

国家发展和改革委员会办公厅文件

发改办高技[2012]3096 号

国家发展改革委办公厅关于组织实施 2012 年 金融领域安全 IC 卡和密码应用专项 有关事项的通知

教育部、工业和信息化部、公安部、安全部、人民银行、质检总局、中科院、国家保密局、国家密码局办公厅(室),各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委,相关中央直属企业:

为加强金融领域信息安全,我委决定组织开展 2012 年金融领域安全 IC 卡和密码应用专项,以加快推进金融领域安全 IC 卡和密码相关关键产品的产业化,提升金融领域信息安全专业化服务水平。现将有关事项通知如下:

一、专项重点支持领域

(一)金融领域安全 IC 卡和密码关键产品产业化

1、高性能双界面金融 IC 卡芯片

支持 SM2/SM3/SM4 等算法,支持 JAVA 应用、数据加解密和签名验签,SM2 签名速率达到 10 次/秒以上。支持 PBOC2.0 规范应用,单次交易时间小于 500ms,达到 GM/T 0008-2012《安全芯片密码检测准则》安全等级 2 或以上要求。

2、高性能金融数据密码机

支持 SM2/SM3/SM4 等算法,支持数据加解密、签名验签、密钥管理、身份鉴别与认证和冗余配置,符合《通用密码服务接口规范》。金融密码服务接口单机交易处理能力不低于 10000 笔/秒,单笔交易时间不高于 50ms,SM2 签名不低于 13000 次/秒,SM4 加解密不低于 2Gbps。

3、高性能签名验签服务器

支持 SM2/SM3 等算法,支持高速签名验签、密钥安全保护、冗余配置和多机热备。SM2 签名不低于 25000 次/秒,验签不低于 15000 次/秒,单笔交易时间不高于 50ms。

4、安全 POS/ATM 机具

采用 SM2/SM3/SM4 等算法,满足金融应用安全需求,SM2 验签不低于 20 次/秒,具有基于 SM4 算法的数据加解密和 MAC 计算功能,并符合银行相关规范。

5、高性能密码芯片

支持 SM2/SM3/SM4 等算法,支持数据加解密、签名验签和密钥安全存储。SM2 签名不低于 25000 次/秒,SM2 验签不低于 15000 次/秒,SM4 加解密不低于 2Gbps,达到 GM/T 0008-2012《安全芯片密码检测准则》安全等级 1 级或以上的要求。

6、安全浏览器

支持 SM2/SM3/SM4 等算法,满足基于 SM2/ SM3 算法的根证书植入和基于 SM2/SM3/SM4 算法的证书应用需求,采用最新版本的安全传输层协议(TLS1.2)建立安全通信,并符合《SSL VPN 技术规范》,具备密钥安全保护能力,支持 PC 机、移动智能终端、平板电脑等的主流操作系统。

(二)金融领域密码关键产品检测服务

支持金融数据密码机、签名验证服务器、智能 IC 卡、智能密码钥匙等产品的密码检测平台建设,实现密码功能、密钥管理机制、密码正确性、协议正确性,以及对 SM2/ SM 3/ SM 4 等密码算法的侧信道攻击防御能力和性能等的检测功能,具备超过 50Gbps 的 SM4 算法测试能力,40000 次/秒的 SM2 算法测试能力,以及 200 款产品的年检测能力。支持高性能双界面金融 IC 卡芯片第三方量产测试服务。

(三)金融领域相关安全标准制修订

1、金融密码产品标准,主要包括:制修订金融数据密码机、签名验证服务器、服务器密码机、金融 IC 卡、智能密码钥匙、动态令牌等标准。

2、金融密码应用标准,主要包括:制修订金融 IC 卡、网上银行、移动支付、电子认证等金融密码应用相关标准。

3、金融信息系统密码检测评估标准,主要包括:制修订金融 IC 卡、网上银行、移动支付、电子认证等金融密码产品检测标准,以及金融信息系统等级保护商用密码应用要求、测评准则等系列标准。

(四)金融领域安全 IC 卡和密码应用试点

1、金融安全 IC 卡与移动支付应用试点

支持商业银行在局部地区,开展金融安全 IC 卡与移动支付应用试点,试点主要包括:应用支持 SM2/SM3/SM4 等密码算法的金融 IC 卡、POS 机、ATM 机,开展圈存/圈提、借贷记和非接触式移动支付等业务应用。试点期内,发卡量不低于 5000 张,发放移动支付终端不少于 200 部,改造 ATM 机不少于 100 台、POS 机不少于 500 台。

2、网上银行安全应用试点

支持商业银行开展网上银行安全应用试点,网上银行用户规模不低于 5000 万,试点主要包括:改造电子认证系统基础设施,采购、升级改造网上银行的软、硬件设备,支持 SM2/SM3/SM4 等密码算法实现安全传输层协议和敏感信息的加解密,并支持大用户量并发。研究验证基于 SM2/SM3/SM4 等密码算法在网上银行应用的技术体系、标准规范,以及相关信息安全软硬件产品。

二、申报要求

(一)请项目主管部门根据投资体制改革精神和《国家高技术产业发展项目管理暂行办法》的有关规定,结合本单位、本地区实际情况,认真做好项目组织和备案工作,组织编写项目资金申请报告并协调落实项目建设资金、环境影响评价、节能评估等相关建设条件,同时汇总相关申请材料并报我委。

(二)通过国务院有关部门及中央直属企业申报的项目,项目单位应与有关部门和中央直属企业有财务隶属关系。其他项目应按照属地管理原则,通过项目单位所在地的省级发展和改革委员会申报。

(三)项目主管部门应对报送的材料,如资金申请报告、银行贷款承诺、自有资金证明、各类许可资质等,进行认真核实,并负责对其真实性予以确认。

(四)项目纸质申报材料包括:项目资金申请报告(达到可行性研究报告深度)、项目简表和项目汇总表,上述材料一式两份。项目简表、项目汇总表、项目备案文件、自有资金证明、投资及信贷承诺等所有附件要与项目资金申请报告一并装订(项目简表和汇总表应订装在报告正文前)。各项目材料一经提供不予退还,请做好备份。资金申请报告的具体编制要求详见附件1、2、3。

(五)项目材料的具体报送时间、地点和相关要求将在2013年1月初在国家发展改革委高技术司网站(网址 <http://gjss.ndrc.gov.cn>)信息化栏目下另行通知。

(六)金融领域安全 IC 卡和密码关键产品产业化和应用试点项目的承担单位原则上应为企业法人。申报项目应具备以下条件:(1)按规定在当地政府备案;(2)已落实项目建设资金;(3)采用的科技成果应具有自主知识产权;(4)项目申报单位必须具有较强的技术开发和项目实施能力,具备较好的资信等级,资产负债率在合理范围内;(5)项目答辩时各单位应已有相关产品(此条适用于产业化项目)。

(七)金融领域密码关键产品检测服务类项目的承担单位可为企业法人或事业法人。申报项目应具备以下条件:(1)经国家密码行政主管部门认定;(2)按规定在当地政府备案;(3)已落实项目建设资金;(4)具有较强的技术开发和项目实施能力,具备较好的资信等级,资产负债率在合理范围内。

(八)金融领域相关安全标准制修订项目承担单位可为企业法人或事业法人,并被中国人民银行或国家密码管理局列入相关标准制修订计划。

(九)本专项所支持的金融领域安全 IC 卡和密码关键产品产业化、金融领域密码关键产品检测服务、金融领域相关安全标准制修订等三类项目的申报日期截止至 2013 年 1 月 17 日。我委组织专家对申报项目进行初步评审后,将组织现场答辩。其中,金融领域安全 IC 卡和密码关键产品将于 2013 年 3 月进行公开测试。有关具体项目答辩和测试名单、时间和地点将另行通知。

(十)本专项所支持的金融领域安全 IC 卡和密码应用试点项

目申报日期截止至 2013 年 6 月 1 日,有关具体项目答辩时间和地点将另行通知。

附件:1、金融领域安全 IC 卡和密码关键产品产业化项目资金
申请报告编制要点

2、金融领域密码关键产品检测服务项目资金申请报告
编制要点

3、金融领域安全 IC 卡和密码应用试点项目资金申请报
告编制要点

4、金融领域安全 IC 卡和密码应用专项项目及承担单位
基本情况简表

5、金融领域安全 IC 卡和密码应用专项项目汇总表



附件 1:

金融领域安全 IC 卡和密码关键产品产业化项目 资金申请报告编制要点

一、项目简介

简要介绍项目基本情况、建设目标、建设内容、总投资等内容。

二、项目的意义和必要性

国内外现状和技术发展趋势，项目的需求和市场需求分析，产业关联度分析，项目建设的必要性。

三、项目的产业化基础

项目单位技术创新、生产和销售的能力，以及相关领域研发基础和研发队伍情况；项目技术成果来源及知识产权情况，已完成的研究开发工作及中试情况和鉴定年限，技术或工艺特点以及与现有技术或工艺比较所具有的优势，该重大关键技术的突破对行业技术进步的重要意义和作用。

四、建设方案

项目的产能规模、建设的主要内容、采用的工艺技术路线与技术特点、设备选型及主要技术经济指标、建设地点、项目实施与进度计划安排、建设期的组织管理等。

五、各项建设条件落实情况

包括环境保护、资源综合利用、节能措施及外部配套条件落实情况等。

六、项目法人基本情况

包括所有制性质、主营业务、近三年来的销售收入、利润、税金、固定资产、资产负债率、银行信用等级、项目负责人基本情况及主要股东的概况。

七、投资

项目总投资规模，投资使用方案和资金筹措方案；申请国家补贴资金的主要理由和政策依据。

八、项目财务分析、经济分析及主要指标

内部收益率、投资利润率、投资回收期、贷款偿还期等指标的计算和评估，项目风险分析与控制，经济效益和社会效益分析。

九、资金申请报告附件

- 1、银行承贷证明(省级分行以上)文件。
- 2、项目法人近三年的经营状况（包括损益表、资产负债表、现金流量表）和项目法人自筹资金保证落实文件。
- 3、地方、部门配套资金及其它资金来源证明文件。
- 4、前期科研成果证明材料(成果鉴定、权威机构认证或出具技术检测报告、专利证书等)；前期科研成果的成熟度，应能够满足产业化试验或产业化示范的要求。
- 5、环保部门出具的环境影响评价文件的审批意见。

6、公安部、国家密码局等相关部门颁发的相关生产、销售许可证明。

7、土地、重要原材料以及其它所需证明材料。

8、企业投资项目的核准或备案的批准文件（在有效期内且未
满两年）；已开工项目需提供投资完成、工程进度以及生产情况
证明材料。

9、项目招标内容（适用于申请国家补贴资金 500 万元及以上
的投资项目）。

10、项目单位对项目资金申请报告内容和附属文件真实性负责
的声明。

附件 2:

金融领域密码关键产品检测服务项目 资金申请报告编制要点

一、项目简介

简要介绍项目基本情况、建设目标、建设内容、总投资等内容。

二、项目的意义和必要性

国内外金融领域密码关键产品检测服务现状，项目的需求和市场分析，项目建设的必要性。

三、项目的基础

项目单位的专业支撑环境、服务领域、技术能力，以及相关领域专业服务的队伍情况；项目技术比较优势，已经实施的成功案例，以及市场占有情况；该项目建设对于保障金融领域信息系统安全稳定运行的重要意义和作用。

四、项目方案

服务能力建设方面：建设规模、主要内容、服务方案、设备选型及主要技术经济指标、建设地点、项目实施与进度计划安排、建设期的组织管理等。

服务模式方面：服务流程、组织管理、技术特点和服务效能等。

五、各项建设条件落实情况

节能、降耗、环保、安全、原材料供应及外部配套条件落实情况等。

六、项目法人基本情况

包括所有制性质、主营业务、近三年来的销售收入、利润、税金、固定资产、资产负债率、银行信用等级、项目负责人基本情况及主要股东的概况。

七、投资

项目总投资规模，投资使用方案和资金筹措方案；申请国家补贴资金的主要理由和政策依据。

八、项目财务分析、经济分析及主要指标

内部收益率、投资利润率、投资回收期、贷款偿还期等指标的计算和评估，项目风险分析与控制，经济效益和社会效益分析。

九、资金申请报告附件

- 1、银行承贷证明(省级分行以上)文件。
- 2、项目法人近三年的经营状况（包括损益表、资产负债表、现金流量表）和项目法人自筹资金保证落实文件。
- 3、地方、部门配套资金及其它资金来源证明文件。
- 4、企业投资项目的核准或备案的批准文件（在有效期内且未满两年）；已开工项目需提供投资完成、工程进度以及生产情况证明材料。

5、环保部门出具的环境影响评价文件的审批意见。

6、项目招标内容（适用于申请国家补贴资金 500 万元及
以上的投资项目）。

7、项目单位对项目资金申请报告内容和附属文件真实性
负责的声明。

附件 3:

金融领域安全 IC 卡和密码应用试点项目 资金申请报告编制要点

一、项目简介

简述试点工作背景、承担单位情况,及试点目标、规模、内容、建设期、总投资和资金来源、经济与社会效益、主要结论与建议等。

二、项目的意义和必要性

国内外金融领域 IC 卡和密码应用现状分析,在我国金融领域应用安全 IC 卡和密码的需求分析,试点工作的意义、必要性和预期效果等。

三、试点工作方案

1、试点原则和思路。围绕验证安全 IC 卡和密码算法的安全性和可靠性,从而为尽快全面推广国产金融 IC 卡和密码算法应用,开展试点工作。

2、试点目标。围绕试点重点支持的领域,提出试点工作的总体目标、具体目标,预期效果要尽可能提出可量化、可考核的目标。明确提出拟开展的具体工作,拟制定、修订并验证的技术体系和标准规范,拟建设和完善的基础设施和信息系统。

3、对于试点工作中涉及的信息系统改造,要制定详细的方案。包括:对现有受理环境、电子认证系统基础设施、应用系统

的改造方案，以及对网上银行系统的升级改造方案。

4、试点工作进度计划安排。

四、投资估算及资金筹措

项目总投资规模，投资使用方案和资金筹措方案；申请国家补贴资金的主要理由和政策依据。

五、项目法人基本情况

包括所有制性质、主营业务、近三年来的销售收入、利润、税金、固定资产、资产负债率、银行信用等级、项目负责人基本情况及主要股东的概况。

六、各项建设条件落实情况

包括环境保护、资源综合利用、节能措施及外部配套条件落实情况等。

七、试点工作效益分析及风险评价

经济效益和社会效益分析，项目风险分析与控制。

八、试点工作保障措施

重点说明试点工作的组织机制，明确主管领导、牵头部门、职责分工、多部门协调工作机制、矛盾问题协同处理机制等方面的情况。

九、资金申请报告附件

1、银行承贷证明(省级分行以上)文件。

2、项目法人近三年的经营状况（包括损益表、资产负债表、现金流量表）和项目法人自筹资金保证落实文件。

3、地方、部门配套资金及其它资金来源证明文件。

4、企业投资项目的核准或备案的批准文件（在有效期内且未满两年）；已开工项目需提供投资完成、工程进度以及生产情况证明材料。

5、环保部门出具的环境影响评价文件的审批意见。

6、项目招标内容（适用于申请国家补贴资金 500 万元及以上的投资项目）。

7、项目单位对项目资金申请报告内容和附属文件真实性负责的声明。

金融领域安全IC卡和密码应用专项项目及承担单位基本情况简表

单位: 万元

项目名称		项目负责人		固定电话 手机	
项目单位名称		项目联系人		电子邮件地址 固定电话 手机	
项目主持部门		项目所属领域 (精确到每个领域子项)		电子邮件地址	
项目单位地址		建设地点			
项目投资情况	单位法定代表人	企业情况	2009年	2010年	2011年
项目总投资	法定代表人电话	企业总资产			
固定资产投资	企业注册登记类型	固定资产净值			
铺底流动资金	银行信用等级	资产负债率			
拟申请银行贷款	职工人数	销售收入			
自筹资金	技术人员数	利税			
	有无银行贷款承诺函	出口创汇			
项目建设必要性:					
项目主要内容及目标: (产业化类项目应包含项目建成后每年产品生产数量)					

填表说明:

- 1、本表由企业填报,主持部门认真审核后打印填报
- 2、项目总投资=自有资金+银行贷款+其他资金 (即申请国家补助资金暂不列入资金来源部分)
- 3、项目所属领域,请按照金融领域安全IC卡和密码应用专项重点所列范围填写 (参见通知正文。务必精确到每个领域子项)
- 4、联系人: 国家发展和改革委员会高技术产业司 刘 勇 姜 伟 010-68501530 15910606878 Email: xxhc@ndrc.gov.cn

附件5:

金融领域安全IC卡和密码应用专项项目汇总表

单位: 万元

序号	主持 部门	企业名称	项目名称	所属 领域	总投资	资金来源		申请国家 补助资金	项目负责 人及联系 方式	项目联系 人及联系 方式	起止 年限	项目建设内容 (产业化类项目应包含项目建 成后每年产品产量)
						企业自筹	银行贷款					
1												
2												
3												
4												

填表说明:

- 1. 项目总投资=企业自筹+银行贷款 (即申请国家补助资金暂不列入资金来源部分)
- 2. 项目所属领域, 请按照金融领域安全IC卡和密码应用专项重点所列范围填写 (参见通知正文。务必精确到每个领域子项)
- 3. 在填写过程中, 请不要合并或者拆分此表单元格, 请不要打乱表头次序。
- 4. 表格中所填数字均不包含小数部份