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

2021 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http://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

根据容诚会计师事务所出具的审计报告,截至2021年12月31日,公司单体报表未分配利润为290,413,075.80元,合并报表未分配利润为282,659,202.24元,按照单体和合并报表未分配利润取低原则,可供分配利润为282,659,202.24元。经董事会决议,公司2021年年度拟以实施权益分派股权登记日登记的总股本为基数分配利润。本次利润分配预案如下:

公司拟向全体股东每10股派发现金红利5.00元(含税),截至2022年4月10日,公司总股本93,127,756股,以此基数合计拟派发现金红利人民币46,563,878元(含税),占公司2021年度合并报表归属于上市公司股东的净利润比例为30.21%,不实施送股和资本公积转增股本。

如在本公告至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份回购注销/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,公司拟维持分配总额不变,相应调整每股分配比例。如后续总股本发生变化,将另行公告具体调整情况。

本次利润分配预案议案所需公司2021年年度股东大会审议通过。

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	不适用

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	丁纯	李明霞
办公地址	北京市西城区宣武门外大街甲1号环球财讯中心C座4层	北京市西城区宣武门外大街甲1号环球财讯中心C座4层
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

公司是国内领先的信息安全产品和解决方案提供商,以密码技术为基础支撑,致力于解决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。

公司的产品和解决方案应用于金融、政府和企业等重要领域。在金融领域,公司的产品和解决方案保障了网上银行、数字货币、跨境支付、证券登记结算、电子保单等重要金融业务系统的安全;在政府领域,公司的产品和解决方案已经应用于交通、人社、烟草、海关、税务、政法等数十个行业;在企业领域,有超过七成的中国百强企业是公司服务的客户。

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。公司产品和服务的具体情况如下:

系列名称	系列简介	产品名称	产品简介
身份安全产品系列	身份安全系列产品提供用户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,认证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信息统一管理、统一审计等的安全需求。	证书认证系统(NetCert)	是公钥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,配置简易。
		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,实现在一个平台对入员信息、组织信息、应用信息、服务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(NetToken)	基于代表身份的密码,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。
		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。
		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、机密性和抗重放性,满足V2X网络安全的需求。该系统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管理功能。
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问题控制,安全代理加/解密、发性能优化,重拟有网络的应用安全,WEB通道的安全构建等功能,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(NSIAE)	可实现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,配合产品目带的负载均衡、防火墙、HTTP压缩等功能,为应用系统提供全方位的安全性可靠性用途服务。
		应用交付系统(NetApp APV)	具备强负载均衡能力和、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,帮助用户提高服务应用程序性能速度,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持续、安全、可靠地交付以及投资回报。
		SSL VPN网关(NetGate/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,相应配置的审计日志记录等功能;为用户提供安全、高效、便捷、稳定的远程接入方式,实现便捷随时随地安全办公。
		安全互联网关(NetSide)	基于SSL安全协议实现的安全加密认证通信系统,可以提供用户端硬件产品、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、抗抵赖和数据提供方身份真实性验证,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。
		应用安全防火墙(NetWAF)	采用先进的04层ipoeDoes多模处理架构,为关键业务应用提供全面防攻击威胁的能力,集合网络WAF和应用WAF模型于一身,不仅能够检测和防范最新的已知安全攻击漏洞,并且能实时、有效地防御未知的、高级别的应用安全攻击威胁,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新增,通过客户端嵌入证提高攻击识别精度。
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安全存储、安全共享、可信时戳服务等需要经办人员名签章才可以办理业务的系统,可以彻底杜绝纸质文件的丢失、篡改、抵赖等问题,提高业务效率,可以在信息系统上开展,并且与传统手写签章具有同等法律效力。	签名验签服务器(NetSign)	依照对称和非对称算法,为客户创造数据安全、可信、可靠、可追溯的数字签名服务,并对签名数据验证其签名真实性和有效性;支持多种国内外用户证书验证,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同方认、信息完整性、抵赖性等需求,并提供相关认证及信息服务。
		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戳,保证数字证书的有效性,以确认系统处理数据在某一时间段存在性和相关操作的相对时间顺序,为信息系统中的时间数据提供基础服务。
		电子签章系统(NetSeal)	将传统印章与电子签名技术完美结合,通过采用椭圆技术、PKI技术、摘要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效果。	
		密码模块软件(iSec)	基于国家密码管理局发布的密码应用标准GM/T0028、GM/T0054、GM/T0016、GM/T0018等密码算法及常见国际密码算法,可提供加解密、签名验签、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。	
移动安全产品系列	移动安全系列产品构建从移动终端、移动应用、移动数据、数据验证等数据全流程进行保护,有效解决移动互联网应用移动设备、安全传输、数据验证等数据安全问题。	移动安全认证系统(MAuth)	采用密钥分散、协同签名、大数据分析感知等一系列技术,为移动端提供动态密钥安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,满足移动应用的基于数字证书的强身份认证、安全传输及抗抵赖性等安全需求,迅速提升移动互联网应用的信息安全的护盾力。
		移动安全中间件	采用密钥分散技术、移动端混淆技术、与移动端安全模块协同,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,解决了如需使用在移动端使用不便或无法与移动端安全模块协同的问题,提升了移动安全解决方案的兼容性和易用性。	
		移动认证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,为企业内部应用的电子信息数据、电子文档等提供安全、可信、可追溯、可抗抵赖的安全防护能力。	
		移动数字证书APP	利用移动安全中间件构建的移动安全应用,根据相关国家密码管理局发布的密码算法,提供基于移动端的数字证书全生命周期管理及密码运算,帮助用户实现移动端的数字证书管理、数据加密、数据签名、数据完整性校验、数字证书信息查看、证书有效性校验、证书吊销列表查看、证书解析、证书导入、证书导出、证书删除、证书口令修改、证书口令重置、证书口令解锁、证书口令校验、证书口令强度设置、证书口令重置方式设置、证书口令重置次数设置、证书口令有效期设置、证书口令重置提示天数设置、证书口令校验方式设置、证书口令校验次数设置、证书口令有效期提示天数设置、证书口令强度校验、证书口令重置方式校验、证书口令重置次数校验、证书口令有效期校验、证书口令重置提示天数校验、证书口令修改方式设置、证书口令修改次数设置、证书口令修改有效期设置、证书口令修改提示天数设置、证书口令修改方式校验、证书口令修改次数校验、证书口令修改有效期校验、证书口令修改提示天数校验、证书口令解锁方式设置、证书口令解锁次数设置、证书口令解锁有效期设置、证书口令解锁提示天数设置、证书口令解锁方式校验、证书口令解锁次数校验、证书口令解锁有效期校验、证书口令解锁提示天数校验、证书口令强度校验方式设置、证书口令强度校验次数设置、证书口令强度校验有效期设置、证书口令强度校验提示天数设置、证书口令强度校验方式校验、证书口令强度校验次数校验、证书口令强度校验有效期校验、证书口令强度校验提示天数校验