



公司及并购法律评述
2019 年 11 月

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门内大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

《密码法》要旨及合规

作者: 潘永建 | 朱晓阳 | 沙莎

2019 年 10 月 26 日,《中华人民共和国密码法》(以下简称“《密码法》”)由全国人大常委会表决通过,将于 2020 年 1 月 1 日生效。《密码法》作为密码领域效力最高、涉及范围最广的法律,经历近三年的立法历程,两次向社会公开征求意见,终于问世。该法将为规范与促进密码事业发展提供指导,也为企业的合规实践提供依据。笔者结合现行密码法律体系及《网络安全法》等相关法律,对《密码法》作出解读,并就企业合规提出建议。

一. 密码的定义及作用

《密码法》所指的密码是“采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”。该定义体现密码的三类特征:第一,密码的工作方法必须是采用特定变换的方法,将明文转换为密文;第二,密码的作用是对信息进行加密保护和安全认证;第三,密码既是产品和技术,也是一种服务。

For more Llinks publications, please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

如您需要了解我们的出版物,
请与下列人员联系:

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

免责声明: 本出版物仅代表作者本人观点,不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

《密码法》要旨及合规

我们生活中经常接触到的“密码”，并不是《密码法》意义上的密码。我们日常生活中用于保护银行账号、App 账号等所使用的“密码”实则是一种“口令”(password)，属于一种明文，不存在明文转换为密文的过程；同时该等口令也不符合《密码法》对于密码(encryption)是一种“产品、技术或服务”的定义。《密码法》下的密码是“一种复杂而庞大的信息处理系统”，¹是对可识别的数字及生物信息(即明文)进行加密的过程，使其变成不能识别的符号序列，从而提供密码保护；或者对上述信息是否被篡改、信息源是否可靠、主体和行为是否真实等进行认证的手段。以商用密码技术为例，商用密码技术是能够实现商用密码算法的加密、解密和认证等功能的技术(包括密码算法编程技术和密码算法芯片、加密卡等的实现技术)，是商用密码的核心。

尽管《密码法》下密码定义与大众通常理解有所差异，但《密码法》与民众的生活息息相关。在《密码法》颁布前，密码的应用已经遍及各行各业。在安全认证方面，电子政务和电子商务中常用的 USB Key 就是一种较为安全的认证方式。USB key 内置 CPU 或安全密码芯片，通过运算对数据进行加解密，将密码运算与用户终端的复杂环境隔离。²每个 USB key 都搭配一个硬件 PIN 码，对用户实行双因子认证，只有用户同时拥有 USB key 和 PIN 码，才能通过身份认证；在加密保护方面，密码的常见应用是在金融交易或企业内网中使用的 HTTPS 加密传输，HTTPS 将 SSL(Secure Sockets Layer, “安全套接层”)作为 HTTP 应用层的子层，SSL 在传输层对网络连接进行加密。例如，支付宝就对明文密码进行处理，用 HTTPS 传输，从而保障数据安全，防范数据泄密和网络攻击。

二. 《密码法》立法背景及目的

(一) 立法背景

《密码法》颁布之前，我国在密码领域的主要立法为 1999 年的《商用密码管理条例》。2000 年至 2010 年间，国家密码局陆续颁布或修订多部关于商用密码的科研、生产、使用、销售等方面的规范性文件。近年来，云计算、物联网和大数据等信息技术迅猛发展，与传统产业不断融合的同时，也激发了新兴业态的蓬勃发展。以互联网技术为支撑的新兴领域需要应用密码技术和产品提升安全性，虽然全国信息安全标准化委员会牵头制定了《信息系统密码应用基本要求(GM/T 0054-2018)》等密码领域的国家标准、行业标准，但立法现状显然不能为密码产业的发展提供足够的法律支撑。此外，现有密码法律体系下的单一执法机关、严格的行政许可制度以及与《网络安全法》等新法规的冲突等问题也愈发凸显。在此背景下，密码领域的统一立法具备现实必要性，国家亟待一部全国性、系统性的密码法规。《密码法》的制定和生效正是为了解决这一现实困境。

《密码法》要旨及合规

(二) 立法目的

1. 保障网络与信息安全

《网络安全法》强调“保障网络安全”，而密码是保障网络信息安全的根基，对国家安全、经济发展与社会稳定起到举足轻重的作用。密码算法和密码产品是信息安全的基础，如果不能形成自主可控的密码产业，则意味着我国的信息安全存在许多不可控因素。例如，2017年国家密码局发布有关SHA-1密码算法的安全风险提示，提示企业应全面支持和应用SM3等国产密码算法³，即体现出建立密码产业对信息安全的现实意义。

《密码法》是国家网络安全框架下，完善国家安全法律体系的重要手段，顺应了信息安全产品国产化的政策要求，是发挥密码技术、产品以及服务在网络空间重要功能的必要手段，推动构建以密码技术为核心、多种技术交叉融合的安全体制。⁴

2. 规范密码应用，促进密码事业发展

《密码法》落实密码管理部门职责，明确涉及密码工作单位的职责范围，提供财政支持，并对密码实行分类管理。在密码科学技术研究方面，《密码法》强调鼓励和支持密码科学技术的创新，保护知识产权并加强密码人才和队伍建设。与此同时，加强密码安全教育，增强全民密码安全意识。《密码法》旨在为密码事业发展提供全面支持。

相比现行商用密码领域法律，《密码法》还体现了为企业减负的理念，拓宽商用密码企业自主发展空间，意在有效管理和支持密码事业。目前区块链技术在金融、教育、劳动就业和医疗健康领域的应用正飞速发展。密码技术是区块链的重要支撑技术，《密码法》在此时通过，也进一步反映出密码与区块链技术融合，为区块链提供核心支撑与保障的格局，这也必将影响中国产业变革和经济转型。

三. 要旨解析：密码分级管理

《密码法》对密码实行分类管理。《密码法》将密码分为核心密码、普通密码和商用密码。三类密码对应不同的信息对象：核心密码、普通密码保护的信息对象为国家秘密信息；商用密码保护的信息对象则为不属于国家秘密的信息。其中，国家秘密分为绝密、机密和秘密三级，核心密码可用于保护全部三级国家秘密，但普通密码仅用于保护机密和秘密级别的国家秘密。

(一) 核心密码、普通密码

核心密码、普通密码本身即属于国家秘密，实行严格统一管理。在核心密码、普通密码的管理

《密码法》要旨及合规

方面,《密码法(草案)》(以下简称“草案”)曾对管理的范畴进行具体划分,包括密码的科研、生产、检测、装备、使用和销毁等,虽然《密码法》删除了上述细分规定,但应理解为立法语言的适度概括,《密码法》规制的范围仍旧是与核心密码、普通密码相关的整个环节。

核心密码、普通密码工作机构⁵应当建立健全安全管理制度,采取严格的保密措施,并落实保密责任制。保密责任也是《密码法》对草案的新增内容,对密码工作机构提出了责任要求,做到“权责一致”,切实保障密码安全。因此,核心密码、普通密码工作机构必须对密码的安全管理予以重视。

除了密码工作机构,密码管理部门也有权针对核心密码、普通密码工作进行指导、监督和检查。密码管理部门与其他相关部门建立安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制,及时消除影响密码安全的重大问题和风险隐患,既是对密码工作的协同监管,也是对密码安全的全面保障。

(二) 商用密码

《商用密码管理条例》及其配套法律规定了商用密码产品研制、生产、进口和使用的严格审批要求,但这种审批要求已经不能适应信息网络及其应用的发展。实践中,《密码法》颁布之前,国家密码局已经取消了大部分涉及商用密码的行政审批。为进一步开发商用密码市场,《密码法》对商用密码管理制度进行诸多改革,其中最突出的是商用密码的“两个自愿”原则。第一,《密码法》明确规定,从事商用密码活动的外商投资企业与内资企业享有平等地位,外商投资企业自愿开展商用密码合作,禁止行政机关强制转让商用密码技术;第二,除了涉及国家安全、国计民生、社会公共利益的商用密码产品,商用密码单位自愿接受检测认证,取消商用密码产品科研、生产、进口、出口和使用的前置许可和专控管理。此外,《密码法》特别提出“大众消费类产品所采用的商用密码不实行进口许可和出口管制制度”。

在商用密码的保密方面,《密码法》也提供了“双重保护”。首先,《密码法》要求密码检测、认证机构对其知悉的国家秘密和商业秘密承担保密义务;其次,行政机关也不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息,行政机关在履行职责中知悉的商业秘密和个人隐私,亦应承担保密义务。

四. 合规建议

下文中,笔者将归纳总结密码使用企业和密码生产销售企业的合规义务。无论是何种企业,作为合规前提,企业应全面、正确地理解密码管理法律体系。

《密码法》要旨及合规

密码领域法律体系		
法律 (全国人大)	专门法律: 《密码法》	其他相关法律: 《国家安全法》《保守国家秘密法》《网络安全法》《反恐怖主义法》《电子签名法》《技术进出口管理条例》等
行政法规 (国务院)	《商用密码管理条例》	
部门规章 (国家密码管理局)	《商用密码产品生产管理规定》 《商用密码科研管理规定》 《电子认证服务密码管理办法》 《信息安全等级保护商用密码管理办法》	
国家标准、行业标准	《GM/T 0054-2018 信息系统密码应用基本要求》 《GM/T 0044-2016SM9 标识密码算法》 《GM/T 0045-2016 金融数据密码机技术规范》 《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》等	

(一) 密码使用者

1. 使用核心密码、普通密码

正如本文第三部分所述，核心密码、普通密码用于保护国家秘密信息，而核心密码、普通密码本身也属于国家秘密。密码使用者在使用密码过程中对其知悉的国家秘密采取严格的保密措施，且应当参照核心密码、普通密码落实保密责任制。企业应当及时消除可能泄露国家秘密的重大问题和安全隐患，一旦出现上述问题，则应立即采取应对措施，并向保密局、密码管理局报告。

2. 使用商用密码

尽管《密码法》对商用密码放宽了限制，但企业在使用商用密码的过程中仍应遵守若干强制义务。

第一，在商用密码的检测、认证方面，《密码法》鼓励商用密码从业单位自愿接受商用密码检测认证。但是，如果在使用商用密码服务的过程中，其中的密码产品涉及国家安全、国计民生和社会公共利益，则必须经过商用密码认证机构对该密码服务进行合规认证。

第二，在商用密码的安全性评估方面，如果企业使用商用密码保护关键信息基础设施，则应当自行或委托商用密码检测机构进行密码应用的安全性评估。《密码法》的安全性评估要求与《网络安全法》等法律下的关键信息基础设施安全检测评估、网络安全等级测评制度

《密码法》要旨及合规

相衔接。另外，如果采购商用密码产品和服务可能影响国家安全，还应当通过国家安全审查。

第三，在商用密码的进口许可与出口管制方面，企业进口的商用密码如果涉及国家安全、社会公共利益且具有加密保护功能，则应当取得国务院商务主管部门、国家密码管理部门的进口许可；企业出口的商用密码如果涉及国家安全、社会公共利益或者中国承担国际义务，则面临国家的出口管制。企业应关注商用密码进口许可清单和出口管制清单(大众消费类产品所采用的商用密码除外)。

3. 相关法规规定的其他义务

企业使用商用密码进行合规时，应当遵守与《密码法》相关的其它法律规范。

《密码法》中对于涉及国家安全、国计民生和社会公共利益的商用密码，与《网络安全法》中网络关键设备和网络安全专用产品的规定一致，即应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供，且安全认证和安全检测结果互认。⁶值得注意的是，中央网信办等部门正在推动制定《网络关键设备和网络安全专用产品相关国家标准要求》，目前已发布两版征求意见稿，预计将于不久实施。

使用商用密码进行保护的关键信息基础设施，与《网络安全等级保护条例(征求意见稿)》⁷要求一致。同时，在安全审查方面，《密码法》规定关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当进行国家安全审查，这也与《网络安全法》⁸《网络产品和服务安全审查办法》⁹《关键信息基础设施安全保护条例(征求意见稿)》¹⁰相互呼应。

(二) 密码产品生产者和销售者

从事核心密码、普通密码生产的企业应当建立健全安全管理制度，采取严格的保密措施和保密责任制，确保核心密码、普通密码的安全。

商用密码生产和销售不得损害国家安全、社会公共利益或者他人合法权益，且应当符合有关法律、行政法规、商用密码强制性国家标准以及从业单位公开标准的技术要求。商用密码的销售企业应当注意，如果销售的密码产品属于列入网络关键设备和网络安全专用产品目录的产品，即密码产品涉及国家安全、国计民生、社会公共利益，则必须由具备资格的机构检测认证合格后，方可销售或者提供，否则可能面临警告、罚款等行政处罚。

《密码法》要旨及合规

五. 结语

《密码法》的颁布对于我国密码行业及任何需要密码保护信息的行业的发展都有着重大意义。《密码法》一方面保护和限制作为国家秘密的核心密码和普通密码，另一方面进一步放宽了对于商用密码的限制，有利于商业领域中密码技术及产品的开发和使用。同时，《密码法》与《保守国家秘密法》《电子签名法》《网络安全法》及《电子商务法》等法律形成强大的协同效应，能够更加系统性地为各行各业的信息保护提供制度指引。

《密码法》要旨及合规

如需进一步信息，请联系：

作 者	
潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com	
上 海	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	刘贇春 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
余 铭 电话: +86 21 3135 8770 selena.she@linkslaw.com	娄斐弘 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@linkslaw.com	孔焕志 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
吴 炜 电话: +86 21 6043 3711 david.wu@linkslaw.com	潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com
姜 琳 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
北 京	
俞卫锋 电话: +86 10 8519 2266 david.yu@linkslaw.com	刘贇春 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
香 港(与方緯谷律师事务所联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	吕 红 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
伦 敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 通力律师事务所 2019

免责声明：本出版物仅代表作者个人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

《密码法》要旨及合规

¹ 上海市司法局: What? 登录密码不是“密码?”《密码法》你了解多少?,

<https://mp.weixin.qq.com/s/cTWbLLkIRuFWLOVSfKdzhQ>, 最后访问时间为 2019 年 11 月 5 日。

² 李明, 史国振, 娄嘉鹏: 《基于密码服务平台的 USB Key 身份认证方案》, 载《计算机应用与软件》2018 年 9 月第 39 卷第 9 期, 第 288 页。

³ 关于使用 SHA-1 密码算法的风险提示,

http://www.sca.gov.cn/sca/xwdt/2017-04/03/content_1002918.shtml, 最后访问时间为 2019 年 11 月 3 日。

⁴ 国家密码管理局负责人就《中华人民共和国密码法》答记者问,

http://www.oscca.gov.cn/sca/xwdt/2019-10/27/content_1057218.shtml, 最后访问时间为 2019 年 11 月 2 日。

⁵ 核心密码、普通密码工作机构, 指从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构。

⁶ 《网络安全法》第二十三条。

⁷ 《网络安全等级保护条例(征求意见稿)》第四条。

⁸ 《网络安全法》第三十五条。

⁹ 《网络产品和服务安全审查办法》第九条、第十条。

¹⁰ 《关键信息基础设施安全保护条例(征求意见稿)》第三十条、第三十一条。