从合规到核心：密码技术如何成为企业数字安全的战略资产

徐沛东
自然资源部信息中心　北京　100812

摘　要：数字化时代密码技术不仅仅是一种企业的合规要求，更是保证企业数据安全、推动企业业务创新、提高企业市场竞争力的一种战略资产。企业要把密码技术由IT成本中心变成保证业务连续性、构建市场信任的关键要素。通过构建统一的密码管理体系，将密码技术深度融入业务场景，并借助智能化运维与自动化手段，提升企业的安全水平与运营效率。企业未来将面临量子计算、技术复杂性与智能化运维等关键挑战，应该提前制定对策，把密码技术和人工智能、物联网等前沿科技结合起来，创建起动态安全数字信任架构。

关键词：密码技术；数字安全；业务创新；量子计算

引言

在数字化的推动下，数据成了企业最核心的资产。大数据、云计算、物联网等技术迅猛发展的同时，企业遇到的数据泄露、网络攻击、身份盗用等安全问题变得越发严峻。然而，许多企业在应对数字安全挑战时，仍仅将密码技术视为一项合规要求，未能充分认识到它在保证数据安全、促进业务创新和增强市场竞争力方面的战略作用。密码技术作为数字世界里的信任基石、安全根基，早已不是合规的工具，而是支撑企业可持续发展、数字转型的关键战略资源。

目前大多数企业对密码技术的投入还比较少，常常把其看作一种“合规负担”。这类企业仅将密码技术的应用视作满足法规要求的手段，未能充分认识其对商业运作可能产生的深远影响[1]。在许多情况下，密码管理仍然存在部门各自为政的孤立系统，缺少统一的战略规划与集中管理。分散化的管理方式使密码技术不能形成合力，无法在保障数据安全、提高运营效率、促进业务发展方面起到应有的作用。

随着全球数字经济的发展，数据作为最重要的生产要素的地位越来越突出，密码技术的战略价值也越来越明显。在此情况下，企业应该从合规的角度出发，全面提高密码技术的战略价值。密码技术不仅是数据安全防线的核心，也是数字经济发展的关键支撑，可以带动数据流通和变现，保证企业信誉，为商业创新和市场信任提供坚实支撑。利用密码技术，企业可以创建完善的数据确权、数据安全保障体系，提高数据资产流动性以及可信度，为业务创新、市场信任与客户隐私保护提供支撑。企业必须认识到，在新的环境下，密码技术的价值就是，它不单是IT成本中心的一部分，更应该是企业数字安全的战略资产，深度融入业务流程和战略决策中[2]。保证业务的连续性、提高市场竞争力、形成企业的市场信任品牌。

一、战略基石：解构密码技术的三层价值体系

密码技术的价值不仅仅体现在保障数据安全，它在企业数字化转型中扮演了更加多元和复杂的角色。随着技术的进步，密码技术已不再局限于传统的安全防护工具，而是深入到企业的各个层面，成为支撑数字化转型、推动业务创新的重要战略资产。因此，密码技术的价值具有多维度、全方位的影响，涉及基础的安全保障、业务赋能以及商业创新三个层次。以下将从这三个层次出发，详细探讨密码技术为企业带来的长期价值。

1.安全保障价值

密码技术的核心功能在于为企业提供基础的安全保障，保证数据的机密性、完整性、可用性以及不可否认性。这些基本的安全要素是建立数字化安全体系的基础，也是其他所有安全技术能够发挥作用的前提[3]。机密性保证只有授权人员可以访问敏感信息，完整性保证数据在传输和存储过程中原始状态不被篡改，可用性保证数据在需要的时候能够及时获取，不可否认性用数字签名、时间戳等技术来保证信息的来源不可否认，防止数据伪

作者简介：徐沛东（1990），男，汉族，江苏省，工程师，硕士，网络安全和密码学。

造或者篡改。对企业而言，确保这些安全要素能够有效降低信息泄露、数据篡改及系统遭受攻击等风险，保证企业业务正常合法进行。在全球信息化进程加速的背景下，数据泄露事件屡见不鲜，企业正依赖密码技术构筑起坚固的“防线”，以此来保护最宝贵也是最容易受到侵害的商业资源——数据。

2.业务赋能价值

伴随着企业数字化转型的深入，密码技术的作用也由单纯的保护功能向业务赋能拓展。尤其在零信任架构的部署过程中，密码技术显得尤为重要。零信任架构的核心理念就是“不信任，始终验证”，它的实现依靠的是基于数字证书的强身份认证机制。传统的网络安全防御模型把内部网络视为可信的，只有外部访问者才需要认证[4]。而在零信任模式下，每一个用户、每一个设备的访问权限都必须经过严格的验证，无论其处于内网还是外网，都需要密码技术的强力支持。除此之外，密码技术对于数据合规与开放也有着重要的作用。比如根据《中华人民共和国数据安全法》等有关法规的要求，企业需要用加密、脱敏等技术手段保证敏感数据在存储、传输和处理过程中安全。此举既能满足合规性要求，又能在合规框架下充分释放数据的商业价值。

3.商业创新价值

随着区块链、数字身份、隐私计算等新技术的发展，密码技术的创新应用不断深入，已经成为企业商业创新的引擎。数字签名被广泛运用于电子合同、电子票据等无纸化交易中，大大提高了交易效率和安全性，促进无纸化办公及智能合约的发展[5]。密码技术给区块链等去中心化技术赋予核心支撑，保障区块链网络内交易数据的安全以及不可篡改，为数字货币、智能合约等创新应用提供了可信的安全基石。未来密码技术同隐私计算、数字身份等技术的融合，将会构建起更为繁杂且多变的安全保障体系，从而给企业创造更为宽广的商业创新天地。

二、实战蓝图：构建企业级密码能力的三步走路径

从理论和战略层面明确了密码技术的重要性之后，企业如何将密码技术落地，构建适合自身业务发展的密码安全体系，是实现其战略目标的关键。建设企业级密码能力，不单单是技术问题，更是对企业运营模式、管理体系、业务发展战略的深度整合。为了保证密码技术同企业各项需求有效对接，企业可以从统一架构、深度融合、智能运维三个方面逐步推进，形成全面、系统的数字安全防护能力。

1.统一架构，集中管理

企业要打破各部门各自为政的局面，建立统一的密码服务平台或者密钥管理系统，实现跨部门的集中化管理。通过集中管理可以优化企业的密码资源配置和调度，减少管理成本，提高安全性，防止由于各个部门密码管理不善造成的安全漏洞。其中的关键工具之一是硬件安全模块（HSM），它可以保证核心密钥的物理安全，防止密钥泄露或者被盗取[6]。HSM不仅是密钥存储的安全堡垒，也是执行密钥生成、加解密、签名验证等操作的核心组件，给企业的密码体系以有力的硬件支撑。利用HSM可以加强密钥生命周期的管理，提高加密操作的效率和安全性，保证敏感数据得到全面的保护。

2.深度融合，场景驱动

企业应依据具体的业务场景，将密码技术融合进去以提高安全水平。在云计算与数据中心环境中，企业对敏感数据需采取“默认加密”策略，即对数据库、大数据平台以及备份数据的加密存储和传输，从而达到防止数据在传输过程中泄露、篡改的目的。远程、移动办公环境下，传统的静态密码已经不能满足安全的要求，企业应该全面部署基于数字证书的VPN和应用访问，保证员工访问企业系统时身份能够被认证，数据通过加密的通道传输。企业还应该采用数字签名技术对代码进行签名，以保证代码在开发、分发、执行过程中的完整性，防止恶意软件被注入或者篡改[7]。此类密码技术的深度应用，有助于构建全方位的安全防护体系，从而提升企业的整体安全水平。

3.智能运维，价值度量

密码技术的运维包含密钥管理及加密算法更新，也包含密码服务的监控、审计和自动化运维。通过建立自动化运维体系，企业能够显著减少因人为因素导致的操作失误，加强系统反应速度和可靠性。密钥轮换、策略下发等操作可实现自动化，从而提升安全性并简化管理流程。自动化系统可以对密码技术进行实时的监控，发现潜在的安全风险并作出及时反应，减少漏洞和安全事件的发生。企业对密码技术的价值度量不能只看是否通过密评，还要对密码技术在降低风险、提高效率、推动业务赋能等方面的实际效果进行评价[8]。通过加密技术降低的数据泄漏风险，不仅能帮助企业规避潜在损失，更能转化为其市场竞争优势；通过数字签名提高的交易效率，则为企业创造了更多的商业机会，从而促进业务

的发展。

三、前瞻视野：应对未来挑战的战略准备

虽然密码技术在目前阶段已经成为企业数字安全的主要支撑，但随着数字化转型的深入推进，密码技术在企业中的应用也面临着一些新的挑战和复杂问题。特别是在技术的不断演进、应用场景的多样化以及外部环境的变化下，企业必须积极应对以下几个主要问题，才能确保密码技术在未来的有效性和安全性。

1.量子计算威胁

量子计算的发展对传统密码算法构成了严峻挑战。随着量子计算机计算能力的不断提升，目前使用的加密算法，特别是广泛使用的RSA、ECC等公钥加密算法，在量子计算面前可能会失去安全的保障。量子计算可借助Shor算法等方法，快速破译传统公钥加密系统，从而引发严重的数据安全问题[9]。因此，企业必须重视量子计算技术的发展，并积极跟踪量子密码学的发展动态。提前规划密码算法迁移路线，评价量子密码算法的适用性，是企业应对未来量子威胁的重要工作。企业应开展量子安全的前瞻性研究，与学术界和技术公司合作，共同研发并测试量子抗性加密算法，为将来可能出现的技术变革做好充分的准备。

2.技术复杂性

随着密码技术的发展，牵涉的技术领域变得越来越复杂，很多企业，尤其是中小企业，会遇到较大的技术门槛。这些企业由于资源缺乏、专业技术能力不足等原因，很难创建并运行复杂的密码系统。企业可以采用密码即服务等手段来解决这一难题。企业通过同云服务提供商合作，可以将密码技术的管理外包出去，简化技术的实现过程，降低技术运维的复杂度。既可以降低企业技术实施的压力，也可以为企业提供弹性、安全、易于扩展的密码服务，使企业在技术变革中保持灵活性、适应性[10]。与此同时云服务商会给企业提供更好的安全保护措施，可以利用云服务先进的安全技术、服务网络和自动化运维的能力来提高安全性和管理效率。

3.未来方向

未来密码技术会更多地同人工智能、物联网这些前沿技术融合起来，形成一个更加智能化的、动态的、自适应的安全防护体系。人工智能的应用在安全领域将起到越来越大的作用。人工智能（AI）可对网络流量进行实时监控，发现潜在安全威胁，并及时响应应急事件。此类系统能够运用深度学习算法识别异常行为与入侵迹象，进而自动调整密码策略、优化密钥管理方式，从而提升系统安全性。随着物联网设备的普及，企业面临的新挑战在于如何确保海量设备间的安全通信。传统的密码技术对于海量设备的身份认证、密钥管理、数据加密等可能会遇到瓶颈，所以需要发展更高效、可扩展的密码管理体系。密码技术可用以保护交易安全，但也可能被滥用以损害竞争。密码技术滥用行为有拒绝提供密码、限制密码技术相关商品或服务的使用条件、限制密码重置、拒绝提供解码服务、破坏密码技术相关商品或服务等形式。对于密码技术滥用行为，不应完全按照传统的垄断行为类型进行认定，还应考虑密码技术滥用行为的特殊性，乃至将其认定为一类新型垄断行为。须理清密码技术保护的商品或服务、密码技术、密码技术影响的其他商品或服务之间的关系，分析密码技术滥用行为究竟是传统的垄断行为还是新型垄断行为，密码技术应用是否产生封锁效应，是否带来用户转移成本，是否存在排除反垄断法适用的正当理由等，特别是安全、产品功能需要、效率、知识产权保护等因素，进而对密码技术滥用行为进行定性并加以反垄断法规制处理。

结论

在数字化时代，企业既是密码技术的使用者，又是数字信任的架构师。企业可以利用密码技术来打造坚固的数字安全防护系统，为客户以及合作伙伴提供可信赖的数字化服务，从而在激烈的市场竞争中抢占先机。企业要从战略高度重新认识密码技术，把密码技术作为数字化转型的重要内容来投资、建设。企业只有在保证业务连续性的基础上，建立起以信任为基础的竞争优势，才能为长期的成功打下良好的基础。通过综合运用密码技术，企业不仅能满足合规性要求，更能将密码技术转化为构建数字信任的核心资产，进而实现业务创新、市场拓展与风险管控的有机统一。随着技术的不断发展，企业应及时调整战略，跟进密码技术的创新与趋势，结合人工智能、区块链等新兴技术，为数字化转型提供坚实的保障。企业需密切关注密码技术滥用可能带来的市场风险，通过合规和技术管理来确保健康的竞争环境和可持续发展，确保能够应对未来复杂的技术挑战和监管要求。

参考文献

[1]林琳，任旭斌，张舒黎.隐私增强密码学：技术

发展与数据安全应用探索[J].通信技术，2025，58（05）：536-543.

[2]许海燕.密码学在网络支付安全中的应用及其挑战[J].山西电子技术，2024，（06）：69-70+97.

[3]张维娜，徐仲，姬少培，等.基于密码的5G数据安全防护体系研究[J].信息安全与通信保密，2024，（08）：84-89.

[4]狄刚，柴跃廷.基于多维安全视角构建数字金融基础设施安全创新体系[J].信息安全研究，2024，10（04）：290-293.

[5]董瑞.可否认加密的数据安全加固技术研究[J].信息记录材料，2022，23（09）：223-226.DOI：10.16009/j.cnki.cn13-1295/tq.2022.09.009.

[6]黎浩.基于密码学的网络信息安全应用[J].现代信息科技，2022，6（06）：104-106+109.DOI：10.19850/j.cnki.2096-4706.2022.06.026.

[7]乔路.数据加密在计算机网络安全中的应用[J].电子技术与软件工程，2022，（01）：17-20.DOI：10.20109/j.cnki.etse.2022.01.005.

[8]荆继武，李畅.密码技术的现状与白盒化发展趋势[J].中国信息安全，2021，（08）：49-53.

[9]任童.网络信息安全中的密码技术[J].计算机与网络，2021，47（14）：50.

[10]夏鲁宁.以密码为基石重塑数据安全新理念[J].数字经济，2021，（06）：79-83.DOI：10.19609/j.cnki.cn10-1255/f.2021.06.016.