工业互联网标识解析—
主动标识载体技术白皮书

工业互联网产业联盟（AII）

2019 年 11 月

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010 62305887

邮箱：aii@caict.ac.cn

编写说明

工业互联网标识解析体系是工业互联网网络架构重要的组成部分，既是支撑工业互联网网络互联互通的基础设施，也是实现工业互联网数据共享共用的核心关键。

2017 年 11 月 27 日，国务院印发了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，将“推进标识解析体系建设”列为主要任务之一。2018 年，工业和信息化部发布了《工业互联网发展行动计划（2018-2020 年）》，提出“标识解析体系构建行动”。2019 年，中央经济工作会议提出“要发挥投资关键作用，加大制造业技术改造和设备更新，加快 5G 商用步伐，加强人工智能、工业互联网、物联网等新型基础设施建设”。目前，构建工业互联网标识解析体系，打造高效、安全、稳定的新型基础设施，开拓网络空间标识应用体系的各项工作正在进入发展快车道。同时，产业界和学术界针对工业互联网标识解析技术的创新探索正在逐步展开，降低工业互联网标识应用推广技术成本、挖掘其核心商业价值，已经成为重点探索方向之一。

本白皮书中所研究的“标识载体”，就是指承载标识编码资源的标签，也是推动标识技术应用落地的关键环节。谈到标识载体技术，过去我们往往会联想到一维条形码、二维条形码等技术，但即便是采用射频电子标签技术，也无法像在移动通信网络中那样，手机等智能终端都可以使用用户身

份识别卡（Subscriber Identification Module，SIM）来随时随地的建立可识别的连接。因此，将通用集成电路卡、芯片、模组、终端等信息通信技术引入工业互联网标识载体，有利于工业互联网标识相关产品的规模化、标准化和低成本化，进而有利于工业企业供应链管理、生产流程管理、产品生命周期管理等核心能力升级。

在这样的背景下，工业互联网产业联盟标识特设组组织编写了《工业互联网标识解析—主动标识载体技术白皮书》，希望提高业界对工业互联网标识载体相关技术的重视和共识，以推动工业互联网标识规模化落地应用，为标识解析等新型网络基础设施对工业企业赋能能力提升与深度融合提供必要的手段。

白皮书主要分为四个部分。第一部分为概述，主要介绍工业互联网标识解析、标识载体的相关概念，以及本白皮书的研究范畴。第二部分为工业互联网标识载体关键技术及其演进趋势，主要包括一维条形码、二维条形码、射频识别、近场通信等被动标识载体关键技术，以及通用集成电路卡、芯片、模组、终端等主动标识载体关键技术。第三部分为工业互联网标识载体产业生态及其发展现状，主要包括产业链、市场规模的梳理，以及重点区域、重点企业形成的产业地图。第四部分为基于主动标识载体技术的典型工业互联网应用，主要包括可信数据采集、数据融合、统一身份认证、

接入安全认证等。最后第五部分对工业互联网载体技术和产业发展提出若干建议。

白皮书编写过程中得到了中国联通、中国电信、中国移动等基础电信运营商及其他联盟成员的大力支持。

组 织 单 位：工业互联网产业联盟

牵头编制单位：中国联合网络通信集团有限公司、中国信息通信研究院

参与编制单位：阿里云计算有限公司、腾讯计算机系统有限公司、中国电信集团有限公司、中国移动通信集团公司、中国科学院计算机网络信息中心、华为技术有限公司、三一重工股份有限公司、联通（黑龙江）产业互联网有限公司、上海路随通信科技有限公司、北京邮电大学、恒安嘉新（北京）科技有限公司、中兴通讯股份有限公司

主要编写人员：贾雪琴、刘阳、马宝罗、邢宇龙、池程、史可、林晨、胡云、杨震、孟昕、蒋晓、柳耀勇、郑乔露、周天乐、刘佳、周亚灵、代晴华、黄韬、庞韶敏、谢人超、李研、王志军、李博鑫、赵大立、孙迪、吴俊、王朋、姚韬、孙阳阳、刘茵、周晓宇、成洁、王剑飞、李双权、田徼、高彦军、李哲、李洁、陈宇、王姝、范小东、刘为华、高峰、刘晋兴、朱岩、田云飞。

目录

缩略语

ASK	Amplitude Shift Keying	幅移键控
CA	Certification Authority	证书授权
CM	Compact matrix	紧密矩阵
CDMA	Code Division Multiple Access	码分多址
CPU	Central Processing Unit	中央处理器
DTLS	Datagram Transport Layer Security	数据包传输层安全性协议
EAN	European Article Number	欧洲物品编码
EDI	Electronic Data Interchange	电子数据交换
eMTC	Enhanced Machine Type Communications	增强型机器类通信
FPGA	Field Programmable Gate Array	现场可编程门阵列
FSK	Frequency-shift keying	频移键控
GM	Grid Matrix	网格码
GPS	Global Positioning System	全球定位系统
GS1	Globe standard 1	全球标准 1
GNSS	Global Navigation Satellite System	全球卫星导航系统
GSM	Global System for Mobile Communications	全球移动通信系统
BOSS	Billing and Order Support System	计费和签约支撑系统
OSI	Open System Interconnection Reference Model	开放式系统互联参考模型
MAC	Media Access Control	媒体访问控制
MCU	Microcontroller Unit	微控制单元
MNO	Mobile Network Operator	移动网络运营商
NAA	Network Access Application	网络接入应用
NB	Narrowband	窄带
RFID	Radio Frequency Identification	射频识别
NFC	Near Field Communication	近场通信
UICC	Universal Integrated Circuit Card	通用集成电路卡
eUICC	Embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	演进的通用陆基无线接入网
LoRA	Long Range	远距离
MCU	Microcontroller Unit	微控制单元
SIM	Subscriber Identity Module	用户识别模块
SMD	Surface Mounted Devices	表面贴装器件

一、概述

（一）基本概念

1.工业互联网标识解析

工业互联网标识解析体系是工业互联网网络架构重要的组成部分，既是支撑工业互联网网络互联互通的基础设施，也是实现工业互联网数据共享共用的核心关键。其中，**工业互联网标识编码**是指能够唯一识别机器、产品等物理资源以及算法、工序等虚拟资源的身份符号；**工业互联网标识解析**是指能够根据标识编码查询目标对象网络位置或者相关信息的系统装置，对机器和物品进行唯一性的定位和信息查询，是实现全球供应链系统和企业生产系统的精准对接、产品全生命周期管理和智能化服务的前提和基础。工业互联网标识解析的基本业务流程如图 1 所示。

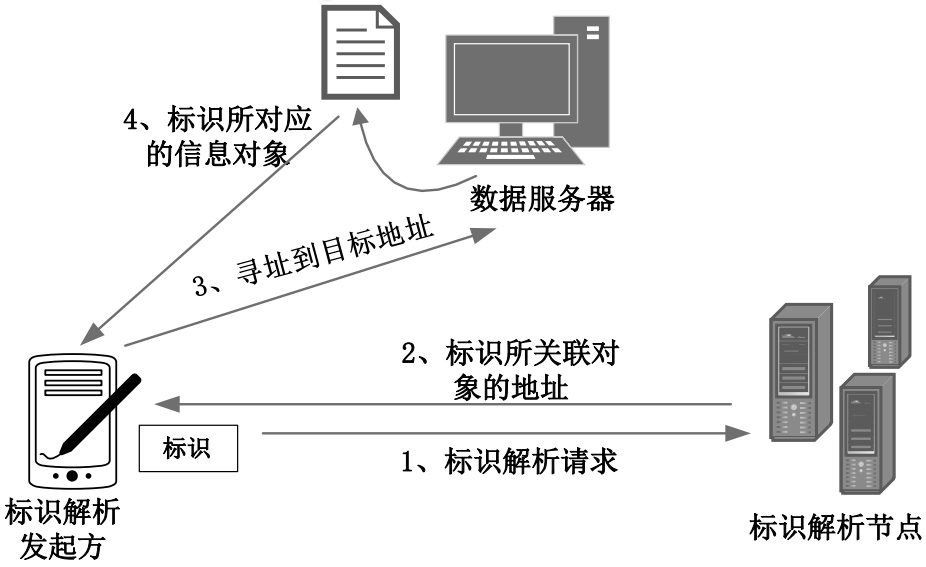


图 1 工业互联网标识解析的基本业务流程

互联网域名解析与工业互联网标识解析的概念辨析

- 互联网域名解析主要发生在应用服务体系(万维网/Web)和互联体系 (TCP/IP)之间，主要用于解决域名到 IP 地址的翻译问题。
- 工业互联网中，标识是赋予每一个产品、零部件、机器设备唯一的“身份证”，解析是通过产品标识查询存储产品信息的服务器地址，或直接查询产品相关信息及其他服务。工业互联网标识解析主要发生在应用支撑体系(万维网、应用协议)和网络互联体系之间，主要用于解决标识到标识、标识到地址、标识到数据的映射和转换问题。

2.标识载体

标识载体，就是指承载标识编码资源的标签。根据标识载体是否能够主动与标识数据读写设备、标识解析服务节点、标识数据应用平台等发生通信交互，可以将标识载体分为主动标识载体和被动标识载体两类。

主动标识载体，一般是指可以嵌入在工业设备的内部，承载工业互联网标识编码及其必要的安全证书、算法和密钥，具备联网通信功能，能够主动向标识解析服务节点或标识数据应用平台等发起连接，而无需借助标识读写设备来触发。如图 2 所示，UICC、通信模组、MCU 等都是主动标识载体的例子。

主动标识载体的主要特征有:

- 嵌入在工业设备内部，不容易被盗取或者误安装；
- 具备网络连接能力，能够主动向标识解析服务器发起标识解析请求；同时也支持被其承载的标识及其相关信息的远程增删改查；
- 除了承载工业标识符，还具有安全区域存储必要的证书、算法和密钥，能够提供工业标识符及其相关数据的加密传输、能够支持接入认证等可信相关功能。

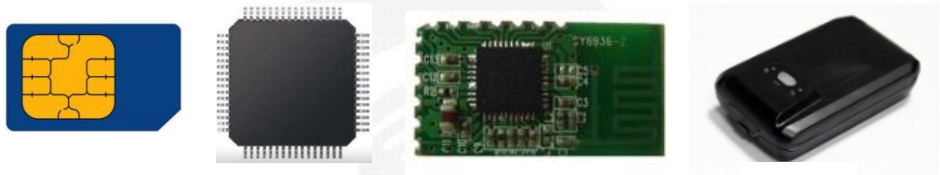


图 2 常见的主动标识载体

被动标识载体，一般是附着在工业设备或者产品的表面以方便读卡器读取。在工业互联网中，被动标识载体一般只承载工业互联网标识编码，而远程网络连接能力缺乏（某些被动标识载体，如 RFID、NFC，只具备短距离网络连接能力），需要依赖标识读写器才能向标识解析服务器发起标识解析请求。如图 3 所示，常见的被动标识载体有一维条形码、二维条形码、RFID、NFC 等。

被动标识载体的主要特征有：

- 一般附着在工业设备/耗材表面，标识信息易被读取、被复制、被盗用和被误用；
- 网络连接能力受限，需要借助读写器向标识解析服务器

发起标识解析请求；

- 安全能力较弱，缺乏证书、算法和密钥等所需的必要安全能力（如安全存储区）；
- 成本低，适用于承载低价值、数量大的工业单品标识。

图 3 常见被动标识载体及其读写设备

二维码究竟是编码技术，还是载体技术？

标识编码就是一串数字或者字符，是数字世界中虚拟的身份描述；而载体就是一个卡片或者标签，是物理世界中可储存标识编码的载体。

二维码技术是在二维的平面空间里进行标识编码信息存储的方式，属于标识载体技术。二维码本身并不是某一种特定的标识编码方案，相反，二维码里可以存储很多种不同标识编码方案。打个形象的比方，二维码就是可存写标识编码的“图形化 USB”。

（二）研究范畴

本白皮书研究范畴主要包括主动标识载体(如卡、芯片、模组、终端)和被动标识载体(如一维条形码、二维条形码、RFID、NFC 等)，及主动标识载体在工业互联网中的创新应用。

二、标识载体关键技术及演进趋势

（一）被动标识载体关键技术

被动标识载体技术，包括但不局限于一维条形码、二维条形码、RFID、NFC 等，本白皮书仅对这四类在工业互联网中大量使用的技术先期进行研究和总结。

1.一维条形码

一维条形码只在一个方向(一般是水平方向)表达信息，而在垂直方向则不表达任何信息，由黑白相间的条纹组成的图案，黑色部分称为“条”，白色部分称为“空”，“条”和“空”代表二进制的 1 和 0，对其进行编码，从而可以组合不同粗细间隔的黑白图案，可以代表数字、字符和符号信息，反应某种信息。如图 4 所示。一维条形码广泛应用在商业零售、仓储、邮电、运输、等许多领域。一维条码技术是实现销售终端系统、EDI、电子商务和供应链管理的技术基础，是实现物流管理现代化、提高企业管理水平和竞争能力的重要手段。

图 4 一维条形码示例

一维条形码可以识别商品的基本信息如商品名称、价格等，但并不能提供商品更详细的信息，要调用更多的信息，需要数据库的进一步配合。一维条形码的应用可以提高信息录入速度、减少差错率；同时，一维条形码也存在容量较小（只有 30 个字节左右）、内容只能包含字母和数字、遭到损坏后不能阅读等缺陷。常用的一维条形码有:UCC/EAN-128 条码、ITF-14 条码、EAN/UPC 条码，如表 1 所示。

表 1 常见一维条形码

条码类型	主要用途
EAN/UPC 条码（包括 EAN-13、EAN-8、UPC-A 和 UPC-E)	用于对零售渠道销售的贸易项标识；同时也可用于标识非零售的贸易项目。
ITF-14 条码	只能用于标识非零售的商品
UCC/EAN-128 条码	用于标识物流单元，不能用于 POS 零售结算。

从载体自动识别技术的角度讲，符号会越来越小型化，占的面积越来越少；载体形式也更加多样化，性能也更加智

能化。彩虹码作为一种“升级”的码制，在国际通用 GS1 商品条码符号的基础上，增添了蓝绿两种颜色维度，可承载额外的信息。理论上可以实现每个物品拥有唯一的单品 ID，从而实现物品的“一物一码”，这在标识载体编码技术领域是一种新的探索和尝试。

2.二维条形码

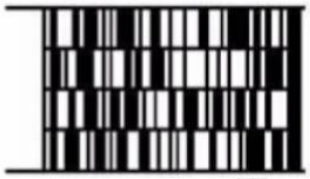
二维条形码是在一维条形码技术的基础上衍生而来的，在水平和垂直方向的二维空间存储信息的条形码，既记录横向信息也记录纵向信息，也是按照“0”和“1”的比特流原理进行设计。二维条形码技术已广泛应用在国防、公共安全、交通运输、医疗保健、工业、商业等领域。目前，在支付领域应用最多。

二维条形码是较为经济、实用的一种自动识别技术，除具备一维条形码的优点外，还具有信息容量大、信息密度高、纠错功能、可表示各种多媒体信息及多种文字信息、译码可靠性高、保密防伪性强等特点。

国内外常见的二维条形码包括 PDF417、QR 码、Data Matrix 码、Maxi Code 码等。从技术角度分类可以分为行排式二维条形码和矩阵式二维条形码两种类型。**行排式二维条形码**（又称堆积式或层排式二维码），其编码原理是建立在一维条码基础之上，按需要堆积成二行或多行。它在编码设计、校验原理、识读方式等方面继承了一维条码的一些特点，

识读设备和条码印刷与一维条形码技术兼容。但由于行数的增加，需要对行进行判定，其译码算法与软件也不完全相同于一维条码。有代表性的行排式二维条码有：PDF417、Code 16K、Code 49 等如图 5 所示。

PDF417



Code 16k

Code 49

图 5 典型行排式二维条形码

矩阵式二维条形码是平常见得最多的二维条形码，通过黑白（其他颜色也有）像素在矩阵中不同的分布进行编码，在矩阵元素区出现的点(方，圆等形状)表示二进制的“1”，不出现则表示“0”，通过点排列确定其信息。矩阵式二维条形码分为若干个小区域，每个区域有一定信息，角上有三个色块，可以保证无论从哪个方向扫描都可正确定位信息，中间色块可以存放个性化图表。有代表性的矩阵式二维条形码有：Maxi Code、QR Code、 Data Matrix、Aztec Code 等。如图 6 所示。

Maxi Code　　QR Code　　Data Matrix　　Aztec Code

图 6 典型矩阵式二维条形码

随着二维条形码生成技术的不断完善，越来越多的推广场景中使用到二维条形码，一张创意十足富有个性的二维条形码能迅速引起用户关注和兴趣。因此，二维条形码也逐渐由普通方形、黑白颜色二维条形码向形状更具个性化的彩色二维条形码转变。彩色二维条形码是一种特殊的二维条形码，具有普通黑白二维条形码的所有功能，同时又能呈现出彩色的外观。两者最大的区别在于外观，彩色的外观更吸引人，两者承载的信息量是同样的，或许以后会有彩色二维条形码独有的识别技术可以增大彩色二维条形码信息存储量，但现阶段没有本质区别。

目前激光蚀刻在基础零部件上有一定的应用，但存在扫码识读困难、技术成本高、打码后无法更改、信息难以读写等技术难题，发展相对缓慢。随着相关技术的发展成熟，激光蚀刻应用前景十分广阔。

二维码知识产权问题

二维码的前身是条形码，起源于 1949 年。二维码的发明者当时只申请了专利权，却没有发现二维码里面蕴藏的潜在商机，所以就主动放弃了使用权。中国意锐新创公司创始人王越在日本接触到了二维码之后发现了商机，于 2002 年创办了意锐公司，并联合国内众多的优秀工程师，共同研发世界上第一款手机二维码引擎;2003 年就获得具有完全自主知识产权的“二维码快速识读引擎”，并申报了条码识读方法和装置的国家专利;2005 年开发了汉信码，即中国第一个国家二维码标准，现已成为 ISO 的国际标准。

此外，早在 2011 年，凌空网创始人徐蔚就已经申请“二维码扫一扫”专利，并先后拿下了中国、美国、日本和欧盟等区域的二维码扫码技术专利权。

所以，中国人在商品二维码业务上不存在任何侵权行为。

3.射频识别

射频识别（RFID），是一种非接触式的自动识别技术，可通过无线电讯号识别特定目标对象并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触，适用于各种恶劣环境。RFID技术是条形码技术的进一步延拓，可识别高速运动物体并可同时识别多个标签，操作快捷方便。目前广泛应用于多个领域，典型的应用包括仓库物流、防伪识别、智能交通、身份识别、食品安全溯源等。

RFID和一维条形码、二维条形码不同，一维条形码和二维条形码都可以认为是打印在纸片上的标识图案，编码在图案上的黑白条或黑白格子里，没有芯片。RFID是电子标签，信息保存在芯片里，芯片可以读写，使用的打印机也是专门的打印机。

RFID 系统通常由标签、识读器和计算机网络系统三部分组成，如图 7 所示。RFID 系统工作过程中，天线与 RFID 电子标签进行无线通信，通常由识读器在一个区域内发射射频能量形式的电磁场，标签通过这一区域时被触发，发送存储在标签中的数据，或根据识读器的指令改写存储在标签中的数据。识读器可接收标签发送的数据或向标签发送数据，并能再解码后通过标准接口与计算机网络进行通信。

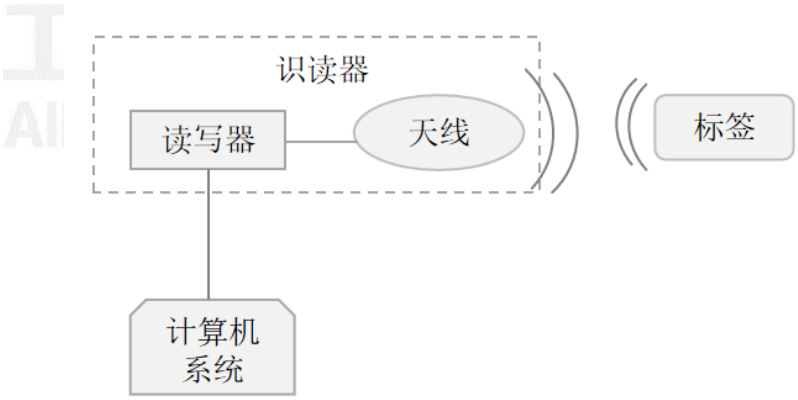


图 7 RFID 系统原理图

目前，RFID 的工作频段有低频、高频和超高频，不同频段的 RFID 产品会有不同的特性及应用场景。各频段 RFID 产品的特点及主要应用领域如表 2 所示。

表 2 不同频段 RFID 的比较

RFID 频段及应用	相关标准	工作频率	工作方式	阅读距离	数据传输	应用领域
低频	ISO 11784/11785	30KHZ-300KHZ。典型工作频率有 125KHZ，133KHZ	电感耦合，标签需位于阅读器和天线辐射的近场区域内	一般情况下小于 0.1 米	低速，数据少	低端应用，动物识别
高频	ISO/IEC 14443，ISO/IEC 18000-3	3MHZ-30MHZ。典型工作频率:13.56MHZ	电感耦合，标签需位于阅读器和天线辐射的近场区域内	一般情况下小于 1 米	中速数据传输	门禁、身份证、车票等
超高频	ISO/IEC 18000-4、-5、-6、-7	433MHz，862-960MHz，2.45GHz，5.8GHz	电感耦合，标签位于阅读器和天线辐射的远场区域内	一般情况下大于 1 米，典型情况为 4-6 米，最大可达 10 米以上	数据传输速率高，更适合快速、大容量高效的物品识别	移动车辆识别、电子身份证、仓库物流应用等

RFID 技术对于工业制造有着明显好处，可以控制生产过程、监控生产状态、形成一个闭合的制造生态圈，在物流、仓储上也能够发挥重要作用，甚至能够对工业制造企业的供应链进行整合。但由于受成本、技术等因素限制，目前 RFID 在工业制造领域中的应用很有限，应用 RFID 技术的工业制造企业大概只有 10%左右，且多以大型的汽车整车制造、汽车零部件制造等汽车相关企业为主，如丰田、尼桑、大众、江森自控等。主要用于解决整个供应链中与制造过程相关内

外资源进行实时综合协调控制和精细化管理等问题，以便及时响应顾客的个性化需求和实现产品增值并为顾客提供更好服务。随着 RFID 成本、技术等限制因素得以解决和 RFID 技术的持续发展，硬件制造技术、中间件技术、系统集成应用等所构成的 RFID 产业链将变得更加成熟，产品也将更加多样化，其在工业制造业的应用范围将不再局限于汽车等部分领域，应用范围将越来越广，从而实现其在工业制造领域需求的较快增长，工业制造领域将成为 RFID 发展的重要推动力。

RFID 技术与其他技术的融合，有利于 RFID 在工业制造领域的应用扩张，也是未来可能存在的一种趋势。如，将采用 ZigBee 协议的 WSN（无线传感网络）与 RFID 进行有机结合，利用 WSN 高达 100m 的有效半径，弥补 RFID 的抗干扰性较差、有效距离较短的不足，构成一种新的网络。WSN 负责获取物理世界的数据，RFID 负责搭建起物理世界与信息世界的桥梁，应用前景将更加广阔。

在 RFID 的标准化工作方面，目前各国家标准间还没有达成一致，尚未形成全球统一的国际标准体系，但从技术和标准的发展来看，多个国际标准并存还将长期持续，如何实现不同国际标准间的兼容和互联互通是未来发展的趋势。

RFID 的发展趋势除增加标签的存储容量以携带更多的信息、缩小标签的体积以降低成本、提高标签的灵敏度以增

加适度距离外，未来的发展方向将在超低功耗电路、安全与隐私技术、密码功能与实现、低成本芯片设计与制造技术、新型存储技术等方面。

4.近场通信

近场通信（NFC)，又称近距离无线通信，是一种短距离的高频无线通信技术，允许电子设备之间进行非接触式点对点数据传输（在 10cm 内）交换数据，主要用于手持设备的短距离数据通信，其通信方式如图 8 所示。它由非接触式射频识别（RFID）演变而来，并向下兼容 RFID。NFC 与 RFID 看似相似，但其实有很多区别，因为 RFID 本质上属于识别技术，而 NFC 属于通信技术。

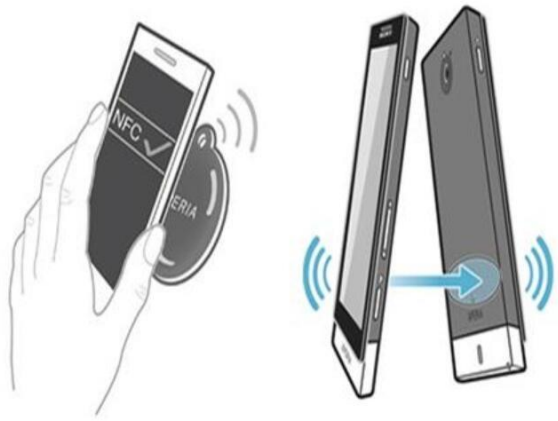


图 8　NFC 通信方式

NFC 的三个特点：**安全性**，相比蓝牙或 WiFi 这些远距离通信连接协议，NFC 是一种短距离通信技术，设备必须靠得很近，从而提高数据传输过程的安全性；**连接快、功耗低**，相比蓝牙连接速度更快，功耗更低，支持无电读取。NFC 设

备之间采取自动连接，无需执行手动配置，只需晃动一下，就能迅速与可信设备建立连接；**私密性好**，在可信的身份验证框架内，NFC 技术为设备之间的信息交换、数据共享提供安全。

NFC 明明有很多强大功能，却得不到市场亲睐的原因

■ **安装 NFC 可能需要重新设计手机**

虽然说全面屏让手机不得不重新设计，但是厂商们肯定有那么几套十分成熟的手机模板，简单升级一下就可以第二年重新发布。而安装 NFC 手机各项零部件又要重新搭配，于是很多厂商选择不安装。

■ **NFC 成本不高，但是隐形成本很大**

虽然说 NFC 芯片成本可能真的只要 20 块人民币，但是要打通手机 NFC 的各项关键节点需要投入很大的资金。

■ **社会对 NFC 认知度不够**

NFC 挺火，但是火的范围并不大。NFC 属于很小众的技术，自然流行的范围也是小众的，导致绝大多数人对 NFC 技术缺乏认知。

NFC 技术的主要应用和应用模式包括以下几个方面：

（1）NFC 技术的主要应用

NFC 是搭载在手机内部的一块芯片，它主要是用来当做手机与其它设备交换数据的通道，比如可以当成电子门禁卡，可以当做公交卡，也可以实现移动支付。

- **手机支付领域。**手机移动支付是 NFC 最有前景的一项应用，消费者在购买商品时，采用 NFC 技术通过手机等设备即可完成支付，支付可在线下进行，不需要使用移动网络，使用 NFC 射频通道实现与 POS 机或自动售货机等设备的通信，是一种新兴的移动支付方式。
- **交通领域。**将城市交通卡的功能集成到 NFC 设备上，通过卡模式实现公交卡的功能，只需 NFC 设备触碰闸机口的读卡区域，即可自动打开闸机。
- **防伪领域。**NFC 防伪技术突破了以往防伪技术的思路，采用了一种新的举措，使其具有难以伪造性、易于识别性、信息反馈性、密码唯一性及保密性、使用唯一性等特点。目前已在茅台酒、茶叶企业得到了广泛应用。通过具有 NFC 功能的手机靠近商品的 NFC 标签，即可显示出产品的一系列信息。
- **广告领域。**NFC 标签因其可重复读写、可记录读取次数等特点，相比传统广告，在互动性、读取数据、收集数据、广告效果等方面具有明显的优势。

（2）NFC 技术的业务应用模式

基于NFC技术的业务支持三种固定模式:

- **卡模式。**将 NFC 芯片安装到一个卡上，这个模式其实就相当于一张采用 RFID 技术的 IC 卡。可以替代大量的 IC 卡场合商场刷卡、门禁卡、公交卡、车票等等。此模式下的优点是卡片通过非接触式读卡器的 RF 域来供电。
- **读卡器模式。**读卡器模式的 NFC 通信作为非接触读卡器使用，可以从 NFC 标签上读取相关信息。读卡器模式的 NFC 手机可以从标签中采集数据资源，按照一定的应用需求完成信息处理功能，有些应用功能可以直接在本地完成。
- **点对点模式。**这个模式和红外差不多，任意两个具备 NFC 功能的设备都可以连接通信，实现点对点数据传输，只是传输距离较短，传输创建速度较快，功耗低。可以实现电子名片交换、数据通信、蓝牙连接等功能。

NFC 通信在发起设备和目标设备间发生，任何的 NFC 装置都可以为发起设备或目标设备。两者之间是以交流磁场方式相互耦合，并以 ASK 和 FSK 方式进行载波调制并传输数字信号。发起设备产生无线射频磁场来初始化；目标设备则响应发起设备所发出的命令，并选择由发起设备所发出的或是自行产生的无线射频磁场进行通信。NFC 与其他载体技术的性能比较如表 3 所示。

表 3 被动标识载体技术比较

识别方式及性能	一维条形码	二维条形码	无线射频识别（RFID）	近场通信（NFC）
信息识别	读取效率低，一次只能读取一个标签内容	读取效率低，一次只能读取一个标签内容	读取效率高，一次可以读取多个标签内容，但存在信息干扰（屏蔽）	读取效率高，但读写器和标签是一对一的关系，识别环境要求低
信息存储	存储量有限	存储量较一维条形码较大	存储量很大	存储量很大
适应环境	易损、易脏	易损、易脏	抗摔、抗油、抗污、可穿透	抗摔、抗油、抗污、可穿透
运营成本	成本低廉	成本低廉	成本较高	成本较高
环保方面	一次性	一次性	可重复使用	可重复使用
信息载体	纸或物表面	纸或物表面	存储器	存储器
读写性	读	读	读/写	读/写
读取方式	光电转换	光电转换	无线通信	近距离无线通信
保密性	低	中	高	最高
抗干扰能力	强	强	一般	最强
识读距离	0-0.5m	0-0.5m	0-2m（超高频）	小于 10cm
基材价格	低	低	高	高
扫描器价格	低	中	高	高

虽然 NFC 是在 RFID 技术基础上发展而来的，但 NFC 的通信距离在 10cm 内，数据传输的保密性与安全性可以得到保障。面向不同的应用场景，两者并不存在替代关系。况且现在 RFID 的应用场景还是非常多的，NFC 已经无法比拟。即使在支付领域和近距离物体识别领域，相对于二维条形码，我国 NFC 支付用户较少，市场普及率较低，主要原因是其应

用场景较少造成的。同时，目前对智能手机来说，NFC 还不是一个必需通信接口。随着商户端 POS 机的覆盖率逐渐提升，以及用户端支持 NFC 功能的手机市场占有率不断扩大，再加上市场对 NFC 支付的大力推动，我国 NFC 支付市场进入迅速崛起阶段。同时，NFC 在一些新领域也开始崛起，如温度控制 NFC 卡，将 NFC Tag 设计在明片型大小的产品中，与包装箱随运，全程记录监控箱内商品的温度及 GPS 定位。只需用手机轻触就可以读取商品在过程中的温度和 GPS 定位等资料，且误差很小。如 NFC 穿戴项链，将 NFC Tag 内嵌在项链中，用于记录幼童健康的资讯，可以通过手机软体即时更新储存的健康资料，使幼童健康履历随身携带，方便后续进行个人健康状况分析。

尽管 NFC 技术在一些领域得到了广泛应用，但仍存在诸多问题。如兼容性问题，目前不同厂家的 NFC 设备兼容性问题还比较突出，如何实现 NFC 设备间兼容互通是未来要解决的重点问题；同时，NFC 应用领域还比较局限，仍有很多新领域有待探索。

一维条形码、二维条形码、RFID、NFC 成本对比分析

- **一维条形码：**一维条形码的标签可以用普通打印纸，也可以用专门的标签纸。专门的标签纸背面带胶，便于粘附在其它商品上，每张标签的成本可以低于 1 分钱；普通打印纸的成本更低。

- **二维条形码:** 二维码的标签打印和一维条形码类似，看具体需求，可以用普通纸，也可以专门标签纸。标签纸可以低至 1 分钱；普通打印纸的成本更低。
- **RFID:** RFID 的标签内含有芯片，相比于条码成本较高。且有源 RFID 标签成本高于无源 RFID 标签。无源 RFID 标签价格可以低至 1 元之内，有源 RFID 标签成本在 5 元之内。
- **NFC:** 相比条码和 RFID，NFC 的成本更高，大致是 20 元。

（二）主动标识载体关键技术

在移动场景下，移动终端可承载主动标识编码。工业互联网标识编码及其相关信息（如证书、密钥、算法等）可以保存在移动终端的部件中。以下三种移动终端部件可作为工业互联网主动标识载体，如图 9 所示:

- UICC 通用集成电路卡
- 移动通信模组
- MCU 芯片

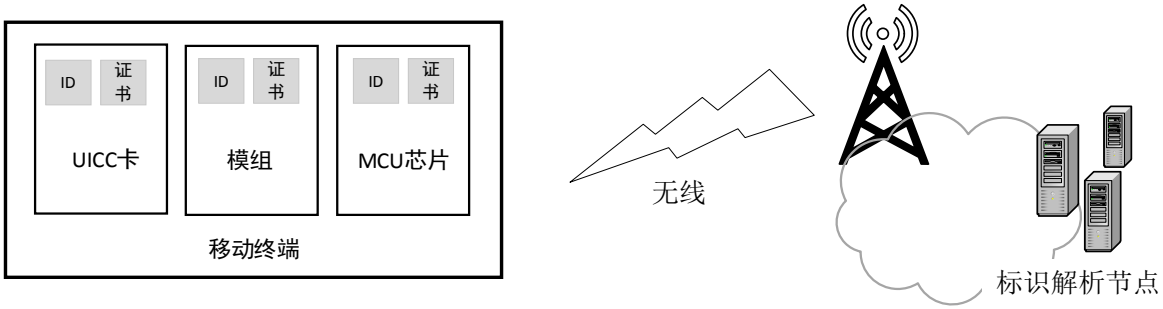


图 9 移动场景下的工业互联网主动标识载体

在固定场景下，固定终端可承载主动标识编码。工业互

联网标识编码及其相关信息（如证书、密钥、算法等）可以保存在固定终端的部件中。以下两种固定终端部件可作为工业互联网主动标识载体，如图 10 所示:

- 通信模组
- MCU 芯片

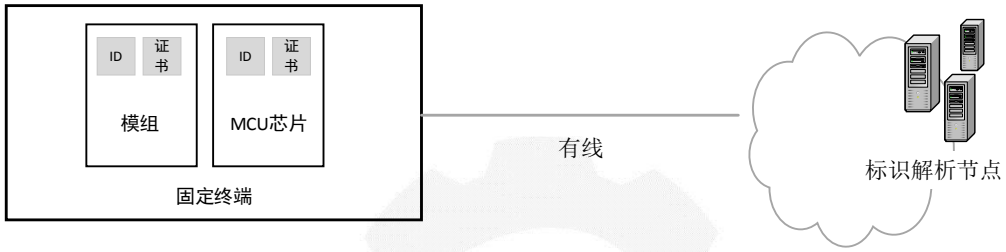


图 10 固定场景下的工业互联网主动标识载体

1.通用集成电路卡

通用集成电路卡（UICC），是在全球移动通信系统中使用的智能卡，主要用于存储用户信息、鉴权密钥、短消息、付费方式等信息，还可以包括多种逻辑应用，例如用户标识模块（SIM）、通用用户标识模块（USIM）、IP 多媒体业务标识模块（ISIM）、以及其他如电子签名认证、电子钱包等非电信应用模块。UICC 中的逻辑应用可以单独存在，也可以多个同时存在。不同移动用户终端可以根据无线接入网络的类型，来选择使用相应的逻辑模块，如图 11 所示。

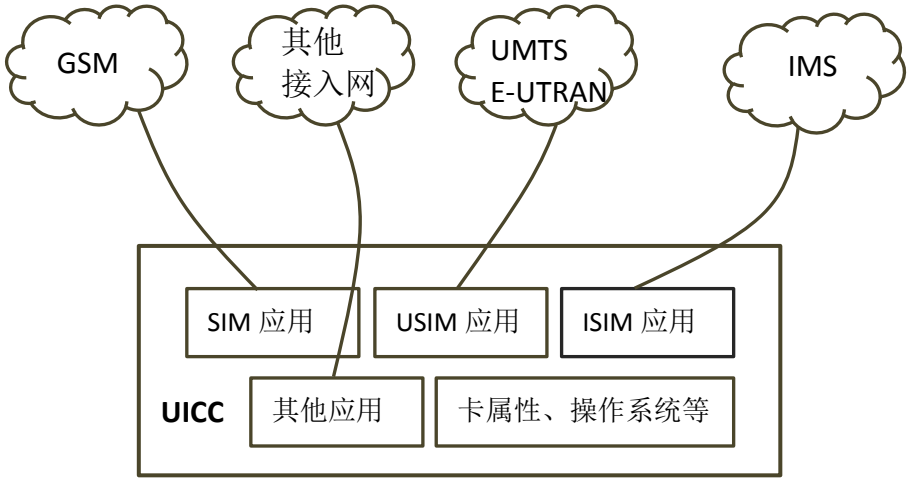


图 11 UICC 及其卡应用

UICC 支持的卡应用与相应的移动通信网络的对应关系如表 4 所示。

表 4 UICC 卡应用与移动通信接入网

序号	UICC 卡应用	接入网技术
1	SIM	GSM（2G）
2	USIM	UMTS（3G），E-UTRAN（4G）
3	ISIM	IMS（NGN）
4	CSIM	CDMA2000（3G）
5	R-UIM	CDMA，GSM，UMTS

UICC 与卡应用的概念辨析

UICC 能够确保卡数据的完整性和安全性，通常可以容纳几百千字节。除了卡应用，UICC 还可以提供电话簿和其他应用程序的存储。

在 2G 网络中，SIM 卡和 SIM 应用程序绑定在一起，因此“SIM 卡”是指具有 SIM 应用程序的 UICC 物理卡。在 3G 网

络之后，从专业角度上，把 USIM，CSIM，SIM，ISIM，R-UIM 称为“卡”是错误的，因为它们都是在 UICC 卡上运行的应用程序，被称为“卡应用”。

UICC 相关标准主要由 ISO/IEC、3GPP、ETSI、GSMA 等组织制定。UICC 相关标准与标准化组织/联盟的对应关系见图 12。

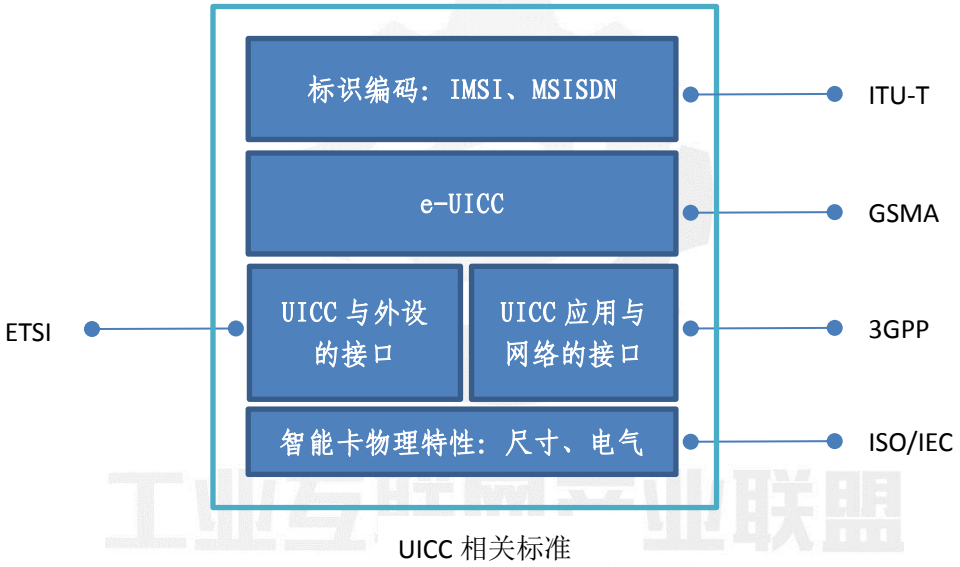


图 12 UICC 相关标准及其标准化组织

- ISO/IEC 7816-1（1987）、ISO/IEC 7816-2（1988）分别定义了标识集成电路卡的物理特性、物理尺寸和触点位置，关注智能卡的物理电气层面，是 UICC 标准的规范性引用文件之一；
- ETSI UICC 系列标准主要关注 UICC 与终端的接口，包括 UICC 应用可编程接口、UICC 终端接口、卡应用工具包一致性、SIM 应用工具包等；

- 3GPP 制定 SIM、USIM 以及智能卡测试规范、终端与 SIM/USIM 的测试规范等;
- GSMA 主要制定 eUICC 及其管理平台的规范;
- ITU-T 制定了 UICC 可承载的全球移动用户编码 IMSI、MSISND（即电话号码）等编码规范等。

将工业互联网标识解析系统的接入能力封装为 UICC 卡的一种卡应用，将有利于工业互联网标识的规模化使用，同时也有利于工业终端通过工业互联网标识及其相关数据安全接入到工业互联网应用中。如图 13 所示，类似于其他卡应用，工业互联网标识的相关应用可打包成工业标识应用，并部署在 UICC 的卡应用区。

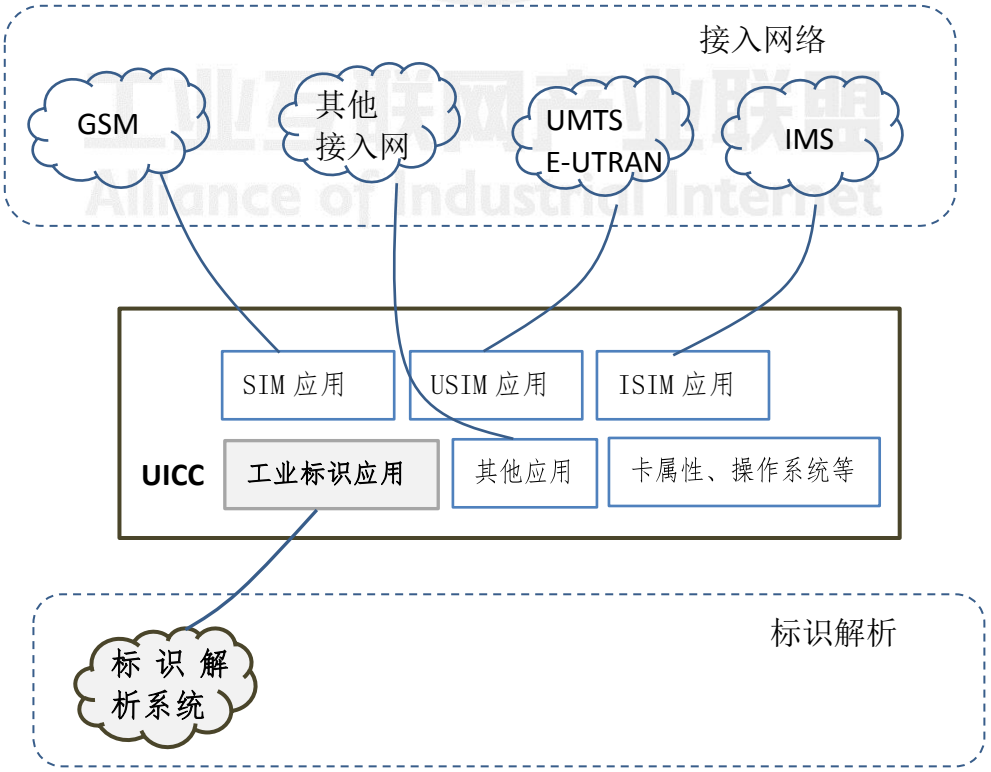


图 13 UICC 在工业互联网标识中的应用

UICC 内部区域介绍

UICC 卡内部包括两个区域，卡数据区和卡应用区。卡数据区主要存储 UICC 卡的属性信息、操作系统信息等。在卡应用区存储各种卡应用。

考虑到工业互联网（面向企业，如野外监控设备）和消费互联网（面向消费者，如手环）的需求，目前 UICC 正朝着 eUICC 的方向发展，不可插拔的 eUICC 更加适合于在工业环境下使用，eUICC 能满足更宽泛的不同等级的工作温度、湿度、持续工作时间的需求，在物理可靠性、功耗和尺寸等方面性能优于传统插拔式 UICC 卡，同时远程写卡应用的能力也更加适合于工业业务流程与运营商卡流程融合，具有支持丰富商业场景的条件。eUICC 卡逻辑架构图如图 14 所示。

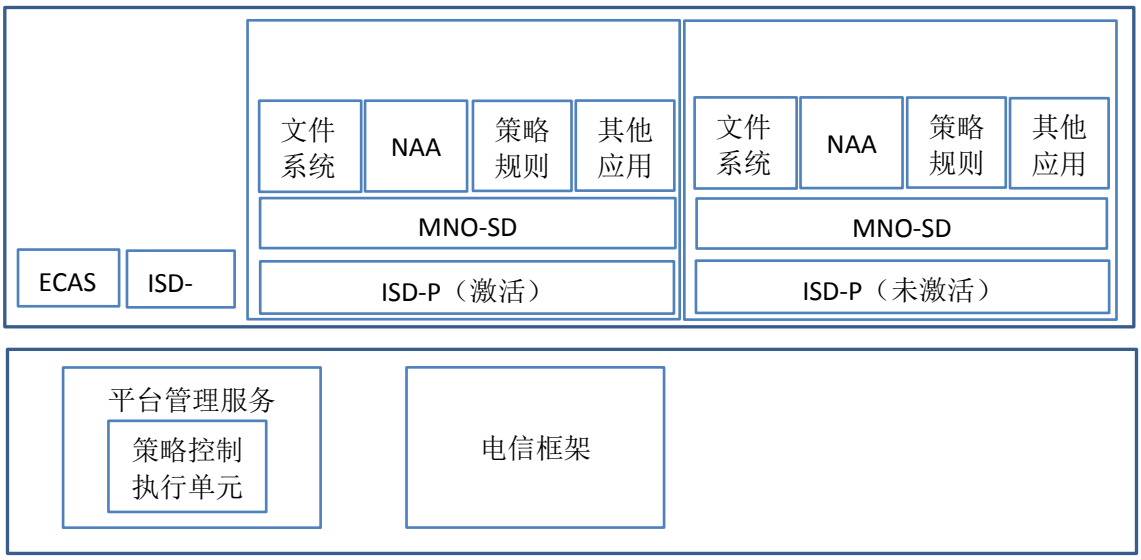


图 14　eUICC 卡逻辑架构图

国际标准组织 ETSI 率先面向物联网领域提出了 M2M eUICC 的概念，eUICC 即嵌入式卡，可为贴片式（SMD）或直接封装于通信模块中（SIP），主要特征是物理形态上由传统的可插拔式变为内嵌式，具有与终端不可分离的特性。GSMA 在原 eUICC 的物理特性基础上，又提出了“可自由切换卡文件”的定义，补充并丰富了 eUICC 的软件特性，即 eSIM 技术。GSMA 面向物联网 M2M 领域和消费电子 Consumer 领域分别制定了 eSIM 架构规范、技术和测试规范，定义了 eSIM 框架结构、传输协议和接口、消息构成及远程管理流程和方式。此外，GSMA 正在制定安全认证规范 SGP.25、测试证书规范 SGP.26。eUICC 卡会下载来自不同远程管理平台提供的 Profile 数据包，这就对 eUICC 卡数据兼容性提出了较高的要求，SIMAlliance 负责制定 eUICC Profile 的下载、安装等相关技术要求和测试规范，验证 Profile 数据是否能够被正确的解析并加载到 eUICC 上，提升 eUICC 卡数据兼容性和互联互通性能。

国际上 eSIM 在物联网领域的应用较多，如车联网、智能表具、智能家居等，尤其是在跨境网联汽车方面已经有较为成熟的应用；在消费电子领域，eSIM 技术被应用于可穿戴设备、平板电脑、笔记本电脑和手机等设备。目前国内 eSIM 技术应用主要集中在物联网和工业互联网等领域，如智能可穿戴设备、车载设备等。

eSIM 技术有多种实现方式，eUICC 是其中较为常见且标准化方案相对完善的一种。除 eUICC 外，eSIM 还可以通过 TEE、eSE 和 iUICC 等方式实现:

- TEE（Trusted Execution Environment）是指利用终端可信执行环境，使用特定软件调用 eSIM 数据，这种方案成本较低，安全性不高。考虑其成本优势，可应用在一些对安全性要求不高的物联网终端设备中。
- eSE（embedded Security Element）是指利用通用安全芯片实现 eSIM 功能，安全级别较高，成本也很高，可应用在金融支付等对安全级别要求较高的场景;
- iUICC（integrated UICC）一体式通用集成电路卡是一种 SoC 解决方案，直接将 SIM 卡封装入通信模块，安全处理器内核与其他内核直接集成在一起，安全性高，成本也相应较高;
- Soft SIM 是指采用纯软件方案实现 eSIM 功能，没有实际的物理安全芯片作为依托，容易部署，但易受到攻击，安全级别非常低。不同实现方式对比如表 5 所示。

表 5 eSIM 不同实现方式对比

	eUICC	iUICC	TEE	eSE	SoftSIM
硬件载体	有	有	无	有	无
安全级别	高	高	中	高	低
成本	高	高	中	高	低

标准依据	有	制定中	制定中	制定中	无
应用演进	主流	主流	主流	主流	不成熟

UICC/eUICC 都具备唯一物理标识，可考虑利用 UICC/eUICC 卡片自身的标识 ICCID/EID 作为工业互联网终端标识。ICCID(Integrate circuit card identity)是 UICC 的唯一标识，共有 20 位数字组成。EID(eUICC ID)是 eUICC 卡芯片的全球唯一物理标识，为 32 位数值，存储在 eSIM 芯片的 ECASD(控制权限安全域)中，主要用于 eSIM 卡管理和远程配置。EID 可以被读取但不能被更改，在远程配置中关联某个卡文件信息。eUICC 发卡形式由于更适应高温高湿、无人值守、震动等环境，未来在物联网领域广泛采用的可能性非常高。EID 在生产环节既被置入卡芯片，作为工业互联网 eSIM 终端唯一标识是对各垂直行业产品生产环节进行追溯非常有效的手段。卡文件的下载、激活、删除和远程维护都要运营商核心网后台通过 EID 来实现，EID 在运营商网络内有记录和追溯，方便调用和远程管理、生命周期管理，不需要标识读取设备采集数据，也不需要与运营商网络再匹配。

总体来看，随着工业互联网标识解析体系的建设和发展，以 UICC/eUICC 卡作为工业互联网标识及其相关保密数据(包括证书、密钥、算法)的载体更适合工业互联网终端接入工业互联网标识解析系统以及工业互联网应用，具有广阔发展前景,其自身的原有标识 ICCID/EID 也具有较高的利用价值。

2.芯片

芯片，又称微电路、微芯片、集成电路，芯片是终端的中央处理器，负责整个终端的正常运行。呈现在大众面前的芯片经过了一系列复杂的工艺过程。首先采集应用需求，将具体需求用实际电路实现，然后通过 VHDL 等硬件描述语言在 FPGA 可编程器件上进行仿真和模拟，最后通过前端设计和后端综合等一系列步骤设计出能够用于生产芯片的模具MASK，芯片封装厂通过MASK 在直径为 12 寸左右的大硅片上雕刻出成百上千颗最终的芯片。一颗芯片就是一个集成了多种电子元器件的小硅片，应用范围涵盖了生产和生活中几乎所有的消费电子。

芯片包括基带芯片、射频芯片、存储芯片等，其中基带芯片（通信芯片）是核心，主要负责信息的处理。射频芯片指的就是将无线电信号通信转换成一定的无线电信号波形，并通过天线谐振发送出去的一个电子元器件。存储芯片技术主要集中于企业级存储系统的应用，为访问性能、存储协议、管理平台、存储介质，以及多种应用提供高质量的支持。基带芯片作为整个终端中最重要的部分，是系统的大脑，内部通过数字信号处理器和控制器对外界输入信息进行加工处理，包括终端各种功能执行控制、各种数据的采集控制、采集数据的处理和运算等。

基带芯片内部包括两个模块，主功能模块和扩展功能模

块，如图 15 所示。主功能模块包括 CPU 处理器，编解码器、数字信号处理器等，负责基带的信息处理等，完成基带芯片的主要功能；扩展功能模块用来承载工业标识及密钥等信息。

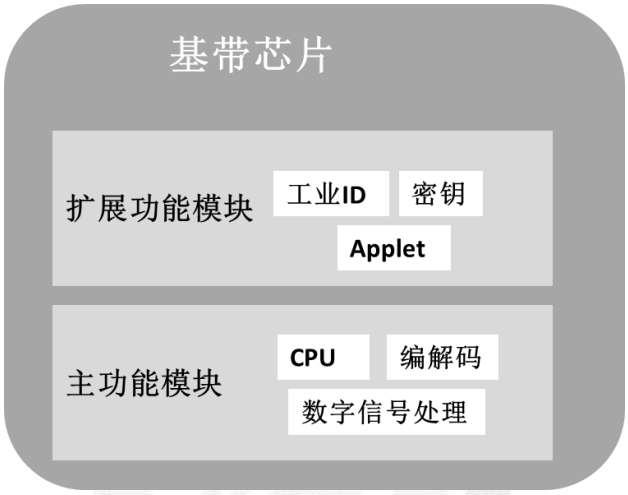


图 15 基带芯片功能模块

芯片架构主要以 x86 和 ARM 为主。相比基于复杂指令集的 x86 架构，ARM 架构由于采用精简指令集，其芯片更为精简、功耗更低。工业互联网的特性和应用场景要求其使用的芯片必须考虑功耗和集成度，这使得基于 ARM 架构的芯片在万物互联的时代占据着先天优势。当前市面上高通、华为、三星、联发科等厂家芯片均为基于 ARM 架构，市面上基于 x86 架构的工业互联网或物联网芯片较少。

3. 模组

模组是连接感知层和网络层的关键环节，属于底层硬件，具备不可替代性，无线通信模块与终端存在一一对应关系。无线模组按功能分为“通信模组”与“定位模组”，如图 16 所示。相对而言，通信模组的应用范围更广，因为并不是所

有的终端均需要有定位功能。本文接下来描述中的模组均指通信模组。

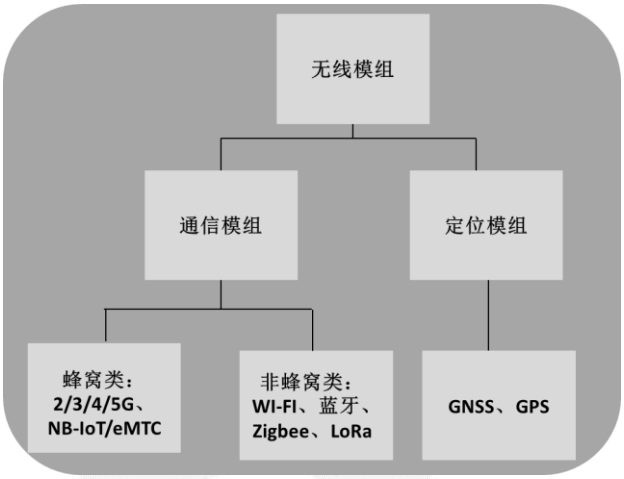


图 16 模组分类

通信模组是指硬件加载到指定频段，软件支持标准的无线蜂窝协议，软硬件高度集成模组化的一种产品的统称。硬件上将射频、基带集成在一块 PCB 小板上，完成无线接收、发射、基带信号处理功能。软件支持语音拨号、短信收发、拨号联网等功能。

通信模组的功能是承载端到端、端到后台的服务器数据交互，是用户数据传输通道，是工业互联网终端的核心组件之一。通信模组的基本功能包括接口功能和通信功能。同时，提供标准接口功能，满足各种终端的数据传输需求；具备远程数据传输功能，将工业互联网终端接入广域网或授权的专用私有网络。随着工业互联网应用的丰富以及半导体技术、数据处理技术的快速发展，新型通信模组集成了感知、前端数据处理、适度远程控制等多种功能。

通信模组主要包括主功能模块、天线接口单元、功能接口单元，如图 17 所示。主功能模块包括基带处理器、RF 模块及电源管理模块。基带处理器是模块中最核心的部分，主要功能为基带编解码、语音编码等，负责基带信号处理和协议处理。工业标识、密钥 Applet 等可以由主功能模块 MCU 承载。天线接口单元块通过 RF 天线接口为终端提供连接射频天线的接口。功能接口单元通过一系列 PIN 脚（或者 SMT 方式）与终端主板连接，提供各种信号的输入输出。

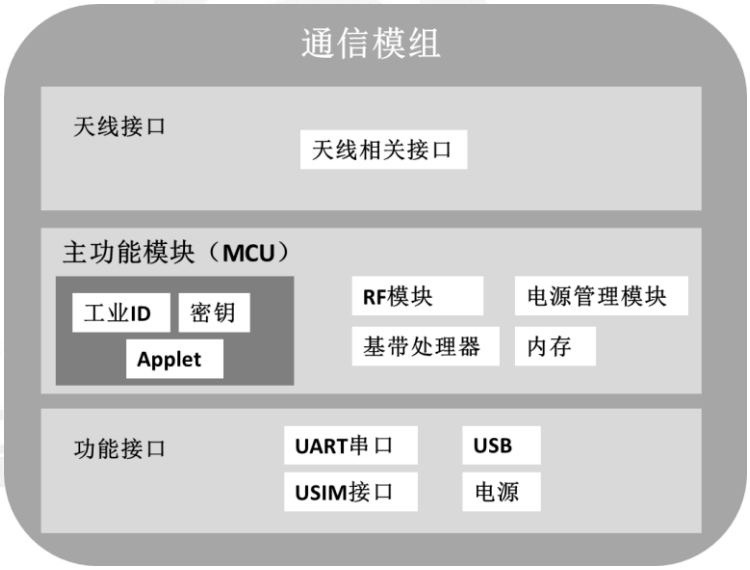


图 17 通信模组的基本组成

相比于通信芯片，模组具有以下特点:

- 模组需要重新设计与集成，主要针对各种芯片和器件，如通信协议、网络标准、体积、干扰、功耗、特殊工艺等，如工业级高低温电阻、抗振动、抗电磁干扰等;
- 模组具有定制化的特点，需要满足不同客户和不同应用

场景的具体需求，同时满足下游用户多样化的通信需求。

当前，用户已经不满足于模组只承担联网功能，还要求模组能够有集成感知、前端数据处理、适度程度控制等综合功能，甚至将 Android、WiFi、蓝牙、GNSS 等功能集成在一起。面对下游终端不断变化的需求，上游芯片制造商无法直接向下游终端制造商提供定制服务，下游终端由于其技术能力和研发成本而难以直接采用通信芯片，因此模组已成为上游芯片和下游终端的关键连接点。

4.终端

工业互联网终端是工业互联网中连接感知延伸层和网络层，实现数据采集(或汇聚)及向电信网络发送数据的设备，它担负着数据采集、预处理、加密、控制和数据传输等多种功能。从通信技术的角度，终端是网络的端节点，是消息传递的末端。从行业应用的角度，终端提供行业所需的功能，因此形态和功能差异很大。工业互联网终端架构包括主控模块、电信网接入模块、数据采集与控制模块、数据汇聚模块、电源模块、外设接口模块等，如图 18 所示。

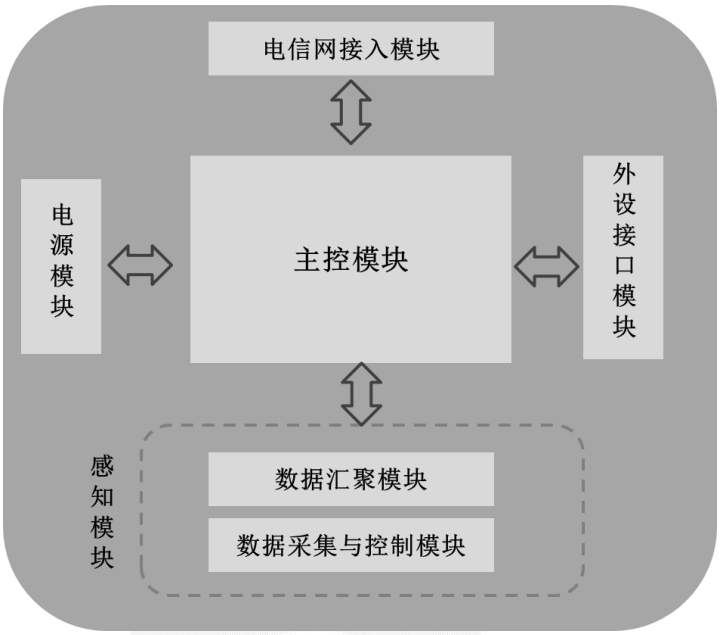


图 18 工业互联网终端架构

主控模块主要实现协议转换、预处理、管理和安全等各方面的数据处理和存储；电信网接入模块采用有线或者无线接入方式将工业互联网终端接入广域网或授权的专用私有网络，提供与工业互联网综合运营管理平台及工业互联网业务平台或应用之间的数据传输；有线接入方式包括 DSL、PON 和有线宽带等，无线接入方式包括 GSM、WCDMA 和 LTE 等；数据采集与控制模块负责数据的采集与封装，以及上层下达的控制命令的执行。根据不同的应用场景，数据采集与控制模块可以是传感器、摄像头、RFID 读卡器和专业数据采集器等；数据汇聚模块负责将数据采集与控制模块获取的数据通过 USB、RS232、RS485、数字 I/O、模拟数据接口或 WiFi、蓝牙、ZigBee 等短距离通信接口进行数据交互，完成物理信息数据的汇聚及远程控制功能；电源模块负责系统供电及节能管理，

可能的供电方式包括市电、太阳能、蓄电池等；外设接口模块提供外设的统一接入接口。

不论何种类型的行业终端，按网络技术的差异性，可分为移动终端和固定终端两类。移动终端一般指支持蜂窝无线通信技术（如 2G/3G/4G/5G、NB-IoT/eMTC 等）的终端，如安装了 4G 移动通信模块的挖掘机。固定终端一般指支持有线通信技术或者近距离/短距离无线通信技术的终端，如监控摄像头。

移动终端和固定终端的基本功能架构是类似的，差别在于，移动终端有 UICC/eUICC，固定终端没有 UICC/eUICC，如图 19 所示。

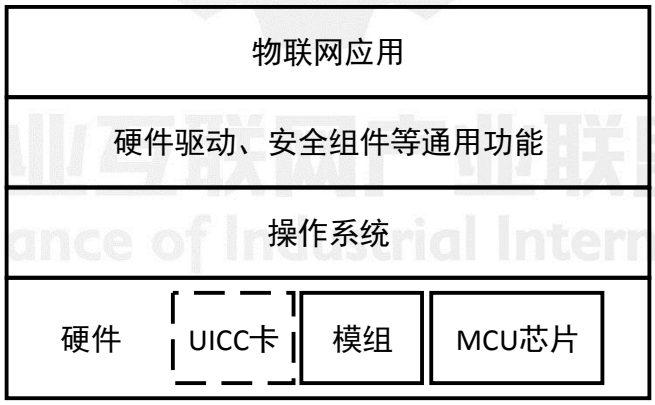


图 19 终端基本功能架构

其中工业互联网标识可在硬件驱动和安全组件等通用功能层实现，为工业互联网应用提供基于标识的身份认证等安全服务。结合工业互联网发展应用环境，工业互联网终端从运算能力和抗风险能力角度可被分为两类：强终端和弱终端。其中，强终端在工业互联网网络中是运算能力相对较强

的终端，成本较高，如网关类或工控类终端产品，其承载的业务场景相对丰富，且所面临的安全风险相对较大，因而对其抗攻击能力要求也较高；而弱终端是工业互联网网络中运算能力相对较弱的终端，成本较低，典型代表如数据采集或预处理设备、传感器等，其承载的业务场景相对单一，且面临的安全风险相对较小，因而对其抗攻击能力的要求也相对较低。

从信息安全角度而言，弱终端应具备的安全能力包括但不限制于：

- 与云端的双向认证；
- 密钥/码管理；
- 应用完整性安全；
- 远程或 OTA 安全固件升级；
- 支持类 SE 安全芯片部署等。

典型的强终端除具备上述能力外还应考虑自身对于来自网络或物理的攻击抵抗能力，包括：

- 安全启动；
- 系统加固或隔离；
- TEE 可信操作环境；
- TPM 可信运算模块；
- 病毒检测能力；
- 端口裁剪等。

典型的工业终端包括工控网关、摄像头等。

5.工业互联网标识载体技术演进趋势

标识的使用，最初是用来辨认商品和商品的种类。将商品加上一维条码,就可以避免人为的错误，举凡进货,销售,盘点等都能利用条码判别商品,这也能加快工作的速度,更能提高效率。作为标识载体，一维条形码价格便宜且容易获得，能够满足这一需求。

随着条形码的使用，人们对条形码中所能承载的信息量有更多需求，比如厂家希望能够通过条形码判别商品来源、商品类别、价格等,以服务相应商业活动，如防止跨区窜货。二维条形码能够承载更多信息，所以逐渐成为更受欢迎的标识载体。一维条形码、二维条形码等技术虽然成本低，但是数据不能重写、不能批量读写，在需要对商品进行批量管理的场景下作用显得局限。于是出现了 RFID、NFC 等可重写、可无线读写的标识载体技术。不过RFID、NFC 等被动标识载体在网络连接能力、防伪和身份认证上有局限。

主动标识载体与运营商的公共网络能力相结合，网络覆盖范围大、具有加密、身份认证等安全能力,除了承载标识,还能承载与标识相关的应用、标识载体能够主动发起与标识相关的服务，更加具有自动化和智能化。主动标识载体是新型的工业互联网标识载体，在当前阶段尚未有商用产品。随着通信技术设施和工业产业的发展，具有广域网络覆盖、良

好安全能力以及具有智能化基础的主动标识载体将是发展方向。

三、标识载体产业生态及发展现状

产业链的本质是用于描述一个具有某种内在联系的企业群结构，是一个相对宏观的概念，存在结构属性和价值属性两维属性。产业链中大量存在着上下游关系和相互价值的交换，向上游延伸一般使得产业链进入到基础产业环节和技术研发环节，向下游环节输送产品或服务及市场拓展环节。

为更好的研究标识载体技术体系架构，本文对二维条形码、RFID、NFC 技术产业链进行了研究分析。

（一）产业链分析

1. 二维条形码产业链分析

二维条形码的产业链主要涉及码制技术、编码、通信硬件、码生成和打印设备、读取 和解析设备等领域，产业链构成如图 20 所示。

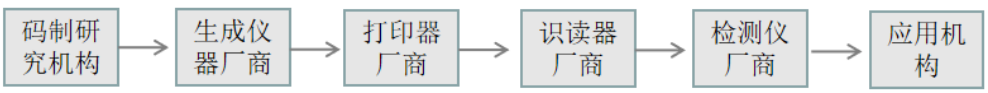


图 20 二维条形码产业链构成图

从全球市场来看，当前世界上 90%的二维码个人用户在中国，我国已成为名副其实的二维码大国，但并不是二维码

强国。目前全球二维码设备市场的主要提供商大多集中在美国、日本等发达国家。

码制研究机构：目前我国使用最广泛的是日本 Denso 公司 QR 码和美国 SYMBOL 公司的 PDF417 码，我国自主研制的汉信码在整个市场中仅占据不到 5%的份额。

生成仪器厂商：主要包括草料二维码、微微二维码等。

打印器厂商：目前主要包括大族激光、华工科技、东芝等。

识读器厂商：主要包括斑马科技、霍尼韦尔、得利捷等国外厂商和华为中兴等手机终端厂商。

2. RFID 产业链分析

一条完整的 **RFID 产业链主要**包括标准的制定、芯片设计和制造、天线设计和制造、标签封装（把天线和芯片封装到一块）、读写设备开发与生产、中间件、应用软件、系统集成等。其中最关键的技术是芯片的设计与制造。产业链构成如图 21 所示。

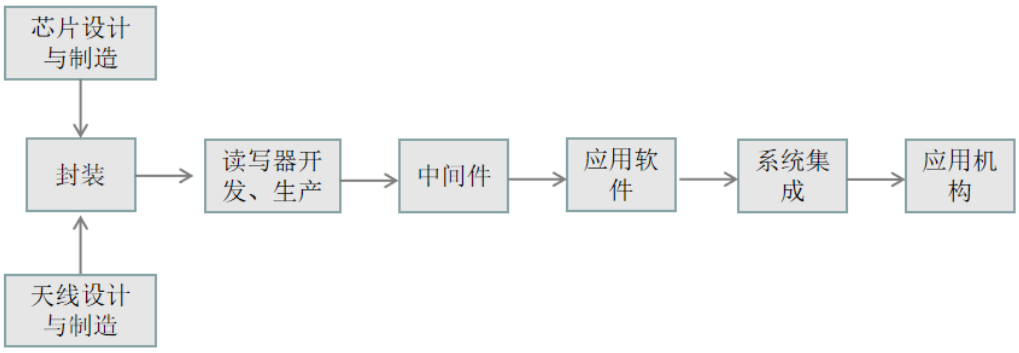


图 21 RFID 产业链构成

从全球产业格局来看，目前 RFID 产业主要集中在 RFID 技术应用比较成熟的欧美市场。飞利浦、西门子、ST、TI 等半导体厂商基本垄断了 RFID 芯片市场; IBM、HP、微软、SAP、Sybase、Sun 等国际巨头抢占了 RFID 中间件、系统集成研究的有利位置; Alien、Intermec、Symbol、Transcore、Matrics、Impinj 等公司则提供 RFID 标签、天线、读写器等产品及设备。相较于欧美国家，我国在 RFID 产业上的发展还较为落后。虽然我国 RFID 企业总数虽然超过 100 家，但是缺乏关键核心技术，特别是在超高频 RFID 方面，由于超高频 RFID 技术门槛较高，国内发展较晚，技术相对欠缺，且从事超高频 RFID 产品生产的企业很少，更缺少具有自主知识产权的创新型企业。在低频领域，由于低高频 RFID 技术门槛较低，国内发展较早，技术较为成熟，芯片、天线、标签和读写器等硬件产品已得到广泛应用，目前处于完全竞争状况。

芯片设计制造: 芯片在 RFID 的产品中占据着重要地位，大概占到 RFID 标签成本的三分之一。目前，国内清华同方、上海华虹、大唐微电子、复旦微电子、北京华大等集成电路企业在智能卡低频和高频芯片领域取得了一定的技术突破，打破了国外厂商垄断地位，但在超高频芯片领域仍面临巨大困难。

标签封装技术: 目前国内已涌现出如深圳华阳、中山达华等一批封装技术较成熟的企业，但大多企业只能做标签纯

封装，缺乏制作 Inlay 的能力。在防水、抗金属等柔性标签封装方面面临巨大困难。

读写器设计制造: 目前国内低频领域读写器生产加工技术已较完善，生产经营的企业很多且实力较强，大致有三四百家，主要有航天金卡、深圳明华、广东德生、深圳先施、北京蓝卡等；高频领域读写器生产加工技术基本成熟，但具备制造能力的企业还比较少，只有远望谷、深圳先施、上海秀派、江苏瑞福等几家十家左右。

系统集成商: 国内集成商大致分为两类:国外大厂商(如 IBM、HP 等）与国内集成商和硬件厂商合作企业；国内较有影响力的集成商，大多应用在中小企业，如中兴、航天信息、实华开、北京维深、倍思得等。

RFID 中间件: 当前我国的 RFID 中间件市场还不成熟，应用较少而且缺乏深层次上的功能。目前比较有影响力的中间件企业基本为国外企业，如 SAP、Manhattan Associatesz、Oracle、OAT Systems 等。国内一些规模较大的软件公司也相继投入了 RFID 中间件的研究，形成了一批中间件专业厂商，如金蝶、东方通、中关村科技等，国内市场基本形成了国内外厂商激烈争夺的局面。

3. NFC 产业链分析

NFC 技术产业链主要包括内容提供商（为移动用户提供所需服务）、终端制造商（芯片厂商提供 NFC 芯片及相关接

口附件）、设备制造商（提供专用的 NFC 手机支付读卡器）、电信运营商（提供移动网络，实现身份鉴定、空中充值以及手机搜索等功能）、应用机构（与移动运营商合作，共同商讨共赢的商业模式）。产业链构成如图 22 所示。

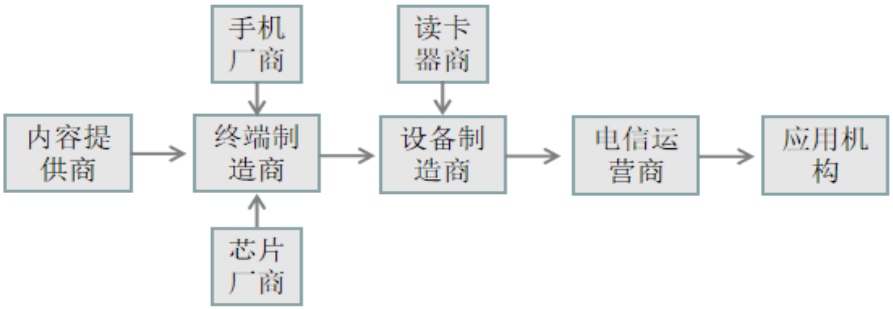


图 22 NFC 产业链构成

终端制造商：芯片厂商提供 NFC 芯片及相关接口附件，终端厂商在此基础上研发制造 NFC 手机等终端。目前 NFC 芯片国际厂商包括 NXP、英飞凌、ST、瑞萨、高通、联发科等；国内厂商则有华虹、同方微电子、复旦微电子、大唐电信等；NFC 天线主要供应商有 TDK、村田等，国内公司有顺络电子、信维通信、硕贝德、瑞声科技等公司。NFC 手机厂商主要有华为、中兴、苹果、小米等厂商。

设备制造商：地铁、公交和电影院等地方安装的专用 NFC 手机支付识读设备，这些设备由 NFC 设备制造商提供，如深圳西莫罗科技、东莞心意通电子、华为、苹果、小米、三星等。

电信运营商：为用户提供移动网络，实现身份鉴定、空中充值以及手机搜索等功能。

4. 物联网卡产业链分析

物联网卡产业链构成可分为三部分，最上游是运营商，中游是渠道商，下游是终端使用者，如图 23 所示。

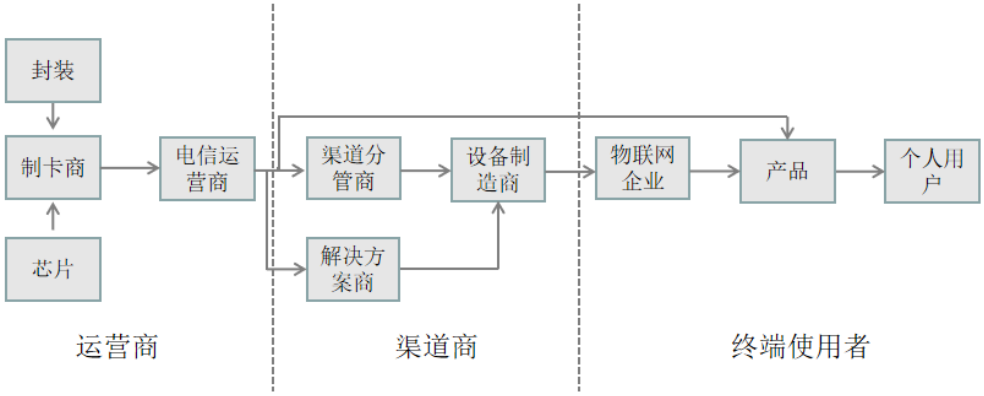


图 23 物联网卡产业链构成

运营商：运营商是网络的提供者，也是物联网卡的最初发售者。运营商搭建通信网络，同时向诸如大唐、金雅拓等制卡商定制物联网卡。即所有的物联网卡都在运营商的定制下进行生产。运营商再将物联网卡在物联网平台上进行录入，此时物联网卡就具备了使用功能。值得注意的是，这里的运营商并非仅仅电信运营商，能够搭建 Lora、Sigfox 网络的运营商也在其列。

渠道商：物联网产业是 B2B2C 的商业模式，从运营商的连接、平台与应用出发，主要用户都不是 C 端的最终用户，而是 B 端的商业用户。这些商业用户主要包括行业合作伙伴，例如通讯模组、定位模组厂商、代理商；物联网系统集成商，例如物联网项目软硬件设计、开发、实施企业；行业运营企业，例如摩拜单车、车联网企业；硬件制造商，例如智能锁

厂、燃气制表厂；物联网产品生产企业，例如小米、360 儿童手环；物联网产品销售企业，例如智能后视镜销售商、360 渠道商分销商。

终端使用者：经过 B2B2C 的商业模式，终端用户将包括项目与产品两类。项目面对的 C 端客户为政府或者企业级项目，产品面对的 C 端客户为使用智能硬件的产品或者个人。

这三部分就构成了物联网卡产业链的 B2B2C 的商业模式。其中有些环节将会由于技术创新或者商业模式创新突然爆发出来，获得海量增长，诸如共享单车、远程抄表、智慧路灯等应用，这些都是值得产业链各方进行关注。

当前，物联网卡的运营以电信运营商为主体，物联网卡的业务流程按照物联网卡物理形态的不同略有差异，如图 24 所示。对于传统物联网卡，电信运营商的省分公司从用户收集物联网的业务需求，电信运营商的终端公司与卡商经过评估，将可以实现的业务需求制定规范并交由卡商生产物联网卡，物联网卡生产完成后由运营商负责发卡。用户在省分公司办理物联网卡后插入物联网终端使用，运营商物联网运营公司负责后续物联网卡的业务运营。eSIM 的业务流程与传统物联网卡类似，区别在于 eSIM 没有实体物联网卡，卡商在 eSIM 时代消亡，运营商终端公司直接和物联网终端厂商完成基于 eSIM 的物联卡生产，生产完成后 eSIM 的运营主体依然为电信运营商的物联网运营公司。

物联卡的数据写入，无论是传统物联网卡还是 eSIM，当前阶段均由发卡主体（电信运营商）完成，如图 24 所示。未来，物联网卡可能承担更多的业务应用（例如标识业务），这部分应用数据（标识信息）的写入可经运营商授权，由终端厂商或者用户写入。

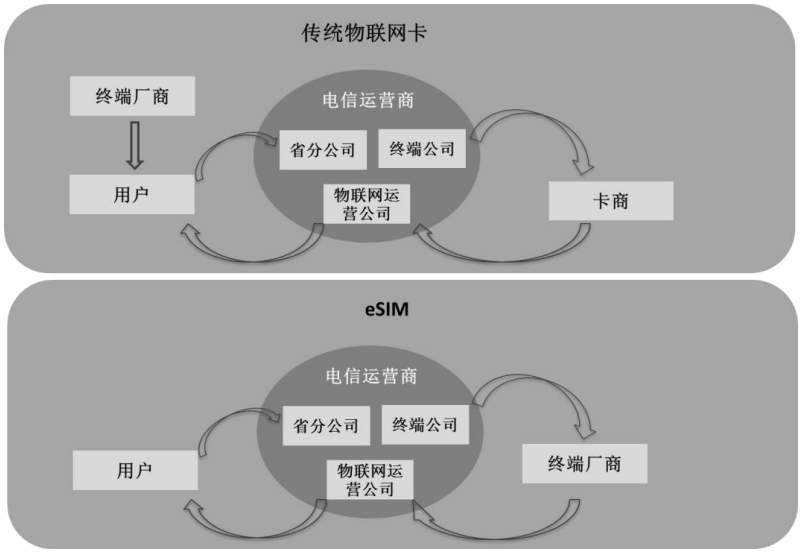


图 24 物联网卡数据写入架构

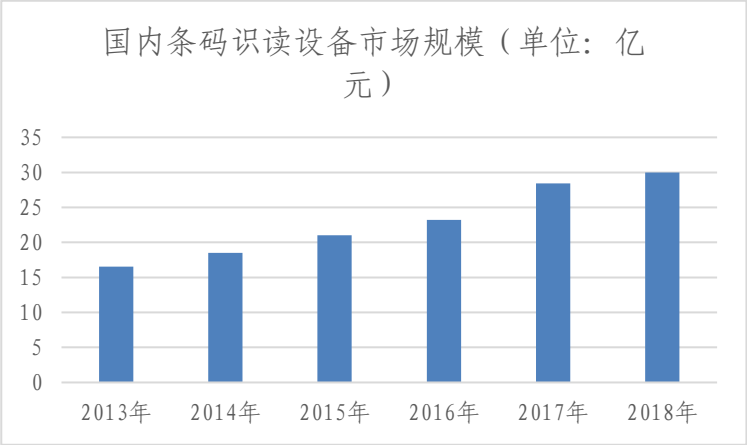
（二）市场规模

1.二维条形码产业市场规模

中国互联网络信息中心（CNNIC）2019 年发布的第 43 次《中国互联网络发展状况统计报告》显示，截至 2018 年 12 月,我国手机网民规模达 8.17 亿,网络支付用户规模达 6 亿,而这其中绝大部分都是通过手机扫描二维码实现的。移动互联网用户数基本等同于二维码个人用户数，这意味着我国二维码个人用户数量应在 6 亿左右，这个数字几乎相当于欧洲人口的总数。最新数据显示，当前世界上 90%的二维码个人

用户在中国，我国已成为名副其实的二维码大国。

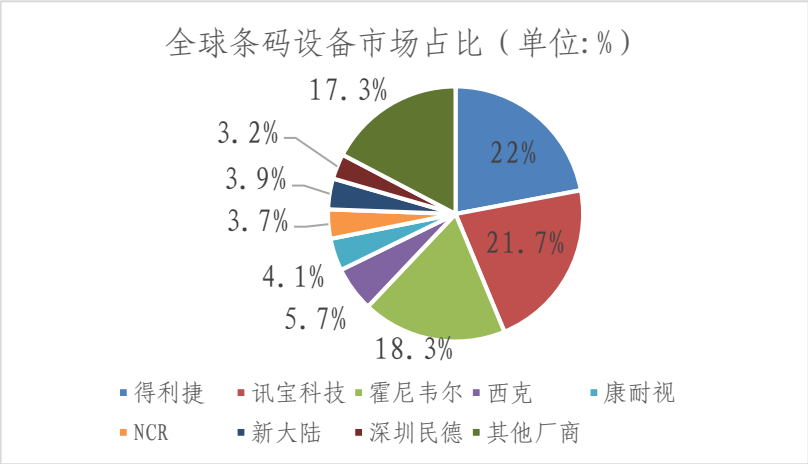
2013 年我国条码识读设备市场规模约 16.53 亿元，2017 年国内条码识读设备市场规模达到了 28.42 亿元，2018 年国内条码识读设备市场规模达到了 30 亿元，如图 25 所示。



数据来源：安全生产监督管理局、前瞻产业研究院

图 25 国内条码识读设备市场规模

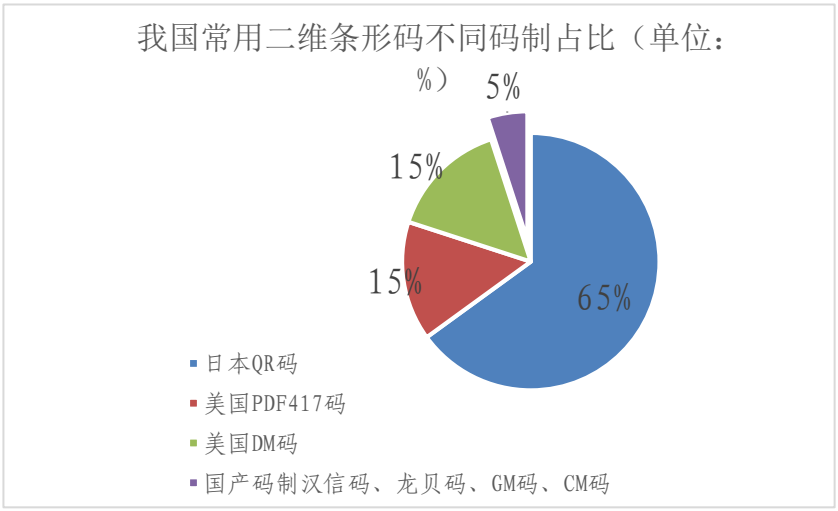
据前瞻产业研究院统计，全球现有的一维码、二维码码制达到 250 多种。从条码识读设备市场的竞争格局来看，全球条码设备市场中，得利捷、讯宝科技(已被斑马技术收购)、霍尼韦尔这三家公司占比约 60%，大幅领先于其他厂商，成为全球条码设备市场的主要提供商。国内厂商凭借技术研发与创新，已在条码设备市场占得一席之地，但市场占比很小；前七强国内厂商包括新大陆(3.9%)和深圳民德(3.2%)，国外厂商依然占据领先优势，具体占比如图 26 所示。



数据来源：前瞻产业研究院

图 26 全球条码设备市场占比

目前我国应用最广泛的是日本 Denso 公司 1994 年研制的快速响应码（QR 码），由于当时国内没有自主知识产权的二维码技术，2000 年 QR 码成为我国国家标准，并广泛应用于政务系统、智能制造、金融支付、电子商务、新闻传媒等领域，其占比为 65%。其次，美国 PDF417 码和 DM 码各占 15%，国产码制汉信码、龙贝码、GM 码、CM 码等加起来还不到 5%，如图 27 所示。



数据来源：前瞻产业研究院

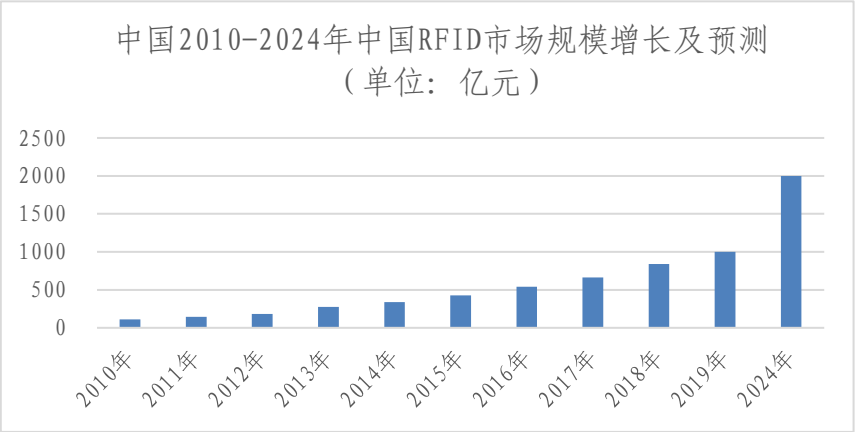
图 27 我国常用二维条形码不同码制占比

当前最为流行的 QR 码，对全球都是免费且开源的，经过二十多年的产业布局，目前在普及和推广上相比其他码制有明显的领先优势。然而，QR 码始终是国外的专利，从信息安全和国家战略的角度长远考虑，我国依然需要大力推广自主二维条形码码制标准，以提升我国在全球二维条形码领域的话语权。尽管目前我国自主研发的汉信码、GM 码、CM 码的标准能力、技术水平等都不低于国外标准，完全具备替换 QR 码和 PDF417 码的技术标准能力和产业配套能力。但国产标准因缺乏政策扶持和驱动而迟迟不能得到有效使用，且目前常用的 APP 终端，如微信、支付宝等不支持汉信码的扫码识别，这极大制约了我国自主研发二维条形码产业的发展。因此，大力推广国产二维条形码技术是势在必行，也是未来发展的大方向。

2. RFID 产业市场规模

自 2010 年中国物联网发展被正式列入国家发展战略后，中国 RFID 及物联网产业迎来了难得的发展机遇。据中国 RFID 产业联盟数据显示，2011-2017 年，中国 RFID 行业的市场规模呈不断上涨趋势，且增速保持较快。2017 年，中国 RFID 行业市场规模为 662 亿元，2018 年达到 840 亿元，2019 年底有望达到 1000 亿元左右。据前瞻产业研究院预计，未来五年，中国 RFID 行业市场规模年均复合增长率将会维持在 15%

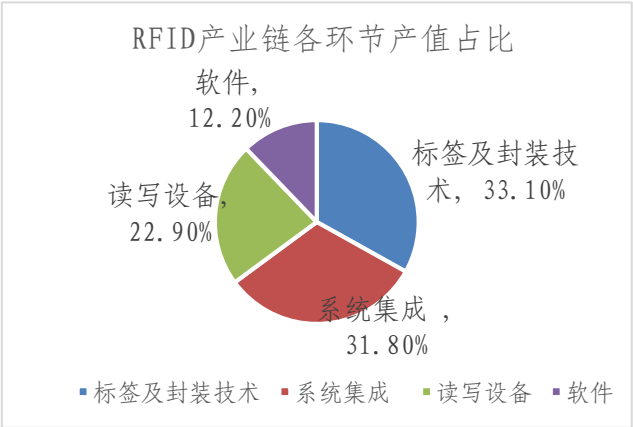
左右，到 2024 年将突破 2000 亿元。中国 2010-2024 年中国 RFID 市场规模增长及预测如图 28 所示。



数据来源：中国 RFID 产业联盟、前瞻产业研究院

图 28 2010-2024 年中国 RFID 市场规模增长及预测

目前 RFID 产业链中，从各环节的产值占比情况来看，比重最大的是标签及封装板块，约为 33.10%；其次是系统集成板块，占比约为 31.80%；读写器具和软件的产值占比分别约为 22.90%和 12.20%。如图 29 所示。

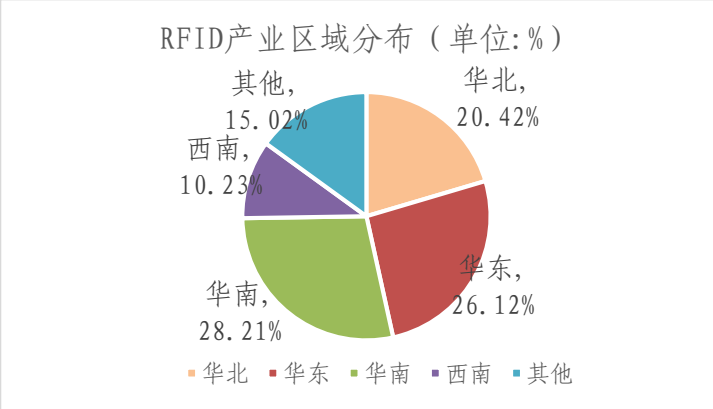


数据来源：前瞻产业研究院

图 29 RFID 产业链各环节产值占比

现阶段，中国 RFID 产业呈现以北京为代表的环渤海湾、以上海为代表的长三角和以广东、香港为代表的粤港地区遥相呼应且快速发展的态势。上海地区以前端（芯片）为龙头，深圳企业以中后端（绑定与封装）和应用为先导，而北京以系统集成为代表。

从市场分布数据为例来看，华南、华北、华东是目前我国 RFID 市场相对成熟的区域，分布如图 30 所示。

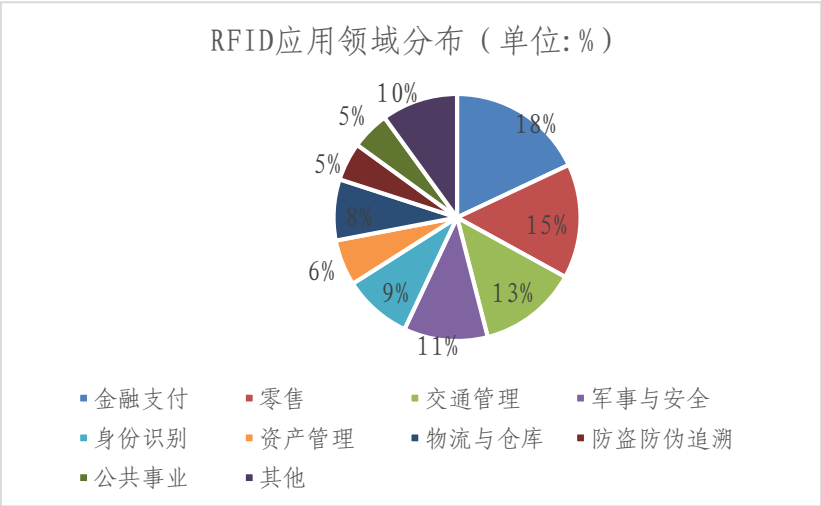


数据来源：前瞻产业研究院

图 30 RFID 区域分布

随着中国经济的高速发展，RFID 在金融支付、物流、零售、制造业、服装业、医疗、身份识别、防伪、资产管理、交通、食品、动物识别、图书馆、汽车、航空、军事等其他领域都将发挥越来越重要的作用。

从我国 RFID 在各个领域的应用市场占比情况来看，目前金融支付是其目前应用最大的市场，占到 18%；其次是零售和交通管理，分别为 15%和 13%。各领域应用市场占比如图 31 所示。



数据来源：前瞻产业研究院

图 31 各领域 RFID 应用市场占比

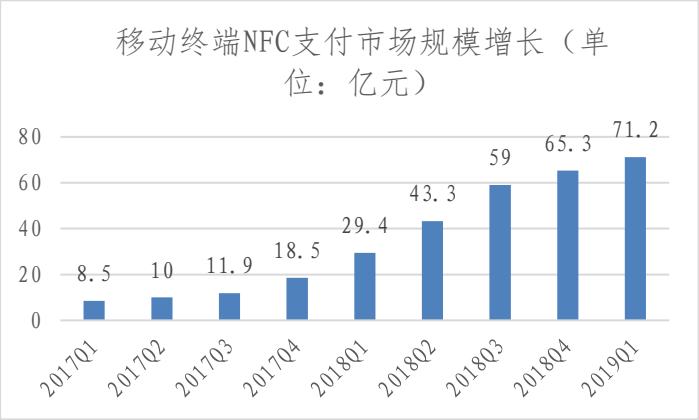
从各个细分应用市场来看，智慧物流仓储及食品溯源领域的代表企业有远望谷、中瑞思创、新大陆、达华智能、万达信息、华宇软件等；零售业领域的代表厂商有中瑞思创、远望谷等；在图书馆系统领域，在 2011 年远望谷收购海恒后，其市场占有率达 80%。

3. NFC 产业市场规模

近年，NFC 增长势头强劲。2016 年，全球智能手机出货量为 13.6 亿部，年成长 4.7%，而具备 NFC 功能的智能手机在这年全球出货量就达到了 3.96 亿。2017 年，我国市场中，NFC 手机销量为 1.29 亿台，同比增长 18.4%，NFC 设备已被较多手机厂商所应用。2018 年以来，市场上 2000 元以上的智能手机都已具备 NFC 功能，NFC 功能的手机拥有钱包功能，可以把所有卡片（银行卡、门禁卡、校园卡、会员卡、公交

卡）统统都装在智能手机钱包 APP 里中，手机钱包的是互联网金融服务公司生态获客的入口，手机 NFC 支付优势明显。

2014 年 10 月年苹果发布了基于 NFC 手机支付功能“苹果付”，美国正式上线。2016 年 2 月，“苹果付”业务中国上线。2016 年 3 月，星与银联合作在中国上线了支持 NFC 技术的“三星付”业务。2016 年 4 中国银联与小米公司联合推出支持 NFC 的“小米付”移动支付产品。2016 年 8 月，国银联携手华为公司推出支持 NFC 的“华为付”，合作银行达 30 家，支持公交地铁乘车刷卡。根据新思界产业研究中心发布的《2018-2022 年中国 NFC 近场通信技术市场分析及发展前景研究报告》显示，用户端与商户端的硬件条件逐渐成熟，带动了我国移动 NFC 支付市场规模快速发展。2017 年我国移动 NFC 支付市场规模达到了 48.9 亿元，到了 2018 年第一季度，我国移动 NFC 支付市场规模达到了 29.4 亿元，据艾瑞研究院最新统计，2019 年第一季度移动智能终端 NFC 支付交易规模达 71.2 亿元。移动智能终端 NFC 支付交易规模增长趋势如图 32 所示。



数据来源：新思界产业研究中心、艾瑞咨询研究院

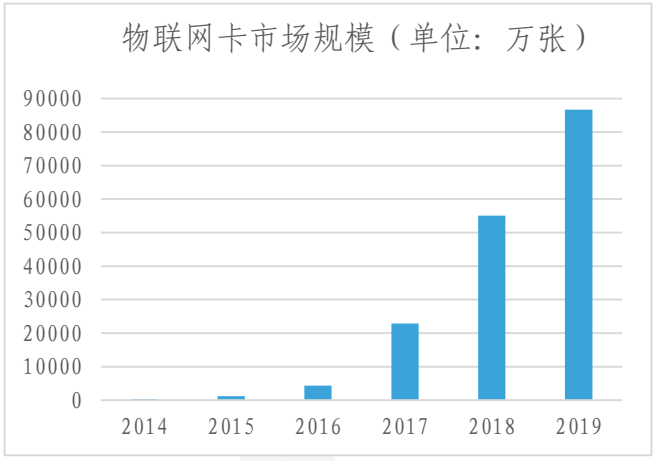
图 32 2017Q1-2019Q1 移动终端 NFC 支付市场规模增长

4. 物联网卡产业市场规模

根据中国信息通信研究院统计数据，截止 2018 年中期，我国物联网产业总体规模已达 1.2 万亿，完成了工信部 2016 年提出的十三五物联网产业规模 1.5 万亿的 80%，发展飞速。同时，公众网络 M2M 连接数已达到 5.4 亿，全国产值超过 10 亿元的骨干企业已达到 120 家，制定了 81 项国家和行业标准，形成了 5 个特色产业聚集地，面对重大的发展机遇，各产业巨头强势入局，生态构建和产业布局正在全球加速展开。

伴随着物联网技术的发展，物联网卡用户数量大幅提升并快速发展。截止 2019 年 6 月，三家基础电信企业物联网卡用户数已达到 8.67 亿，相比 2018 年 12 月，中国电信物联网卡用户数同比增长约 0.22 亿，中国移动物联网卡用户数同比增长 1.82 亿，中国联通物联网卡用户数同比增长约 0.35 亿。相比于 2018 年底，国内物联网卡用户数达到净增

2.4 亿，预计 2020 年底将达到 14 亿左右。如图 33 所示。



数据来源：中国信息通信研究院

图 33 物联网卡市场规模及增长趋势

当前物联网卡按使用场景不同可分为流量卡、语音卡和短信卡三类。不同类型的物联网卡根据使用量的不同又分为高中低三档。例如，高流量卡（500M+）主要应用场景包括智能制造、车联网、安全和移动医疗。中流量卡（50~500M）主要应用场景为智慧物流和可穿戴。低流量卡（50M 以下）主要应用场景为公共事业和能源。语音物联网卡和短信物联网卡也有类似流量物联网卡的分类，具体应用场景如表 6 所示。

表 6 物联网卡应用场景分类

流量			语音			短信		
高流量 500M+	中流量 50~500M	低流量 50M以下	高语音 100分钟+	中语音 20~100分钟	低语音 20分钟以下	高短信 50条+	中短信 5~50条	低短信 5条以下
智能制造	智慧物流	公共事业	智慧物流	智能制造	公共事业	智慧物流	安全	能源
车联网	可穿戴	能源	车联网	安全	能源	车联网	可穿戴	
安全				移动医疗		智能制造	移动医疗	
移动医疗				可穿戴			公共事业	

来自市场研究公司 Machina Research 的最新数据显示，全球物联网连接数量在 2015 年-2025 年之间将增长 4-5 倍，2017 年，全球物联网连接数量预计为 80 亿个，根据预期，到 2025 年这一数字将增至 270 亿个，这些增长来自于智能设备、应用平台和终端用户。按照比例，中国将占据物联网连接数的 20%左右的市场，也就是说，按照 Machina Research 的预测，到 2025 年，中国的连接数将达到 54 亿左右，人均连接数达到 5 个。

物联网卡的概念

物联网卡是三大运营商（移动、联通、电信）基于物联网公共网络服务网络，面向物联网用户提供的移动通信接入业务的卡种，它采用专用号段（11 位或 13 位）和独立网元来对智能软件和物联网设备进行管理，提供用户自主的通信连接管理和终端管理等智能连接服务。

从使用物理外型看，物联网卡有三种类型：普通物联网卡、贴片物联网卡和 eSIM，如表 7 所示。普通物联网卡外形和手机用的 SIM 卡相似，可插拔。贴片物联网卡直接焊接在物联网模组上或终端内部，以实现紧密牢固的物理连接和可靠的接口通信，具有较高的抗震动性。普通物联网卡和贴片物联网卡根据使用环境的不同，可分为普通级和工业级。eSIM 就是将传统 SIM 卡直接嵌入到设备芯片上，而不是作为独立的可移除零部件加入设备中。这一做法允许用户更加灵

活的选择运营商套餐，或者在无需解锁设备、购买新设备的前提下随时更换运营商。

表 7 物联网卡分类

物联网卡类型		材质	抗震动	温度	寿命	可插拔	体积(mm*mm)
普通物联网卡	普通插拔卡	ABS/PVC 材质	500Hz	-25~75℃	2~10 年	√	Mini SIM:25*15 Micro SIM:15*12 NANO SIM：12.3*8.8
	工业插播卡	工业塑料/陶瓷	500Hz	-40~105℃	15~20 年	√	
贴片物联网卡	普通贴片卡	电路板贴装	200Hz	-25~75℃	15~20 年	×	5*6
	工业贴片卡	电路板贴装	200Hz	-40~105℃	15~20 年	×	5*6
eSIM	芯片卡(内置晶元)	-	符合芯片及模组本身属性	-40~80℃	符合芯片及模组本身属性	×	0
	集成软SIM的芯片	-				×	0
注释：①将晶元与通信芯片进行封装 ②以软件形式集成，写入芯片或模组存储隔离区							

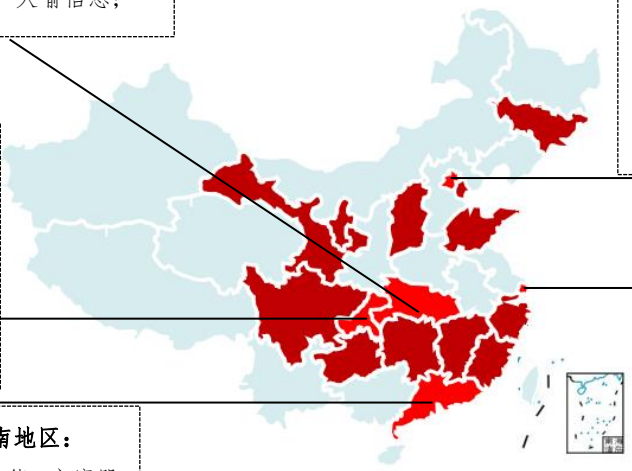
我国目前是物联网发展大国，在国际上占据着举足轻重的地位。但由于我国的物联网技术发展相较于欧美以及日韩起步较晚；再加上发达国家对我国的技术封锁，使我国的物网卡平台等技术，和欧美、日韩等国家相比仍处于一定的弱势。物联网卡虽然有着很多优势，但目前普及的程度并不高，且目前整个行业处于一种“不正规”的状态，尚未形成统一的标准。如何共同推动物联网卡标准的统一是未来发展的大趋势，也是解决物联网卡“不正规”问题的关键。其次，如何解决物联网卡行业面临的如安全问题、通信稳定性问题和升级困难等难题，也是未来发展的必然趋势。

物联网卡和普通 SIM 卡的区别

- **售后客服：**物联网卡的售后服务是由代理商或经销商负责，运营商不能提供相关服务；
- **管理方式：**物联网卡由独立的物联卡管理平台管理，与普通的 SIM 卡管理平台相互独立；
- **购买方式：**物联网卡是通过代理商或经销商购买的，不能通过营业厅办理；
- **充值方式：**物联网卡只能通过代理商提供的管理平台进行充值，不能通过其他渠道进行充值；
- **注销方式：**物联网卡通过代理商提交注销申请，或者不续费，三个月后自动注销。

（三）产业地图

从目前标识载体主要厂商分布来看，北京、上海为代表的长三角和深圳为代表的华南地区厂商数量在整个产业生态中处于绝对领先地位，华南、华北、华东已成为我国标识载体市场相对成熟的区域。在目前建设的工业互联网标识解析体系国家顶级节点区域中，重庆为代表的西南地区和以武汉为代表的华中地区几乎没有典型的标识载体厂商，在标识载体产业发展方面相对落后于华南、华北和华东地区。国内标识载体技术产业生态地图如图 34 所示。



以武汉为代表的华中地区：
二维码厂商：大族激光、华工科技；
物联网卡商：天喻信息；

以北京为代表的华北地区：
二维码厂商：华宇软件、中科金财、航天信息；
RFID 厂商：高鸿股份、同方股份、航天信息；
NFC 厂商：同方微电子、大唐电信、小米；
物联网卡商：握奇数据；

以重庆为代表的西南地区：
二维码厂商：兆麟电子；
RFID 厂商：诺塔斯科技、兆麟电子、重庆五盾科技；
NFC 厂商：重庆五盾科技；

以上海为代表的华东地区：
二维码厂商：华铭智能、浙江众合科技、新大陆；
RFID 厂商：厦门信达、新大陆、上海贝岭、中瑞思创；
NFC 厂商：上海华虹、复旦微电子；
物联网卡商：恒宝股份、梵利特智能、上海华虹、捷德科技、金雅拓；

以广东为代表的华南地区：
二维码厂商：达实智能、宝鹰股份、民德电子；
RFID 厂商：中兴、东信和平、远望谷、艾特姆射频科技；
NFC 厂商：信维通信、顺络电子、华为、中兴、OPPO；
物联网卡商：星汉智能、东信和平、楚天龙智能卡、欧贝特科；

图 34 标识载体技术产业地图

据《证券日报》市场研究中心最新数据统计，目前二维条形码产业链中共有 10 家上市公司，分别为：深圳达实智能、深圳宝鹰股份、深圳民德电子、北京华宇软件、上海华铭智能、深圳证通电子、北京中科金财、航天信息、新大陆、浙江众合科技。

RFID厂商大致有110家。其中上市公司主要有中兴通讯、厦门信达、高鸿股份、新大陆、东信和平（珠海）、远望谷（深圳）、同方股份、上海贝岭、航天信息。

NFC 国内终端厂商主要有华为、OPPO、vivo、中兴、小米、酷派等终端手机厂商；国内芯片厂商主要有上海华虹、同方微电子、复旦微电子、大唐电信等。

物联网卡国内厂商主要包括星汉智能、东信和平、恒宝股份、梵利特智能、楚天龙智能卡、天喻信息、握奇数据、上海华虹、捷德科技、欧贝特科技、金雅拓。其中上市公司有东信和平和恒宝股份。

四、面向工业互联网的标识载体技术典型应用

（一）可信数据采集

1.可信数据采集需求分析

工业数据采集作为物理世界到数字世界的桥梁，是智能制造和工业互联网的基础。工业数据采集基本功能框架包括设备接入、协议转换、边缘数据处理、中心云四部分，如图

35 所示。

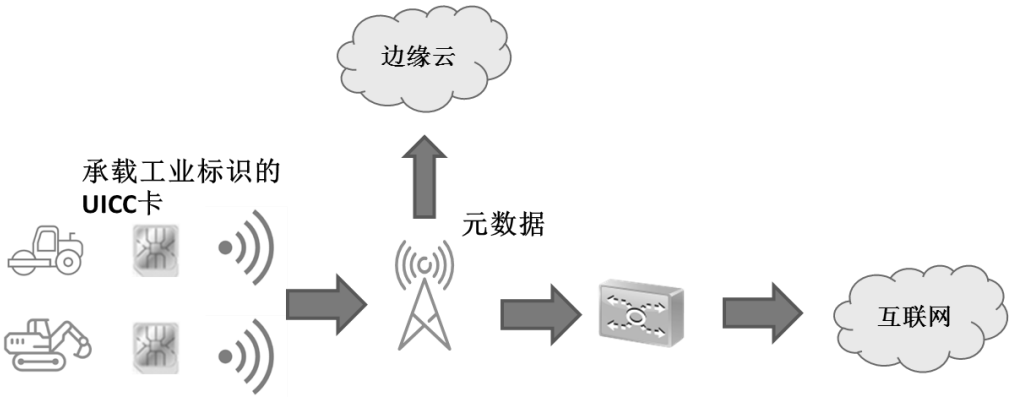


图 35 工业数据采集基本功能框架

- 设备接入指通过工业以太网、工业总线、蜂窝网络(2G、3G、4G、NB-IoT 及 5G)等各类有线和无线通信技术，接入各种工业现场设备、智能产品。
- 协议转换指通过中间件等兼容不同的工业协议，实现数据格式的统一。
- 边缘数据处理通过在靠近设备侧或数据源头的网络边缘侧对数据进行分析处理和存储，以达到降低数据响应时延、降低网络拥塞等目的。最常见的一种边缘计算处理即采用边缘云的形式，边缘云位于基站和核心网之间，在本地向用户提供功能强大的云计算服务。
- 根据应用需要，中心云接收来自端侧和边缘云的数据，向用户提供更大范围的服务。

2. 可信数据采集应用场景

目前，工业互联网领域的数据采集场景分为以下两类:

- 数控机场/专用智能设备：这类设备通过工业总线、以太网等与工业数据采集系统通信，通常为有线传输方式。此类方式成本较高、灵活性差，但安全性高。
- 物料标识读取设备：物料身份标识主要采用一维条形码/二维条形码、NFC、RFID。这类方式成本低，适用于低值单品识别。可信数据采集方案主要适用于第一种场景。

3.典型案例：中国联通可信数据采集解决方案

传统上，工业数据采集模型包括端和平台，以及连接端和平台的网络，见图 36 所示。

图 36 传统的工业数据采集模型

在这种模型下，工业终端与平台之间的数据采集等互操作主要依靠用户名+密码的方式进行访问控制与权限管理。

该模型的优点是：结构简单、技术实现容易、成本低。缺点是：当工业终端的数量较大时，用户名和密码的管理难度变大。为了便于实际操作，部署人员往往对批量终端采用相同的用户名和密码，会导致安全问题爆发，使终端成为“肉鸡”，为工业互联网的安全埋下重大隐患。

针对工业数据采集安全隐患，有必要建立基于 UICC 建

立可信数据采集系统，赋能工业产品从生产到使用贯穿通信服务商、网络运营商、模组生产商、工业企业等多个参与方接入认证，为工业企业数据安全提供保障。

基于UICC的可信工业数据采集模型，如图37所示。

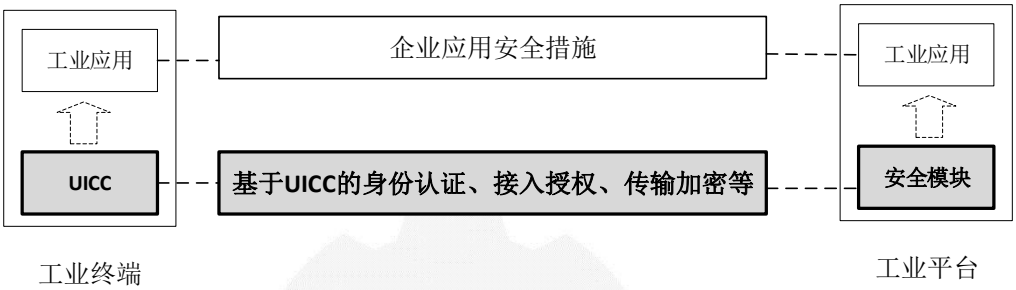


图37 基于UICC的可信工业数据采集模型

图37中，在工业终端侧采用UICC卡保存工业互联网标识及其相关的证书密码。UICC卡对工业互联网标识及其相关的证书密码进行安全保护。

UICC卡及其业务系统将网络层的终端身份识别、接入授权、传输加密等能力赋能给应用层的企业相关应用。

工业平台可根据UICC卡的终端身份识别结果接收/拒绝来自终端的数据写入。

要实现图 37 所示模型，需要在工业终端和工业平台之间增加工业标识 UICC 卡验证平台，同时还需要构建对应的UICC卡平台，如38所示。

在图38中，工业标识UICC卡验证平台：对工业终端中的 UICC 卡信息（包括工业标识符、相应的证书等）进行验证，可以验证UICC的合法性，进而验证UICC所绑定终端的

合法性。

UICC 卡平台：负责将工业互联网标识符、证书、密钥、applet 等数据写入到 UICC 卡中，同时还需要对接工业标识 UICC 卡验证平台以及其他管理平台等（如工业互联网标识符管理平台等）。

在基于 UICC 的可信工业数据采集模型中，UICC 可以充当安全锚点，企业应用的安全方案可以构建于 UICC 之上。企业应用的安全也可以独立于 UICC。可以根据需要，灵活部署。

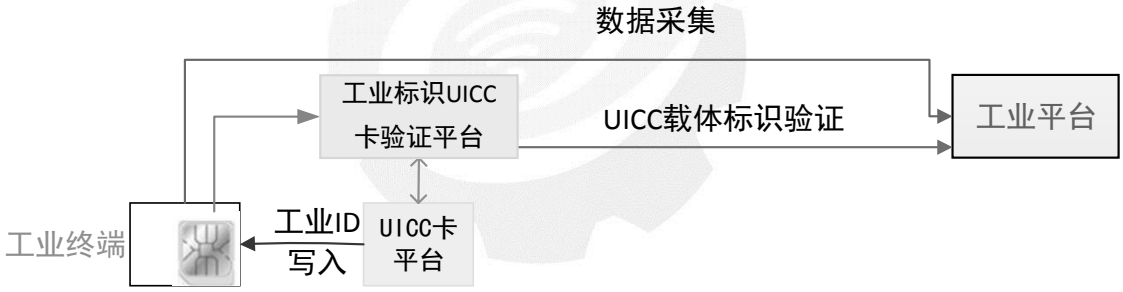


图 38 UICC 赋能工业可信数据采集

对图 38 中的各个模块进行说明如下：

- 工业终端：工业终端中需嵌入 UICC。其中 UICC 负责存储工业标识、证书、密钥、applet 等，具备通过 UICC 卡平台对 UICC 进行远程配置、远程激活、并通过无线空中接口写入工业标识的能力。
- UICC 卡平台可在运营商 SIM 卡平台基础上改造，需支持工业终端的工业标识写入，支持 profile 下载、状态管理、信息查询等功能。

- UICC 卡验证平台独立于现有运营商使用的 eSIM CA 系统，专门设计服务于工业互联网应用场景。因 eUICC 卡做为工业标识载体，可承载工业互联网标识身份认证卡应用及数据。
- 在图 39 中，工业平台是一个抽象的概念，在本文中主要指负责采集工业终端数据的平台，在实际中，数据采集能力可能会集成在不同的平台上。

将工业互联网标识灌装入 UICC 涉及到复杂的业务流程，涉及到多个利益相关方，如图 39 所示，需要多方共同协作。

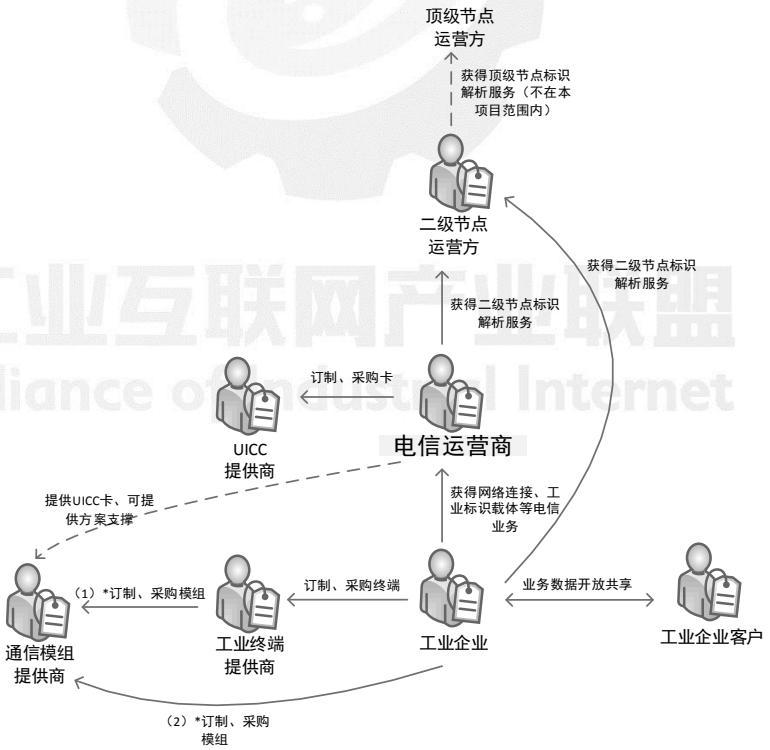


图 39 工业数据采集的部分利益相关者

（二）数据融合

1.数据融合需求分析

工业互联网的核心之一是工业数据的价值发现，即通过对工业产品在生产、销售、维护等环节数据的全面感知、实时交换、快速处理，实现智能控制。然而，由于历史原因，企业内部、企业间“信息孤岛”问题普遍存在，造成了大量数据或者未被采集、或者采集到未被有效利用，严重制约了传统工业企业向以工业互联为基础的智能制造转变的进程。

面向工业互联网的数据融合问题，具体有三种实施方案。

（1）通过采用同一标识，实现企业、行业内数据表达的统一。企业、行业采用同一种标识解析体系，实现本领域的标识数据互通。

（2）通过云平台实现不同行业、不同标识体系间的数据互通。不同标识数据在云平台汇聚，经过标识解析后，根据需求完成标识之间的转换，实现基于标识的数据互通。

（3）基于人工智能的工业数据融合。根据各类标识对应的物理实体、应用汇聚相关的数据信息，采用人工智能、机器学习等技术对工业数据进行深层次挖掘。

本白皮书主要针对采用同一种标识在行业内实现数据融合进行介绍。

2.数据融合应用场景

在实际应用中，企业间的数据关联、融合会产生新的价

值。工业互联网标识可作为不同企业间进行数据关联的媒介，实现跨企业间数据的融合。

3.典型案例：中国联通多维数据融合解决方案

以工业企业的数据与运营商数据进行融合为例，将物联网卡作为工业互联网标识载体，可实现工业企业数据与运营商数据的融合。具体示例如下:

（1）承载工业标识的物联网卡可关联运营商信息、物联网卡号以及物联网卡相关数据存放地址 URL。如图 40 所示。

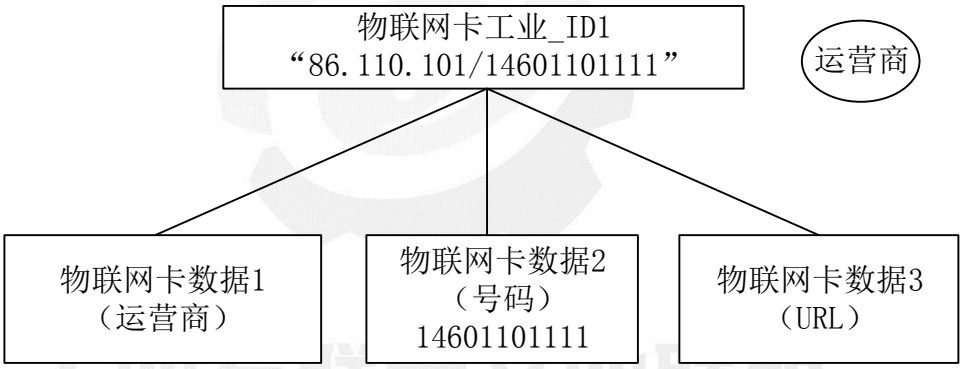


图 40 承载工业互联网标识的物联网卡数据

（2）工业互联网设备的工业标识可关联供应商信息、设备内物联网卡号信息、设备数据地址 URL 等。如图 41 所示。

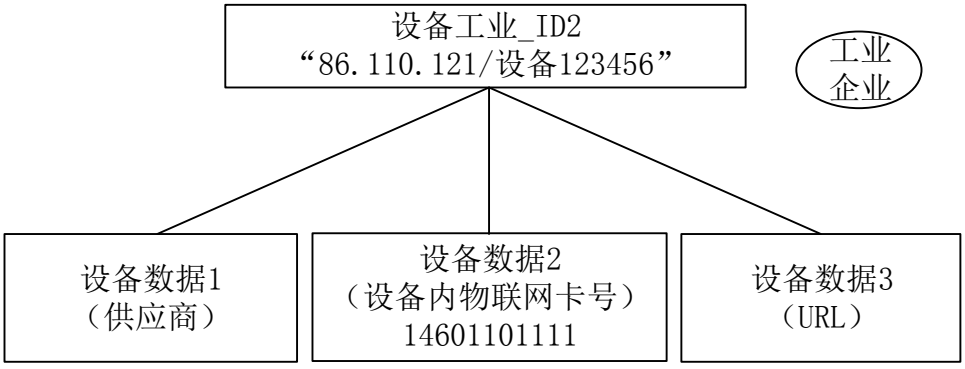


图 41 工业互联网标识所关联的设备相关数据

承载工业互联网标识的物联网卡数据和工业互联网标识所关联的设备相关数据都可以通过自己的工业标识在工业互联网标识解析系统中被解析出来，相关企业在合法的权限下可实现运营商数据与工业企业设备数据的融合，如图 42 所示。

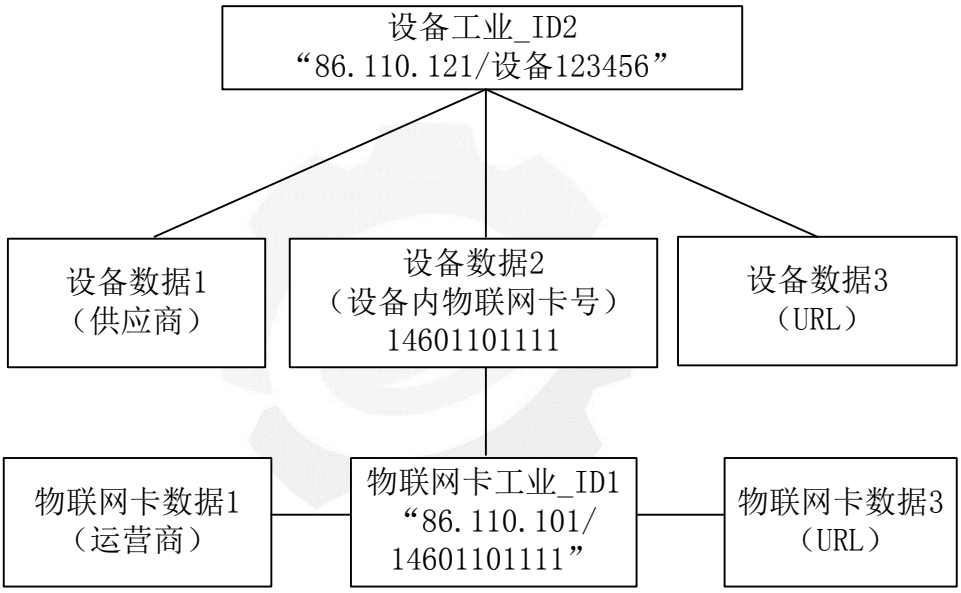


图 42 基于工业标识实现运营商数据与工业企业设备数据的融合

“设备 123456”的供应商（某工业企业）通过服务平台查询“设备 123456”的工业 ID“86.120.121/设备 123456”，除了获得设备的相关开放数据“设备数据 1”、“设备数据 3”外，还能通过物联网卡卡号获得物联网工业 ID“86.110.101/14601101111”，以此获得更多物联网卡的相关信息，完成行业间工业数据融合。

（3）eSIM 应用涉及跨运营商之间的数据交换与融合，

eUICC 卡可承载工业互联网标识和 EID 标识信息，工业标识可关联供应商信息、设备内物联网卡号信息、设备数据地址 URL 等,EID 标识可关联 eSIM 对应的 Profile（IMSI、MSISDN、ICCID）及对应的卡清单服务信息。基于 eSIM 设备的工业互联网标识跨运营商设备数据融合实现如图 43 所示。

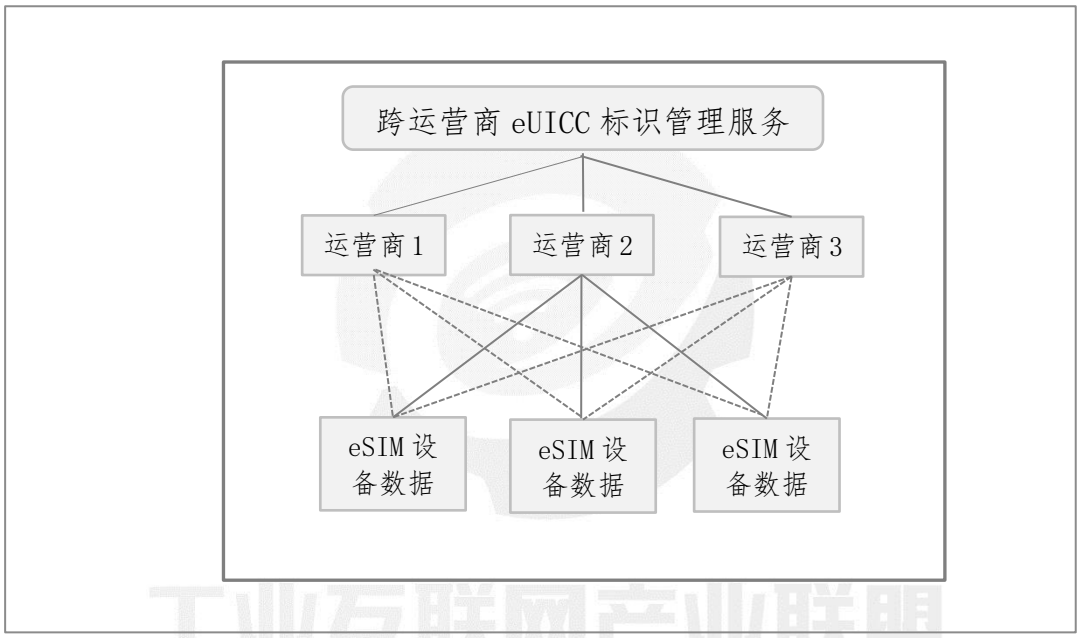


图 43 基于 eSIM 设备工互标识实现的跨运营商设备数据融合

（三）统一身份认证

1.统一身份认证需求分析

网络世界经过了互联网、移动互联网、产业互联网三个阶段，但密码输入方式一直没有改变。移动互联网向产业互联网转型的今天，密码输入面临着极大的安全挑战。万物互联时代，产业互联网渗透到生活诸多方面，智慧城市发展已初具规模。门锁、公共交通、医院就诊等不同的场合，我们

需要不同的身份认证实体，即针对每一个设施都要带一把“钥匙”。随着产业互联网的深入实施，未来我们每天可能要随身携带好几百个钥匙。之所以产生这种情形，是因为不同设施的身份认证协议并没有一个统一的全国标准。未来如果可以通过技术实现不同产业互联网设施之间的统一身份认证，通过一把“钥匙”实现所有智能设备的身份认证，那将大大便利人们的生产生活。

2.统一身份认证应用场景

在被智能设备包围的未来世界，统一身份认证方案可满足用户在不同的生活场景下的鉴权需求，应用范围辐射制造、教育、交通、医疗、社区、公共服务等业务场景。

在日常生活动，进入不同的大楼需要不同的身份识别设备，这给人们的生活和社区的管理都带来了一定的不便。结合生物识别、联网设备，利用统一身份认证方案可以解决身份交叉互信问题，协助物业更便捷高效准确地管理进入人员。

在交通领域，不同的小区、停车场采用不同的车辆身份信息（卡、车牌、公共 ETC 标签等）对车辆进行识别，这给管理和使用带来了很大的困难。基于统一身份认证方案，可以在全国范围内采用统一的汽车电子标识（如 RFID），科学高效管理车辆。

3.典型案例：腾讯公司 TUSI 解决方案

身份认证是产业互联网应用中必不可少的一个环节。通

常的处理方式是，每个应用单独管理自己发行的身份证书、单独做身份认证。由于身份及其身份认证的方式不能互通，这种方式对数据的开放共享造成了一定的障碍。

互联网统一身份认证的基本思想是：在统一的技术框架下,各应用主体可以使用不同的 CA 中心发行标识及其证书，并用区块链来对已发行的标识及其证书进行验证。该方案兼顾了灵活性和可信性，为数据共享提供了统一身份认证使能。腾讯公司的 TUSI（Tencent User Security Infrastructure）即腾讯用户安全基础设施是互联网统一身份认证的例子。该方案的基本原理如下，如图 44 所示：

- 物联节点、装置等装有 TUSI 下发的可信 TUSI-ID，可以对设备的身份进行追溯及鉴权，通过现有物联网入口，将多维度的数据收集到 TUSI 前置；
- 通过 TUSI 身份区块链系统，把数据加密后上链，各个行业及相关管理部门有 TUSI 前置节点用于解密及数据上传，同步；
- 通过 TUSI-大数据汇聚平台，实现多维度，多方面信息的筛选，汇聚，分类，清洗，建模等，输出可以供第三方使用的接口与能力；
- 相关的管理部门可以实时调取相应的物及装置的身份数据及敏感数据，比如设备状态、信息、历史记录、操作权限、生命周期等。

TUSI 可信身份区块链，借助区块链的特性，实现隐私保护，信任传递，身份索引，交叉认证等安全特性。

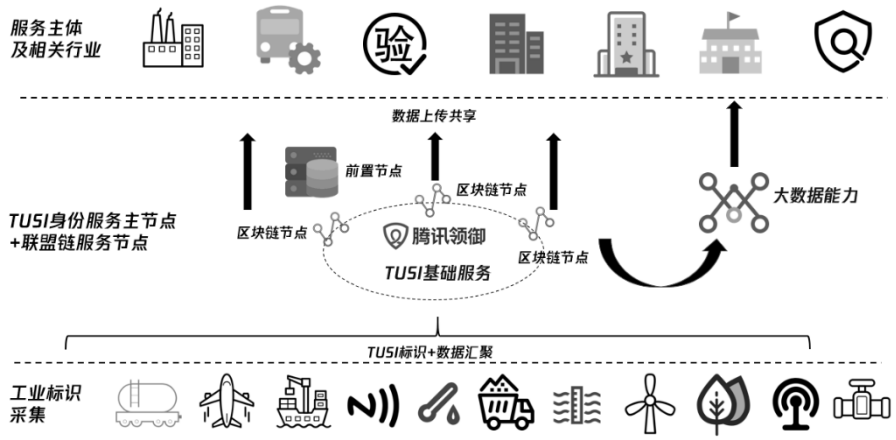


图 44 统一身份认证框架

统一身份认证涉及到 4 类利益相关者，如图 45 所示:

- CA 中心: 发行标识 ID、及其证书密钥等。
- 工业互联厂商: 通过区块链身份验证平台，对接入的工业互联网设备进行认证。
- 区块链身份验证平台:加密存储了 CA 中心发行的标识、证书等信息，为工业互联网厂商提供身份验证等服务。
- 工业互联设备: 作为标识的载体，加载了 CA 中心认证的安全模块。

由于需要具备联网能力和计算能力，互联网统一身份认证的标识载体采用 UICC 或者模组或者 MCU 芯片。

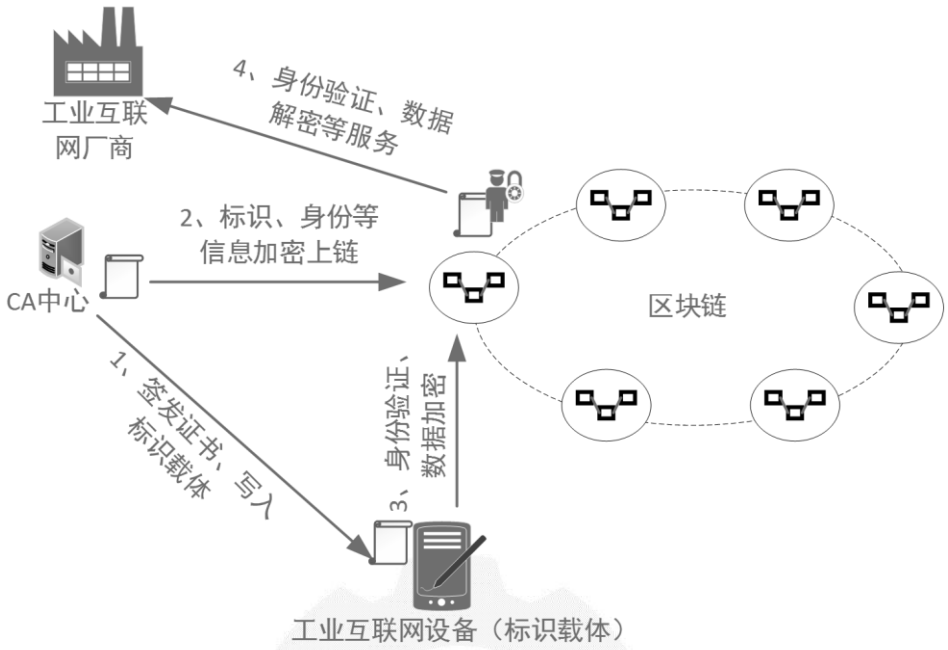


图 45 互联网统一身份认证基本流程

TUSI 身份区块链完成了从物联网设备到云端的安全闭环，其优势包括：TUSI 身份区块链是联盟区块链，相比公链更高效、更可控；TUSI 身份区块链通过 TUSI 协议形成设备端到云端的安全闭环；TUSI 身份区块链部署灵活，可封装在硬件载体亦可作为云端服务；TUSI 身份区块链高度重视用户隐私，只留存脱敏的身份索引；TUSI 身份区块链为同一用户不同场景提供交叉认证服务。

（四）接入安全认证

1.接入安全认证需求分析

当今时代，信息通信技术飞速发展。物联网作为信息通信技术的典型代表，在全球范围内呈现迅猛发展的态势。物联网应用涉及城市管理、智慧家庭、物流管理、智能制造、零售、医疗、安全等在内的众多领域、物联网应用的普及和

物联网技术的成熟推动世界进入了万物互联的新时代，可穿戴设备、智慧家庭等数以百亿计的新设备将接入网络。

物联网终端设备的规模不断增大，随之而来的威胁也越来越大，如软件漏洞、不安全通信、数据泄露、恶意软件感染等，物联网设备已成为僵尸网络的主要载体，已可形成超高容量的 DDoS 攻击源，物联网 DDoS 攻击的规模、频度、复杂性、影响和损失正在快速增长。终端智能化在给人们带来方便的同时，也暴露出越来越多的安全问题，威胁到使用者的隐私、财产甚至生命安全，安全问题已成为阻碍物联网发展和用户接受度提升的一个重要因素。

同时，全世界范围内针对物联网终端的安全解决方案也在迅速发展当中，这些安全解决方案包括了硬件安全解决方案（如安全芯片 SE）、软件解决方案（如软件沙箱）及软硬结合的方案（如可信执行环境 TEE）等，部分方案的产生源于金融、移动通信等领域的安全诉求，在适配到物联网终端并进行大规模应用时，存在安全成本与应用场景匹配难的问题，终端厂商对安全方案的衡量指标缺失、消费者用户感知及可区分性差等都造成了安全方案部署到物联网设备时面临较大挑战。

物联网设备身份认证 Link ID^2（Internet Device ID），是阿里云推出的物联网设备身份认证系统，通过可信计算和密码技术为物联网系统提供设备安全认证、安全连接、业务

数据加密等端到端的可信接入能力。ID²是物联网设备的可信身份标识，具备不可篡改、不可伪造、全球唯一的安全属性，是实现万物互联、服务流转的关键基础设施。ID²支持多安全等级载体，合理地平衡物联网在安全、成本、功耗等各方面的诉求，为客户提供用得起、容易用、有保障的安全方案，适应物联网碎片化的市场需求。

2.接入安全认证应用场景

物联网设备身份认证 Link ID²（Internet Device ID）已覆盖近 30 种应用场景，包括智能门锁、安防产品、可穿戴设备、网关、三表、无人货柜等。截止目前，阿里云 IoT 安全产品已为超过 4000 万设备提供安全服务，已有 60 多款载体接入 ID²硬件生态，100 多家生态合作伙伴。

3.典型案例：阿里云公司 Link ID²解决方案

阿里云 Link ID²提供密钥分发中心和认证中心两个服务，如图 46 所示。

分发中心采用硬件加密机和安全存储技术，确保密钥云端生成和存储的安全；与合作伙伴的安全产线对接，确保密钥安全烧录到各种安全等级的载体上。

客户将安全载体（如安全芯片 SE、SIM 卡、Secure MCU、TEE 以及软沙盒）集成到物联网设备（即终端），基于设备端和云端的 SDK，调用 ID²认证中心提供的设备认证、信息加密等接口，建立安全通道，保障业务数据的不可抵赖性、完

整性和保密性。

图 46 阿里云 ID² 原理图

核心功能：

- 设备身份认证：为每个 IoT 设备提供唯一的身份标识，基于 ID² 提供双向身份认证服务，防止设备被篡改或仿冒。
- 安全连接：提供兼容 TLS 和 DTLS 的轻量级安全协议：iTLS/iDTLS。更适合物联网设备，在保障安全性的同时大幅减少 IoT 设备的资源消耗。
- 业务数据保护：基于设备可信根派生的秘钥支持多种加密算法，为设备固件、业务数据、应用授权等敏感数据

提供安全防护。

- 密钥管理：为 IoT 系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发。

核心特点：

- 轻量化：使用 ID^2 代替 CA 证书，即节省了存储空间又节省了网络资源的消耗。仅连接握手阶段就可以节省 70%的网络资源消耗。
- 高安全：为 IoT 设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保 IoT 设备的合法性和数据的安全性。
- 广覆盖：适用于多种安全等级的 IoT 应用场景，支持不同安全等级的载体（SE、SIM、TEE、Secure MCU、软件沙箱）。

五、发展建议

（一）加强核心技术研究，构筑标识产业生态

加强工业互联网标识载体核心技术和标识解析协议等方面的研究，探索主动标识载体技术在多种场景下的典型应用，并组织进行规模性的应用示范，以引发更多技术研究和产业应用力量投入到以主动标识载体为中心的技术改造和升级活动中，形成新型工业标识载体的生产和管理能力，构筑包括标识产业基础、标识资源分配与解析服务、标识解析

应用和标识生态支撑为一体的标识产业生态，全面促进工业基础设施升级和制造业高质量发展。

（二）完善核心标准体系，加强国际标准合作

标识体系不完善是我国工业互联网发展与发达国家相比的重要差距之一，尽快构建完整的工业互联网标准体系是当务之急。同时需积极做好国际标准化组织和联盟的战略布局工作，促进我国产业界与学术界诉求与国际组织达成共识，有力推动相关核心技术成为国际标准和规范。

（三）立足垂直行业需求，聚焦联动发展创新

为进一步夯实工业互联网标识体系载体基础，需要加强信息通信产业与工业产业融合。在国家层面，要着力营造包容有序发展的环境，引导信息通信产业优势企业积极投入到工业互联网的标识载体技术创新和应用中来；在企业层面，要加快推进标识载体技术在不同行业场景的应用实践，推动工业互联网标识体系建设。共同促进工业基础设施升级改造健康、有序的开展。

（四）构建安全防护体系，保障标识数据安全

主动标识载体作为新型工业互联网标识载体可更好的实现标识接入控制和身份认证等功能，赋能工业标识解析；但技术创新往往是一把“双刃剑”，即可能为攻击者带来新的窗口。因此在研究和发展主动标识载体的同时，需要加强

在工业互联网主动标识载体证书、密钥和认证授权体系等方面的研究，提升工业基础设施安全能力，保障标识数据和解析行为的安全，从而提升工业互联网标识解析体系的安全水平。