

苏州国芯科技股份有限公司

关于公司与中云信安（深圳）科技有限公司合作研发的抗量子密码金融 POS 机芯片新产品内部测试成功的自愿性披露公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

近日，苏州国芯科技股份有限公司（以下简称“公司”）与中云信安（深圳）科技有限公司（以下简称“中云信安”）合作研发的抗量子密码金融POS机芯片CUni360SQ-ZX新产品在公司内部测试中获得成功。现将相关事项公告如下：

一、新产品的基本情况

公司与中云信安合作的抗量子密码金融POS机芯片CUni360SQ-ZX是基于国产40nm工艺制程进行研发，采用公司自主CPU内核设计的一款低功耗抗量子密码金融POS机芯片。该芯片的典型工作功耗和静态低功耗可分别低至150mW和0.16mW左右，芯片内集成了抗量子密码算法、公钥密码算法、对称密码算法和杂凑密码算法等引擎。抗量子密码算法引擎支持NIST抗量子密码算法标准中基于格原理的用于密钥封装的ML-KEM算法以及用于签名的ML-DSA算法。公钥密码算法引擎支持RSA/SM2/ECC等传统的公钥密码算法。对称密码算法引擎支持DES/AES/SM4/SM1等算法。杂凑密码算法引擎支持SHA2/SHA3/SM3等算法。芯片内置真随机数发生器，并具有电压检测、温度检测、频率检测、电源毛刺检测、光检测和金属防护网等多种安全防护设计。芯片支持免晶振USB接口、SSI/SPI接口以及UART、IS07816、I2C等必要的外设接口。片内集成的PCI模块支持8路防拆接口，可配置为动态或静态检测模式。芯片具备低功耗、高安全性以及高扩展性特点，可广泛应用于金融POS和物联网终端的安全领域。

2025年5月29日，国际PCI安全标准委员会（PCI安全标准委员会（PCI SSC），是保障全球支付卡交易安全的核心国际组织）颁布了PCI PTS 7.0标准，正式将抗量子算法列入PCI要求，金融POS机等终端将有望成为国际上抗量子密码技术较

早实际规模应用的领域。

针对上述PCI安全标准委员会颁布PCI PTS 7.0标准的新情况，公司联合中云信安设计了支持抗量子密码算法的CUni360SQ-ZX芯片。CUni360SQ-ZX芯片可以同时支持抗量子密码算法和传统密码算法应用，采用CUni360SQ-ZX芯片的终端产品可以通过抗量子密码算法和传统密码算法共存方式，逐步进行抗量子密码算法应用迁移，在保障原有业务不受影响的情况下开展抗量子密码算法在新业务中应用，既满足现有业务系统密码应用，又能有效抵御量子计算攻击，从而增强安全产品或设备抗量子计算攻击的能力，实现产品的安全防护能力从传统密码防护向抗量子密码防护的跃升。

二、对公司的影响

公司与中云信安对上述新的芯片产品共同拥有产权。本次公司与中云信安在行业内率先成功研发抗量子密码金融POS机芯片新产品，是公司在量子安全领域长期坚持创新驱动的结果，实现了公司安全芯片产品的抗量子化提升，增强了公司在金融安全领域产品的竞争力，进一步完善了公司信创与信息安全芯片产品在金融领域的布局，将为金融等领域抗量子密码技术的迁移提供技术支撑，对公司未来市场拓展和业绩成长性预计将产生积极的影响。

三、风险提示

本次测试目前是公司内部测试成功，尚未完成第三方机构检测测试。本次公司与合作方中云信安共同推出抗量子密码金融 POS 机芯片新产品尚处于市场导入初期，尚未实现规模化销售，存在检测标准变化、市场推广与客户开拓不及预期、客户验证失败等风险，将对公司收入及盈利带来不确定性，公司将及时根据后续进展履行信息披露义务，敬请广大投资者注意投资风险。

特此公告。

苏州国芯科技股份有限公司

董事会

2025年12月9日