公司代码:688201 公司简称:信安世纪

北京信安世纪科技股份有限公司 2022年年度报告摘要

第一节 重要提示

1本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到 https://www.sse.com.cn 网站仔细阅读年度报告全文。

2重大风险提示

公司已在本报告中详细阐述公司在经营过程中可能面临的各种风险，敬请查阅本报告第四节 “经营情况讨论与分析”中“风险因素”相关的内容。

3本公司董事会、监事会及董事、监事、高级管理人员保证年度报告内容的真实性、准确性、完整性，不存在虚假记载、误导性陈述或重大遗漏，并承担个别和连带的法律责任。

4公司全体董事出席董事会会议。

5容诚会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

6公司上市时未盈利且尚未实现盈利

□是 √否

7董事会决议通过的本报告期利润分配预案或公积金转增股本预案

2023年4月17日,公司于第二届董事会第二十八次会议审议通过了《关于公司2022年度利润分配及资本公积金转增股本方案的议案》,拟实施权益分派股权登记日登记的总股本为基数,分配利润/转增股本。具体如下:向全体股东每10股派发现金红利人民币3.65元(含税)。截至2023年4月16日,公司总股本137,829,078股为基数计算,合计拟派发现金红利人民币50,307,613.47元(含税),占公司2022年度合并报表归属于上市公司股东的净利润比例为30.69%,不实施送股。公司拟以资本公积金向全体股东每10股转增4.8股。截至2023年4月16日,公司总股本137,829,078股为基数计算,合计转增66,157,957股,转增后公司总股本增加至203,987,035股。如在本次董事会起至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份归属/重大资产重组股份回购注销等致使公司总股本发生变动的,公司拟维持每股现金分红金额不变,相应调整现金分红总额不变,相应调整每股现金分红金额,按以每股转增股数不变,相应调整转增股本总额。

8是否存在公司治理特殊安排等重要事项

□适用 √不适用

第二节 公司基本情况

1公司简介

公司股票简况

√适用 □不适用

公司股票简况				
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称
A股	上海证券交易所科创板	信安世纪	688201	

公司存托凭证简况

□适用 √不适用

联系人和联系方式

联系人和联系方式	董事会秘书(信息披露境内代表)	证券事务代表
姓名	于纯	李明霞
办公地址	北京市海淀区建枫路(南延)6号院2号楼1层	北京市海淀区建枫路(南延)6号院2号楼1层101
电话	010-68025518	010-68025518
电子信箱	ir@infosec.com.cn	ir@infosec.com.cn

2报告期公司主要业务简介

(一)主要业务、主要产品或服务情况

公司以密码技术为基础支撑,致力于解决多种网络环境中的身份安全、通信安全和数据安全等信息安全问题。随着公司研发力量增长,公司的产品已经从密码安全领域拓展到网络安全领域。在信息技术互联网化、移动化和云化的发展趋势下,公司形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列,并积极部署车联网安全、物联网、工业互联网安全等领域的应用安全产品。

具体产品系列服务内容如下表所示。

系列名称	系列简介	名称	简介
身份安全产品系列	身份安全系列产品提供用户的身份信息和认证凭证的全生命周期管理,统一身份认证、单点登录功能,以及系统内硬件设备的安全管理和运维审计,满足各种应用系统对强身份认证及认证授权后统一管理、统一审计等的安全需求。	数字证书认证系统(NetCert)	是公切密码基础设施解决方案的基础支撑系统,由CA数字证书认证系统、RA证书注册系统、KM密钥管理系统、OCSP服务器等组成,能够提供数字证书全生命周期的管理功能,支持X.509 V3/V4标准规范,采用安全的架构设计和权限管理,具备高级别安全机制及完善的管理、配置策略。
		车联网安全认证管理系统(V2X SCMS)	综合采用数字证书、数字签名、匿名化等技术手段,有效保障车载设备(OBU)、路侧设备(RSU)等V2X通信节点的身份合法性,以及通信消息的完整性、机密性抗抵赖性、防篡改和隐私保护。可以为各类V2X终端设备签发符合相关标准的证书及全生命周期管理,提供制作各类BSM及SPDU消息的API,并提供全方位的安全监控及预警功能。
		统一身份认证管理系统(NetAuth)	提供统一身份管理、统一身份认证、单点登录和统一安全审计,实现在一个平台对人员信息、组织信息、应用信息、账号信息的高效统一管理,支持多种身份认证方式,支持单点登录SSO实现一次授权可访问所有应用,满足隐私保护条例等法律法规要求,满足多维度实时审计要求。
		动态密码系统(NetPass)	基于代表身份的密钥,结合时间、事件或挑战信息,生成每隔一段时间变化一次的动态密码(口令),避免静态口令泄漏带来的安全隐患。为用户的合法身份认证提供了简捷、有效的认证手段。
		安全认证网关(NetIAG)	以安全、合规为原则,融合零信任架构理念,提供基于商用密码技术实现的安全认证、网络隐身、动态授权和虚拟门户等安全服务,在全面保障企业应用访问安全性的同时,最大程度简化接入过程,提升企业生产效率。
		统一安全管理及运维审计平台(NetPort)	是集用户管理、授权管理、认证管理和综合审计于一体的集中运维管理平台系统。该平台系统能够为客户提供集中的管理平台,提供全面的用户和资源管理,通过制定严格的资源访问策略,采用强身份认证手段,全面保障系统资源的安全;详细记录用户对资源的访问及操作,达到对运维操作行为全面审计的需要。
通信安全产品系列	通信安全系列产品提供数据传输过程中的访问控制、安全代理加/解密、及性能优化,虚拟私有网络的远程安全接入,WEB通道的安全传输等功能,可以为应用系统打造一个安全、高性能的专属通信空间,提高系统整体的安全性。	应用安全网关(NSAE)	支持基于证书的服务器和客户端身份认证,提供数据在传输过程中的机密性和完整性保护,全面支持SSL/TLS协议,配合产品自带的负载均衡、防火墙、HTTP压缩等功能,为应用系统提供全方位的安全代理和应用加速服务。
		安全互联网关(NetSafe)	基于SSL安全协议实现的安全加密认证通信客户端硬件产品。集成身份认证、SSL安全链接、数字签名、验证签名、日志审计等功能,保证关键数据的数据安全,实现关键数据的防篡改、抵抗赖和数据提供方身份的真实性验证,为企业内部网络和银行、互联网电子商务等应用服务器之间构建安全的Web通道,保证交易数据的安全传输。
		应用交付系统(APV)	具备服务器负载均衡、链路负载均衡、全局负载均衡功能、HTTP压缩和WEB高速缓存等功能的专业硬件设备,帮助用户提高业务应用稳定性和质量,避免服务器宕机或链路故障对业务应用的影响,确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展。
		安全接入网关(AG)	基于SSL安全协议的VPN设备,集成了身份认证、访问控制和资源管理等功能;提供用户接入控制和数据传输的加/解密功能,具备强大的访问控制权限管理、细粒度的审计和日志记录等功能;为用户提供安全、高效、快速、稳定的远程接入方式,实现随时随地的安全访问。
		应用安全防火墙(NetWAF)	采用先进的64位SpeedCore多核处理架构,为关键业务应用提供全面的攻击和威胁的检测与防护。集负向WAF和正向WAF模型于一身,不仅能够检测和防范最新的已知安全攻击和漏洞,还能有效地防范“零日”攻击。可提供精细化的攻击防护控制,支持自动学习和动态防护模板刷新,通过客户端群认证提高攻击识别精度。
		流量编排	通过改变传统安全设备的部署方式,打造网络安全资源池,实现设备与流量的统一调度。该方案以流量编排设备为核心,提供SSL加解密、安全资源池化、流量可视化、自定义流量路径、实时监控等能力,帮助用户解决安全架构难定义、安全资源难调度、防护路径难定义、加密流量难识别等问题,从实际业务度出发,重塑企业安全架构,满足了个性化、差异化的安全流量编排需求,提升企业安全防护能力。
数据安全产品系列	数据安全系列产品用于对电子数据和文档提供数字签名/签章、签名验证,可信时间戳等功能,使得诸如网上交易、公文审批、互联网+政务等需要经办人签名签章才可以办理业务的系统,可以借助于数字签名/签章技术得以在信息系统上开展,并且与传统手写盖章具有同等法律效力。	签名验签服务器(NetSign)	能够对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务,并对签名数据验证其签名真实性和有效性;支持不同CA的用户证书验证,提供CRL/OCSP等多种方式的证书有效性验证。满足用户在网络行为中不可否认、信息完整性、私密性等需求,并提供相关认证交易信息溯源验证。
		电子签章系统(NetSeal)	将传统印章与电子签名技术完美结合,通过采用组件技术、PKI技术、图像处理技术等对电子文档签名并加盖签章,用于辨识电子文档签署者身份,保护文档完整性,防止对文档未经授权的篡改,确保签名行为的不可否认,并实现数字签名的可视化展现。
		可信时间戳服务器(NetTSA)	将经过时间戳服务器签名的一个可信赖的日期和时间与特定电子数据绑定在一起,对外提供精确可信的时间戳服务。通过采用精确的时间源、高强度高标准的安全机制,以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序,为信息系统中的时间防抵赖提供基础服务。
		数据加解密服务系统(NetEDS)	是基于商用密码算法与技术实现的高性能数据安全产品,该产品可提供统一密钥管理、通用数据加解密、数据库加解密等安全服务,用户方业务系统、数据库、云基础设施等通过集成SDK或标准协议,即可与该产品对接,实现概感数据、重要信息的加密保护,从而降低非授权访问或数据泄露带来的安全风险。
		密码模块软件(iSec)	是符合国密相关标准的软件密码模块产品,支持SM2、SM3、SM4商用密码算法及常见国际密码算法,可提供加解密、签名验签名、证书解析等基础密码运算功能,同时可提供TLS/TLCP等安全协议处理能力。
		隐私计算平台(NetPEC)	是一种保护数据隐私的安全计算技术方案,该方案以NetPEC隐私计算平台为核心,以多方安全计算为基础,综合运用同态加密、混淆电路、不经意传输、秘密共享等技术,提供数据加密、安全计算、数据共享、数据授权等多种服务,在满足数据隐私、安全、合规的前提下,实现多机构的联合协同计算、数据融合与联合建模,极大地拓宽了风控、营销和政企互联的覆盖能力,提升挖掘和使用数据要素所蕴含的巨大价值能力,解决数据孤岛和数据隐私保护两大问题,助力金融、保险、政务等领域的数据安全融合与共享流通。
移动安全产品系列	移动安全系列产品构建从移动终端－管道－云的全方位移动安全防护体系,从移动终端客户端数据输入、数据显示、数据存储、数据传递、数据验证等数据全流程进行保护,有效解决移动互联网中身份认证、业务数据完整性、安全传输、防抵赖等问题。	移动统一认证安全管理平台(MAuth)	采用密钥分割、协同签名、大数据分析感知等一系列技术,为移动端提供移动数字证书全生命周期管理及基于移动数字证书的协同签名服务,对移动应用服务提供签名数据验证其签名真实性和有效性;支持不同CA的用户证书验证,提供CRL/OCSP等多种方式的证书有效性验证。满足用户在网络行为中不可否认、信息完整性、私密性等需求,并提供相关认证交易信息溯源验证。
		移动安全中间件(MAuth SDK)	采用密钥分割技术、移动隔离技术,与移动安全认证系统协同,实现在移动终端的密钥、数字证书全生命周期管理及密码运算,解决了加密硬件在移动端使用不便或无法与移动端结合的问题,提升了移动安全解决方案的兼容性和易用性。
		移动安全认证客户端(MAuth APP)	利用移动安全中间件构建的移动安全应用,能够通过“扫一扫”实现PC操作系统(Windows、Linux)或PC上各类应用的用户安全登录,为移动应用开发者和企业管理者提供简单快捷的基于数字证书的双因子认证解决方案;对各类移动应用的电子信息数据、电子文档等提供基于数字证书的协同签名服务,满足移动应用对信息不可否认、信息完整性、私密性等的需求。
云安全产品系列	云安全系列产品以密码技术为核心,将密码应用与云计算技术深度融合,对虚拟化资源池进行统一管理,并实现平台自动化的运维。	密码应用一体化系统(CCypher)	采用密码基融合架构将国密算法、网络、密码整合到同一个系统平台,通过网络设备虚拟化技术和密码卡虚拟化技术,在一台硬件密码设备上实现同时运行多个虚拟化的密码安全设备和安全系统,与云计算管理系统无缝对接,提供云计算环境中身份、数据、通信安全所需IaaS、PaaS以及SaaS级别的密码应用服务。
		密码安全服务管理平台(CSSP-Cloud)	以“密码即服务”为核心理念,在安全、合规的原则基础上,实现密码设备资源池的弹性调度管理、典型密码应用服务的发布与管理、租户化管理与计费等功能的一体化密码云管理平台,可全面覆盖公有云模式、混合云模式、多云架构模式等复杂场景,完美解决用户在业务上云、数据上云过程中所面临的密码应用安全性合规难题。
平台安全产品系列	平台安全系列产品将业务系统所需的各种密码服务进行集中管理,将后台密码资源进行抽象包装整合,转化为前台友好的可复用共享的核心密码能力,同时运用态势感知技术实现系统运行情况的全景展示、监控及预警。	密码安全可视化监管系统(NetCVM)	密码安全可视化监管系统采用B/S架构方式,提供统一、集中的密码应用设备集中监管服务,帮助用户实时监控密码应用设备的状态、密码服务的状态以及代理状态的监控以及密码应用日志的集中审计。
		全密码安全服务平台(CSSP)	利用平台化技术手段实现识别、沉淀和复用密码服务,构建密码服务生态,提供标准化统一的密码服务和管理服务,有效支撑业务系统的快速创新;同时,针对海量安全数据可提供采集、存储、计算、分析等功能,实现对业务、安全中台、设备、系统的全景运行态势展现。
		密评工具箱(iCET)	信安iCET密评工具箱系统是商用密码应用安全性评估工作的一体化专业便携装备,具有测评流程引导和管理、测评工具调用、测评结果分析和报告展示等功能;为测评机构提供了流程引导、数字化管理、以及专业的检测及分析工具。提高了密评工作整体的标准化、合规性和专业性。
服务			公司自有产品的运维服务、安全技术咨询和风险评估,定制开发服务等。

(二)主要经营模式

公司为客户的网络应用提供产品和解决方案,保障在多种网络环境下的身份安全、数据安全和通信安全,同时向客户提供自有产品服务。公司具有完善的研发、采购、生产、销售、服务模式和流程,实现从对经营各环节的有效控制。

1.研发模式

公司坚持“前沿技术驱动创新+业务需求驱动创新”的双轮创新机制,以技术创新为驱动,市场需求为导向进行产品研发,公司以“一院两所三中心”为研发基本建制,设有信息安全研究院、产品部门和测试部门,北京武汉西安等三大研发中心,在软件成熟度模型CMMI L5和ISO9000质量管理体系的规范指引下,建立了完善的研发制度和管理流程。具体职责和分工如下。

信息安全研究院:致力于前沿技术预研、创新业务探索,并解决产品研发中的关键技术问题;

产品部门:对公司产品进行全生命周期管理。根据市场调研结合技术发展,并展需求分析以确定产品方向;把控产品研发的质量和时间节点,通过评审等机制确定产品发布;并不时根据技术发展水平和新需求提出新版本或新产品规划;

测试部门:通过集成测试、自动化测试、安全攻防等系列测试手段,并建立云测平台,在产品研发全过程中保证研发的质量;

研发中心:公司在北京、武汉和西安三地建有研发中心,分别负责不同的产品线或模块,在研发过程中,运用“灏布+迭代”相结合的开发模式,并结合敏捷开发,经过概要设计、系统设计、编码实现等研发流程,实现产品需求;公司设置了研发管理部门,对开发全过程进行严格把控。

2.采购模式

公司采购的主要物料为产品所需的各类硬件设备和配件,包括服务器、加密卡、加速卡等硬件,由供应中心负责公司供应链的管理。

公司建立了独立、完整的供应链体系,包括供应商管理、重要物料招标和采购等环节。

公司定期对供应商进行评估、走访,就供应商资质、以往供货质量、供货规模和交货期等进行评估,并要求供应商符合环保要求,执行RoHS标准,就工序变动通知(PCN)达成一致,符合要求的供应商进入供应商名录,建立稳定的商务合作关系,签订合作框架协议。

为进一步降低成本,公司对用量较大的物料进行年度招标。公司邀请相关供应商就产品性能、供货速度和价格等内容进行投标,并提交相关资料交给产品进行测试,组织评审会,对相关指标打分和评审,确认入围价格和年供货量基准,确定建立稳定的供应关系,持续支持公司业务发展。

公司采购计划以库存预警式为主,订单驱动式为辅,确定批次采购后,通过签订订单、跟踪交期、检验入库、给付货款等环节,来保证供应链正常进行,对不合格物料进行退换货处理,或要求供应商进行整改,直到质量过关恢复供货。

3.生产模式

公司的产品形态主要为软硬一体机,需要将自主研发的软件灌装至硬件设备。

生产环境恒温恒湿,全部铺设防静电地板,按检验区、组装区、包装区和库房划分区域,设置明显标识,生产区域建立了独立的局域网,与外网隔绝,以防病毒和恶意软件攻击。

生产组装工作按生产工序拆分,进行流水作业,并定制了数字化的ERP生产系统,设有仓储条码系统,通过SN条码来定位设备和配件,具有防呆、防错误和追溯功能,组装检测工作过程更精准。

公司建立了包括原材料质量管理、生产过程控制、产成品出入库等方面的全过程质量管理,严格管控生产组装全过程。对采购物料进行质验,合格后方可入库;对软件灌装、组装、调试环节进行过程检验,保证规范操作;对产成品检验合格后方可进入产成品库房。确保产品的质量符合规定要求,保质保量交付至下游客户。

4.营销模式

公司采取“纵向深耕行业,横向拓展区域”的矩阵式销售模式,建立了全国性营销网络。公司在金融、交通、人社、烟草等重点行业销售及技术团队,深刻理解行业需求和特点,针对性地提出行业解决方案,纵向深耕行业;同时设有北京总部和华东、华南、华中、西南、西北、东北六个大区、二十七个省级办事处,为客户提供快速响应服务。

公司充分发挥行业代表性客户、网络应用中心节点的资源优势,打造行业典型应用案例,快速向全国各大区、各办事处拓展,形成覆盖全面、流程完善的营销体系。公司积极联合各细分行业的独立软件开发商(ISV),开展业务合作,拓展细分行业的应用安全业务,并积极各地合作伙伴合作,提升当地业务局势。

公司建立了客户关系管理系统,精准管理客户和销售环节。通过项目立项、技术交流、合同评审与签订、项目实施、交付与验收等一系列活动,及时记录项目进度、接收和处理客户反馈信息,保证对营销活动全周期的良性管理。

5.方案和交付模式

公司在北京总部和六大区、二十七个省级办事处均设立了产品方案中心和服务交付中心,由多年形成的专业化信息安全队伍提供标准化服务,形成了覆盖全国的营销服务网络。

公司的产品方案中心依据信息安全相关技术标准、网络安全等级保护等相关法律法规的规定,结合客户系统的商用密码应用安全性评估情况,凭借对行业应用的丰富案例经验和对该地区的数字化进展的发展程度,针对客户的安全需求和痛点,向客户提供完整先进、贴合应用的产品和解决方案。

公司的服务交付中心遵循ISO9000质量管理、ISO20000IT服务管理标准以及ISO27000信息安全管理体系理念,向客户提供产品交付、质量保障、运行维护等专业化的标准化安全服务。根据客户的具体情况,制定各等级的《技术服务标准》,对重点行业、重点客户提供7*24小时的全天候安全保障、关键时段值守、重点保障、应急处理等金牌安全服务,保证客户业务系统的安全性和连续性。

(三)所处行业情况

1.行业的发展阶段、基本特点、主要技术门槛

根据证监会《上市公司行业分类指引》(2012年修订)及国家统计局《国民经济行业分类》(GB/T 4754-2017),公司所处行业属于“I65 软件和信息技术服务业”;根据国家统计局《战略性新兴产业分类(2018)》,公司所属行业为“新一代信息技术产业”;根据《科创板企业推荐暂行规定》,公司所处行业属于“新一代信息技术领域”。

公司细分行业为基于密码技术的信息安全行业。

(1)行业发展阶段

2022年Q3月,IDC发布了V1版《2022年全球网络安全支出指南》(IDC Worldwide Security Spending Guide),根据市场动态对未来五年(2021-2025)全球网络安全(Cybersecurity)IT投资规模进行了预测。IDC数据显示,2021年全球网络安全相关硬件、软件、服务总投资规模有望达到1,519.5亿美元,预计在2025年增至2,233.4亿美元,五年复合增长率(CAGR)将达10.4%。

IDC数据显示,2021年中国网络安全相关支出有望达到102.6亿美元,在2021-2025的五年预测期内,中国网络安全相关支出将以20.5%的年复合增长率增长,预计到2025年,中国网络安全支出规模将达214.6亿美元。

根据赛迪研究院网络安全研究所2022年11月发布的《2021-2022年中国商用密码行业发展白皮书》,目前我国商用密码法律法规体系基本形成,商用密码标准体系基本完善,商用密码技术产品创新丰富,商用密码产业初具规模。对于我国商用密码行业发展趋势,该报告显示,政策环境持续向好,产业规模快速增长,产业结构加快优化,密码技术与新兴技术加速融合,应用范围不断扩大,应用生态稳步完善。

(2)行业基本特点

商用密码是网络安全的核心技术。商用密码技术可以解决网络环境中的身份安全、数据安全和通信安全等三个基础安全问题,受电子政务、电子商务等数字化社会经济新模式的不断带动,金融、政务等重要领域网络应用不断增长,对网络安全和密码安全的需求也在快速增长,网络空间将形成以密码为核心的安全可控体系。

商用密码应用领域不断扩大。随着更多行业的数字化转型,商用密码的应用领域从金融、财政、烟草、交通、通信、政务等重要应用领域向外拓展,向医疗、教育、农业等新的应用领域拓展。随着云计算、移动互联网、物联网、车联网、工业互联网技术的推进,大量新业态、新应用、新场景不断涌现,针对新技术环境下的数据安全和隐私保护等问题,商用密码的应用机遇在快速增长。

多种技术融合。随着大数据和数字经济时代的来临,数据资产面临的网络环境和攻击手段日趋复杂,现有的密码技术和数据安全手段需要和多种新技术的结合,像安全多方计算、同态加密、可搜索加密、联邦学习、隐私计算等,数据共享安全和隐私保护,为数字经济新时代注入新的发展动力。

国产化进程在加速。网络安全作为国家战略的一部分,在国产密码算法及国产化技术已经成熟的条件下,基于国产商用密码算法的产品和相关国产软硬件的结合已经成为趋势。发展信创是国家战略,解决本质安全的问题。信创产业发展已经成为经济数字化转型、提升产业链发展的关键,密码应用安全产品需要和各类国产硬件平台、国产操作系统、国产数据库和中间件等进行适配,形成全国产化的产品,才能满足信创的要求。

政策鼓励和合规监管。近年来,国家高度重视网络空间安全及密码安全领域,国家和相关部委出台了多个政策,以密码为核心的信息安全相关法律法规体系逐步完善。

依据《中华人民共和国密码法》《网络安全等级保护条例(征求意见稿)》《国家政务信息化项目建设管理办法》《商用密码应用安全性评估管理办法(试行)》等法律法规,国家密码管理局会不定期发布商用密码应用安全性评估机构名单,由密评机构对关键信息基础设施、网络安全等级保护第三级及以上信息系统进行定期评估,保证网络空间安全。

序号	名称	发文单位	日期
1	《中华人民共和国网络安全法》	全国人大	2017-06-01
2	《中华人民共和国电子签名法(修正案)》	全国人大	2019-04-23
3	《中华人民共和国密码法》	全国人大	2020-01-01
4	《商用密码管理条例(征求意见稿)》	国家密码管理局	2020-02-20
5	《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》	公安部	2020-07-01
6	《密码应用与安全性评估指导性文件》	国家密码管理局	2020-12-08
7	《中华人民共和国数据安全法》	全国人大	2021-09-01
8	《关键信息基础设施安全保护条例》	国务院	2021-09-01
9	《中华人民共和国个人信息保护法》	全国人大	2021-11-01
10	《证券期货业网络安全管理办法(征求意见稿)》	中国证监会	2022-4-29
11	《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》	工业和信息化部	2023-01-03

主要技术门槛

1)专业技术门槛

PKI体系(Public Key Infrastructure,公开密钥基础设施)是密码技术的基础,该体系不属于计算机及信息行业的通用技术,不为大众所熟知,研发基于密码技术的信息安全产品,首先需要对PKI体系有较深入的理解,包括对理论基础的理解以及实践经验的积累,结合安全需求和以用基本场景,才能研发出较高安全性的产品。

随着信息技术产业的持续发展和完善,研发安全产品除了需要通用软件技术外,还需要和其他软件或密码相关硬件结合的技术,才具有较强的软硬件适配能力;密码产品需要适应云计算、移动互联网、物联网、车联网、工业互联网等多种业态,在技术上要结合区块链、大数据、人工智能等技术,结合零信任、安全多方计算、同态加密、可搜索加密、联邦学习、隐私计算等多种密码安全技术,符合行业技术发展要求。

2)行业应用门槛

网络应用安全产品总是和网络应用场景、应用行业相关,产品和解决方案设计者需要了解和贴近行业的应用,才能有效地解决应用的身份安全、数据安全和通信安全这三个基础安全问题。对行业的理解是一个探索、积累、再探索的过程,需要多个不同行业积累的机会和经验,才可能具备行业应用能力,适合在各类行业快速拓展。

3)产品资质门槛

根据《密码法》的第二十五条规定,“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”。商用密码生产单位应根据产品确认证各类,并向具备资格的机构提交密码模块等级的申请,经过资料审查、型式试验、工厂检查等过程,确认产品的安全性和持续生产保障能力,方可获得产品认证资格,在获证的五年有效期内,应接受管理部门的不定时证后监督检查。

根据《计算机信息系统安全专用产品检测和销售许可证管理办法》第三条的规定,“中华人民共和国境内的安全专用产品进入市场销售,实行销售许可证制度。安全专用产品的生产者在其产品进入市场销售之前,必须申领《计算机信息系统安全专用产品销售许可证》(以下简称销售许可证)”申请单位将样品送指定检测机构进行检测,检测合格后,按规定提交证书申请的相关材料,经审批通过后,方可获得相关产品的销售许可证。

2.公司所处的行业地位分析及其变化情况

作为国内较早从事密码产品和解决方案研究、生产和销售的公司,公司在科研、研发、市场等方面持续投入,不断提升经营业绩和企业影响力,推动行业发展,成为行业领先者。

(1)科研地位

公司已累计牵头或参与了《GB/T 25069-2022 信息安全技术 术语》《信息安全技术 大数据服务安全能力要求》等14项国家标准的编写工作;

公司已累计牵头或参与了《GM/T 0118-2022 浏览器数字证书应用接口》《GM/T 0122-2022 区块链密码检测规范》等48项行业标准的编写工作;

公司申报的国家级课题(面向海峡两岸多源数据安全与隐私保护理论及关键技术研究)已经入选2021年度国家自然科学基金联合基础项目;

公司参与创建跟北省区块链技术创新研究院,致力于对区块链核心关键技术的研究,以解决区块链实际应用的系列关键问题。

(2)研发能力

公司已获得美国软件工程学会(Software Engineering Institute,SEI)软件成熟度模型CMMI-Level5最高级别认证,标志着公司在研发能力、规范化管理等方面都是达到了国际先进水平,可有效控制进度偏差、提升开发效率、控制开发成本、提升产品质量和客户满意度。

公司参与的工信部工业互联网创新发展工程《工业互联网商用密码应用公共服务平台项目》已成功验收。

公司拥有自主创新的独立知识产权,已获得208项软件著作权书和154项专利(其中发明专利134项)。

公司的密码产品均取得了商用密码产品认证证书,并全系列通过信创适配,满足国产化要求。

(3)市场地位

在安全牛发布的“2022中国网络安全企业100强”榜单中,从企业经营、技术创新、行业应用和信创能力四大维度综合评比,公司位列百强第18位;

《汽车企业OTA升级密码安全创新应用方案》获数字中国建设峰会2022数字中国创新大赛网络安全赛道－车联网安全赛一等奖;

凭借《基于鲲鹏的一体化移动安全认证解决方案》,在2022鲲鹏应用创新大赛河南赛区荣获数字政府赛道一等奖,全国总决赛荣获科技金融赛道优胜奖,作为华为鲲鹏生态圈的紧密合作伙伴,并分别在河南、湖北地区荣获最佳实践伙伴奖以及武汉云优秀生态伙伴奖。

公司组织“源信至安”《自盒SM4算法》获得2022年“金融密码杯”全国密码应用和技术创新大赛团队三等奖。

公司的《以密码技术构筑零信任安全架构解决方案》《车联网安全认证解决方案》《全球化物联网设备制造商数字认证安全方案》《贵州省水库工业控制系统密码应用案例》分别入选“2022安全样板工程”的零信任板块、身份安全板块、密码安全板块和工业互联网安全板块。

报告期内公司在商密市场、网信自主创新、身份治理与管理等方向完成4个行业报告的参编;

公司在北京商用密码协会、江苏商用密码协会等四个商用密码协会担任副会长职务,并在国家密码行业标准化技术委员会和全国信息安全标准化技术委员等机构担任专家,担长职务,全力推动密码事业的发展。

3.报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

密码及信息安全技术快速发展。随着网络安全和密码安全行业的快速发展,零信任等技术已经进入成熟期,在相关产品和解决方案中发挥重要作用,并持续增强零信任产品能力,成为身份安全重要技术保障;隐私计算、动态防御技术等作为新兴技术也正在被快速整合到相关网络安全和密码安全产品中,以应对更复杂的网络环境和数据安全需求。

云计算带来了安全需求。随着云计算技术逐渐成熟,各类基于云计算的网络应用也在持续增长中,如大型企业的业务上云,各地政府的办公系统上云等,云计算催生的直接安全需求,以及由于密评机制催生的云计算安全需求也在快速增长,云安全的相关产品需求上升。

国产和信创迫机会。作为国家安全战略的一部分,网络安全产品的国产化要求越来越高,金融行业和央企等行业纷纷提出信创的规划,安全厂商需要将自有产品和各类硬件平台或相关软件进行适配,以保证客户的国产化需求,充分保障安全。

数字化转型和密码机会。随着国家“十四五”数字经济发展规划的发布,各行业也在加快信息化作局和数字转型工作,并针对性地提出了对应的安全需求。国家密码管理部门也按照指定密评企业,对密码应用进行评估,推动了商用密码行业的需求和发展。

3公司主要会计数据和财务指标

3.1近3年的主要会计数据和财务指标

单位:元 币种:人民币

	2022年	2021年	本年比上年增减(%)	2020年
总资产	1,328,770,448.71	1,208,653,633.15	9.94	589,817,834.38
归属于上市公司股东的净资产	1,152,821,656.32	1,026,425,727.79	12.31	422,918,177.14
营业收入	658,076,109.27	524,604,415.42	25.44	416,302,460.58
归属于上市公司股东的净利润	163,924,540.37	154,126,856.05	6.36	107,307,245.67
归属于上市公司股东的扣除非经常性损益的净利润	155,548,322.01	142,967,479.91	8.80	101,725,587.48
经营活动产生的现金流量净额	72,870,758.88	93,935,530.17	-22.42	101,386,559.11
加权平均净资产收益率(%)	15.88	17.98	减少2.10个百分点	26.74
基本每股收益(元/股)	1.1893	1.2199	-2.51	1.5363
稀释每股收益(元/股)	1.1883	1.2199	-2.59	1.5363
研发投入占营业收入的比例(%)	20.32	19.15	增加1.17个百分点	19.60

3.2报告期分季度的主要会计数据

单位:元 币种:人民币

	第一季度(1-3月份)	第二季度(4-6月份)	第三季度(7-9月份)	第四季度(10-12月份)
营业收入	64,012,858.89	106,557,709.99	140,647,930.94	346,857,609.45
归属于上市公司股东的净利润	-1,565,047.52	26,861,562.93	29,121,245.69	109,506,779.27
归属于上市公司股东的扣除非经常性损益后的净利润	-3,063,064.28	23,365,702.37	28,935,823.54	106,309,860.38
经营活动产生的现金流量净额	-34,299,951.49	-19,572,898.64	-32,356,328.10	159,099,937.11

季度数据与已披露定期报告数据差异说明

□适用 √不适用

4股东情况

4.1普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前10名股东情况

单位:股

截至报告期末普通股股东总数(户)	4,485
年度报告披露日前上一月末的普通股股东总数(户)	5,194
截至报告期末表决权恢复的优先股股东总数(户)	0
年度报告披露日前上一月末表决权恢复的优先股股东总数(户)	0
截至报告期末持有特别表决权股份的股东总数(户)	0
年度报告披露日前上一月末持有特别表决权股份的股东总数(户)	0

前十名股东持股情况

股东名称(全称)	报告期内增减	期末持股数量	比例(%)	持有有限售条件股份数量	质押、标记或冻结情况		股东性质
					股份状态	数量	
李伟	11,232,000	34,632,000	25.13	34,632,000	34,632,000	无	境内自然人
王晓心	4,176,000	12,876,000	9.34	12,876,000	12,876,000	无	境内自然人
丁纯	4,176,000	12,876,000	9.34	12,876,000	12,876,000	无	境外自然人
天津恒信世安企业管理咨询合伙企业(有限合伙)	2,880,000	8,880,000	6.44	8,880,000	8,880,000	无	其他
东方证券股份有限公司-中庚价值先锋股票型证券投资基金	3,510,450	4,172,079	3.03	0	0	无	其他
杭州雅思捷商股权投资合伙企业(有限合伙)	396,026	3,975,839	2.88	0	0	无	其他
北京恒信同安信息咨询合伙企业(有限合伙)	1,137,446	3,507,127	2.54	3,507,127	3,507,127	无	其他
上海浦东发展银行股份有限公司-中欧创新未来18个月封闭运作混合型证券投资基金	2,851,592	2,851,592	2.07	0	0	无	其他
中国建设银行股份有限公司-中欧电子信息产业沪港深股票型证券投资基金	3,172,778	2,238,954	1.62	0	0	无	其他
北京恒信庆安企业管理咨询合伙企业(有限合伙)	700,851	2,160,957	1.57	2,160,957	3,507,127	无	其他

上述股东关联关系或一致行动的说明 李伟、丁纯、王晓心为一致行动关系,其他未知。

表决权恢复的优先股股东及持股数量的说明 无

存托凭证持有人情况

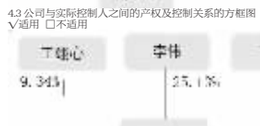
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

4.2公司与控股股东之间的产权及控制关系的方框图

√适用 □不适用

4.3公司与实际控制人之间的产权及控制关系的方框图

√适用 □不适用