

证券代码：300386

证券简称：飞天诚信



飞天诚信科技股份有限公司

2020 年度非公开发行股票  
募集资金使用的可行性分析报告

二〇二〇年五月

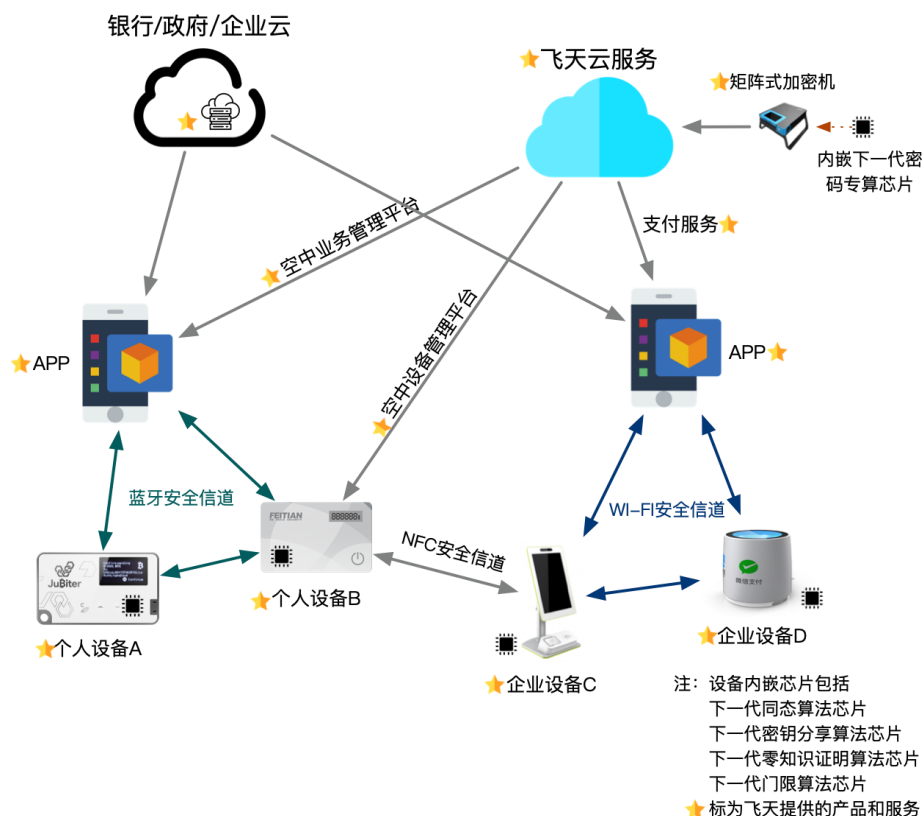
## 一、本次募集资金用途

飞天诚信科技股份有限公司（以下简称“公司”）本次非公开发行 A 股股票（以下简称“本次非公开发行”或“本次发行”）募集资金总额不超过 85,000.00 万元，扣除发行费用后的募集资金净额将全部用于以下项目：

单位：万元

序号	项目名称	总投资	拟投入募集资金
1	下一代安全芯片、设备、系统的研发及产业化项目	168,375.00	85,000.00

本项目研发的安全芯片、设备和系统面向新一代信息技术，是一个有机的整体。公司研发的芯片，用于安全设备研发，实现一定的垂直一体化，可以有效降低成本，增强产品性能，促进安全设备市场推广和销售规模的扩大；安全设备为安全芯片提供基础市场需求，降低芯片研发的市场风险；安全芯片也可独立对外销售，丰富了公司产品种类，降低了项目投资风险。安全系统的研发可以增强公司“系统级”信息安全方案解决能力，促进安全设备、安全芯片的市场推广。通过本项目的实施，公司将形成“芯片-设备-系统”体系化的产品组合，可以为客户提供全方位的安全产品和服务。图示如下：



项目完成后，将强化公司在信息安全领域的技术水平、自主创新能力以及垂直一体化产业链整合能力，进一步增强公司盈利能力、盈利水平和竞争优势。

在本次发行募集资金到位之前，公司将根据项目进度的实际情况以自筹资金先行投入，并在募集资金到位之后按照相关法规规定的程序予以置换。若本次发行实际募集资金净额低于拟投入募集资金额，不足部分由公司自筹资金解决。

## 二、本次募集资金投资项目的的基本情况

### （一）募投项目实施背景

#### 1、网络空间安全已经成为国家战略，信息安全产业面临良好的外部环境

2015年7月公布的《国家安全法》中首次提出网络空间主权这一概念，《国家安全法》第二十五条规定：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”网络空间已成为继“陆、海、空、天”之后第五大主权领域空间，在这种情况下，大多数国家都把特定网络置于自己主权管辖之下，并对相关网络行为进行约束和规范。

2016年12月27日，《国家网络空间安全战略》发布，强调“没有网络安全就没有国家安全”，网络安全的重要性和意义不断得到提升；2017年6月1日，《网络安全法》正式实施，进一步明确了相关责任主体的法律责任，覆盖网络运营商、关键信息基础设施运营者、信息与网络设备和服务的提供者，将为整个国家及全行业的网络安全工作提供了法律保障；相关工作将进入有法可依、强制执行阶段。

《“十三五”国家信息化规划》提出，着力增强以信息基础设施体系为支撑、信息技术产业生态体系为牵引、数据资源体系为核心的国家信息化发展能力，着力提高信息化在驱动经济转型升级、推进国家治理体系和治理能力现代化、推动信息惠民、促进军民深度融合发展等重点领域的应用水平，着力优化支持网信企业全球化发展、网络空间治理、网络安全保障等的发展环境，加快推动我国信息化水平和安全支撑能力大幅提升。

《北京市国民经济和社会发展的第十三个五年规划纲要》提出，将提升城市信息化、智能化水平作为构筑首都未来核心竞争优势的一项战略性举措，把信息基础设施作为重要的城市基础设施进行规划建设，加快建设高速泛在、畅通便捷的信息网络和服务体系，构建城乡一体光网城市、移动互联无线城市和数据信息安全城市，让市民充分享有信息时代的便捷工作和生活。加强水电气热、能源、交通等领域控制系统和政务、金融、社保、通信、医疗等信息系统的安全防护，完善信息安全管理规范和标准，提升安全管理、态势感知和风险防范能力。建设完善网络安全监测监管、风险评估、监督管理、标准认证体系、应急处置预案，增强关键信息基础设施、重要信息系统、关键数据资源及服务的安全保障能力，加大网络数据和用户信息保护力度，营造安全网络环境。

在国家政策的大力支持下，网络安全市场空间将得到不断的扩大，产业投入和建设也将步入持续稳定的发展轨道，对于各行业、企事业单位等，急需建立以密码技术为基础的信息安全保障体系，信息安全产业迎来更大的发展机遇和良好的外部环境。

## 2、金融科技、物联网、区块链等新一代信息技术将推动信息安全产业发展

2019年9月，中国人民银行《金融科技发展规划（2019-2021年）》（以下简称“规划”）提出，进一步增强金融业科技应用能力，实现金融与科技深度融合、协调发展，明显增强人民群众对数字化、网络化、智能化金融产品和服务的满意度，推动我国金融科技产业繁荣发展。安全是金融科技、金融创新的红线。随着越来越多的新技术、新创新被引入金融领域，行业内对信息安全需求也随之上升。

物联网是新一代信息技术的高度集成和综合运用，对新一轮产业变革和经济社会绿色、智能、可持续发展具有重要意义。当前，物联网正进入跨界融合、集成创新和规模化发展的新阶段。工信部《信息通信行业发展规划物联网分册（2016-2020年）》提出，到2020年，具有国际竞争力的物联网产业体系基本形成，包含感知制造、网络传输、智能信息服务在内的总体产业规模突破1.5万亿元，公众网络M2M连接数突破17亿。随着物联网的推进，相应的智能信息服务和信息安全需求均将大幅度增加。

区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域，区块链技术的集成应用在新的技术革新和产业变革中起着

重要作用。国家要求把区块链作为核心技术自主创新的重要突破口，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑，加快推动区块链技术和产业创新发展。《“十三五”国家信息化规划》提出，加强量子通信、未来网络、类脑计算、人工智能、全息显示、虚拟现实、大数据认知分析、新型非易失性存储、无人驾驶交通工具、区块链、基因编辑等新技术基础研发和前沿布局，构筑新赛场先发主导优势。

《北京市促进金融科技发展规划（2018年-2022年）》中也提出了相关规划，包括“重点推动移动互联、物联网为代表的互联技术创新。大力推动移动互联网技术发展，促进移动互联网与金融功能的全面融合，更好地应用于公共服务领域”、“着力推动物联网技术发展，支持物联网技术在供应链金融、支付、信用体系建设、动产融资等金融领域的应用，鼓励银行、保险等金融机构充分应用物联网”、“支持区块链技术在基础层、中间协议层、应用服务层的创新，加快推进区块链技术在数字身份、信息存证、公证确权、可信验证、流程溯源、城市管理、精准扶贫等领域的应用，审慎探索区块链技术在金融监管与风控、供应链金融、普惠金融、贸易金融、征信、保险等金融领域的应用”、“着力推动以密码技术、量子技术、生物识别技术为代表的安全技术发展。支持密码技术在数字身份、身份验证、反欺诈、网络安全、数据加密等领域的应用。大力支持基础密码技术、进阶密码技术等底层密码技术的研究”等。

综上，金融科技、物联网、区块链等新一代信息技术的快速发展将对信息安全提出更多的需求，必将推动信息安全产业大发展。

### 3、新一代信息技术的飞速发展对信息安全提出了新的要求和挑战

随着互联网、移动互联网、物联网、工业互联网、云计算、大数据、区块链、金融科技、信息通信、智能制造等新一代信息技术的飞速发展，网络空间在促进社会和经济发展的同时，维护国家安全中发挥着越来越重要的作用，同时也使国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

中国已经步入大数据时代，但大数据如同一把双刃剑，在我们享受大数据分析带来的精准信息的同时，其所带来的安全问题也开始成为隐患。信息泄露、黑客袭击、病毒传播等等互联网信息安全问题层出不穷。

随着互联网、移动互联网、物联网和云服务的发展，尤其是商务类应用（电

子商务、移动支付、网上银行等)的快速发展,带动了信息产业的发展,同时也带来了日益严重的信息安全问题。专门针对网上银行服务的欺诈和病毒攻击现象与日俱增,网络安全问题日益严峻,网络信息安全隐患极大地制约了网上银行等网络应用的推广和普及,互联网信息安全亟需加强。《“十三五”国家信息化规划》指出,当前我国信息化发展还存在一些突出短板,包括技术产业生态系统不完善,自主创新能力不强,核心技术受制于人成为最大软肋和隐患;网络安全技术、产业发展滞后,网络安全制度有待进一步完善,一些地方和部门网络安全风险意识淡薄,网络空间安全面临严峻挑战。

新一代信息技术的飞速发展,必将对信息安全提出新的要求和挑战,同样需要下一代的信息安全技术与之相匹配。随着科学技术的发展,安全产品应用环境日益复杂,各种攻击手段层出不穷;同时指纹、人脸、声纹及 DNA 等新方式也应用于信息安全的保护。技术的发展进步,客观上要求公司产品不断升级换代,以应对挑战。

#### 4、公司已经具备了向上下游拓展实现垂直一体化的能力

技术是公司核心竞争力的重要组成部分,截至 2019 年 12 月 31 日,公司及下属子公司已拥有计算机软件著作权登记证书 231 篇;获得授权专利 1,226 篇,其中发明专利 948 篇(含 157 篇国外专利)、实用新型专利 70 篇、外观设计专利 208 篇;并参与制定/修订的已发布的国家标准 9 项,行业标准 13 项。

2017 年 1 月,公司完成了对北京宏思电子技术有限责任公司(以下简称“宏思电子”)的收购。宏思电子成立于 1996 年,是国内较早专业从事密码芯片研制的集成电路企业,在国内信息安全集成电路设计领域处于骨干领军地位,是较早获得国家认证的集成电路设计企业,是国内信息安全集成电路产品最完整的集成电路设计企业之一,目前已经形成物理噪声源、安全主控 SOC、专用密码算法芯片三大系列的芯片产品以及众多应用解决方案,产品广泛应用于信息安全与通讯领域,涉及金融、税务、公安、海关、电信、电子商务等多个行业和领域。宏思电子是经北京市认证的高新技术企业,研制的信息安全芯片四次获国密局颁发的密码科技进步奖,研制的 32 位 CPU 系统级安全芯片(HS32U2)获得 2018 年第十三届“中国芯”安全可靠产品。

收购三年来,宏思电子的芯片研发能力与公司片内操作系统(FTCOS)及

应用开发能力结合，进一步提高了公司安全芯片的竞争力，从而带动公司芯片业务的市场份额和业绩的不断提升。

公司多年的行业技术积累和研发能力，使公司具备了利用新一代信息技术进行上下游拓展的能力。

## （二）本次募投项目与公司现有业务关系

本次募集资金运用均围绕公司主营业务进行，符合公司的发展规划。募集资金投资项目是公司发展战略的具体实施步骤，募集资金项目的实施将应用下一代信息安全相关技术对现有产品升级和新产品开发，增强公司安全芯片、设备和系统的垂直一体化能力，巩固公司的技术和市场优势。本项目对安全芯片的系列化研发，安全设备和安全系统领域的产品布局，将不断丰富公司业务线，强化公司在信息安全领域的技术水平、自主创新能力以及成本等方面的优势，与现有业务具有较强的关联性，是现有业务的继承与发展。

## （三）募投项目建设内容

本项目是公司把握住信息安全产业高速发展的战略机遇，实现技术和市场突破的战略选择。项目实施后将极大地丰富公司产品系列，提升公司技术水平、研发和生产能力，增强公司可持续发展能力。本项目建设内容包括安全芯片、设备、系统的一体化研发和客户服务、规模化生产及市场推广四个方面。本项目计划开发以下产品：

### 1、安全芯片

本项目计划在公司现有安全芯片和技术储备的基础上，紧跟芯片技术的发展方向，积极采用新技术、新工艺，瞄准目标市场，进一步对现有安全芯片升级和新芯片的开发，具体主要包括以下系列安全芯片：

名称	功能说明	应用场景
安全 MCU 芯片	在 MCU 上集成安全、通讯等功能	物联网、金融科技、数字交通等
安全生物识别芯片	支持指纹、人脸生物特征识别，安全性符合相关标准	个人智能设备、安全终端、智能门锁、手机、平板电脑等

超低功耗安全芯片	在网络支付、移动支付中负责交易关键数据的安全存储和运算	安全终端、智能家居、可穿戴设备、物联网设备等
车规级安全芯片	符合汽车电子元件规格标准的安全芯片	车载 OBD 等车联网领域
低功耗工业级安全芯片	适应工业使用环境的安全芯片	工业互联网安全领域
安全通讯芯片	在安全芯片上集成 WIFI、蓝牙、13.56M、5.8G 等通讯功能	物联网、车联网等需安全通讯领域
区块链密码应用安全芯片	应用于区块链等信息安全领域，支持群签名、盲签名、零知识证明等应用	区块链、分布式账本等
支持指纹识别的金融 IC 卡芯片	在金融 IC 卡芯片中集成指纹传感器，支持基于指纹识别的消费者设备持卡人验证（CDCVM）机制	指纹金融 IC 卡、金融支付终端等
高性能专用算法芯片	支持国密、零知识证明、同态加密等加密算法，支持适用于磁盘级加密的高速加密模式，支持服务器端、网关数据的高速加解密；支持视频图像信息的高速加解密	网关、路由器、加密卡、加密机、加密磁盘、数据中心、数据安全存储、安全视频监控等领域
基于 LPWAN 的安全接入芯片	支持无证书非对称密码算法（SM9 算法），支持 LPWAN（Low-Power Wide-Area Network，低功率广域网络）与服务器建立加密通道	物联网、智能家居、车联网

## 2、安全设备

本项目计划开发的安全设备包括安全终端、安全模组和加密机等，安全终端有包括个人安全终端、企业安全终端和金融安全终端。本项目将在公司现有安全产品和技术储备的基础上，紧跟新一代信息安全技术，瞄准目标市场，进一步对现有安全产品升级和新产品的开发，具体主要包括以下系列安全设备：

名称	功能说明	应用场景
支付设备（终端）	支持银联二维码支付标准；生成带数字签名的交易二维码、与支付服务器建立加密通道，实现扫码支付	POS，云音箱、扫码盒子、电子码牌等
个人安全终端	实现个人身份校验，双因素认证	个人身份认证器、FIDO、卡式令牌等
指纹金融 IC 卡、指纹 IC 卡	卡上集成指纹传感器，支持基于指纹识别的持卡人设备验证机制，保障基于银行卡的交易安全，及其他门禁等安全应用	银行支付、门禁、办公身份校验等



支持 dCVV 的可视金融 IC 卡	卡上集成电池和屏幕，支持 dCVV 机制，生成动态的信用卡验证码	信用卡网络支付等
分布式账本便携个人终端（数字货币硬件钱包）、金融可视 IC 卡	支持区块链零知识证明协议和指纹识别，保障个人数字资产安全，可以查询数字货币金额、交易情况	数字货币、“区块链+”政务等
支持“无感”活体检测的自助支付终端	支持面部识别，使用静默识别技术	商场、超市等
物联网终端安全模组	嵌入物联网设备中，实现信息的安全校验、传输	电表、冰箱、电视、空调等物联网设备
工业互联网终端安全模组	嵌入工业互联网设备中，实现信息的安全校验、传输	工业互联网领域
高性能金融数据加密机	支持基于国密算法的 XTS 加密模式，对服务器存储的交易数据进行磁盘级加密	路由器、数据中心等

### 3、安全系统

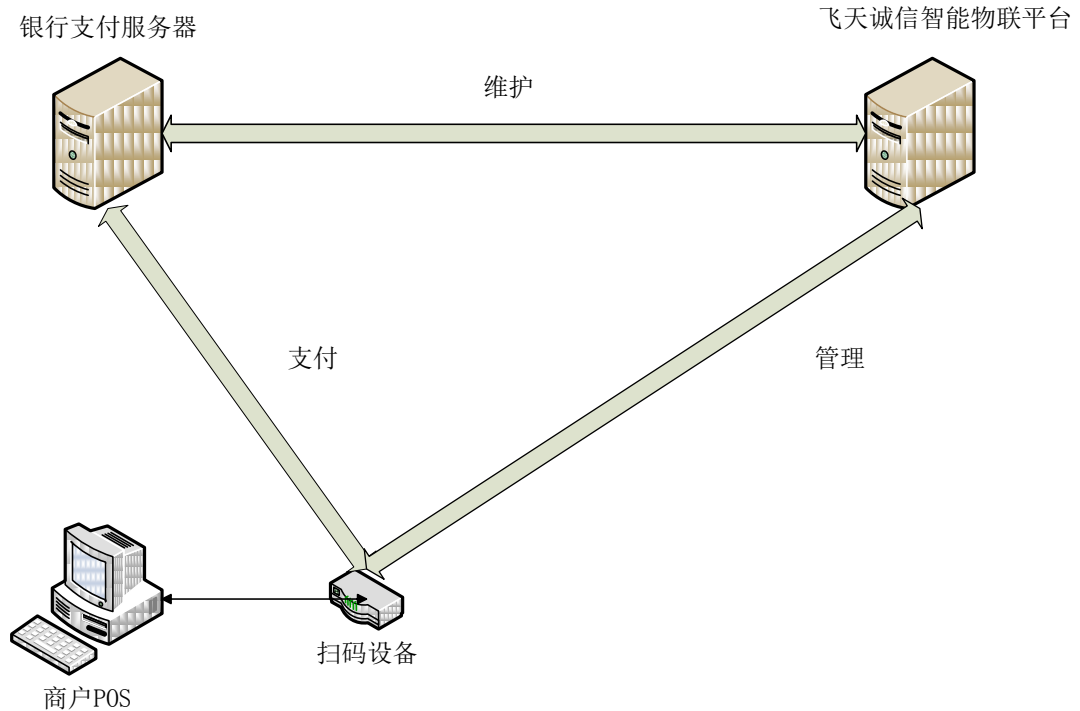
本项目将在公司现有产品和技术积累的基础上，进一步开发和升级的安全系统包括安全设备的云管理平台、基于区块链技术的云应用系统和云签章系统等，具体开发的产品如下表：

名称	功能说明	应用场景
支付设备管理平台（飞天智能物联平台）	基于物联网技术框架，对部署在小微商户的支付设备（扫码支付设备和刷脸支付设备）进行集中管理，向银行提供高效的维护服务。可对数量达千万级的扫码设备进行在线管理，可对接多家银行和众多商户	扫码支付、刷脸支付
基于区块链的智能合约系统	基于区块链的分布式网络系统，支持容错共识算法，向上层应用提供智能合约解释器及相关接口服务	分布式账本、“区块链+”政务
云签章系统	将强身份认证与电子签章技术相结合，并接入法律服务及存证公证服务等司法保障服务的电子签章平台，实现了电子合同签署时“人”可信、“技术”可靠、“存证”可依三位一体保障目标	云办公、电子签章等
云上统一密码管理平台	分为密码设备云化、密码管理和密码服务云化等几部分，实现快速响应、低时延的统一密码管理服务	物联网、车联网、智慧城市等

#### （1）支付设备管理平台（飞天智能物联平台）

该平台基于物联网技术框架，对部署在超市、商场、小微商户等场景的扫码设备进行集中管理，向银行提供高效的维护服务，并提供便于与现有收款机

(POS) 集成的信息化解决方案。如下图所示：



该平台具备以下职能：

设备开机后自动在管理平台登录，报告状态信息（包括位置、所属商户等）；支付时，扫码设备从现有收款机自动获取支付信息（或由商户手动输入），向银行支付服务器发送支付请求，完成支付；

如支付出现故障，银行支付服务器将相关信息发送给管理平台，管理平台对故障进行自动分析和排除，或通知售后人员进行处理。平台可对数量在千万级的扫码设备进行管理，可对接多家银行和众多商户，符合等保三级要求。

### （2）基于区块链的智能合约系统

该系统能够支持在无可信第三方的情况下，执行可追溯、不可逆转和安全可信的交易。研发基于区块链的分布式网络系统，支持容错共识算法，向分布式账本应用提供智能合约解释器及相关接口服务。

### （3）云签章系统

云签章系统可以为物流网站、电子商务网站、P2P 平台、旅游平台、保险平台、虚拟运营商平台及企业内部办公系统等提供完善的电子签章接入方案。云签章支持 SaaS 接入或独立部署模式，各应用系统只须调用系统电子签章相关 API，就可以实现用户使用电脑、手机、平板等任意终端随时随地、实时在线签署及管

理审批电子合同的需求，替代传统纸质合同，提高签署效率。

#### (4) 云上统一密码管理平台

本项目将在公司身份认证技术优势的基础上，开发基于云的统一密码管理平台，为物联网、车联网、智慧城市等提供云上密码管理服务。平台框图如下：



#### 4、市场推广

本项目还将支持营销队伍建设，加强新技术、营销理论与销售技能的培训，提升人员综合素质，提高企业的市场营销和产品销售能力，整合市场资源，加快国内外市场拓展，确保本项目市场目标的实现。

#### (四) 投资概算

本项目投资总额 168,375 万元，主要包括安全芯片、设备和系统的研发及产业化投入，拟使用募集资金 85,000 万元，项目具体投资概算如下：

单位：万元

项目名称	项目总投资金额及比例		募集资金拟投入金额及比例	
	总投资	占比	拟投入募集资金	占比
下一代安全芯片、设备、系统的研发及产业化项目	168,375	100.00%	85,000	100.00%
其中：安全系列芯片	92,702	55.06%	60,000	70.59%
安全设备	59,138	35.12%	20,000	23.53%
安全系统	16,535	9.82%	5,000	5.88%

本项目投资具体包括办公物业、软硬件设备购置费、研发费用、铺底流动资金等，项目具体投资概算如下：

单位：万元

序号	项 目	项目总投资金额及比例		募集资金拟投入金额及比例	
		投资金额	占比	拟投入募集资金	占比
1	办公场地购置及装修费	27,400	16.27%	-	-
2	设备及软件购置费	41,592	24.70%	40,000	47.06%
3	研发费用：	63,784	37.88%	27,000	31.76%
3.1	模具开发、软件使用费	5,700	3.39%	3,000	3.53%
3.2	工程样片测试验证费	9,397	5.58%	7,000	8.24%
3.3	量产测试费	4,800	2.85%	3,000	3.53%
3.4	知识产权费	2,200	1.31%	2,000	2.35%
3.5	研发人员薪酬	41,687	24.76%	12,000	14.12%
4	资质认证费	3,400	2.02%	3,400	4.00%
5	铺底流动资金	14,600	8.67%	14,600	17.18%
6	预备费：	12,200	7.25%	-	-
6.1	基本预备费	6,100	3.62%	-	-
6.2	涨价预备费	6,100	3.62%	-	-
7	其他费用：	5,400	3.21%	-	-
7.1	申请专利费用	1,000	0.59%	-	-
7.2	市场推广费用	3,200	1.90%	-	-
7.3	培训费用	1,200	0.71%	-	-
	<b>合 计</b>	<b>168,375</b>	<b>100.00%</b>	<b>85,000</b>	<b>100.00%</b>

### （五）项目建设规划

#### 1、项目建设周期

本项目建设周期预计为 48 个月。安全芯片、设备和系统研发同步进行，分期建设分批投入使用，即在建设期即可产生效益。

#### 2、项目实施主体

本项目实施主体为飞天诚信科技股份有限公司。

#### 3、项目建设地点

本项目建设地点为北京，计划在北京购置、租赁相关物业用于研发、办公、测试等工作。

## （六）经济效益评价

经测算，项目全部达产后，本项目回收期（含建设期）为 6.92 年（税后），内部收益率为（税后）22.65%，具有较好的经济效益。

## （七）项目备案情况

本项目已经获得中关村科技园区海淀园管理委员会出具的《北京市非政府投资工业和信息化固定资产投资项目备案证明》（京海科信局备 [2020] 90 号）。

# 三、本次募集资金投资项目的必要性和可行性分析

## （一）募集资金投资项目的必要性

### 1、项目是公司抓住信息安全市场大发展的需要

一直以来，国家都高度重视信息技术带来的发展契机及可能导致的安全威胁，国务院发布的《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）明确要求“大力推进信息化发展，切实保障信息安全。”《“十三五”国家信息化规划》指出，将坚持安全与发展并重作为我国信息化发展的原则之一树立科学的网络安全观，正确处理安全和发展关系，坚持安全和发展双轮驱动，以安全保发展，以发展促安全，推动网络安全与信息化发展良性互动、互为支撑、协调共进。

信息安全行业受到国家政策的大力支持，具有巨大的发展机遇，广阔的市场前景。《“十三五”国家信息化规划》提出的发展目标之一是到 2020 年，信息领域核心技术设备自主创新能力全面增强，新一代网络技术体系、云计算技术体系、端计算技术体系和安全技术体系基本建立。目前，互联网、移动互联网、物联网、工业互联网、云计算、大数据、区块链、金融科技、信息通信、智能制造等新技术、新应用的出现，对信息安全提出了更高的要求，拓展了信息安全产业的发展空间，加快了信息安全技术创新发展，催生了云安全、工业互联网安全等新的信息安全应用领域。

在国家相关政策的推动下，信息安全芯片、设备、系统将在各个领域得到快速的推广和应用，本项目是公司抓住信息安全市场大发展的需要。

## 2、项目是公司实现产业升级、行业整合的战略需要

公司是全球领先的数字安全系统硬件设备提供商和解决方案服务商，主营产品以 USB Key 和动态令牌（Token）为主，处于信息安全产业链的中上游。

随着移动互联网和智能手机的大规模普及，用户对产品易用性与去介质化（去硬件化）要求逐渐提高，公司传统 USBKey 和动态令牌产品的需求已经不足以满足市场需求，加之市场过度竞争，难以获得较好的销售价格，从而很大程度影响了公司的经营业绩。

2017 年 1 月，公司通过收购宏思电子，逐步进入上游安全芯片领域。公司把收购的安全芯片与公司片内操作系统（FTCOS）、应用软件、市场等资源进行有机整合，公司安全芯片业务取得了明显的进步，较公司传统产品，芯片产品的市场空间、毛利率水平均较高。

因此，公司计划通过本次非公开发行，进一步加大在信息安全领域的研发和产业化工作，逐步开发各类信息安全芯片、设备和系统，有针对性地面向 5G、互联网、区块链、数字货币等新场景的交易安全、运行安全领域，逐步实现向产业链上下游的拓展，实现公司战略转型升级。

## 3、垂直一体化是提升公司竞争力的有效手段

公司拥有完备的硬件、固件以及软件的研发和测试体系，建立了成熟高效的开发流程，培养了一支高素质、人员稳定、经验丰富、善于攻关的研发团队；通过收购也已经全面掌握安全芯片核心技术。公司片内操作系统（FTCOS）技术领先，安全设备与安全芯片深度融合，并向安全系统拓展，将大幅度提升公司应用方案开发能力和产品创新能力以及“系统级”的方案能力。

安全芯片、设备、系统垂直一体化整合，实现针对新场景、新应用的一系列安全芯片及其终端、系统产业化，将进一步增强公司的产品开发能力和满足市场需求的能力，是提升公司竞争力的有效手段。

### （二）募集资金投资项目的可行性

#### 1、项目符合国家信息安全产业发展政策，市场空间巨大

信息安全是 IT 系统的“稳定器”，是 IT 系统得以正常运行的基础和保证，在政务、金融、医疗、能源、交通、工业、军工等领域以及居民个人生活中，都

发挥着重要的作用。自“十五”规划以来，国家连续四个五年规划中，均将信息安全保障体系建设列为重要内容。信息安全领域在产业政策上获得了大力支持，主要体现在以下方面：

(1)《国家网络安全产业发展规划》公布，这是继 2017 年《中华人民共和国网络安全法》颁布之后对网络安全产业做出的第一项国家规划，信息安全的国家战略地位得到了进一步的肯定。根据规划，工业和信息化部与北京市人民政府决定建设国家网络安全产业园区；到 2020 年，依托产业园带动北京市网络安全产业规模超过 1,000 亿元，拉动 GDP 增长超过 3,300 亿元，打造不少于 3 家年收入超过 100 亿元的骨干企业。

(2) 等保 2.0 相关标准逐渐出台、完善，提升行业准入和经营标准

2019 年，国家标准化管理委员会发布了新修订的《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》（简称“等保 2.0”）等国家标准，与传统的等保 1.0 只针对网络和信息系統领域安全保护不同，等保 2.0 还将大数据、云计算、物联网、移动互联、工业控制在内的新技术、新场景均纳入监管的范围。另外，与传统的等保 1.0 相比，等保 2.0 在安全防护的要求上也大大提高，提出了主动防御、安全可信、动态感知、全面审计等新理念。

在等保 2.0 新标准的要求下，政府、金融机构、企业等单位在信息安全上面临着更大的合规压力，预计将进一步加大在信息安全产品、服务上的投入；网络安全产品及服务的市场空间将迎来进一步的发展。

(3)《密码法》的正式实施

2020 年 1 月 1 日，《中华人民共和国密码法》正式施行。《密码法》作为我国密码领域的综合性、基础性法律，将在推动动密码在网络安全与信息化发展中发挥更大的作用。《密码法》实施后，国家将进一步推进商用密码检测认证体系建设，对关系国家安全、社会公共利益的商业密码产品，依法列入网络关键设备和网络安全专用产品名录，认证合格后才可销售，并采取进口许可。《密码法》同时规定县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。

因此，预计《密码法》将进一步提升行业准入门槛，并通过政府采购拉动产

业发展。

#### （4）工业互联网安全获支持

工业互联网代表着国家新一代信息基础设施重要发展方向，工业互联网作为传统工业与新一代信息技术的深度融合，新技术的融入使得数据跨境流动更为频繁，工业互联网数据规模化增长速度越来越快，内外网数据交互流通，海量数据集中汇聚分析等导致对自身信息或数据控制能力下降，盗取、篡改数据的路径不断增多，攻击面不断扩大，带来新的工业信息安全问题。

2019年7月，工信部等十部委联合印发《加强工业互联网安全工作的指导意见》明确“到2020年底，工业互联网安全保障体系初步建立。制度机制方面，建立监督检查、信息共享和通报、应急处置等工业互联网安全管理制度，构建企业安全主体责任制，制定设备、平台、数据等至少20项亟需的工业互联网安全标准，探索构建工业互联网安全评估体系。技术手段方面，初步建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境。产业发展方面，在汽车、电子信息、航空航天、能源等重点领域，形成至少20个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。到2025年，制度机制健全完善，技术手段能力显著提升，安全产业形成规模，基本建立起较为完备可靠的工业互联网安全保障体系。”

#### （5）国产替代的政策背景，赋予信息安全市场未来广阔的发展空间

自主可控是信息安全的基础，随着国际局势的日益波动、各类安全事件的频频发生，信息技术领域实现国产替代、自主可控，已经成为产业发展的必由之路。信息安全领域的关键设备、关键软件早日实现国产替代、自主可控，守住国家网络安全的大门，也成为信息产业发展的重要目标。

综上，在上述产业政策的支持之下，我国信息安全市场发展空间巨大。工信部《2019年软件和信息技术服务业统计公报》数据显示，2019年，信息安全产品和服务实现收入1,308亿元，同比增长12.4%；而工信部《关于促进网络安全产业发展的指导意见（征求意见稿）》显示，到2025年我国网络安全产业规模将超过2,000亿元；未来几年我国信息安全市场仍将保持较快的发展趋势。

## 2、项目符合新技术、新应用场景对信息安全产业升级演进的要求

### （1）5G、物联网等新技术、新概念的提出，对信息安全提出了更高的要求，



进一步扩大了信息安全市场的规模

5G、物联网技术的发展创新，深刻改变了传统的产业形态和社会生活方式，催生了信息安全产业在产品、服务、模式上的创新。物联网作为5G的经典应用场景，以“万物互联”为特征，与4G时代的一个不同是，除了应用于家庭用消费电子设备之外，物联网设备将广泛应用于市政公用设施、大型制造业、能源产业、农业等部门，随着数以亿计的工业、农业、公用设施等设备接入物联网，其产业规模将呈现指数级的增长；但是后者容易成为被入侵和控制的目标，因此如何保护基础的网络环境，如何保护物联网设备、网络以及应用平台的安全使用，已经成为新的社会问题，同时也催生了物联网安全产业的发展。

### （2）数字货币的推进，为信息安全市场带来了新的发展空间

数字货币（Digital Currency Electronic Payment, DCEP）是指由中央银行依法发行，具备无限法偿性，具有价值尺度、流通手段、支付手段和价值贮藏等功能的数字化形式货币；是一种具有电子支付功能的加密数字支付方式，与现有的实物现金货币具备完全相同的效力。2020年1月，人民银行宣布已经完成法定数字货币的顶层设计、标准制定、功能研发、联调测试等基础工作，目前我国数字货币正在按原定计划有序推进。目前，数字货币已经开始进行内部测试和部分城市的试点工作。

数字货币既具备实物货币的强匿名性特征，又具备明显的留痕性，通过大数据分析可以掌控每一笔数字货币的流向。这种“可控”+“匿名性”的双重特征给数字货币的安全保障提出了新的挑战，也为金融信息安全市场的发展开拓新的空间。

### （3）金融科技、金融创新的发展，推动了金融信息安全的发展

金融科技是技术驱动的金融创新，通过现代科技成果可以改造或创新金融产品、经营模式、业务流程等，推动金融发展提质增效。在新一轮科技革命和产业变革的背景下，金融科技蓬勃发展，人工智能、大数据、云计算、物联网等信息技术与金融业务深度融合，极大地促进了金融行业的发展，金融科技已经成为推动金融转型升级的新引擎。

安全是金融科技、金融创新的红线。随着越来越多的新技术、新创新被引入金融领域，行业内对安全的需求也随之上升。2019年10月中国人民银行发布的

《金融科技（FinTech）发展规划（2019-2021）》便提出，“构建适应互联网时代的移动终端可信环境，充分利用可信计算、安全多方计算、密码算法、生物识别等信息技术，建立健全兼顾安全与便捷的多元化身份认证体系，不断丰富金融交易验证手段，保障移动互联环境下金融交易安全，提升金融服务的可得性、满意度与安全水平。综合运用数字签名技术、共识机制等手段，提升金融交易信息的真实性、机密性和完整性”。

金融科技、金融创新的发展，必将进一步推动金融信息安全的发展。

#### （4）国内工业互联网安全产业规模不断增长

随着新型基础设施建设和应用的开展，相关业务安全风险、应用场景安全风险和关键技术安全风险将逐渐浮出水面，国家、产业及社会各界对工业互联网安全的高度重视，这也是未来安全行业的机遇。根据中商产业研究院整理数据显示，2019年工业互联网安全市场规模将近125亿元，与2018年相比增长近30%。到2021年，中国工业互联网安全市场规模或将达到230亿元，涨幅超35%。

### 3、公司多年的行业技术积累和研发能力是项目顺利推进的技术基础

（1）技术是公司核心竞争力的重要组成部分，公司先后被评为北京市专利试点先进单位、北京市专利示范单位、国家级知识产权优势企业、企业知识产权管理标准化单位。2019年7月“中国企业专利500强榜单”正式发布，公司位列榜单前十。截至2019年12月31日，公司及下属子公司已拥有计算机软件著作权登记证书231篇；获得授权专利1226篇，其中发明专利948篇（含157篇国外专利）、实用新型专利70篇、外观设计专利208篇。

（2）公司积极参与行业标准的编制与起草工作，发挥了作为行业领军企业的责任，截至目前，公司及其下属子公司主持或参与制定/修订的国家标准已发布9项，行业标准已发布13项。

（3）公司已与中钞信用卡产业发展有限公司杭州区块链技术研究院签署战略合作框架协议，双方将致力于整合技术与资源，通过业务上的协同，开启区块链技术应用发展的新征程。

（4）公司于2016年成为FIDO（Fast Identity Online）联盟董事会成员；FIDO（Fast Identity Online）联盟，即线上快速身份验证联盟。FIDO联盟成立于2012年7月，联盟成员包括Google、微软、苹果、ARM、英特尔、PayPal、联想、阿里

巴巴、MasterCard 等。截至本报告发布之日，公司已有 21 款产品通过 FIDO 认证。

(5) 对安全芯片企业的收购、整合，为公司垂直整合提供了技术和经验积累。2017 年 1 月公司完成对宏思电子的收购，三年多来，宏思电子在公司的支持下，获得了高速的发展。

#### 4、广泛的客户资源为项目的实施提供了市场基础

(1) 公司在金融领域客户群日覆盖较为广泛，公司为包括工行、建行、农行、中行、交通银行等在内的多家银行的网上银行系统安全提供完善的解决方案和专业的技术服务，是国内银行客户数较多的智能网络身份认证产品提供商。

(2) 公司连续获得金蝶集团颁发的 2018 年度、2019 年度“优秀供应商”荣誉称号。

(3) 2019 年 6 月，公司获得 MISA（微软智能安全协会）的会员资格，成为国内首家入选企业。

(4) 2019 年 12 月，公司正式通过了 CMMI3 级认证。CMMI3 级认证的通过代表公司在软件研发能力、服务交付以及项目管理水平得到了权威机构的认可。

公司以北京总部为中心，在广州、上海等地成立了营销中心，在深圳、杭州和昆明等多个地区建立了办事处，在全球范围内建立起市场推广和营销服务体系，并配有专业的系统解决方案和服务团队，公司产品销售至全球多个国家和地区，积累了金融、政府、邮政、电信、交通、互联网等领域多家客户。公司广泛的客户基础，为本项目的实施，提供了强大的市场基础。

### 四、本次发行对公司经营管理和财务状况的影响

本次发行完成后，公司资产总额、净资产规模均将有所增加，公司资产负债率将相应下降，进一步优化资产负债结构，提高公司抗风险的能力，为公司未来的发展奠定基础。

本次发行完成后，公司筹资活动产生的现金流入将大幅度增加；在资金开始投入募投项目后，投资活动产生的现金流出量将大幅增加；在募集资金投资项目建成运营后，公司经营活动产生的现金流量净额将得到显著提升。

本次发行完成后，公司股本总额将即时增加，而募集资金投资项目在短期内无法即时产生效益，因此，公司的每股收益短期内存在被摊薄的可能。本次募集资金投资项目的实施有利于提高公司的主营收入与利润水平，增强公司的竞争优势，提升公司未来整体盈利水平。

## **五、募集资金投资项目可行性结论**

综上所述，本次发行募集资金的用途合理、可行，项目符合国家产业政策，是国家鼓励投资的产业。项目建设有利于完善公司业务结构，提升公司综合实力和核心竞争力，促进公司持续、健康发展，符合本公司及本公司全体股东的利益。

飞天诚信科技股份有限公司

2020年5月25日