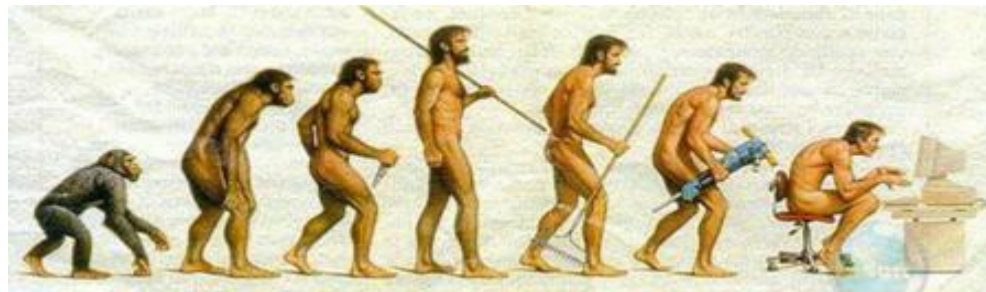


交通运输网络安全与密码应用

中国交通通信信息中心 信息安全中心

李璐瑶

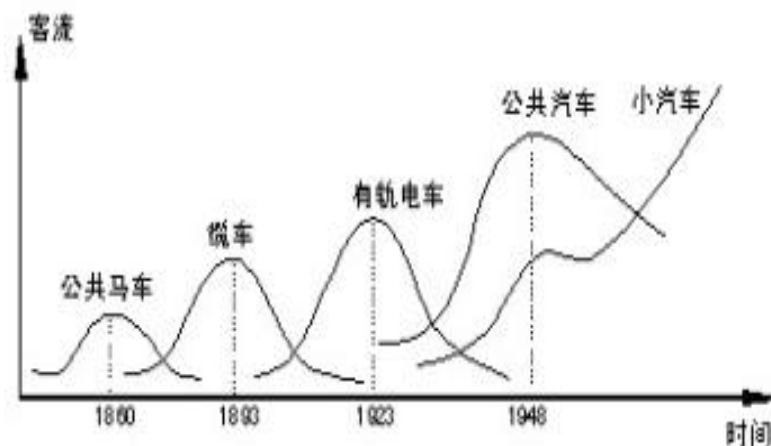
一、行业网络安全战略定位



交通运输是人类社会发展的重要活动之一。

基本概念

交通运输是以满足人民群众出行、货物流通为目的，由交通运输基础设施、交通运输工具、交通运输主体、交通运输管理与服务相互联系和相互作用的一种社会化活动。



一、行业网络安全战略定位

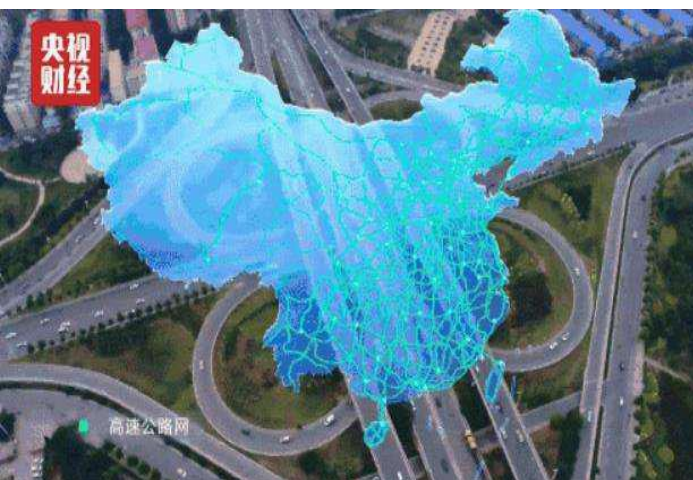


我国根据2008年国务院机构改革方案，重新组建交通运输部。原交通部、中国民用航空总局、铁道部、国家邮政局，建设部指导城市客运的职责，整合划入交通运输部。

我国交通运输业为综合交通运输业，其领域包括：**公路、水路、铁路、民航、邮政、救捞、海事及支撑交通运输有关的管理服务业务。**



一、行业网络安全战略定位



一、行业网络安全战略定位

共享单车对城市经济贡献度

共享单车行业成为拉动城市经济的重要一环。武汉、成都、北京三地因共享单车对城市经济的贡献度较高而位列前三甲。

摩拜经济贡献度Top5城市



城市居民车均热量消耗

36个城市平均每辆摩拜单车帮助市民日消耗**309卡路里**热量，效果等同于每日在跑步机上运动**30分钟**。



图例 = 200卡路里

共享单车就业吸引力

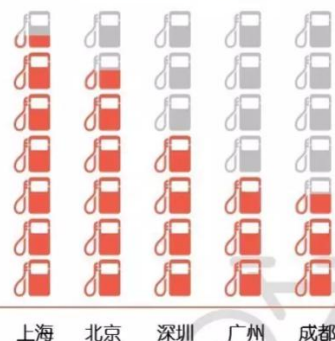
摩拜单车为36个主要城市在运营管理、调度以及零部件供应、生产制造、维修等上下游产业提供超过**5万个**就业机会。



节约油耗当量

自摩拜单车投入使用以来，36个城市累计骑行量可降低油耗当量**38万吨**，相当于我国**4.5天**从科威特进口的原油总量。

摩拜节约油耗Top5城市



城市居民车均骑行状况

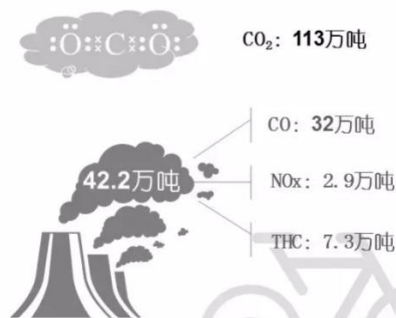
沈阳荣登榜首，成为骑行活跃度最高的城市。

摩拜车均骑行状况Top5城市



减少排放当量

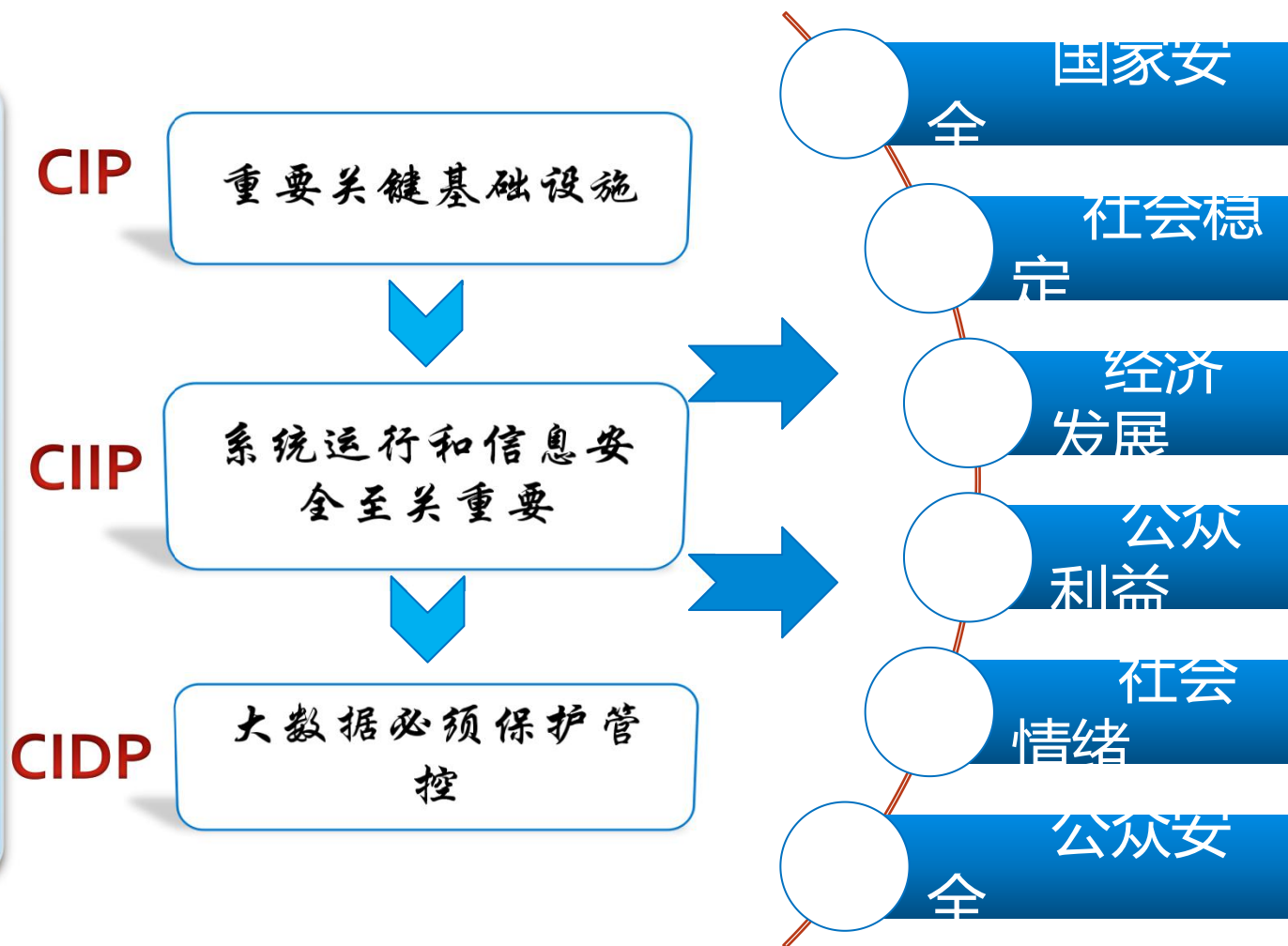
自摩拜单车投入使用以来，36个城市累计减少CO₂排放**113万吨**，降低CO排放**32万吨**，THC排放**7.3万吨**，NOx排放**2.9万吨**。



一、行业网络安全战略定位

第三十一条 国家对公共通信和信息服务、能源、**交通**、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在**网络安全等级保护制度**的基础上，实行重点保护。

《中华人民共和国网络安全法》



二、行业信息化发展及安全风险

行业风险分析

1. 感知层

数据采集设备种类多样，缺少对设备的有效监控，存在**设备被盗、信号干扰、节点伪造、无法网络监控**等威胁。

2. 网络层

多种网络配合，除传统网络层安全威胁外，还会受到**虚假网关、路由伪造、选择性转发、跨网病毒传播**等威胁。

3. 数据资源层

数据**信息篡改、数据泄露、数据丢失、恶意代码**
数据**可靠性**影响

4. 应用层

存在大量应用系统与工业控制系统结合的复合性结构系统，**脆弱性的多样化**带来更多安全风险。

5. 展示层

综合信息服务系统、智能终端、移动执法系统，传输**不统一或不准确**等现象

机密性

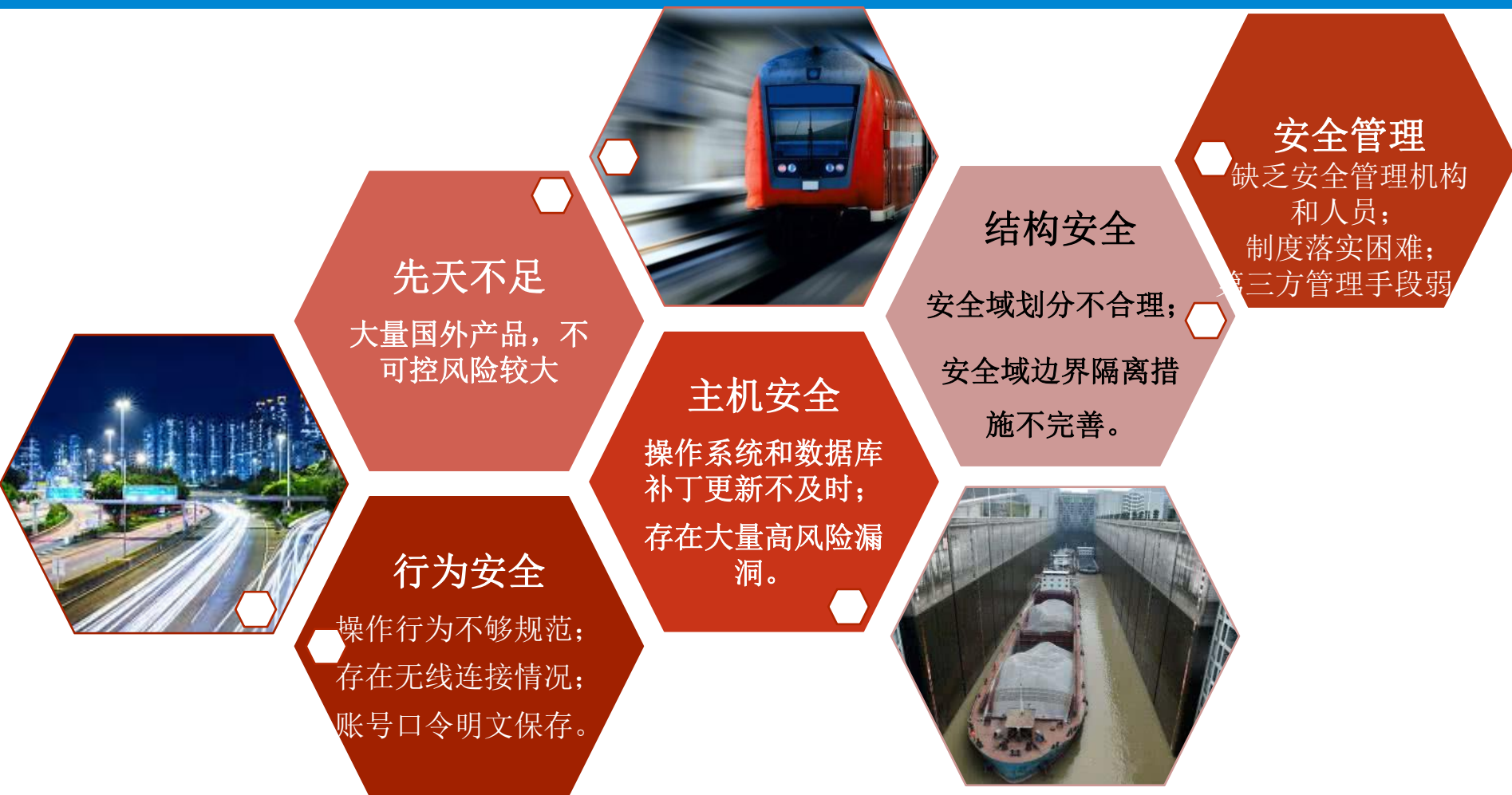
隐私性

完整性

认证性

可靠性

二、行业信息化发展及安全风险



二、行业信息化发展及安全风险

无需密码校验，通过分析目标手机用户的短信验证码，可以登录任意手机账号。

以共享单车为例，据不完全统计，目前全国共有互联网租赁自行车累计投放车辆超过1000万辆，累计服务超过10亿人次，蕴藏281亿元的市场，上下游产业链可达千亿规模。

账户
安全
隐患

个人
信息
泄露

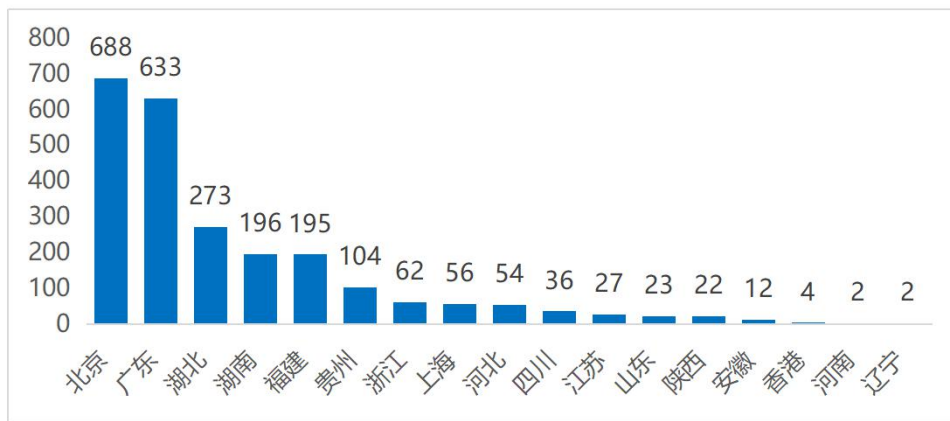
占比
14.7%

恶意
骚扰

网络
攻击

短信验证码可以反复发送，恶意骚扰用户。

某些APP，存在任意文件上传漏洞，可能导致恶意代码传播、系统瘫痪和用户被攻击



三、行业密码应用工作开展



三、行业密码应用工作开展

行业密码产品及算法应用研究（交通运输部）

行业商用密码使用情况专项检查（部密码办）

船联网内河船舶电子身份认证

行业重要信息系统密码应用推进研究（国家密码局）

行业密码应用规划
网络安全十三五规划

2012
年5月

2013
年10月

2014
年8月

2014
年10月

2015
年4月

三、行业密码应用工作开展

★《关于开展商用密码使用情况检查的通知》（国密字【2014】230号）

— 要求中央和国家机关各部委、各人民团体，对非涉密重要网络和信息
系统商用密码使用情况开展检查

★《关于开展交通运输行业商用密码使用情况专项检查的通知》（交办函【2014】675号文）

— 组织开展交通运输行业非涉密的重要网络和信息
系统商用密码使用情况专项检查；

《交通运输行业商用密码技术体系 和应用情况调研报告》

- 普遍未采用国产密码算法
- 独立建设，扁平散乱化
- 无统一技术规范、管理要求
- 不支持行业业务的互联互通

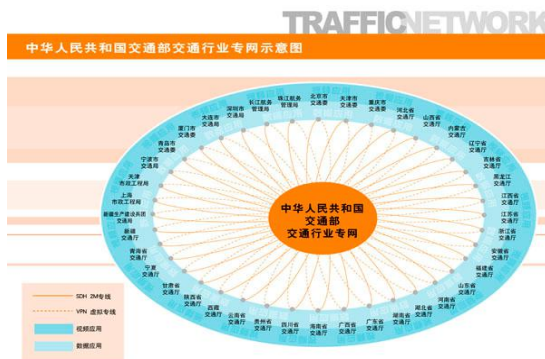
四、推进规划-1 推进基础信息网络密码应用

高速公路光纤网、各政务专网等基础信息网络，将国产密码应用纳入信息化建设整体规划，完善网络数据加密国产密码应用安全体系。建立应急通信国产密码应用安全体系，实现数据中心、电子交易、政务办理等信息服务和平台的网络用户身份识别和信息保护。规范基础信息网络电子认证服务密码应用。推进国产密码在物联网、移动互联网的身份识别、安全接入、安全定位和信息保护等方面的应用。

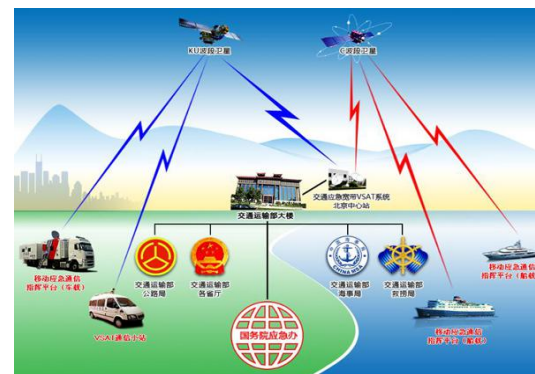
全国高速公路信息通信系统联网工程干线传输系统
一期工程组网图



光纤网



行业专网



卫星网络

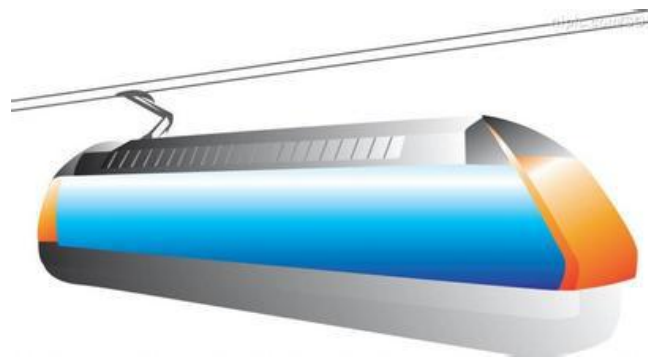
四、推进规划 - 2 规范重要信息系统密码应用

高速公路不停车收费系统（ETC）、城市公交一卡通系统、联网售票系统、出行服务系统、运政管理系统、地理信息系统、海事、救捞政务管理系统、物流公共信息平台等涉及国计民生和基础信息资源的重要信息系统，将国产密码应用纳入信息化建设总体规划，建立健全国产密码应用标准体系，逐步实现基于国产密码的安全体系跨领域应用。建立健全基于国产密码的身份认证、访问控制、数据保护、可信服务、安全审计等安全防护措施。



四、推进规划-3 促进工业控制系统密码应用

城市轨道交通、船闸控制等领域的重要工业控制系统应将国产密码算法应用纳入信息化建设整体规划，实现国产密码技术在数据采集与监控、分布式控制系统、过程控制系统、可编程逻辑控制器等工业控制系统中的深度应用，充分发挥密码在系统资源访问控制、数据存储、数据传输、可视化控制、安全审计等方面的支撑作用，建立基于国产密码的安全生产、调度管理等安全体系。



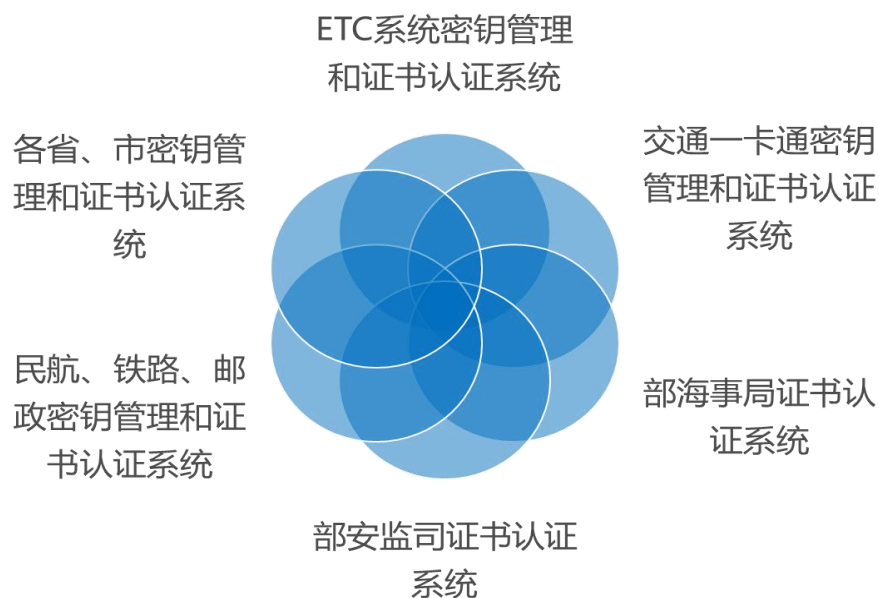
四、推进规划-4 加强政务信息系统密码应用

交通运输行业各级党政机关和使用财政性资金的事业单位、团体组织使用的门户网站、公众出行服务系统、物流服务和管理平台、路网信息服务平台、行政审批系统等面向社会服务信息系统。

加快推进基于国产密码的网络信任、安全管理和运行监管体系建设，规范国产密码在电子文件、电子证照、电子印章、身份认证、电子签名、数据存储和传输等方面的应用，实现面向社会服务的政务信息系统运行的安全可靠。

四、推进规划 - 5 提升国产密码基础支撑能力

建设完善交通运输行业密码基础技术、应用技术、标准规范和检测评估体系。加强面向云计算、物联网、大数据、移动互联网和智慧交通等新方向的密码应用技术研究，促进密码技术与新技术的融合与发展。完善密钥管理、身份认证、授权管理、责任认定、可信时间、电子签章等密码基础设施。



四、推进规划-6 健全国产密码应用管理体系

由交通运输部密码领导小组牵头，建立健全交通运输行业国产密码应用推进组织体系，统筹交通运输行业国产密码应用推进资源，依据新的商用密码管理条例、ETC和一卡通相关技术标准，出台交通运输行业国产密码应用管理办法，指导交通运输行业各领域制定国产密码应用技术标准，规范交通运输行业各领域国产密码应用推进工作。

感谢聆听！