科学 准确 客观 规范

国内领先的金融行业信息安全实验室

可信赖的信息安全服务专业机构

CFCA
中国金融认证中心

CFCA官方微信

信息安全服务

信息安全实验室

地址：北京市亦庄经济技术开发区科创十四街20号院2号楼

电话：010-80864639　传真：010-63555032

网址：www.cfca.com.cn/anquan

信息安全实验室

INFORMATION SECURITY LABORATORY

CFCA 中国金融认证中心
China Financial Certification Authority

国内领先的

金融行业信息安全实验室

可信赖的

信息安全服务专业机构

中金金融认证中心有限公司（即中国金融认证中心China Financial Certification Authority，简称CFCA），是由中国人民银行于1998年牵头组建、经国家信息安全管理机构批准成立的国家级权威安全认证机构，是国家重要的金融信息安全基础设施之一。在《中华人民共和国电子签名法》颁布后，CFCA成为首批获得电子认证服务许可的电子认证服务机构，目前已经成为国内最大的电子认证服务机构之一。

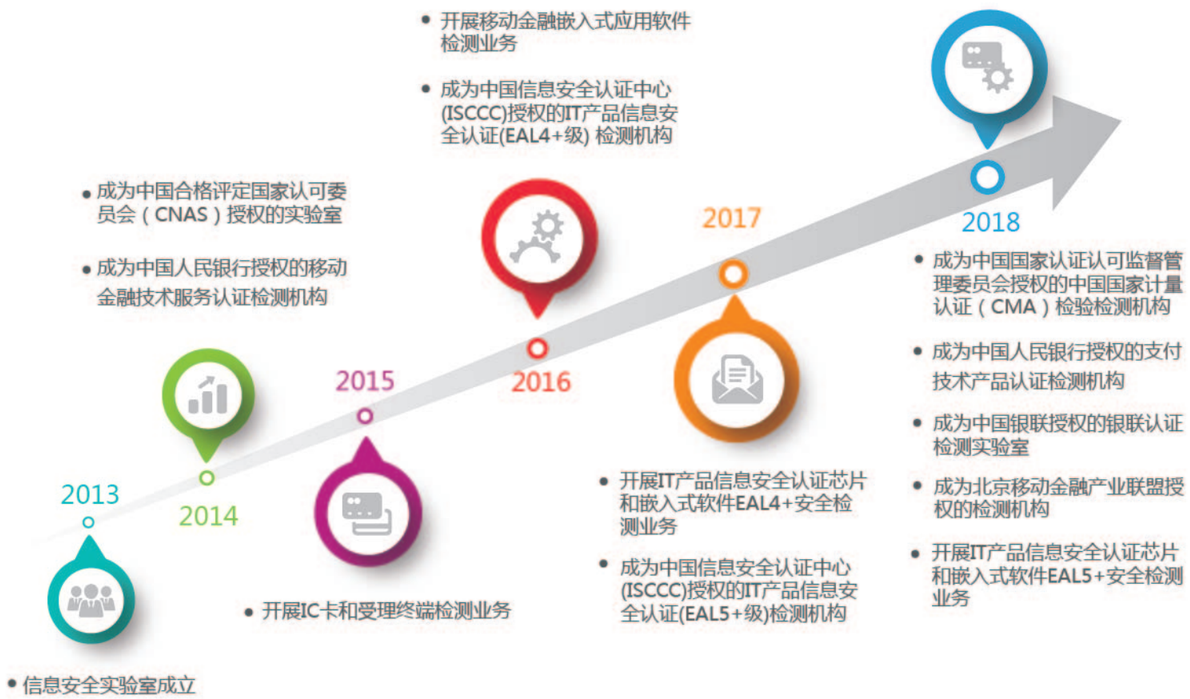
CFCA自2004年开始从事信息安全服务，于2013年正式成立信息安全实验室，从事金融支付产品检测服务。

信息安全实验室拥有一支由博士生、硕士生及本科生组成的高素质专业技术人才队伍，大部分工程师都拥有多年的信息安全服务工作经验和信息安全产品开发经验。

目前，信息安全实验室的业务范围已覆盖芯片、嵌入式软件、移动终端应用软件（APP）、条码技术、可信执行环境及其应用（TEE和TA）、金融IC卡及其受理设备、网银安全产品（USBKey和OTP）、移动金融安全载体（SE）、移动金融嵌入式应用软件等检测服务，以及金融领域安全IC卡和密码应用示范工程验收（国密算法改造验收）检测服务等。作为独立的第三方检测实验室，已面向金融、电信、交通、社保等行业以及物联网领域提供了多种产品检测服务。

信息安全实验室秉承科学、准确、客观、规范的管理方针，发挥自身人才、技术和经验的优势，积极为广大客户提供优质全方位的信息安全服务。

信息安全实验室发展历程



信息安全实验室服务类型

- 检测服务
  针对安全产品开展功能检测、安全检测和委托测试
- 主管部门与监管部门技术支撑
  参与国标委、金标委、中国互联网金融协会、中国支付清算协会、北京移动金融产业联盟、中国银联等多项国标、行标、团体或企业标准的修订
- 培训服务
  标准解读、安全产品检测认证、产品检测技术

信息安全实验室业务种类

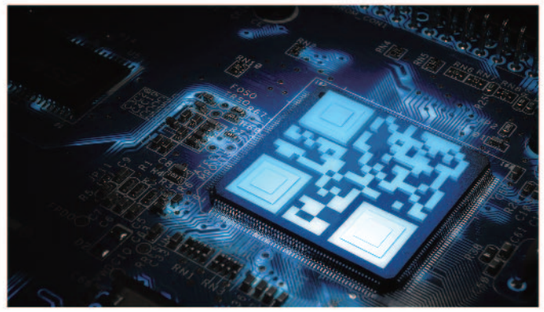
- 产品检测项目
  芯片、嵌入式软件、金融IC卡、受理终端、USBKey&OTP
- 支付技术检测项目
  移动金融安全载体（SE）、移动金融嵌入式应用软件、TEE、TA、条码技术
- 其他服务
  金融领域安全IC卡和密码应用示范工程验收测试、信息安全资讯与同业动态通报

CONTENTS

CHIP SECURITY TEST

芯片安全检测

随着信息时代的日益深化，芯片逐步成为各领域信息产品的核心，上至通讯卫星，下至生活中常见的手机、身份证、银行卡、汽车、物联网设备等都离不开芯片。在数字化时代，信息的流失、泄密随时能成为影响个人、社会乃至国家安全的隐患。保证信息安全的重中之重，就是确保做为信息产品核心芯片的安全。目前安全芯片产业已被列为国家信息安全战略之一，在政策的大力推动下，市场中涌现了大量应用于不同领域甚至不同业务场景的安全芯片。



随之而来芯片的安全性检测也被越来越多的行业所重视。针对日益增长的检测需求，信息实验室立足于金融行业，开展芯片 EAL4+/EAL5+ 认证检测、移动金融安全芯片检测业务。未来实验室将不断开拓智能家居、车联网、工业控制等新领域，面向全行业开展芯片安全检测。

一、芯片EAL4+/EAL5+认证检测

参考依据

GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》

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》

检测内容

- EAL4+/EAL5+检测内容

型式试验

针对芯片的安全功能进行型式试验，确保厂商声明的安全功能实现的正确性、有效性，满足标准中所有的安全功能要求。

安全保障评估

评估芯片从研发环节到最终交付给用户整个生命周期的安全保障措施，确保其完整性和可靠性。

渗透性测试

结合设计资料，对芯片开展渗透性测试，以确保安全防护的有效性。

- EAL4+/EAL5+的区别

EAL5+在EAL4+的基础上，提高了对芯片本身与其整个生命周期的安全性要求。型式试验方面增加了对安全功能测试的范围和强度；渗透性测试由验证性测试转为攻击性测试，将芯片抗攻击能力从中级提高为高级；安全保障能力评估方面增加了半形式化的设计描述、具有可经受结构化分析的架构体系以及其他保证TOE生命周期不可篡改性的机制，进一步增强了用户对芯片产品安全性的信心。

二、移动金融安全芯片检测

参考依据

JR/T 0088-2012《中国金融移动支付 应用基础》

JR/T 0089-2012《中国金融移动支付 安全单元》

JR/T 0098-2012《中国金融移动支付 检测规范》

检测内容

检测内容分为对芯片安全功能的验证性测试和芯片抗攻击能力测试两部分。

- 验证性测试包括验证密码算法功能、随机数发生器功能、异常检测功能等。
- 攻击性测试包括：

1 非侵入式攻击

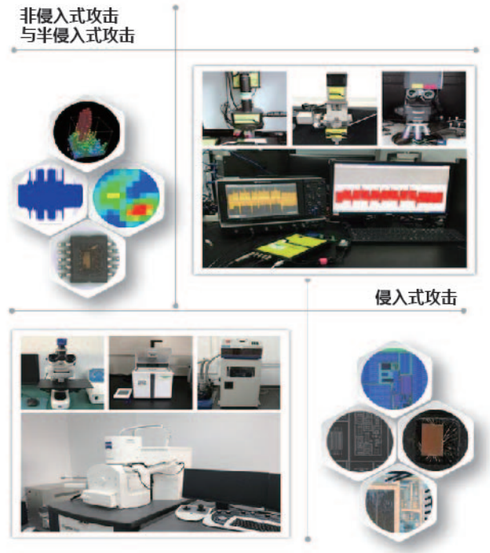
简单功耗分析（SPA）、差分功耗分析（DPA）、电磁辐射（EMA）等

2 半侵入式攻击

供电电源操纵、光注入、差分错误分析（DFA）等

3 侵入式攻击

安全芯片表面详细分析、传输系统的物理位置探测、传输系统的FIB修改、逻辑建立模块的干扰、逻辑建立模块的修改等



EMBEDDED SOFTWARE SECURITY TEST

嵌入式软件安全检测

嵌入式软件安全检测通过对产品安全性进行评价来保障用户信息安全，维护用户利益。获EAL4+/EAL5+认证证书的产品，表明其符合相关标准的技术要求，具有抵抗较高强度恶意攻击的能力。目前国内银行、电信、税务、石化、交通、社保等行业的智能卡产品多数要求EAL4+及以上安全级别，信息安全实验室立足于金融行业，提供针对嵌入式软件（COS）EAL4+/EAL5+的安全检测。

参考依据

GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》

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》

ISCCC-TR-041-2014《Java卡通用安全技术要求（EAL4+级）》

检测内容

密钥生成、密钥销毁、密码运算、子集访问控制等29个检测项目。

EAL4+/EAL5+

MOBILE TERMINAL APPLICATION SOFTWARE（APP）TEST

移动终端应用软件（APP）检测

移动终端应用软件（APP）已逐步渗透入我们生活的方方面面。据预测，到2022 年全球 APP 年度下载量将超过2500亿次，收入达1565亿美元。中国市场在此次增长中将继续发挥主导作用。面对日益快速增长的庞大用户和资金，信息安全检测发挥着至关重要的作用。目前，大量用户敏感信息泄露、资金被盗刷、APP被攻击，行业形势十分严峻，因此保障移动终端APP的安全，是保护支付业务与用户隐私数据的第一个阶段。依据以上安全需求，信息安全实验室面向广大商业银行、第三方支付机构以及APP开发商，提供移动终端应用软件（APP）安全检测服务和银联卡支付应用软件安全检测服务。

参考依据

JR/T 0092-2012《中国金融移动支付 客户端技术规范》

JR/T 0098.3-2012《中国金融移动支付 检测规范 第3部分：客户端软件》

Q/CUP 056-2013《银联卡支付应用软件安全规范》

Q/CUP 067-2016《中国银联二维码支付安全规范》

《银联云闪付二维码APP安全指引》

检测内容

信息安全实验室凭借自身多年的技术沉淀，将移动终端应用软件安全检测进行了详细的划分，测试范围涵盖生命周期安全、人机交互安全、程序安全、数据安全、通信安全五个维度、数十个检测项目以及上百个检测点。

安全检测范围	
生命周期安全	
• 项目启动	• 反编译保护
• 产品风险评估	• 程序权限安全
• 安全编码策略	• 程序API/函数安全
• 安全测试策略	数据安全
• ……	• 数据输入安全
人机交互安全	• 数据访问安全
• 登录安全控制	• 数据存储安全
• 支付安全控制	• 数据传输安全
• 密码管理安全	通信安全
• 会话安全控制	• 网络通信协议安全
程序安全	• 安全认证
• 程序异常检测	• 抗抵赖

安全检测领域

- 1.生命周期支持
- 2.客户端管理安全
- 3.身份认证安全
- 4.会话管理安全
- 5.数据保护
- 6.通信安全
- 7.用户安全

BAR CODE TEST

条码技术检测

条码(一维码和二维码)支付作为移动支付的主力军，凭借时尚、便捷的客户体验，在支付领域得到了广泛推广。2017 年 12 月人民银行下发《条码支付安全技术规范(试行)》和《条码支付受理终端技术规范(试行)》，强化条码支付技术风险防范；推进条码支付受理终端注册管理和规范支付交易报文管理。各商业银行、非银行支付机构、清算机构、行业协会严格落实《中国人民银行 国家认证认可监督管理委员会关于加强支付技术产品标准实施与安全管理的通知》，强化条码支付产品质量和安全管理，健全条码支付风险防控机制。信息安全实验室参与了条码支付技术检测规范的编制，并依据《条码支付安全技术规范(试行)》和《条码支付受理终端技术规范(试行)》规范，开展条码支付客户端软件和条码支付受理终端检测。

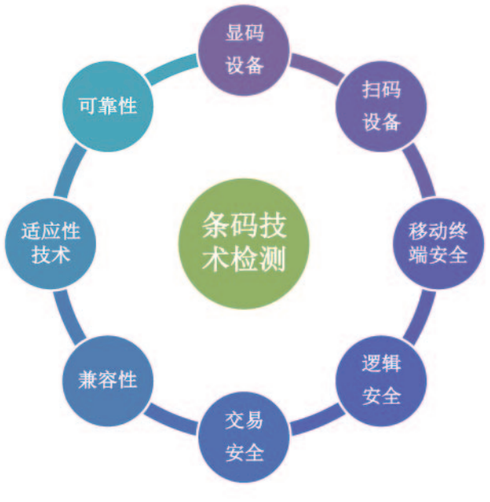
参考依据

《中国人民银行关于强化银行卡受理终端安全管理的通知》（银发[2017]21号）

《中国人民银行办公厅关于加强条码支付安全管理的通知》（银办发[2017] 242号）

《中国人民银行关于印发《条码支付业务规范（试行）》的通知（银发[2017]296号）

检测内容



TEE AND TA TEST

TEE和TA检测

近些年智能穿戴设备的广泛普及，移动端消费已经成为人们日常生活中不可或缺的一部分，为保障移动金融业务的快速、稳定的发展，人民银行在 2017 年制定了《移动终端支付可信环境技术规范》，其中对移动终端产品的安全性提出了要求。为响应人民银行的政策，并推动移动金融产业的健康发展，“北京移动金融产业联盟”推出《移动终端安全金融盾规范》，要求联盟成员的手机盾产品通过检测认证。信息安全实验室现已成为授权检测机构，并向社会大众提供可信操作系统(TEE)和可信应用(TA)类产品的检测认证服务。

移动终端支付可信环境架构示意图

参考依据

JR/T 0156-2017 《移动终端支付可信环境技术规范》

T/BMFIA 00001-2017 《移动终端安全金融盾规范》

检测内容

TEE安全检测

安全启动检测、数据存储安全检测、运行数据安全检测、应用管理检测、密钥管理安全检测、访问控制安全检测、代码安全检测

TEE规范符合性检测

API接口符合性检测、通信功能检测、加密算法功能检测、时间管理检测

TA安全性检测

TA代码安全检测、访问控制管理检测、生命周期管理检测、逻辑功能异常检测、密钥调用检测

TEE扩展能力检测

可信UI界面安全性检测、外部设备通信安全检测、可信UI接口功能检测、SE通信功能检测

移动终端支付可信环境应用场景

FINANCIAL IC CARD AND TERMINAL TEST

金融IC卡及其受理终端检测

金融行业对安全尤为关注，在金融 IC 卡产品的检测认证管理方面要求非常严格，无论是对银行卡及其受理终端产品还是提供银行卡及其受理终端产品的企业都严格执行统一的标准。由第三方检测机构对银行卡及其受理终端产品进行功能检测和安全评估，以确保不同品牌的银行卡及其受理终端产品安全可靠和兼容通用。

信息安全实验室立足金融行业，依据 EMVCo 规范、PBOC 3.0 中国金融集成电路（IC）卡规范、银行卡受理终端安全规范等，提供接触式 / 非接触式银行 IC 卡及其受理终端（POS 终端、银行自助终端、互联网终端等终端）的功能、性能、电气特性、通信协议和安全性测试服务。

参考依据

JR/T 0025-2013《中国金融集成电路（IC）卡规范》

JR/T 0045-2014《中国金融集成电路（IC）卡检测规范》

JR/T 0120-2016《银行卡受理终端安全规范》

T/PCAC0003-2018《银行卡销售点（POS）终端检测规范》

T/PCAC0004-2018《银行卡自助柜员机（ATM）终端检测规范》

Q/CUP 007-2014《银联卡受 终端安全规范》

EMV Contactless Communication Protocol Specification, Version 2.6

EMV Integrated Circuit Card Specifications for Payment Systems Book1-Book4,Version4.3

检测内容

信息安全实验室将从金融 IC 卡及其受理终端的机械性、电特性、通讯协议、应用功能符合性、性能符合性和安全性等几个方面开展检测。

- 金融IC卡检测

类　别	金融IC卡检测
金融应用类	PBOC3.0借记/贷记应用规范符合性检测
	PBOC3.0快速借记/贷记应用规范符合性检测
	PBOC3.0基于借记/贷记应用的小额支付应用规范符合性检测
	PBOC3.0非接触式IC卡小额支付扩展应用规范符合性检测
	PBOC3.0电子现金双币支付应用规范符合性检测
	EMV 接触式IC卡 level1规范符合性检测
	EMV 非接触式IC卡 level1规范符合性检测
其 他	其他行业应用规范符合性检测，如交通、社保等

- 银行卡受理终端检测（POS、mPOS、智能POS和ATM等）

类　别	受理终端检测
基础通信类	PBOC3.0接触式IC卡支付终端通讯协议检测
	PBOC3.0非接触式IC卡支付终端通讯协议检测
	EMV 接触式终端卡level1规范符合性检测
	EMV 非接触式IC卡 level1规范符合性检测
金融应用类	PBOC3.0接触式IC卡支付终端应用检测
	PBOC3.0非接触式IC卡支付终端应用检测
	EMV 接触式终端卡level2规范符合性检测
安全测评类	银行卡销售点（POS）终端安全测评
其 他	行业应用规范符合性检测，如交通、社保等。

USBKEY AND OTP TEST

USBKey与OTP检测

逐年增长的电子商务已经成为金融支付的重要应用场景，也带动了网上银行业务的高速发展，由于网络病毒、木马等威胁日益增多，如何保证金融交易的安全性成为社会各界关注的焦点。为解决用户的后顾之忧，各家银行都推出了网银安全产品 - 智能密码钥匙（USBKey）和动态令牌（OTP）。而检测 USBkey 和 OTP 的安全性是否达到相关规定的要求就是信息安全实验室的使命。

参考依据

GB/T 18336-2015《信息技术 安全技术 信息技术安全性评估准则》

GB/T 20276-2016《信息安全技术 具有中央处理器的IC卡嵌入式软件技术要求》

JR/T 0068-2012《网上银行系统信息安全通用规范》

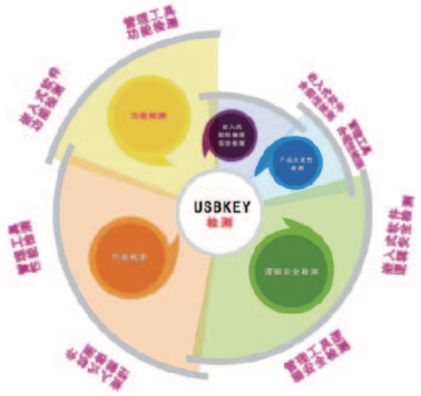
JR/T 0114-2015《网银系统USBKey规范 安全技术与测评要求》

检测内容

信息安全实验室凭借多年的技术积累，遵循现行国家标准、行业标准，制定了一套完备的安全检测流程，并将网银安全产品 USBKey 与 OTP 的检测项分别进行了详细的划分，依次从产品合规性、逻辑安全性、物理安全性、功能及性能五个方面展开全方位测试。

- USBKey检测

根据 USBKey 产品特性分别对每个功能模块展开 5 个方面的测试



管理工具安全性检测：本项测试针对管理工具的逻辑安全性、产品合规性展开。通过对上位机软件实施代码篡改，数据窃听等渗透攻击，验证 USBKey 产品的上位机软件安全性，保障用户密码的输入安全。

嵌入式软件安全性检测：依据相关规范的安全要求对 USBKey 嵌入式软件展开安全检测，从功能符合性和逻辑安全性两个方面发掘应用流程中潜在的安全隐患，从而保障用户在交易过程中的个人利益。

物理安全性检测：通过对产品硬件环境进行电磁干扰、故障注入等攻击性检测，以验证其芯片不会在运行过程中泄露敏感数据，从而保证产品安全性。

性能测试：根据应用需求展开测试，分别对产品的嵌入式软件和上层管理工具进行检测，保证产品稳定性和使用效率。

- OTP检测

OTP 具体检测内容涵盖五个模块

产品合规性测试以流程为根本，通过对 OTP 的合规性进行测试，可以保证产品研发的规范性。

逻辑安全着眼于安全功能有效性测试，通过对 OTP 的逻辑安全性进行检测，可以及时发现用户交易安全漏洞，从而降低安全风险。

物理安全以防止芯片攻击为出发点，通过对 OTP 的物理安全性进行检测，可以确保 OTP 内敏感信息的保密性。

功能测试以功能的正确性为基准，通过对 OTP 的功能性进行检测，可以保证 OTP 功能的正确性。

性能测试以产品的性能指标为基准，通过对 OTP 的性能进行检测，可以保证产品符合市场需求。

CHINA FINANCIAL MOBILE PAYMENT SECURE ELEMENT(SE) TEST

移动金融安全载体（SE）检测

随着金融支付新业务、新产品、新管理模式的不断涌现，以及移动终端的普及，金融支付具备了移动性的特征，从而打破了金融业固化站点模式，有效地突破了地域、时间的限制，使金融服务方式产生了革命性变革。安全载体（SE）负责对移动支付交易关键数据进行安全存储和运算，确保敏感交易具有安全认证和不可抵赖性，并支持多应用动态管理。信息安全实验室立足于金融行业，提供针对移动金融安全载体 SE 进行功能、性能和其安全性检测服务。

参考依据

JR/T 0088-2012《中国金融移动支付 应用基础》

JR/T 0089-2012《中国金融移动支付 安全单元》

JR/T 0098-2012《中国金融移动支付 检测规范》

检测内容

SE物理特性检测

（U）SIM卡物理特性检测和SD卡物理特性检测

SE电气特性和通信协议检测

接触式电气特性和通讯协议检测、非接触式电气特性和通讯协议检测、SWP协议检测和HCI架构检测

SE嵌入式系统软件功能检测

SE多应用平台规格符合性检测项、平台API规格符合性检测项、基本服务功能规格符合性检测项和多应用平台与嵌入式应用软件兼容性

SE嵌入式系统软件安全检测

安全功能检测和SE安全保证检测

CHINA FINANCIAL MOBILE PAYMENT EMBEDDED SOFTWARE TEST

移动金融嵌入式应用软件检测

随着移动支付的不断普及，以客户需求为主导的金融电子化与电子商务等业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。嵌入式应用软件作为运行在 SE 嵌入式系统软件之上的软件，负责与受理终端或远程服务器进行交易支付，其功能、性能和安全性直接影响到移动支付业务的正常运行。信息安全实验室立足于金融行业，提供针对嵌入式金融应用软件的功能、性能和其安全性检测的技术类服务。

参考依据

JR/T 0088-2012《中国金融移动支付 应用基础》

JR/T 0089-2012《中国金融移动支付 安全单元》

JR/T 0098-2012《中国金融移动支付 检测规范》

检测内容

功能符合性和性能测试

嵌入式应用软件交易功能的有效性验证、业务响应时间测试和稳定性测试等

安全性测试

评估对象ID、数据访问控制、密钥功能、多应用、生命周期功能、数据传输安全、初始化、安全审计、错误注入防护、信息泄漏防护、逻辑保护和重放攻击防护等

FINANCIAL IC CARD AND CRYPTOGRAPHY ALGORITHM APPLICATION DEMONSTRATION PROJECT ACCEPTANCE TEST

金融领域安全IC卡和密码应用示范工程验收测试（国密算法改造验收）

金融领域安全IC卡和密码应用示范工程项目由人民银行、国家密码管理局、中国银联股份有限公司牵头推进，建设银行、工商银行、农业银行、交通银行、邮政储蓄银行等全国89家商业银行作为第一批国密改造试点验收单位。

信息安全实验室根据《金融安全IC卡和密码应用示范工程验收测试工作方案》及其附件《验收测试大纲》编制工作方案，对项目建设单位的项目实施情况执行验收检测，出具客观公正的检测报告。目前已累计完成包括工商银行、建设银行、农业银行、中国银行在内的近40家商业银行国密算法改造验收工作。

参考依据

《国家发展改革委办公厅关于组织实施2015年国家信息安全专项有关事项的通知》（发改委办高技〔2015〕1541号）

《关于2015年国家信息安全专项项目的复函》（发改办高技〔2016〕1168号）

《金融领域安全IC卡和密码应用示范工程实施要点》（发改办高技〔2016〕 1168 号）

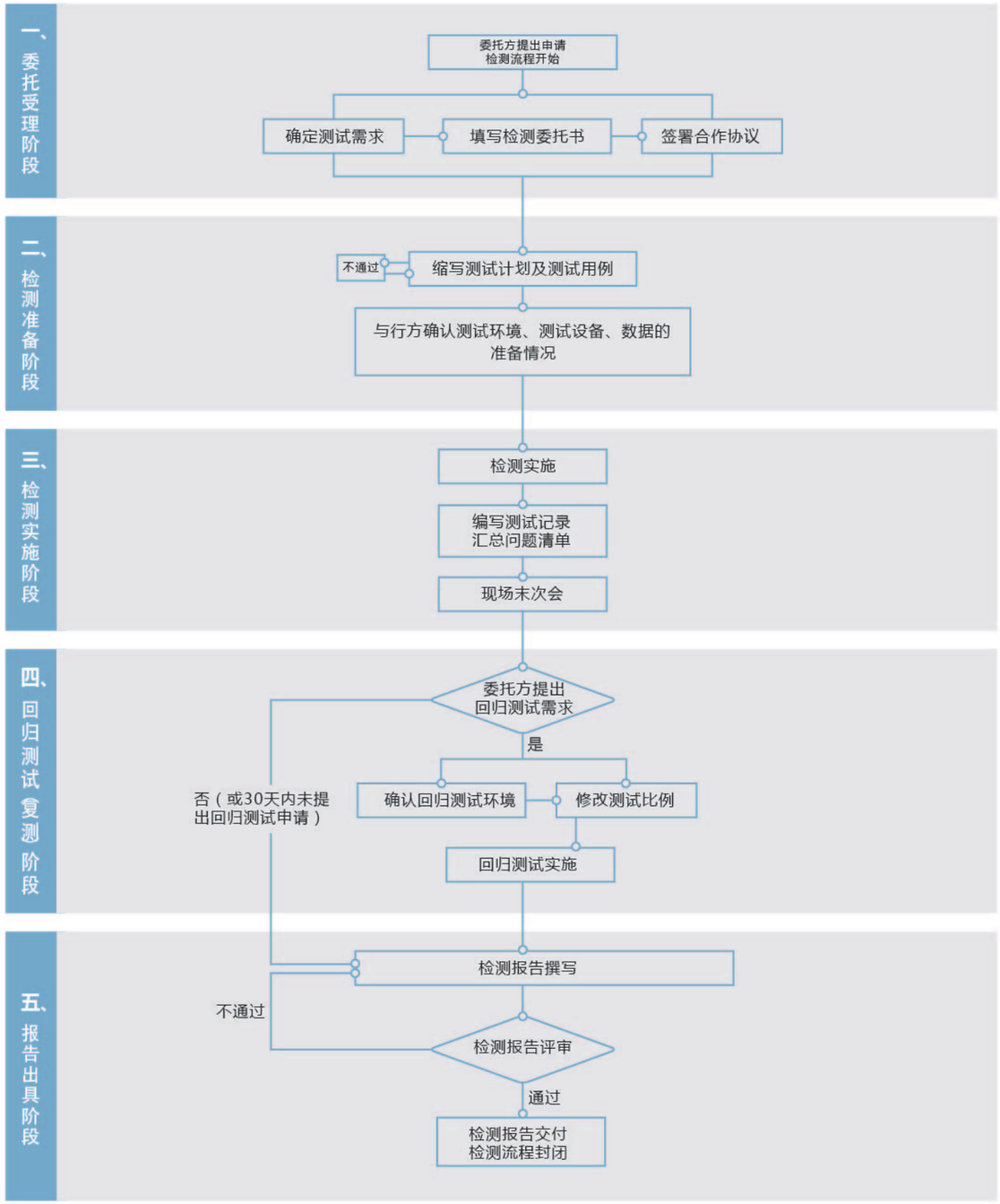
《2015年金融领域安全IC卡和密码应用示范工程项目管理办法》

《金融安全IC卡和密码应用示范工程验收测试工作方案》及其附件《验收测试大纲》

检测内容

- 金融安全IC卡系统验收测试
- 网上银行系统验收测试
- 跨行交易接入系统验收测试
- 科技攻关类项目验收测试
  - 移动支付终端及互联网Key验收测试
  - 智能终端北斗安全模组验收测试
  - 银行核心系统验收测试
  - RCC移动支付系统验收测试

服务流程



INFORMATION SECURITY AND FINANCIAL INDUSTRY DYNAMICS NEWS REPORT

信息安全资讯与同业动态通报

依托于CFCA信息安全服务业务积累所得、参与标准制定和修订积攒的经验，信息安全实验室推出《信息安全资讯与同业动态通报》服务，致力于向银行业及其他企事业、政府部门传递信息安全领域内最新的安全资讯和技术分析。

每期《信息安全资讯与同业动态通报》分为国内篇和海外篇两部分。国内篇主要关注金融行业，分析国内金融业的动态、创新业务以及相关技术研究；海外篇面向整个信息安全行业，关注海外的信息安全事件以及安全威胁播报。

具体内容如下

篇幅名称	板块名称	
国内篇	行业聚焦	金融业、银行业的重大会议、监管动态、技术趋势、行业报告等
	业务聚焦	银行业和支付产业的业务创新
	技术聚焦	金融业安全势态、安全技术报告
海外篇	行业观察	海外出台的政策、监管、法律、标准、行业报告等
	聚焦安全	海外的安全事件报道，不仅限于金融业
	安全威胁播报	病毒漏洞新闻和分析

我们的资质

- 中国国家认证认可监督管理委员会授权的中国国家计量认证（CMA）检验检测机构资质
- 中国合格评定国家认可委员会（CNAS）认可的国家实验室
- 中国合格评定国家认可委员会（CNAS）认可的检验机构
- 中国人民银行授权的支付技术产品认证检测机构资质
- 中国人民银行授权的非金融机构支付服务业务系统检测机构资质
- 中国人民银行授权的移动金融技术服务认证检测机构资质
- 中国人民银行授权的国密算法改造验收检测机构资质
- 公安部授权的信息安全等级保护测评资质
- 中国网联安全审查技术与认证中心授权的IT产品信息安全认证（EAL4+/5+级）检测机构资质
- 中国网联安全审查技术与认证中心授权的信息安全风险评估检测机构资质
- 中国网联安全审查技术与认证中心授权的电子招投标系统认证检测机构资质
- 中国银联授权的银联认证检测实验室资质
- 中国银联授权的银联第三方机构入网安全技术检测资质
- 中国银联授权的银联卡账户信息安全合规评估检测资质
- 北京移动金融产业联盟授权的联盟团体标准检测机构资质