁或入侵证据	对盖与门的入侵检测与响应	入侵检测与反应的封装，EFP/EFT
运行环境	单操作员，可执行代码，核准的完整性技术	经EAL2评估或等价的可信操作系统自主访问控制机制与审计	经EAL3评估或等价的可信操作系统以及可信路径和安全策略	经EAL4评估或等价的可信操作系统
密钥管理	密钥管理机制：随机数与密钥的产生、密钥的建立、分配，密钥的输入与输出，密钥的存储与密钥的清除。			
	利用人工手段所建立的密钥和私钥，可以用明文的格式输入与输出。		利用人工手段所建立的密钥和私钥，应当进行加密或用知识拆分的方法来输入与输出。	
EMI/EMC	47CFR FCC 第15部分，B分册， A类（商用）使用的FCC要求。		47CFR FCC 第15部分，B分册， B类（家用）。	
自测试	通电测试，加密算法测试，软件/固件集成测试，关键功能测试，状态测试。			
设计保证	配置管理（CM）：安全安装与生成，设计与策略的一致性，指导性文档。	配置管理系统：安全分发。功能规格	高级语言的实现	正式的型号，详细的说明书（非正式封装的），预处理与后处理
其他入侵的缓解	其他入侵的缓解说明，目前没有可测试的要求			

安全要求摘要

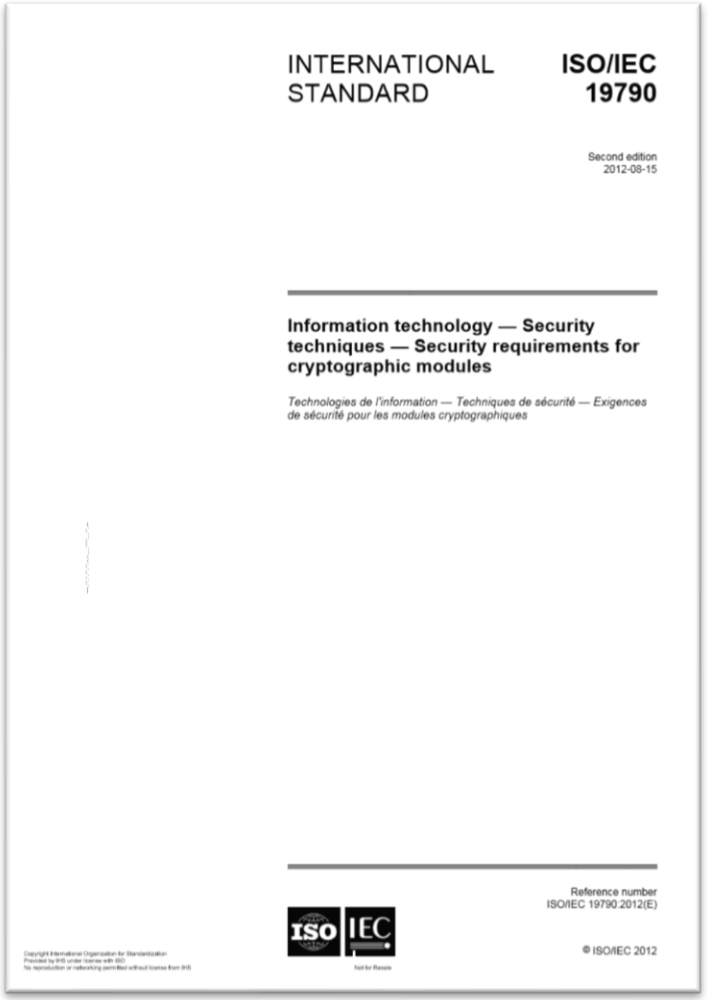
FIPS 140-2 标准定义的安全级别

- **Level 1**：最低的级别，为密码模块指定基本的安全要求（如加密算法是经过 NIST 认可的）。
- **Level 2**：增加明显的防窜挠外壳、封条或防撬锁等要求来改进密码模块的物理安全。
- **Level 3**：在Level 2中所要求的加密模块的物理安全性结构基础上，还要求防止对由加密模块内部所控制的关键安全参数过程的攻击，即安全性进一步增强。
- **Level 4**：最高级别，物理安全在密码模块周围提供检测察觉从任何方向试图渗透的保护封套，检测到破坏后所有的关键安全参数清零。

ISO/IEC 19790:2012

ISO/IEC 19790和FIPS 140的关系

ISO/IEC 19790是FIPS 140-2的演进，相当于FIPS 140的国际标准版。
ISO/IEC 19790:2006于2006年3月发布，粗略等同于FIPS 140-2。
FIPS 140-3 草案和ISO/IEC 19790:2012时间上基本同步，正式版内容基本一致，附录略有区别。


INTERNATIONAL STANDARD

ISO/IEC 19790

Second edition
2012-08-15

Information technology — Security techniques — Security requirements for cryptographic modules

Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques

Reference number
ISO/IEC 19790:2012(E)

© ISO/IEC 2012

实施ISO/IEC 19790的国家

- 日本IPA的加密模块验证程序（JCMVP），以ISO / IEC 19790为基础。
- 韩国加密模块验证计划（KCMVP）成立于2005年，以ISO / IEC 19790为基础，指定韩国批准的加密算法和安全功能。
- 西班牙的加密模块验证程序基于ISO标准
- 土耳其的加密模块验证程序基于ISO标准

资料来源：https://atsec-information-security.blogspot.com/2012/10/isos-cryptographic-module-work.html

Revisions / Corrigenda

Previously
Ø ISO/IEC 19790:2006
Ø ISO/IEC 19790:2006/Cor 1:2008

Now confirmed
Ø ISO/IEC 19790:2012

Corrigenda/Amendments
Ø ISO/IEC 19790:2012/Cor 1:2015

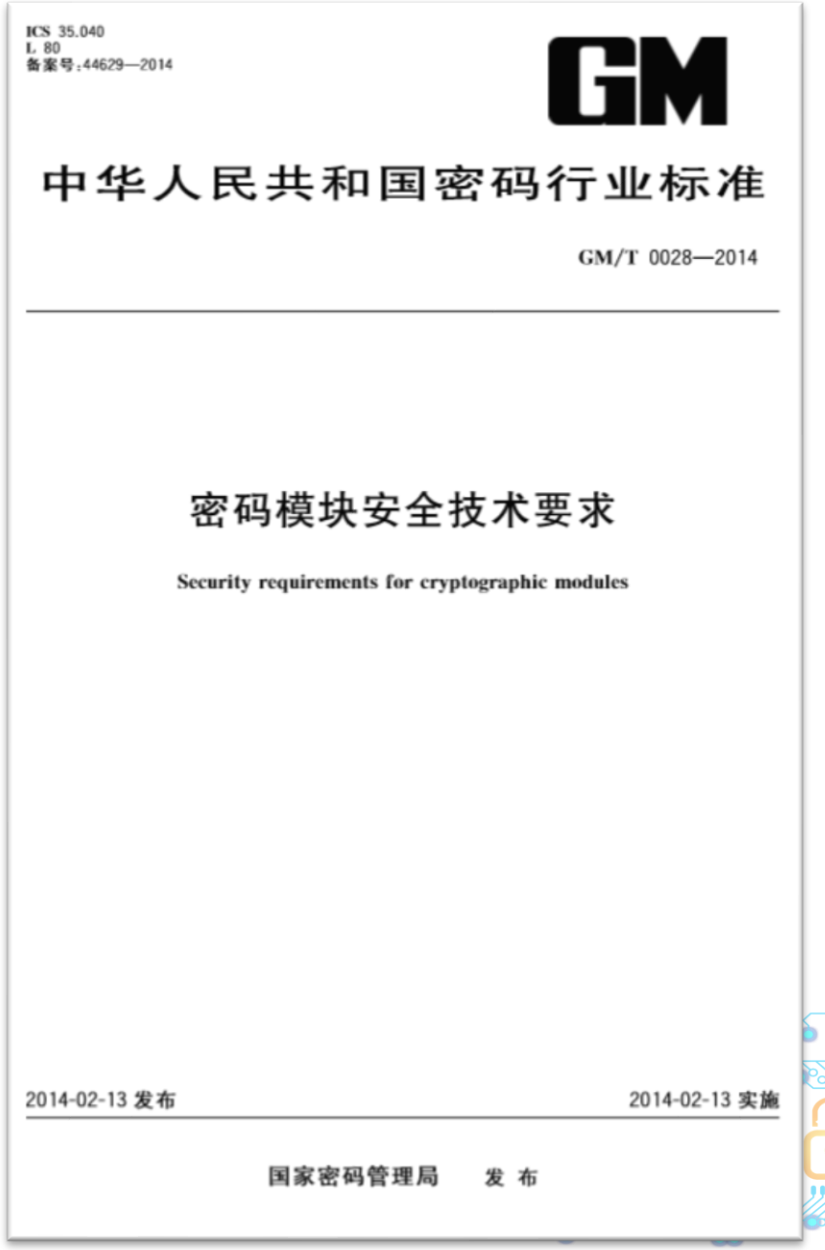
GM/T 0028-2014

本标准使用重新起草法参考ISO 19790:2012《密码模块安全要求》编制，与ISO 19790:2012的一致性程度为非等效。
针对国内商用密码体系和相关政策做了调整，如核准的安全功能和密码算法等。

2014年2月正式发布，2016年5月第一款产品认证通过。

其他相关标准

GM/T 0039-2015　密码模块安全检测要求（ISO/IEC 24759）
GM/T XXXX-XXXX 密码模块物理攻击缓解技术实施指南（ISO/IEC TS 30104）
GM/T XXXX-XXXX 密码模块非入侵式攻击缓解技术实施指南（ISO/IEC 17825）


ICS 35.040
L 80
备案号:44629—2014

GM

中华人民共和国密码行业标准

GM/T 0028—2014

密码模块安全技术要求

Security requirements for cryptographic modules

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　发布

GM/T 0028与FIPS 140-2的比较

	Level1	Level2	Level3	Level4
密码模块规格	密码模块的说明、边界、认可的加密算法、认可的操作模式。密码模块的说明，包括所有硬件、软件与固件，安全策略的描述			
密码模块端口和接口	所需与可选的接口，所有的接口与所有的输入、输出数据的路径的说明。		对用于未保护的关键安全参数的数据连接端口，应当在逻辑或物理上与其他数据连接端口分开。	
角色、服务与鉴别	要求逻辑上分开的可选角色和服务。	基于角色或基于身份的操作员鉴别。	基于身份的操作员鉴别。	
有限状态模型	有限状态模型说明，要求的状态与可选的状态。状态转换图与状态转移说明。			
物理安全	产品级装置	锁或入侵证据	对盖与门的入侵检测与响应	入侵检测与反应的封装，EFP/EFT
运行环境	单操作员，可执行代码，核准的完整性技术	经EAL2评估或等价的可信操作系统自主访问控制机制与审计	经EAL3评估或等价的可信操作系统以及可信路径和安全策略	经EAL4评估或等价的可信操作系统
密钥管理	密钥管理机制：随机数与密钥的产生、密钥的建立、分配，密钥的输入与输出，密钥的存储与密钥的清除。			
	利用人工手段所建立的密钥和私钥，可以用明文的格式输入与输出。		利用人工手段所建立的密钥和私钥，应当进行加密或用知识拆分的方法来输入与输出。	
EMI/EMC	47CFR FCC 第15部分，B分册， A类（商用）使用的FCC要求。		47CFR FCC 第15部分，B分册， B类（家用）。	
自测试	通电测试，加密算法测试，软件/固件集成测试，关键功能测试，状态测试。			
设计保证	配置管理（CM）：安全安装与生成，设计与策略的一致性，指导性文档。	配置管理系统：安全分发。功能规格	高级语言的实现	正式的型号，详细的说明书（非正式封装的），预处理与后处理
其他入侵的缓解	其他入侵的缓解说明，目前没有可测试的要求			

	安全等级1	安全等级2	安全等级3	安全等级4
密码模块规格	密码模块、密码边界、核准的密码功能以及正常的工作模式的说明； 密码模块的描述，包括所有硬件、软件和固件部件； 所有服务提供状态信息以指示服务何时按照核准的方式使用核准的密码算法、安全功能或过程			
密码模块接口	要求的和可选的接口； 所有接口和所有输入输出数据的说明		可信信道	
角色、服务与鉴别	要求的角色、服务与可选角色、服务逻辑隔离	基于角色或基于身份的操作员鉴别	基于身份的鉴别	多因素鉴别
软件/固件安全	核准的完整性技术，以及定义的SFMI、HFMI以及HSMI；可执行代码	基于核准的数字签名或带密钥消息鉴别码的完整性测试	基于核准的数字签名的完整性测试	
运行环境	不可修改的、受限的或可修改的；对敏感安全参数的控制	可修改的；基于角色或自主访问控制；审计机制		
物理安全	产品级部件	拆卸证据； 不透明的遮盖物或外壳	封盖或门上的拆卸检测与响应电路；牢固的外壳或涂层；防止直接探测的保护；EFP或EFT	拆卸检测和响应封壳；EFP； 错误注入的缓解
非入侵式安全	能够缓解附录F中规定的非入侵式攻击			
	文档阐明附录F中规定的缓解技术和有效性		提供缓解测试方法	缓解测试
敏感安全参数管理	随机比特生成器、敏感安全参数生成、建立、输入和输出、存储以及置零			
	自动的敏感安全参数传输或敏感安全参数协商使用核准方法			
	手动建立的敏感安全参数可以以明文的形式输入或输出		手动建立的敏感安全参数可以以加密的形式、通过可信信道或使用知识拆分过程输入或输出	
自测试	运行前：软件/固件完整性测试、旁路测试以及关键功能测试			
	条件：密码算法、配对一致性、软件/固件加载、手动输入、旁路以及关键功能测试			
生命周期保障 1）配置管理	密码模块、部件和文档的配置管理系统；每一项在整个生命周期中都有唯一标识并可追踪		自动配置管理系统	
2）设计	模块设计成允许对所有提供的安全相关服务进行测试			
3）FSM	有限状态模型			
4）开发	有注释的源代码、版图或HDL	软件高级语言； 硬件高级描述语言		文档注明模块部件执行的前置条件，以及当部件执行完毕时预期为真的后置条件
5）测试	功能测试		底层测试	
6）配送与操作	初始化流程	配送流程	使用厂商提供的鉴别信息的操作员鉴别	
7）指导文档	管理员和非管理员指南			
其他攻击的缓解	缓解其他攻击的说明，目前对这些攻击还没有可测试要求			验证缓解技术的有效性

说明：左侧表格是FIPS 140-2安全要求，右侧表格是GM/T 0028安全要求

CONTENTS

PCI 对HSM的安全要求

Number	Description of Requirement
A1*	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device. There is no demonstrable way to disable or defeat the mechanisms and access internal areas containing sensitive information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation.
B5*	The device provides secure interfaces that are kept logically separate by distinguishing between data and control for inputs and also between data and status for outputs.

PCI Security Standards Council

FIPS 140-2 Requirements

Some requirements in this manual are derived from requirements in Federal Information Processing Standard 140-2 (FIPS 140-2). These requirements are identified in this document with an asterisk (*) in the number column.

Because many FIPS 140-2 evaluations only cover a subsection of the HSM and with a number of possible security levels, existing evaluation evidence for an HSM certified against FIPS 140-2 will be assessed as follows.

The evaluator will establish:

- The HSM components that were evaluated;
- The security level of the evaluation;
- That the existing FIPS certification covers the full HSM functionality for all the related requirements.

PCI Security Standards Council

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Hardware Security Module (HSM)

Modular Security Requirements Version 3.0

WebTrust 对CA私钥的安全要求

#	Criterion	Ref
11	The CA maintains controls to provide reasonable assurance that: • CA private keys are protected in a system or device that has been validated as meeting at least FIPS 140[-2] level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats; • CA private keys outside the validated system or device specified above are protected with physical security, encryption, or a combination of both in a manner that prevents disclosure of the private keys; • CA private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048-bit minimum); • CA private keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment; and • physical and logical safeguards to prevent unauthorized certificate issuance.	5.2.2, 6.2, 6.2.7

GM/T 0054 中对密码模块的安全要求

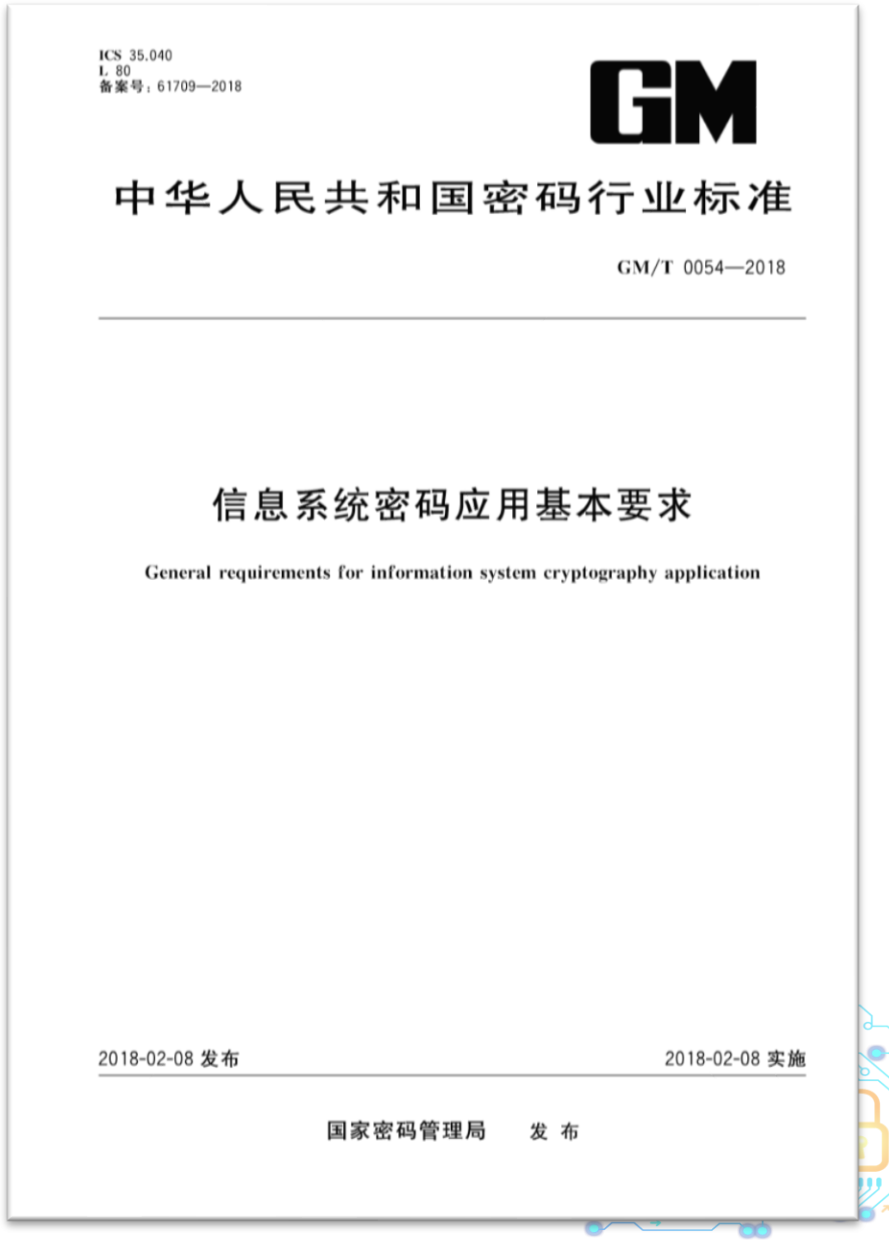
等级保护第三级信息系统要求

宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

等级保护第四级信息系统要求

应采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

“宜”表示推荐、建议，是推荐型描述，表示该条款是首选但不是必须要求；
“应”表示应该、要求，是要求型描述，表明符合标准 需要满足的要求。


ICS 35.040
L 80
备案号：61709—2018

GM

中华人民共和国密码行业标准

GM/T 0054—2018

信息系统密码应用基本要求

General requirements for information system cryptography application

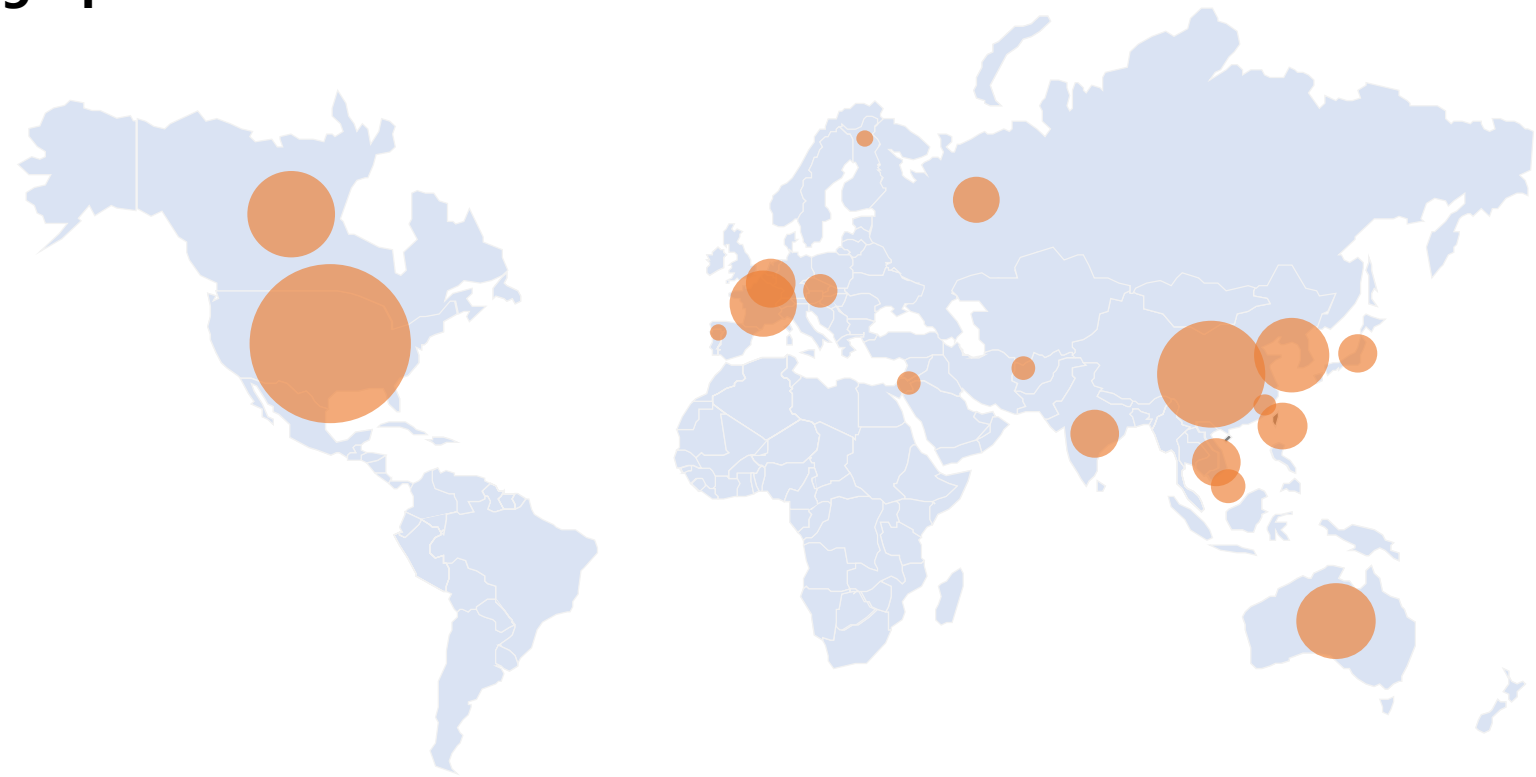
2018-02-08 发布　　2018-02-08 实施

国家密码管理局　发布

CONTENTS

FIPS 140-2 国家与TOP统计

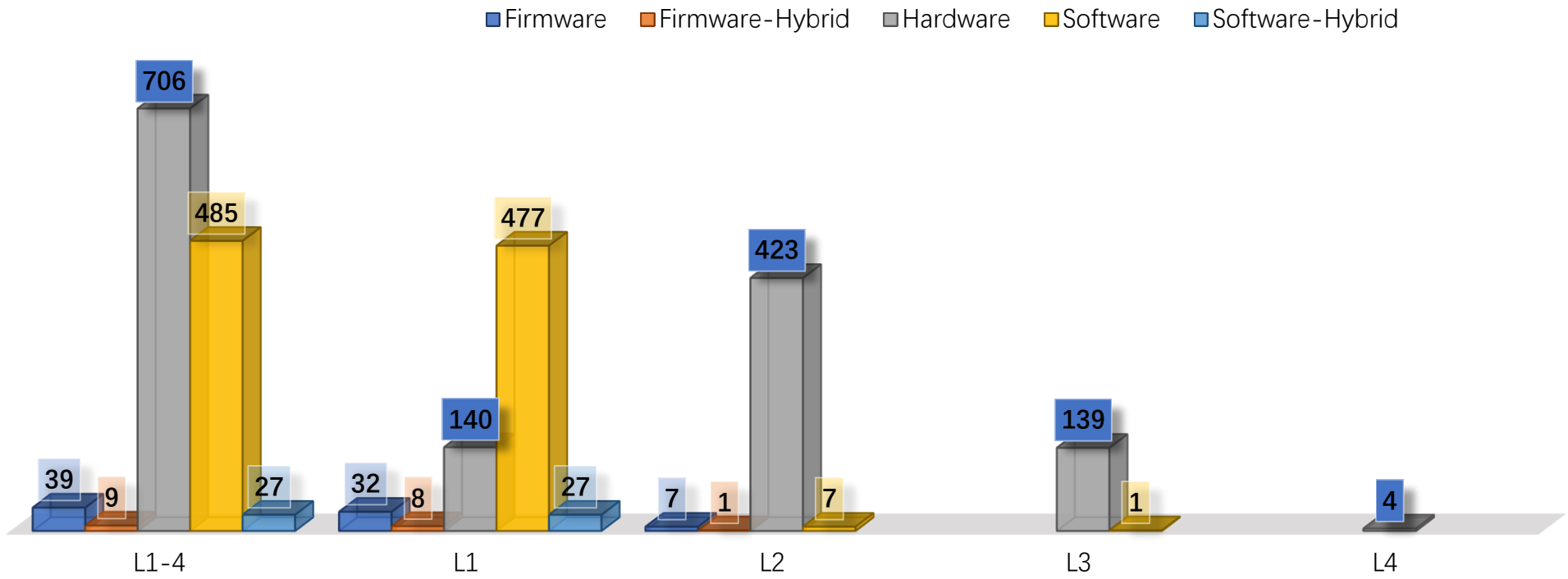
FIPS cryptographic modules



国家	美国	日本	德国	加拿大	英国	中国	澳大利亚	中国台湾	法国	瑞士	新加坡	印度	韩国	比利时	俄罗斯	芬兰	荷兰	马来西亚	乌兹别克斯坦	斯里兰卡	香港	西班牙	以色列	...
公司数	230	11	9	8	8	8	6	5	3	3	3	3	2	1	1	1	1	1	1	1	1	1	1	
产品数	976	18	24	31	17	46	26	12	8	10	3	5	32	1	4	7	2	1	1	2	3	1	1	

数据来源：https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search (Active, 06/05/2019)

FIPS 140-2 认证情况(Active, 05/02/2019)



	L1-4	L1	L2	L3	L4
Firmware	39	32	7		
Firmware-Hybrid	9	8	1		
Hardware	706	140	423	139	4
Software	485	477	7	1	
Software-Hybrid	27	27			
Total	1266	684	438	140	4

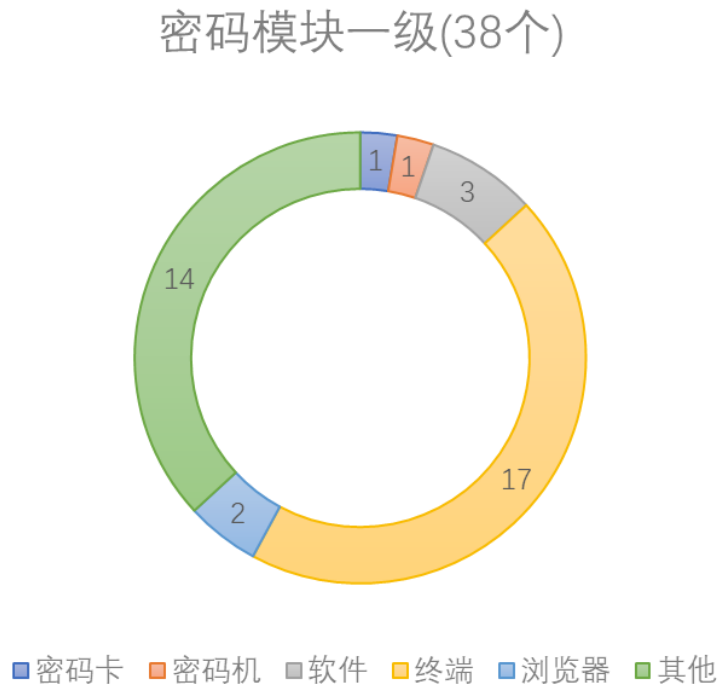
FIPS认证产品中高安全等级主要是**硬件形态**

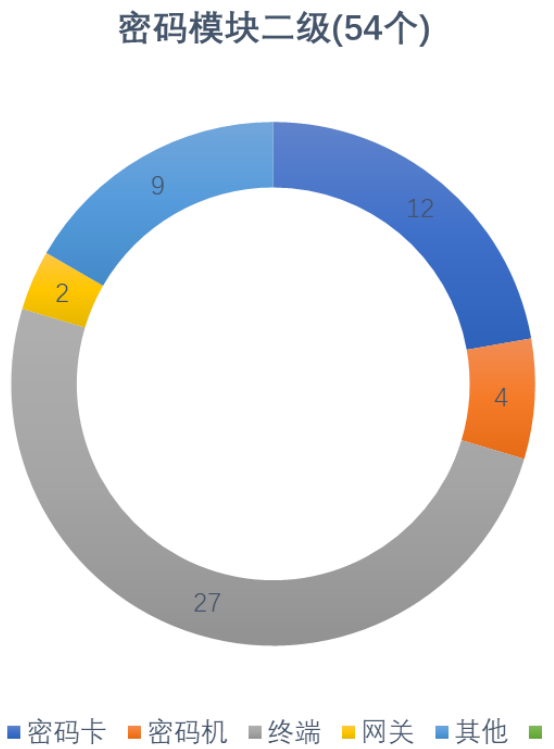
软件模块在Level 2中占比很小约为1.6%，Level 3只有1个（实际是PCI-E密码卡）

历史数据来看Level 2（共1405个）中软件模块（70个），占比为5%

数据来源：https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

商密产品密码模块认证情况(2018-11-30)





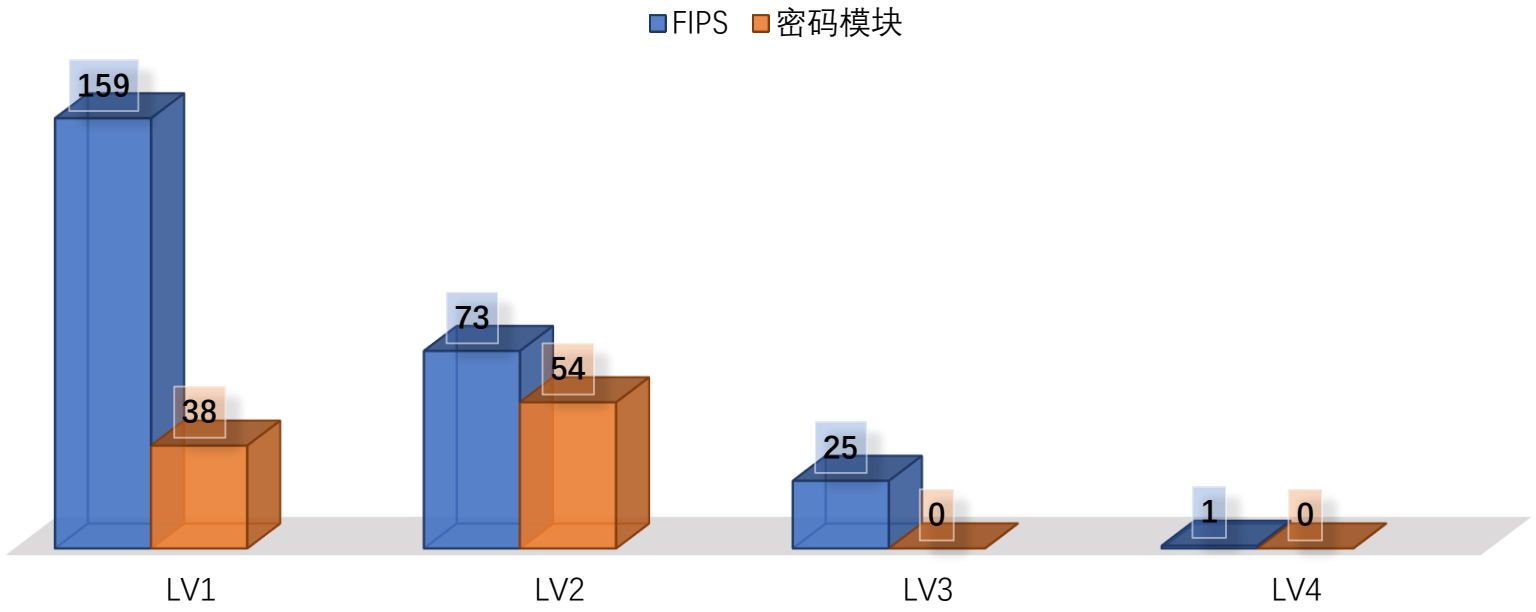
密码模块三级(0个)

二级模块中软件（SHM/SRM）共15个
占比27.78%，远高于FIPS

数据来源：国密局网站 http://www.sca.gov.cn (截止时间2018年11月30日)

2018年密码模块数量统计对比

2018年FIPS与密码模块数量统计对比



FIPS等级	lv1	lv2	lv3	lv4	总计
通过数量	159	73	25	1	258
密码模块	一级	二级	三级	四级	
通过数量	38	54	0	0	92

我国在二级密码模块的占比率高于FIPS 140-2 lv2在整体中的比率，但同时我国在三级和四级的设计上需要不断推进和完善。

CONTENTS

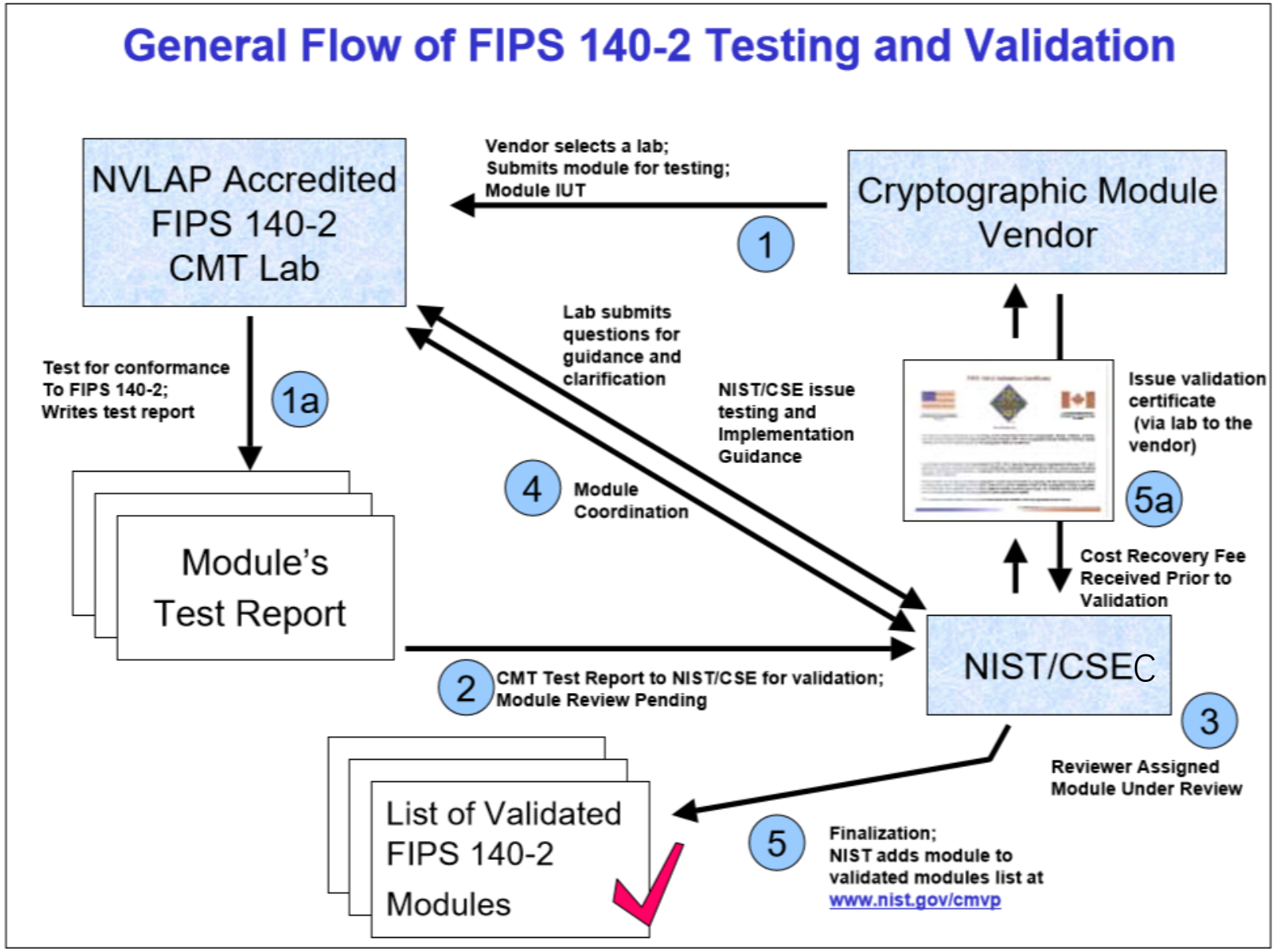
FIPS 认证流程

0、差距分析，支付咨询费用
1、厂商选择实验室，进入IUT阶段
1a、评估测试
2、实验室将评估报告提交给NIST
3、NIST分配审核人员
4、实验室和NIST及厂商之间互动
5a、支付评估费用
5、NIST网站发布

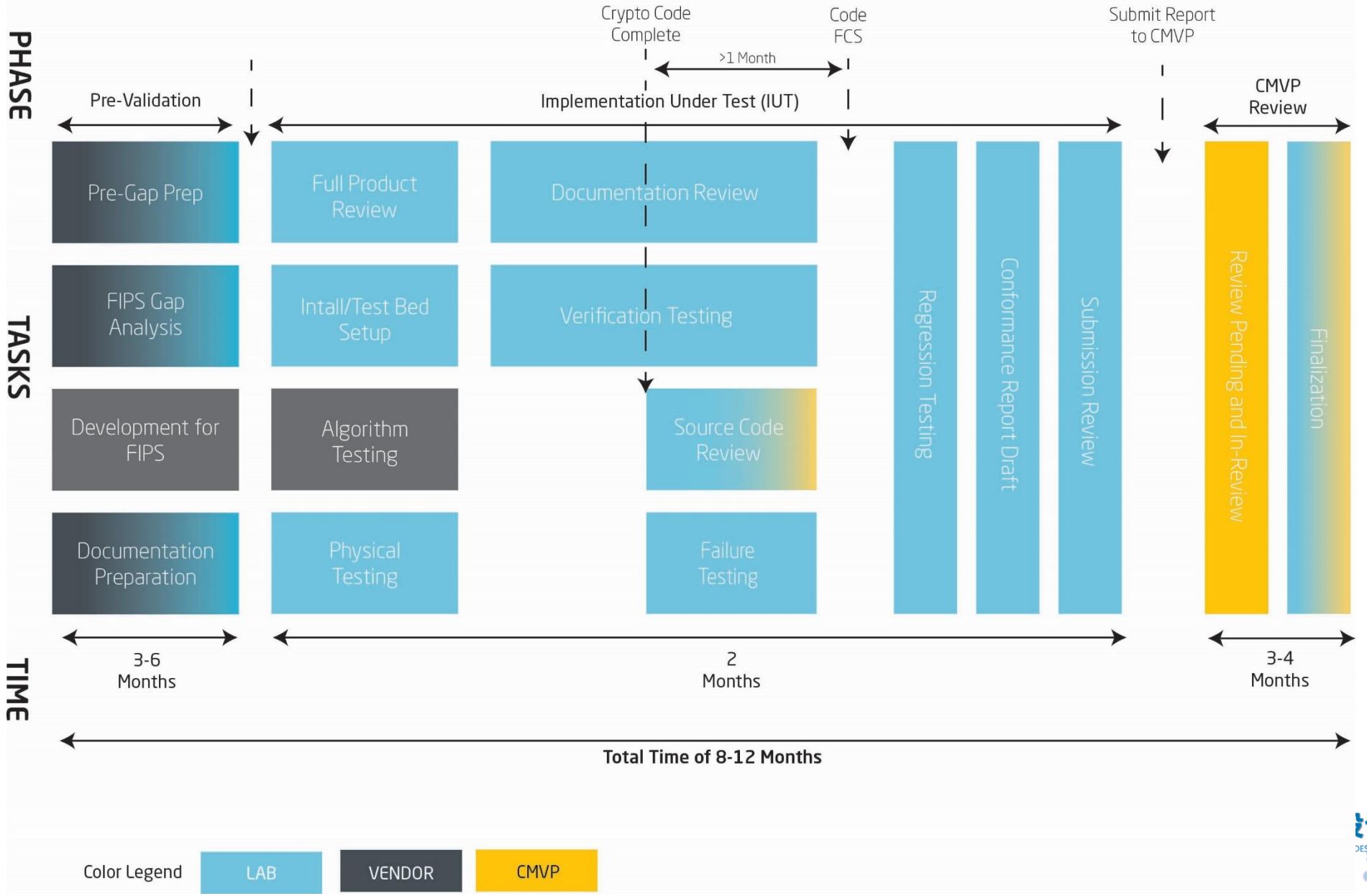
IUT：
https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List

MIP：
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Modules-In-Process/Modules-In-Process-List

Validated：
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search



FIPS 认证周期


PHASE
TASKS
TIME
Crypto Code Complete
Code FCS
>1 Month
Submit Report to CMVP
Pre-Validation
Implementation Under Test (IUT)
CMVP Review
Pre-Gap Prep
Full Product Review
Documentation Review
Regression Testing
Conformance Report Draft
Submission Review
Review Pending and In-Review
Finalization
FIPS Gap Analysis
Intall/Test Bed Setup
Verification Testing
Development for FIPS
Algorithm Testing
Source Code Review
Documentation Preparation
Physical Testing
Failure Testing
3-6 Months
2 Months
3-4 Months
Total Time of 8-12 Months
Color Legend
LAB
VENDOR
CMVP

国内首款密码模块三级产品

SJK1926 PCI-E密码卡

1. 密码模块规格
2. 密码模块接口—可信信道
3. 角色、服务与鉴别
4. 软件/固件安全
5. 运行环境
6. 物理安全—响应电路/防探测/EFP/EFT
7. 非入侵式安全—能量/计时/电磁/测试方法
8. 敏感安全参数管理
9. 自测试
10. 生命周期保障
11. 其他攻击的缓解

整机类密码模块三级的挑战

1. 密码模块规格
2. 密码模块接口
3. 角色、服务与鉴别
4. 软件/固件安全
5. 运行环境
6. 物理安全
7. 非入侵式安全
8. 敏感安全参数管理
9. 自测试
10. 生命周期保障
11. 其他攻击的缓解

黑色—比较容易实现
绿色—继承密码卡安全方案
红色—重新设计安全方案

谢谢！

北京三未信安科技发展有限公司　　高志权