关于《关于三未信安科技股份有限公司首次公开发行股票并在科创板上市的审核中心意见落实函》的回复说明

信会师报字[2022]第 ZG12036 号

防 伪 编 码:	310000062022797O4Y
被审计单位名称:	三未信安科技股份有限公司
报 告 文 号:	信会师报字[2022]第ZG12036号
签字注册会计师:	王娜
注 师 编 号:	420003200741
签字注册会计师:	胡碟
注 师 编 号:	310000060149
事 务 所 名 称:	立信会计师事务所（特殊普通合伙）
事 务 所 电 话:	021-23280000
事 务 所 地 址:	南京东路61号4楼

立信会计师事务所（特殊普通合伙）

关于《关于三未信安科技股份有限公司首次公开发行股票并在科创板上市的审核中心意见落实函》的回复说明

信会师报字[2022]第 ZG12036 号

上海证券交易所：

根据贵所 2022 年 5 月 12 日出具的《关于三未信安科技股份有限公司首次公开发行股票并在科创板上市的审核中心意见落实函》（上证科审（审核）〔2022〕203 号），立信会计师事务所（特殊普通合伙）（以下简称“立信”、“申报会计师”、“会计师”）作为三未信安科技股份有限公司（以下简称“三未信安”、“发行人”或“公司”）本次发行的申报会计师，按照贵所的要求对意见落实函中提出的涉及会计师问题进行了审慎核查，具体回复如下，请予审核。

如无特别说明，本问询回复所述的词语或简称与招股说明书中“释义”所定义的词语或简称具有相同的涵义。

请发行人进一步说明：（1）外购 IP 核之外，密码芯片密码功能的相关核心技术先进性以及安全等级与核心技术的对应关系；（2）外购 IP 核占发行人产品成本的比例；（3）发行人市场占有率为 0.41%的情况下属于行业前列的依据；（4）在行业集中度较低、市场参与企业较多的情况下，行业资质门槛较高的结论是否客观准确。

请保荐机构和申报会计师核查并发表明确意见。

回复：

一、发行人说明

（一）外购 IP 核之外，密码芯片密码功能的相关核心技术先进性以及安全等级与核心技术的对应关系

1、公司密码芯片密码功能的相关核心技术先进性说明

（1）核心技术具有高度集成化效果，且核心性能指标实现大幅提升

公司 XS100 密码安全芯片通过多种关键技术协同应用，实现芯片内部各个功能模块的高速互联能力，将公司原密码板卡中 FPGA 芯片、主控芯片、SM1 算法芯片、SM2 算法芯片、RSA 算法芯片、随机数芯片等 6 个独立芯片及其功能高度集成为 1 个芯片，集中完成了包括对称算法引擎、非对称算法引擎、算法调度模块、片内 COS、片内高速总线模块、硬件虚拟化模块等密码功能，具体情况如下：

原独立芯片名称	原独立芯片功能	XS100 密码功能	对应的核心技术
FPGA 芯片	可编程器件芯片，公司使用该芯片进行自研编码设计以实现 PCI-E 高速链路功能及 AES、DES、SM4、SM3、SM2、RSA 等算法	算法调度模块、片内高速总线模块、硬件虚拟化模块	1、高性能密码算法硬件实现技术 2、SR-IOV 硬件虚拟化技术 3、高速 PCI-E 通信技术 4、高可靠的硬件设计技术 5、高安全密码模块设计技术
主控芯片	为公司自研的密钥管理及算法调度等程序提供计算资源	片内 COS	
SM1 算法芯片	提供 SM1 算法功能	对称算法引擎	
SM2 算法芯片	提供 SM2 算法功能	非对称算法引擎	
RSA 算法芯片	提供 RSA 算法功能	非对称算法引擎	
随机数芯片	提供真随机数功能	对称算法引擎	

公司通过高性能密码算法硬件实现技术、高速 PCI-E 通信技术等核心技术的协同应用，研制出的 XS100 密码安全芯片集合了 6 款芯片的功能，芯片的核心性能指标大幅提升，同时基于 XS100 单芯片的产品设计，可以大幅降低产品的复杂度，提高产品的可靠性。此外 XS100 芯片可以有效降低采购成本，提高产品的性价比。

公司的 XS100 密码芯片的 SM1 加解密速度 9.8Gbps、SM2 签名速度 30 万次每秒；同时相对于原独立芯片组合，XS100 还增加了对 SM3、SM9 等国密算法的支持，其中 SM3 运算速度 9.6Gbps、SM9 签名速度 1,000 次每秒，以上算法性能指标较外购芯片实现了大幅提升，具体对比情况如下：

项目	外购芯片						XS100 芯片
	FPGA 芯片*	主控芯片	SM1 芯片	SM2 芯片	RSA 芯片	随机数芯片	
PCI-E 通信	√	×	×	×	×	×	√
CPU	×	√	×	×	×	×	√
SM1 加解密（Gbps）	×	×	1	×	×	×	9.8
SM2 签名（Tps）	×	×	×	50,000	×	×	300,000
SM3（Gbps）	×	×	×	×	×	×	9.6
SM4 加解密（Gbps）	7	×	×	×	×	×	9.5
SM7 加解密（Gbps）	×	×	×	×	×	×	0.9
RSA2048 签名（Tps）	×	×	×	×	1,000	×	10,000
SM9 签名（Tps）	×	×	×	×	×	×	1,000
AES 加解密（Gbps）	1	×	×	×	×	×	8
DES 加解密（Gbps）	0.4	×	×	×	×	×	3
随机数（Mbps）	×	×	×	×	×	20	40

（2）核心功能指标达到国内公司先进水平，且系目前唯一支持硬件虚拟化芯片产品

公司 XS100 密码芯片与苏州国芯、北京宏思、恩智浦等密码芯片公司的主流产品相比，核心指标各有优势，公司在产品设计中选择多项指标领先的原则，以便适应不同合作厂商不同场景的广泛性需求，因此公司产品功能较为全面，总体而言公司 XS100 密码芯片的综合核心功能指标达到国内公司先进水平。

与目前国内主流的密码芯片厂商的主流产品相比，公司的 XS100 芯片系目前唯一支持硬件虚拟化的密码安全芯片。XS100 密码芯片中采用的 SR-IOV 硬件

虚拟化技术可以将一个密码设备虚拟成多个密码设备，并确保各密码虚机之间密钥互相隔离，杜绝越界访问及非法访问。XS100 密码芯片的硬件虚拟化技术在提升密码资源性能的同时并降低了多虚机环境下的密码资源集成成本，灵活有效地满足云计算环境下的海量密码需求。

公司 XS100 核心功能指标的先进和硬件虚拟化功能来源于公司自主研发的高性能密码算法软硬件实现技术、高速 PCI-E 传输和数据处理技术和云计算的密码服务虚拟化及海量密钥管理技术。以上核心技术是公司专注于密码领域多年，并保持不断研发投入的成果。公司作为国内最早布局云计算密码产品的厂商之一，在研发云密码产品的过程中形成了云计算的密码服务虚拟化及海量密钥管理技术。

（3）公司在密码领域有明显优势，密码芯片的核心密码技术先进

公司在商用密码领域具有多年积累，对密码技术和应用有着深刻的理解和丰富的经验，积累了高性能密码算法硬件实现技术、高速 PCI-E 通信技术、SR-IOV 硬件虚拟化技术等多项密码芯片相关的核心技术，解决了密码芯片的密码算法快速实现、高速数据传输、虚拟化等技术难度很高的问题。公司熟悉密码芯片的应用场景，深入理解密码芯片的需求，可以更好地优化密码芯片性能。除外购 IP 核外，公司密码芯片的核心密码技术均为公司自主研发，目前公司密码芯片累计获得 7 项发明专利和 6 项集成电路布图。

公司深刻理解技术创新是公司发展的基石，是核心竞争力，依托行业多年的研发投入、技术积累和行业经验，并不断保持对密码技术的前沿性研究，提升公司密码创新的系统能力，使得公司的核心技术一直保持在行业先进水平。

公司密码芯片相关的主要核心技术先进性及具体表征如下：

核心技术	技术先进性	技术来源	知识产权
高性能密码算法硬件实现技术	密码算法的快速实现是密码芯片和设备最重要的核心技术，该技术有效优化了运算性能，解决了传统密码运算性能的衰减和密码设备的性能瓶颈，实现网络加密的高性能调度。公司密码芯片 SM2 签名速度突破 30 万次每秒、SM1 加解密速度 9.8Gbps、SM3 运算速度 9.6Gbps、SM4 加解密	自研	一种基于椭圆曲线的分布式签名方法及系统； 一种基于 RSA 的分布式签名方法与系统

核心技术	技术先进性	技术来源	知识产权
	速度 9.5Gbps。		
SR-IOV 硬件虚拟化技术	该技术在提升密码资源性能的同时并降低了多虚机环境下的密码资源集成成本，灵活有效地满足云计算环境下的海量密码需求。 虚拟化和密钥管理技术集成到密码芯片中，是高性能密码芯片的重要功能。公司密码芯片系目前唯一支持硬件虚拟化芯片产品	自研	一种 SR-IOV 环境下多虚拟机并发 DMA 的顺序调度方法及系统
高速 PCI-E 通信技术	该技术解决了密码芯片的通信瓶颈问题，为密码芯片的高性能实现奠定了基础	自研 + 外购	自研主要包括基于 PCI-E 协议的高速数据处理方法，解决密码芯片的通信瓶颈，形成两个相关专利：一种对 CPLD 数据包进行有序存储的方法及系统； 一种基于 PCIe 接口的密码卡及该密码卡的数据加密方法。 外购主要是通用的 PCI-E 协议相关 IP，分为两部分：PCI-E 控制器和 PCI-E PHY
高可靠的硬件设计技术	该技术可以提升产品的可靠性，设计研发高性价比、低成本的产品，满足物联网、工业互联网等场景的需求	自研	一种 PCI 密码卡和海量密钥密码运算方法及系统
高安全密码模块设计技术	该技术设计了高安全密码模块的安全防护机制，实现了高安全物理安全防护、防测信道攻击保护、软件固件安全防护等技术，可以达到密码模块安全三级水平，是公司高安全等级产品的核心技术。	自研	一种安全升级 PCI 密码卡卡内程序的方法及系统

2、安全等级与核心技术的对应关系

（1）不同安全等级的技术要求及产品数量分布情况

国家密码管理局 2014 年发布的国密标准 GM/T 0028-2014《密码模块安全技术要求》对密码的四个安全级别做出了明确要求，具体情况如下：

安全等级	技术要求
安全一级	安全一级提供了最低等级的安全要求，该等级阐明了密码模块的基本安全要求，该等级密码模块的例子有：个人计算机中的硬件加密板卡、运行在手持设备或通用计算机上的密码工具包。密码模块的使用者可以选择多种密码解决方案来满足安全需求。
安全二级	安全二级在安全一级的基础上增加了拆卸证据的要求，该等级要求基于角色的鉴别，密码模块需要鉴别并验证操作员的角色，该等级的软件密码模块可以运

安全等级	技术要求
	行在可修改的环境中，软件密码模块能够达到的最大整体安全等级设定为安全二级。
安全三级	安全三级在安全二级的基础上要求更强的物理安全机制，以进一步防止对密码模块内敏感安全参数的非授权访问，该等级要求基于身份的鉴别机制，密码模块应当设计有环境保护特性，该等级的密码模块应提供非入侵式攻击缓解技术的有效性证据和测试方法，安全三级的密码模块增加了生命周期保障的要求等。
安全四级	安全四级是本标准中的最高安全等级，该等级包括较低等级中所有的安全特性，以及一些扩展特性，该等级的物理安全机制应当在密码模块周围提供完整的封套保护，特别适用于无物理保护的环境，该等级要求对操作员进行多因素鉴别，密码模块应当设计有环境保护特性，安全四级要求模块的设计应通过一致性验证。

国密标准 GM/T 0028-2014《密码模块安全技术要求》对产品的各项功能做了明确要求，如软件固件安全、运行环境、物理安全等指标，产品整体的各项功能指标决定了产品的安全等级，而非产品的组成部件如芯片、PCB 板等。

截至 2021 年 12 月 31 日，市场上安全等级一级、二级、三级的产品共 1,356 个，尚无等级四级的产品，具体情况如下：

安全等级	数量
安全三级	5
安全二级	982
安全一级	369

注: 截至 2021 年 12 月 31 日，根据商用密码认证业务网等公开渠道查询。

密码产品的安全等级越高，其自身的安全防护能力越强，密码产品的安全性越高，可应用于更高安全等级的网络信息系统。安全等级三级密码产品的安全要求提升较大，研制技术难度高，一定程度上反映了商用密码企业的研发创新能力。

（2）高安全等级产品的技术门槛要求较高

高安全等级产品对企业的综合全面的技术能力、技术开发能力、密码经验、密码技术的前瞻性和实践能力有着较高的要求，需要大量的技术积累和投入，研发难度很高，国内目前仅有少数几家企业具备安全等级三级产品的资质。

1）需要技术能力广

根据《密码模块安全技术要求》，在进行评级时，会针对各安全域（功能指标）独立评级，部分域随着安全等级的递增，安全要求也相应增加，最后以 11 个域所获得的最低评级作为产品的整体评级。产品要达到安全等级三级的标准需

要满足 11 个域均不低于安全等级三级，对企业的整体技术实力有着全面和较高的要求，企业在各项技术上不能有短板，一旦有一个域无法达到相应要求，则无法获得安全等级三级的认证。

2）需要技术能力深

自公司的 SJK1926 密码卡出现之前，国内一直没有达到安全三级以上的密码产品，主要由于从安全等级三级开始，安全要求提升较大，研制技术难度很高。例如安全等级三级要求密码模块接口需要建立可信信道、软件固件安全需要基于数字签名的完整性测试、非入侵安全需要提供非入侵式攻击缓解及缓解测试方法等，安全要求高，需要企业在商用密码行业有丰富的密码经验，对密码理论、密码技术和密码应用有深入的理解，理解高安全等级各项技术要求的实现方式，并具备技术开发能力，需要企业在密码领域做到专精。

3）需要具备前沿密码技术的前瞻性和实践能力

公司一直紧跟前沿密码技术的发展，敏锐察觉到高安全等级产品是未来的发展方向，为了填补安全等级三级密码产品的空缺，公司基于在密码技术和经验的积累，积极投入人力、物力资源进行研发。由于公司研发的 SJK1926 密码卡是国内首款安全等级三级产品，产品在通过国家密码管理局检测中心检测时，检测中心非常谨慎，不断和公司探究技术细节，并多次组织会议征求专家意见，对产品的各项功能进行交流，过程中公司对产品不断完善，最终公司的产品获得了安全等级三级认证。安全等级三级产品的开发不仅需要企业对前沿技术有敏锐的嗅觉，还需要具备产品落地的实践能力，对企业的综合实力和研发团队要求较高。

（3）安全等级与公司核心技术的对应关系

1）公司有能力、有意愿研发安全等级三级产品

公司在密码理论的研究、密码技术、密码产品的研发及密码应用方面具备深厚的理论功底和实践经验。公司具备密码算法的芯片实现、FPGA 开发、硬件板卡的设计、嵌入式程序和驱动程序的开发、上层软件的程序设计等全阶段研发能力的技术团队，核心研发设计均由自主完成。公司研发人员公司核心研发团队由国内较早从事商用密码产品和技术研发的专家、资深技术人员组成，多位专家参与国内网络安全相关技术标准、规范的制定工作，对密码行业标准和规范有着较

深的理解。此外公司深刻理解技术创新是发展的基石，是核心竞争力，一直保持着对密码技术的前沿性研究，不断投入对新产品的研发。公司作为国家网络信息安全产业的重要参与者，有能力、有意愿去研发安全等级三级产品，推动商密产业的进步和发展。

2）安全等级对应的公司核心技术情况

公司在研发安全等级三级产品的过程中，形成了公司核心技术之一的高安全密码模块设计技术。该核心技术设计了高安全密码模块的安全防护机制，实现了高安全物理安全防护、防测信道攻击保护、软件固件安全防护等技术，达到了密码模块安全三级水平。

密码等级安全三级对密码产品的安全要求较高，实现难度较大，主要为以下几个方面：密码模块接口、软件固件安全、运行环境、物理安全、非入侵安全、敏感安全参数管理、自测试、生命周期保障等。公司的核心技术高安全密码模块设计技术可以满足各项指标的具体要求，公司高安全密码模块设计技术与安全等级三级主要指标的对应关系如下：

主要指标	具体要求	对应高安全密码模块设计技术的具体内容
密码模块接口	可信信道	设计了专用协议的可信信道，与状态接口、控制接口、数据接口物理隔离及逻辑隔离
软件固件安全	基于数字签名的完整性测试	密码板卡固件采用数字签名技术保障完整性； 密码整机采用了不可修改的固件操作系统，并支持固件及重要程序文件的完整性保护
运行环境	受限或不可修改运行环境的操作系统	
物理安全	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；环境失效测试或环境失效保护	采用多个微触开关，外壳破坏立即销毁密钥；密码板卡采用封闭外壳，密码整机散热部分采用双层外壳，具备防止单铰链探针探测能力；内置传感器能够根据电压、温度等变化停止服务或销毁密钥
非入侵安全	非入侵式攻击缓解；提供缓解测试方法	采用掩码法等技术基于 FPGA 实现抗侧信道攻击的密码运算；采用防电磁泄漏外壳、电源整流等技术；设计能量分析攻击、计时分析攻击、电磁泄露攻击测试模型，提供测试数据
敏感安全参数管理	随机比特生成器、全生命周期管理；自动安全传输或协商；	采用多路物理噪声源随机数发生器提升随机数安全性和可靠性；支持密钥等

主要指标	具体要求	对应高安全密码模块设计技术的具体内容
	手动加密、可信信道或知识拆分输入输出	敏感安全参数置零；支持可信信道
自测试	运行前自测试；条件自测试	支持程序完整性、随机数安全性、密钥一致性、密码算法正确性等自测试和条件测试功能
生命周期保障	配置管理、设计、FSM、开发、测试、配送与操作、指导文档	公司通过了 CMMI-ML3、ISO 9001、ISO 27001 等认证，配置管理、开发过程、生产质量等方面满足要求

公司研发的 SJK1926 PCI-E 密码板卡于 2019 年取得商用密码产品型号证书，是国内首款通过国家商用密码检测机构认证的安全三级密码产品，SJJ1212-A 密码整机于 2020 年获得国家商用密码检测机构的安全三级认证。

（二）外购 IP 核占发行人产品成本的比例

关于 XS100 芯片，公司外购 IP 核相关费用的主要约定情况如下：

IP 核	协议主要约定	收益、费用约定或其他权利约定
CPU	一次授权使用权	1、一次性费用 95.07 万元，不含税金额为 89.69 万元； 2、权利金：在后续芯片量产销售环节，IP 供应商按照销量收取一定的权利金，小于 300 万片为 0.29 元/片，300 万-500 万片为 0.26 元/片，大于 500 万片为 0.22 元/片。
PCI-E 控制器	一次授权使用权	一次性费用 77.19 万元，不含税金额为 68.31 万元
PCI-E PHY	一次授权使用权	一次性费用 101 万元，不含税金额为 101 万元

注：PCI-E PHY 授权协议中约定税率为零。

公司外购 IP 核授权相关的一次性费用合计 259 万元计入研发费用；合同中约定权利金的，在公司芯片产品实现销售时，根据合同约定计算应支付的权利金金额并计入营业成本。

公司研发 XS100 芯片产生的研发费用合计为 1,556.54 万元，其中外购 IP 核相关授权一次性费用合计 259 万元，占该产品研发费用比例为 16.64%。报告期内，公司研发费用无资本化处理的情况。

由于外购 IP 核相关费用中绝大部分（一次性授权费用）已计入前期研发费用，只有很小部分（权利金）将计入产品成本，以下通过测算外购 IP 核相关总体费用占公司密码芯片 XS100 研发费用和成本总和的比例来反映外购 IP 核对该款芯片产品的综合财务影响。

公司自研芯片的营业成本主要包括光罩制作成本、流片成本、封装测试成本、外购 IP 核权利金等。公司 2021 年密码板卡产量约 10 万张，根据公司密码板卡需求预测及市场需求反馈，假设公司密码板卡 50%采用自研芯片，公司自研密码芯片平均年产 5 万片，根据公司芯片新产品的研发情况，假设该产品生命周期为 4 年，则 XS100 芯片总产量预计为 20 万片。以公司密码芯片首批次 1.8 万片和预计总产量 20 万片分别测算，相关费用和成本情况如下：

单位：万元

项目		情景 1： 首批次 1.8 万片	情景 2： 假设总产量 20 万片	备注
研发费用	公司内部研发费用	1,297.54	1,297.54	-
	外购 IP 核授权费用	259.00	259.00	-
营业成本	光罩制作成本	337.29	337.29	假设光罩设计可重复使用
	流片成本	47.82	531.36	假设后续流片单位成本与首批次相同
	封装测试成本	57.78	642.00	假设后续封装测试单位成本与首批次相同
	外购 IP 核权利金	0.49	5.44	根据授权合同约定为 0.29 元/片
外购 IP 核相关费用占芯片研发费用和营业成本之和的比例		12.95%	8.43%	-

注 1：假设 XS100 芯片后续不再产生新的研发费用；

注 2：不测算其他可能与芯片产品相关的成本费用。

根据上述测算，公司 XS100 芯片在产量分别为 1.8 万片和 20 万片时，公司外购 IP 和相关费用占该款芯片的研发费用和营业成本合计的比例分别为 12.95%和 8.43%，整体占比较低，并且随着公司芯片产量增加而降低。综上，外购 IP 核相关费用占公司 XS100 芯片产品综合费用成本的比例较低，财务影响较小。

（三）发行人市场占有率为 0.41%的情况下属于行业前列的依据

1、现有市场报告统计的商用密码产业规模包含范围较广，远大于密码产品范畴

根据赛迪发布的《2020-2021 中国商用密码产业发展报告》，商用密码产业由商用密码产品（硬件、软件）和商用密码服务组成。密码产品包括密码芯片、密码模块、密码板卡、密码整机、密码系统和密码软件等，商用密码服务则包括

密码应用系统集成服务、密码咨询服务、密码知识和技术培训服务、密码应用系统运营服务、密码应用系统维护保障服务等。上述报告在统计产业规模时，不仅包含了密码产品还包含了密码应用系统集成服务、密码咨询服务等范围，涵盖范围较广，涵盖了产业链上下游各个环节，从而使得涉及的企业主体较为广泛，市场规模也相对较大。

关于商用密码产品的市场情况，作为网络信息安全领域的一个细分子市场，目前暂无独立统计数据。

2、发行人属于行业前列的依据

（1）报告期内公司密码产品业务快速增长，逐渐缩小与行业龙头卫士通的差距

卫士通作为国内商用密码行业的龙头企业，是国内首家于 2008 年上市的密码企业，是中国电子科技集团有限公司、中国电子科技网络信息安全有限公司在网络信息安全领域的唯一资本运作平台和重要产业平台，在加密认证类产品市场长期保持领先，在安全信息系统集成市场占据重要地位。卫士通密码产品在国内市场占有率排名第一。

公司聚焦密码技术，创新能力强，成长速度快。2019 年-2021 年，公司营业收入的复合增长率为 42.15%，卫士通营业收入的复合增长率为 15.14%；2021 年公司密码产品收入的增速为 34.42%，卫士通密码产品收入的增速为 17%，双方的增速均超过 2021 年赛迪统计的行业平均增速。

公司与卫士通密码产品的收入及市场占有率情况如下：

单位：亿元

项目		2020 年		2021 年	
公司名称	主要产品类别	收入	市场占有率	收入	市场占有率
卫士通	密码芯片、密码模块（包含密码板卡）、密码整机和密码系统	5.93	1.27%	6.94	1.32%
发行人	密码板卡、密码整机、密码系统	1.90	0.41%	2.55	0.48%

注 1：卫士通 2021 年报中的产品分类中并未披露密码产品的收入，因此根据其 2020 年密码产品的占比测算其 2021 年密码产品的收入；

注 2：2021 年商用密码产业规模为赛迪的预测。

2021 年公司市场占有率上升至 0.48%，卫士通的市场占有率增加为 1.32%，市场占有率均有所上升。

此外根据卫士通年报披露，密码产品作为卫士通一直以来的核心产品，主要包括密码芯片、密码模块（密码板卡）、密码整机和密码系统等产品，而目前公司的密码芯片正在商业化中，尚未推向市场形成收入。随着公司密码芯片正式推向市场并形成收入，公司产品系列也将进一步完善，产业链也更加独立和完整。

（2）公司产品的安全等级认证产品数量位于行业前列

根据行业内密码产品安全等级的认证数量情况，目前商用密码行业主流产品以安全等级一级和二级为主，业内各主要企业均主要从事安全等级一级和二级密码产品的生产销售，行业内主要企业的不同安全等级产品数量如下：

排名	公司名称	安全等级三级	安全等级二级	安全等级一级
1	三未信安	2	24	6
2	江南天安	1	18	8
3	渔翁信息	0	21	0
4	卫士通	0	18	3

注: 截至 2021 年 12 月 31 日，根据商用密码认证业务网等公开渠道查询。

公司的密码板卡于 2019 年 4 月获得国内首个密码模块安全等级三级认证、密码整机于 2020 年 12 月获得密码模块安全等级三级认证、FIPS 密码整机于 2019 年 10 月获得国内首个 FIPS 140-2 Level 3（美国联邦信息处理标准 3 级）安全认证。安全等级三级密码产品的安全要求提升较大，研制技术难度高，一定程度上反映了商用密码企业的研发创新能力和产业实力。截至目前，公司的安全等级二级和三级产品数量均位于行业前列。

（3）公司通过国家密码管理局检测中心认证的产品数量位于行业前列

国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。商用密码产品的认证数量情况一定程度可以反映商用密码厂商的研发能力、商用密码产业规模及实力。

行业内主要企业的商密产品认证数量如下：

排名	公司名称	商密产品认证数量

排名	公司名称	商密产品认证数量
1	三未信安	44
2	卫士通	38
3	江南天安	33
4	渔翁信息	23

注:根据商用密码认证业务网等公开渠道查询，截止至 2021 年 12 月 31 日。

截止至 2021 年 12 月 31 日，公司拥有通过国家密码管理局认证的产品数量为 44 个，属于商用密码企业的前 1.25%，位于行业前列。具体情况如下：

类型	公司数量	占全国商用密码企业的比例
持有 1 个证书	255	21.25%
持有 2 到 4 个证书	183	15.52%
持有 5 到 10 个证书	73	6.08%
持有 11 到 20 个证书	34	2.83%
持有 20 个以上证书	15	1.25%
合计	**560**	**46.67%**

注：根据赛迪发布的报告全国商用密码企业约为 1200 家，此处为便于分析假设为 1200 家。

（4）公司参与制定的行业标准数量位于行业前列

公司参与行业标准制定数量属于行业前列。公司作为国家密码标准化委员会和密码行业标准化技术委员会的成员单位，参与了 18 项密码行业标准的制定。

我国商用密码的快速发展离不开密码标准体系的重要支撑，密码标准体系是促进密码产业发展、保障密码产品质量、规范密码技术应用的重要保障。参与标准的制修订工作是密码厂商把握标准要求、掌握新技术动向的重要途径，是密码厂商技术实力的重要体现。

截至 2021 年底，密码行业标准化技术委员会共发布了 118 项商用密码行业标准，公司牵头或参与了 18 项标准，虽然较行业龙头卫士通有一定差距，但领先于其他行业内主要企业。公司与行业内主要企业参与商用密码行业标准的数量对比情况如下：

排名	公司名称	参与密码行业标准数量
1	卫士通	51
2	三未信安	18

排名	公司名称	参与密码行业标准数量
3	江南天安	8
4	渔翁信息	1

注：根据国家密码管理局及密码行业标准化技术委员会网站等公开渠道查询，截止至2021年12月31日统计数据。

综上所述，公司专注于密码产品的研发、生产和销售，而行业规模统计数据中除密码产品外还包括密码服务业务，并未区分消费端和服务器端的市场，使得公司市场占有率较低。随着公司业务快速增长，公司与市场龙头卫士通的市场占有率逐步接近。此外，公司产品的安全等级认证产品数量位于行业前列，公司通过认证的产品数量位于行业前列，公司参与制定的行业标准数量位于行业前列，根据 Market Research Intellect 2021 年统计，公司在全球密码硬件安全市场中位列第九、国内第三，公司在商用密码产品行业综合实力属于行业前列。

（四）在行业集中度较低、市场参与企业较多的情况下，行业资质门槛较高的结论是否客观准确

1、我国商用密码行业集中度较低、市场参与企业较多的背景原因

（1）商用密码行业高速发展且需求多样化，需要产业链企业分工配合，使得纳入统计的市场企业数量众多

目前国内商用密码行业处于高速发展期，具有较大的市场发展潜力，同时由于密码产品的基础性特点，密码产品应用广泛且与用户业务结合紧密，需求多样化，因此吸引了较多的企业加入商用密码产业。由于商用密码产品的技术水平要求相对较高，商用密码整体解决方案是个较大的系统工程，通常一家厂商难以独立完整地开发并部署所有相关技术与产品，需要产业链不同位置的企业分工配合，具体还包括密码应用系统集成服务、密码咨询服务、密码知识和技术培训服务、密码应用系统运营服务、密码应用系统维护保障服务等，涵盖了产业链上下游各个环节，从而使得涉及的企业主体较为广泛，因此纳入统计的市场企业数量众多。

（2）消费端低门槛产品的市场规模相对较大，参与企业数量也相对较多

商用密码产品可分为消费端、服务器端产品，其中消费端的产品技术水平相对较低，如密码 Ukey、日常使用的 U 盾等产品，但市场规模相对较大，参与企业的数量相对较多；服务器端的产品技术水平相对较高，如 PCI-E 密码板卡、服

务器密码机等产品，参与企业数量相对较少。

公司的产品主要为服务器端产品，基本不涉及消费端的商用密码产品。服务器端的商用密码产品的功能、性能及安全性较高，可以满足关键行业及领域对密码的需求，可以代表商用密码行业最高的技术水平，是商用密码行业的关键产品。

（3）商密产品资质主要为产品资质，对产业链中从事产品销售和技术、咨询服务等没有资质要求

根据目前商用密码相关法律法规要求，商用密码的资质主要为产品资质，不再对企业和销售资质有要求，因此部分商用密码企业不需要密码产品资质也可以生产经营。

根据赛迪发布的《2020-2021 中国商用密码产业发展报告》，全国共有 1,200 余家商用密码企业，中小型密码企业偏多，主要包括密码产品提供商，提供密码芯片、密码板卡、密码整机等密码产品；密码应用集成商，提供密码应用系统集成等工作；密码服务商，提供密码咨询服务、密码培训服务、密码应用运营服务等。

根据目前商用密码相关法律法规要求，并非所有企业需要具备商用密码的产品资质，例如对于密码应用集成商及服务商而言，商用的产品资质不是必要条件。

2、商用密码行业的资质门槛要求较高的具体体现

（1）拥有较为全面资质的企业数量相对较少

密码板卡、密码整机等密码基础产品研发的技术门槛高，对企业的综合研发能力有着较高的要求。此外密码产品的资质门槛较高，密码产品检测认证的环节各方面要求较高，密码产品资质证书的获得有一定难度。因此，综合实力较强且研发能力全面的企业才有能力拥有较全面的密码产品资质证书，而商用密码行业中小型密码企业偏多，综合实力较弱，此类企业拥有的密码产品资质证书相对较少。

商用密码应用中通常会用到多种产品组合，产品种类少难以覆盖大多数密码应用场景。密码厂商的商用密码产品资质证书过少，一方面其难以独立自主地开展业务，另一方面也反应其综合技术能力较弱，难以开发出全面的满足用户需求的商用产品。

截至 2021 年 12 月 31 日，全国具备商用密码型号证书产品的企业共 560 家，合计占全国商用密码企业的比例为 46.67%。其中持有 1 个产品证书的企业 255 家，占比为 21.25%；持有 2-4 个产品证书的企业 183 家，占比为 15.52%；持有 5 个及以上产品证书的企业为 122 家，占比为 10.17%。商用密码行业的主要厂商如卫士通、三未信安、江南天安等企业综合实力较强，均拥有 20 个以上证书，属于商用密码企业的前 1.25%。

目前商用密码产品的应用场景为公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域。公司客户在采购商用密码产品时基于相关密码应用技术标准对商用密码产品的合规性要求，一般均会采购经具备资格的机构检测认证合格的商用密码产品。持有 5 个及以上产品证书的企业占全国商密企业的比例为 10.17%，却拥有市场上 66.29%的产品资质，说明商用密码的产品资质主要被综合实力较强的企业所拥有，综合实力较弱的企业拥有密码产品资质较少，反映出商用密码行业的资质门槛较高。具体情况如下：

类型	公司数量	占全国商用密码企业的比例	产品资质数量	占全国产品资质数量的比例
持有 1 个证书	255	21.25%	255	11.57%
持有 2 到 4 个证书	183	15.52%	488	22.14%
持有 5 到 10 个证书	73	6.08%	481	21.82%
持有 11 到 20 个证书	34	2.83%	518	23.50%
持有 20 个以上证书	15	1.25%	462	20.96%
合计	**560**	**46.67%**	**2204**	**100%**

注：根据赛迪发布的报告全国商用密码企业约为 1200 家，此处为便于分析假设为 1200 家。

（2）高安全等级产品的资质要求高，高端产品门槛极高

密码产品的安全等级越高，其自身的安全防护能力就越强，密码产品的安全性就越高，可应用于更高安全等级的网络信息系统，在进行产品资质检测时对产品的各方面要求也更高。目前市场上最高安全等级的三级产品数量仅为 5 个，占比为 0.37%，反映出高安全等级产品的资质要求很高，目前极少有企业可以满足安全等级三级资质的要求。

截至 2021 年 12 月 31 日，市场上安全等级一级、二级、三级的产品共 1356

个，尚无等级四级的产品，具体情况如下：

安全等级	数量	占比
安全三级	5	0.37%
安全二级	982	72.42%
安全一级	369	27.21%

国密标准 GM/T 0028-2014《密码模块安全技术要求》对当前市场上安全等级三级产品的资质要求很高，需要满足以下标准：安全三级在安全二级的基础上要求更强的物理安全机制，以进一步防止对密码模块内敏感安全参数的非授权访问，该等级要求基于身份的鉴别机制，密码模块应当设计有环境保护特性，该等级的密码模块应提供非入侵式攻击缓解技术的有效性证据和测试方法，安全三级的密码模块增加了生命周期保障的要求等。

综上，虽然行业企业数量较多但密码产品的资质门槛较高，其中安全等级三级产品的资质门槛要求则更高，对企业技术实力和产业能力提出了更高要求。

二、申报会计师核查情况

（一）核查程序

申报会计师就上述事项主要履行了以下核查程序：

1、查阅了发行人对应采购协议，获得外购 IP 核的具体内容、协议主要约定等情况；访谈了发行人核心技术人员、研发人员，分析除外购 IP 核之外，密码芯片密码功能的相关核心技术先进性；

2、查阅了密码行业相关技术标准，从商用密码认证业务网等公开渠道查询统计了不同安全等级产品的资质数量，访谈了发行人核心技术人员，分析安全等级与发行人核心技术的对应关系；

3、查阅了发行人代理流片合同、封装合同、采购意向合同等，获取发行人芯片研发相关资料，测算外购 IP 核占发行人产品成本的比例；

4、查阅了行业相关报告，查阅了卫士通官网及年报，查询了密码行业标准的制定情况；访谈了发行人管理层，深入了解商用密码产业规模、企业数量、竞争格局等行业情况。

（二）核查结论

经过核查，申报会计师认为：

1、外购 IP 核之外，发行人密码芯片密码功能的相关核心技术具有先进性；发行人已说明安全等级与核心技术的对应关系；

2、外购 IP 核相关费用占发行人 XS100 芯片产品综合费用成本的比例较低，财务影响较小；

3、发行人专注于密码产品的研发、生产和销售，而行业规模统计数据中除密码产品外还包括密码服务业务，并未区分消费端和服务器端的市场，使得发行人市场占有率较低。随着发行人业务快速增长，发行人与市场龙头卫士通的市场占有率逐步接近。此外，发行人产品的安全等级认证产品数量位于行业前列，发行人通过认证的产品数量位于行业前列，发行人参与制定的行业标准数量位于行业前列，根据 Market Research Intellect 2021 年统计，发行人在全球密码硬件安全市场中位列第九、国内第三，发行人在商用密码产品行业综合实力属于行业前列；

4、商用密码行业企业数量较多，但密码产品的资质门槛较高，安全等级三级产品的资质门槛很高。

（此页无正文，为《立信会计师事务所（特殊普通合伙）关于〈关于三未信安科技股份有限公司首次公开发行股票并在科创板上市的审核中心意见落实函〉的回复说明》之签字盖章页）

立信会计师事务所（特殊普通合伙）

中国·上海

中国注册会计师：

中国注册会计师：

2022 年 5 月 16 日