实施《密码法》
维护国家安全和人民群众利益

2020 年 1 月 1 日，《中华人民共和国密码法》（以下简称《密码法》）正式施行。《密码法》是总体国家安全观框架下，国家安全法律体系的重要组成部分，是我国密码领域的综合性、基础性法律。

一、《密码法》解读

《密码法》坚持党管密码和依法管理相统一、创新发展和确保安全相统一、简政放权和加强监管相统一三大原则。重点以法律形式明确了以下内容:**一是密码是什么。**“是指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”。**二是如何分类及应用。**密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息；商用密码用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。**三是如何分类管理。**坚持党管密码根本原则；对核心密码、普通密码，由密码管理部门依法实行严格统一管理；对商用密码，明确了标准化制度、检测认证制度、市场准入管理制度、关键信息基础设施使用要求、进出口管理制度、电子政务电子认证服务管理制度、行业协会发展要求以及商用密码事中事后监管制度等。**四是法律责任。**任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密

码保障系统；任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动；明确了对各类密码管理和应用违法行为的处罚措施。密码法的出台有重大意义，是构建国家安全法律制度体系、维护国家网络空间主权安全的、推动密码事业高质量发展的重要举措。

二、时代对商用密码管理和从业人员的呼声

我国商用密码在管理制度、科技创新、产业发展、应用推进等方面取得系列成果，实现了跨越式发展。商用密码科研取得 142 项国家或省部级科技成果，其中 10 余项达到国际先进水平；形成了比较完备的商用密码算法体系，其中自主设计的 ZUC 和 SM2/SM3/SM9 算法已成为国际标准；发布密码行业标准 91 项、国家标准 29 项，覆盖密码算法、协议、产品、检测、应用、管理等各方面；新一代密码算法征集工作正扎实有序开展，已初步遴选出一批优秀研究成果；密码产业从业单位超过 2000 家，商用密码累计产值超千亿元，呈快速发展趋势；取得产品型号证书商用密码产品达 2000 余款，51 家电子认证服务机构完成基于 SM2 的公钥基础设施升级改造并接入国家根 CA；商用密码检测认证体系不断健全，已形成商用密码产品全品类、全要素检测能力；商用密码检测中心取得认证机构资质，2 家商用密码产品检测机构通过试点培育;初步建立商用密码应用安全性评估体系，培育认定 27 家机构；商用密码应用推进持续发力，从开创金融领域密码应用，到加强重要领域密码应用，再到实施密码应用与创新发展工作规划，商用密码应用工作成效显

著。

密码发展正处于百年未有之大变局，肩负着重构网络空间新格局的历史使命，同时也面临严峻复杂的挑战。密码经历了从艺术到科学、从黑屋走向公众的历史进程。当今的密码，已经从传统的通信密码保障拓展到了信息化密码保障，正在逐步拓展到网络空间密码保障;已经从最初的战争工具，拓展为生产、生活工具;已经从维护国家安全，延伸到了推动经济社会发展、保护人民群众利益。当前，密码在管理、产业、应用、创新等方面尚面临很大挑战，一些重要信息系统和关键信息基础设施密码防护薄弱，系统“裸奔”，数据“裸跑”;企业网络安全环境堪忧，普遍不重视或不实施对数字资产的保护，在认识上存在不属于国家秘密就无需密码保护的误区;密码高质量供给不足，密码与新兴信息技术体系的融合不够，基础软硬件支持密码的生态尚未形成;密码服务“一带一路”作用发挥不够，国际影响力与我国大国地位不相称;密码学科建设和人才培养与密码的时代发展要求不相适应，制约着密码的广泛应用和科学发展。

商用密码发展将开启新征程。切实提升密码保障与管理水平，服务国家治理体系和治理能力现代化重大部署。持续增强密码创新与支撑能力，助力国家经济和社会高质量发展。发挥密码在保障网络空间安全的核心技术和基础支撑作用，推动密码与云计算、大数据、物联网、人工智能、区块链、5G 等数字经济新技术、新业态的融合，引领数字化、网络化、智能化安全发展，助力我国在新兴信息技术领域实

现“换道超车”，改变网络空间争夺格局，构建可信可管可控数字世界；大力推进商用密码嵌入通用处理器、操作系统等基础软硬件的技术攻关，加紧突破一批新兴技术领域密码应用关键技术，形成支持密码应用的良好产业生态;加强密码学科体系建设，推动设立密码院系和特色专业，积极开展密码人才培养和社会化培训。积极推动密码服务“一带一路”建设，共建网络空间命运共同体。

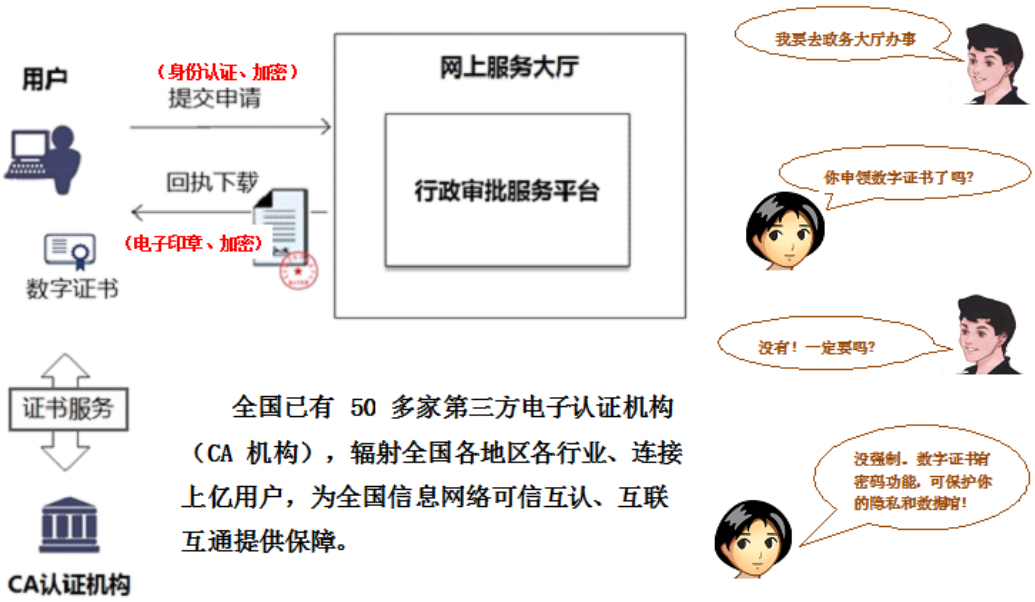
三、商用密码与我们日常生活息息相关

我们常说的用户名“密码”只是“口令”，并不是《密码法》中的“密码”。

“进不来”、“拿不走”、“看不懂”、“改不了”、“走不脱”，是密码在保障信息安全中发挥的身份认证、访问控制、机密性、完整性、不可抵赖性等作用的通俗表述。网络连到哪，数据跑到哪，安全需求在哪，密码保障到哪。

1.密码与政务服务

政务服务中的密码应用



2.密码与身份证

密码与二代身份证

● 第二代居民身份证是公安部委托清华大学微电子学研究所和清华同方微电子有限公司共同研制的，在二代身份证中，解开密码是某种自主加密算法的密钥。

- 15 亿张，高度防伪，无法复制
- 电子签名：自主公钥密码算法
- RFID（无线射频识别），非接触式读取

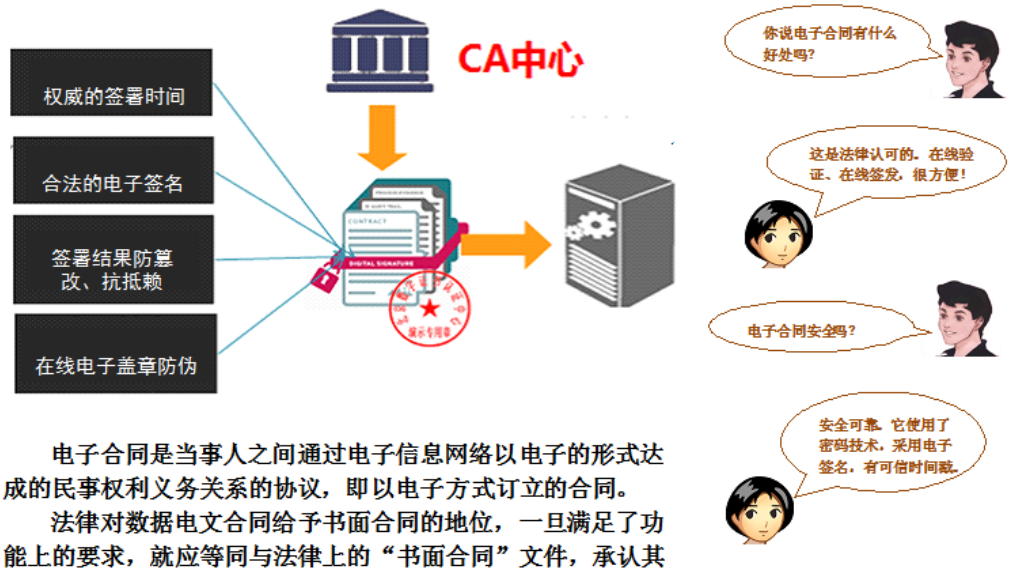
3.密码与银行卡

密码与银行卡

金融 IC 卡又称芯片银行卡，是以芯片作为介质的银行卡。芯片卡容量大，可以存储密钥、数字证书、指纹等信息，其工作原理类似于微型计算机。它安全保密性好，有密码技术保护，具备很强的抗攻击能力，很难被复制与伪造。

4.密码与电子商务

密码技术为电子合同保驾护航

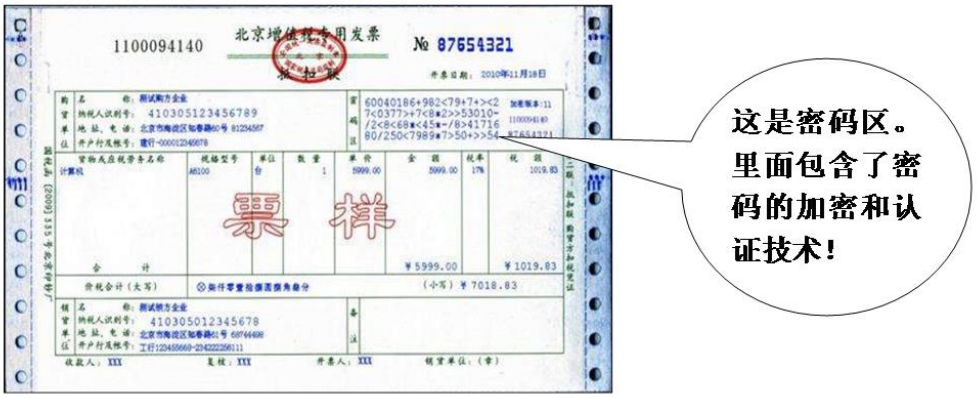


电子合同是当事人之间通过电子信息网络以电子的形式达成的民事权利义务关系的协议，即以电子方式订立的合同。

法律对数据电文合同给予书面合同的地位，一旦满足了功能上的要求，就应等同与法律上的“书面合同”文件，承认其效力。

5.密码与发票

增值税发票的密码应用



密码应用于增值税发票中，可以防伪、防篡改，杜绝了各种利用增值税发票偷、漏、逃、骗国家税收的行为，方便税务稽查。

6.密码与 ETC（不停车收费系统）

ETC(电子不停车收费系统)

ETC 是一种用于公路、大桥和隧道的电子自动收费系统。汽车经过收费站时，不用停车，瞬间就自动完成收费过程。

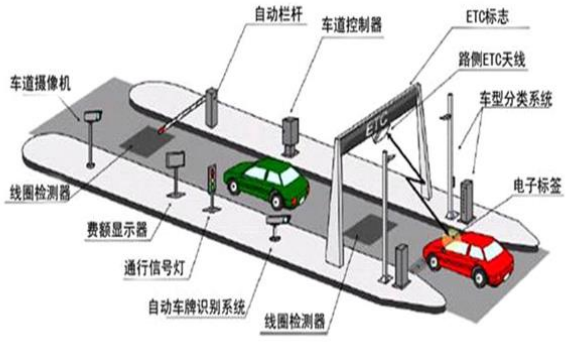


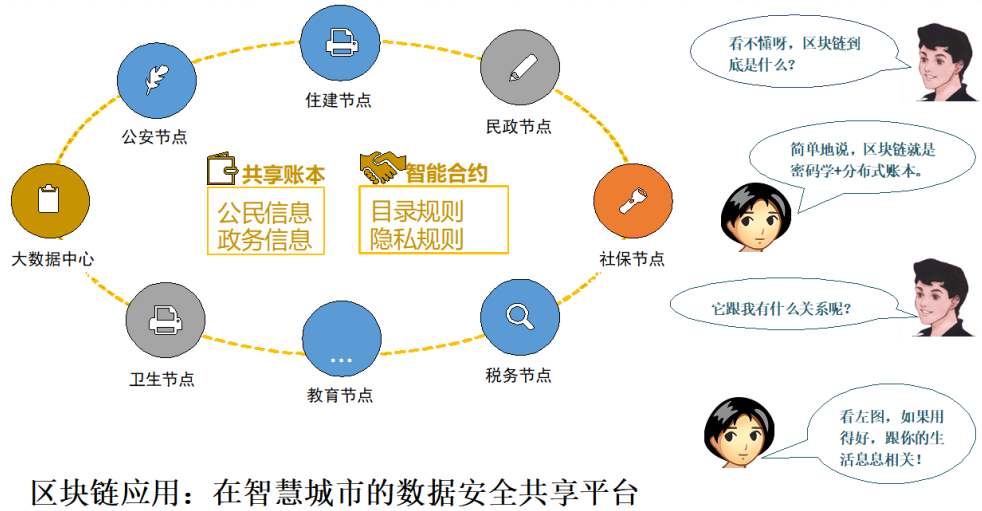
图5-6 ETC车道组成

- 收费站和汽车要双向身份认证，以防假冒。
- 收费设备读汽车数据前，要提供有效访问身份码。
- 收费设备接收数据前，汽车要提供有效的信息鉴别码。
- 传递数据是用密码算法保护的。

7.密码与区块链

密码与区块链

●区块链是一种按照时间顺序将数据区块以顺序相连方式组合成的一种数据结构，并以密码学方式保证不可篡改和不可伪造的分布式帐本。



区块链应用：在智慧城市的数据安全共享平台

在银行办理业务、向网站或 APP 填报个人数据、使用物联网产品等多种涉及数据上网的场景中，记得问一句“数据加密保护了吗？”如果某些组织或个人窃取您加密保护的信息或者非法侵入您的密码保障系统，或者利用密码从事危害到您合法权益的违法活动，请用《密码法》维权！

2020 年，集“产、学、研、用、测、管、行”于一体的广东省商用密码应用和创新示范基地已经在广州开发区挂牌设立并进入实施建设阶段，广东省商用密码协会也已经正式成立，期待相关机构、企业、人才共同参与，推动我国密码应用和创新发展。