中国移动
China Mobile

移动通信商用密码应用及可传递信任链安全赋能体系

www.10086.cn

目录

Contents

商用密码在通信领域的应用

中国移动 China Mobile

商用密码应用

加密电话 | 加密连接 | 加密视频 | 加密网络 | ……

专用密码芯片
国产商用密码算法

安连宝

SAFE Link 安全接入产品族
安全设备/硬件/网关

云视讯

加密视频

5G组网

可信计算体系 | 认证体系 | 密钥分发体系 | 网络标识体系 | ……

商用密码体系

加密芯片

加密协议

SM2非对称 | SM3哈希 | SM4对称 | ZUC序列 | ……

加密电话

和密话产品支持VoLTE下的端到端语音加密功能。通过商密算法的加密终端，主叫用户向被叫用户拨打加密电话，电话接通后，主被叫双方进行密钥协商，协商成功后，双方的话音信息在通话过程中被全程加密。

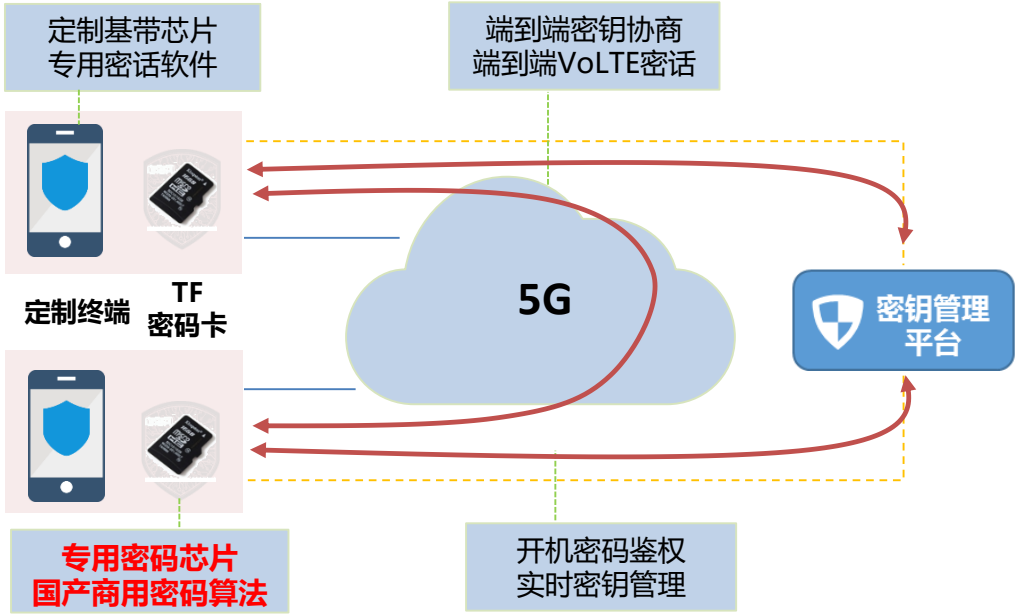
产品组成

加密终端

在标准VoLTE终端的基础上，实现VoLTE加密语音电话、密码管理等功能。

TF密码卡

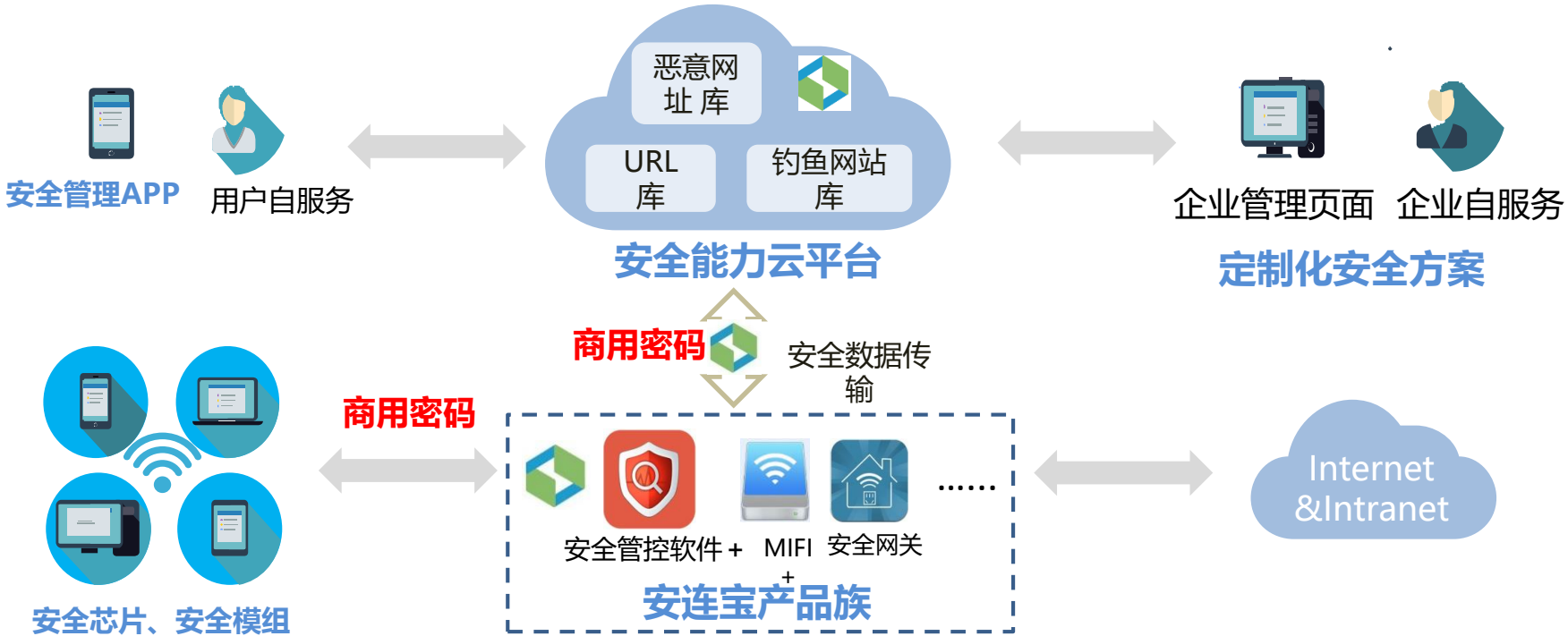
专用TF密码卡，实现密码算法运算、随机数产生、密钥产生、密钥存储、证书存储等功能。



RTP承载的语音帧加密，采用zuc128算法

加密连接

以安连宝产品族为基础，通过商用密码体系实终端设备与网关、网关与安全平台的加密连接，为物联网设备安全、信息安全管控、移动办公安全等场景提供解决方案。



加密视频会议

公有云加密视频会议

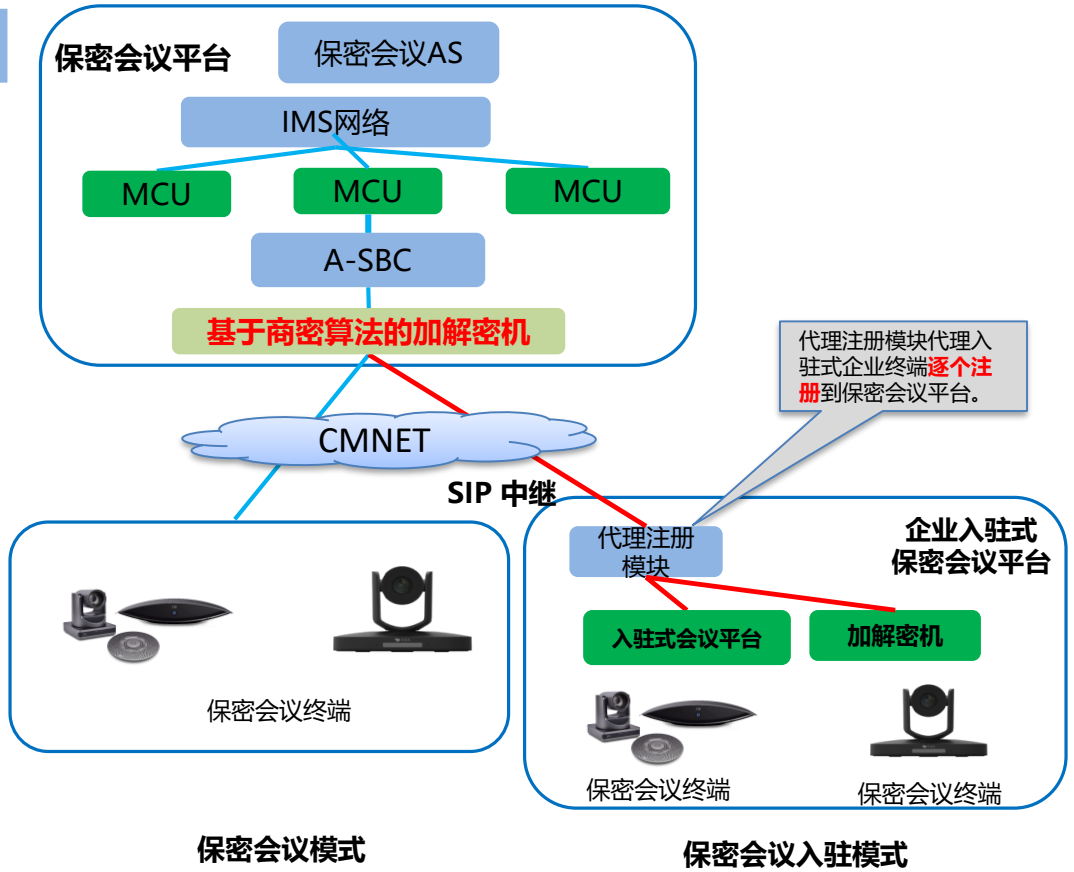
方案：在保密会议室部署终端，通过互联网专线接入保密会议平台。

优势：部署快速、简单，方便迁移、扩容，在开非密会议时，可与云视讯终端互通。

入驻融合加密视频会议

方案：在企业内网布署入驻专用MCU，满足客户在内网使用视频会议的安全需求；支持与云平台级联，通过大平台与外网保密终端互通。

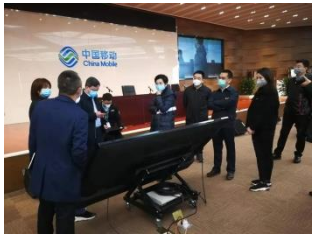
优势：保留与大网保密平台互通，统一随平台远程升级。



云视讯高效服务战疫

疫情期间共召开748万次会议，单日最高会议时长10.7亿分钟，是疫情前的660倍，高清用户累计达13.3万，软终端用户915万。

指挥调度



河南省省委举办省办公厅会议

钟南山及团队对玉溪预防新冠工作进行远程指挥

远程慰问

江苏省委书记远程连线疾控中心进行视察慰问

上海市委书记李强远程连线慰问赴武汉医疗队

新闻发布

安徽省新冠肺炎疫情防控新闻发布会

四川省新冠肺炎疫情防控工作新闻发布会

网上招商

山东泰安市商务局举办大型视频签约项目

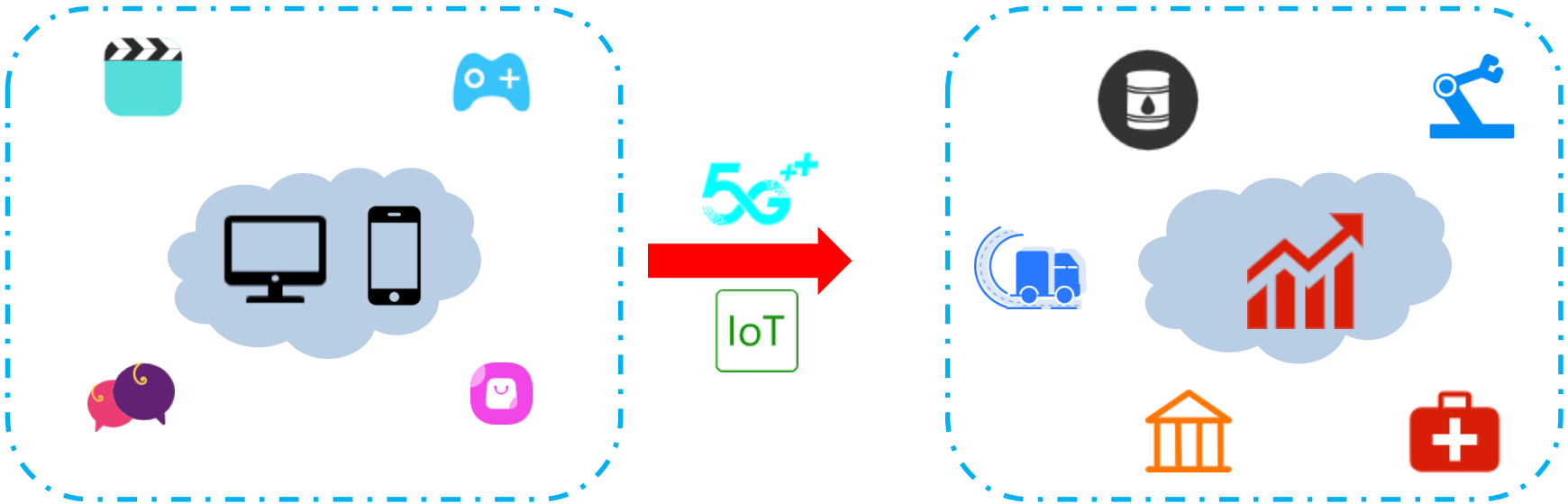
江西吉安市举办“屏对屏”招商推介会

目录

Contents

网络安全需求的变化

消费互联网 -> 产业互联网



产业互联网的蓬勃发展，将对网络安全提出新的挑战

- 网络世界和现实世界映射
- 网络安全暴露面增多
- 网络威胁后果增强
- 网络+安全融合
- 端到端传输安全->体系化安全
- 事后审计的强溯源需求

网络安全设计理念转变

中国移动 China Mobile

防护理念的变化 1

概率性风险控制 » 确定性信任

- 没有安全信任的根基

➢信任为基础，确保网络行为可预期

防护主导权的变化 2

安全由终端主导 » 安全由网络主导

- 系统安全和网络安全割裂
- 端到端传输加密OTT

➢系统和网络统筹安全能力

➢以网络为基础的传输安全，审计与安全的结合

安全运营方式的变化 3

业务主体 » 网络运营方

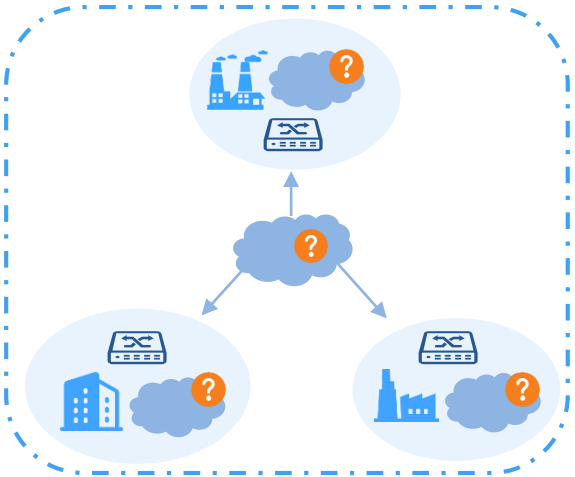
➢区域性、烟囱式的安全防护无法有效应对未知威胁

➢ 通过人工智能构建知识运营，综合全网，实现安全能力的演进

网络安全体系的变化

中国移动 China Mobile

传统网络安全形式



- 带宽受限
- 缺乏互通
- 高算力终端
- 传输不可靠
- 域内不可信
- 安全无保证

高通量\低时延的产业互联网安全形式

- 统一安全运营
- 安全互通
- 低算力高通量
- 可靠传输
- 域内安全共识
- 信任链保证

安全知识的智慧演进

描述性知识　规范性知识　实践性知识

知识的形成 → 知识积累与更新 → 知识使用

知识的反馈

基于知识运营的安全能力

安全云

关联分析与智能决策

①安全检测	②安全防护	③数据安全	④攻击溯源与审计
网络空间测绘	网站安全防护	敏感数据扫描	
高危端口监测	攻防演练	数据关联分析	
弱口令检测	DDoS防护	敏感数据脱敏	
新型终端测评	URL检测与防护		

智能决策 ⟺ 智慧执行

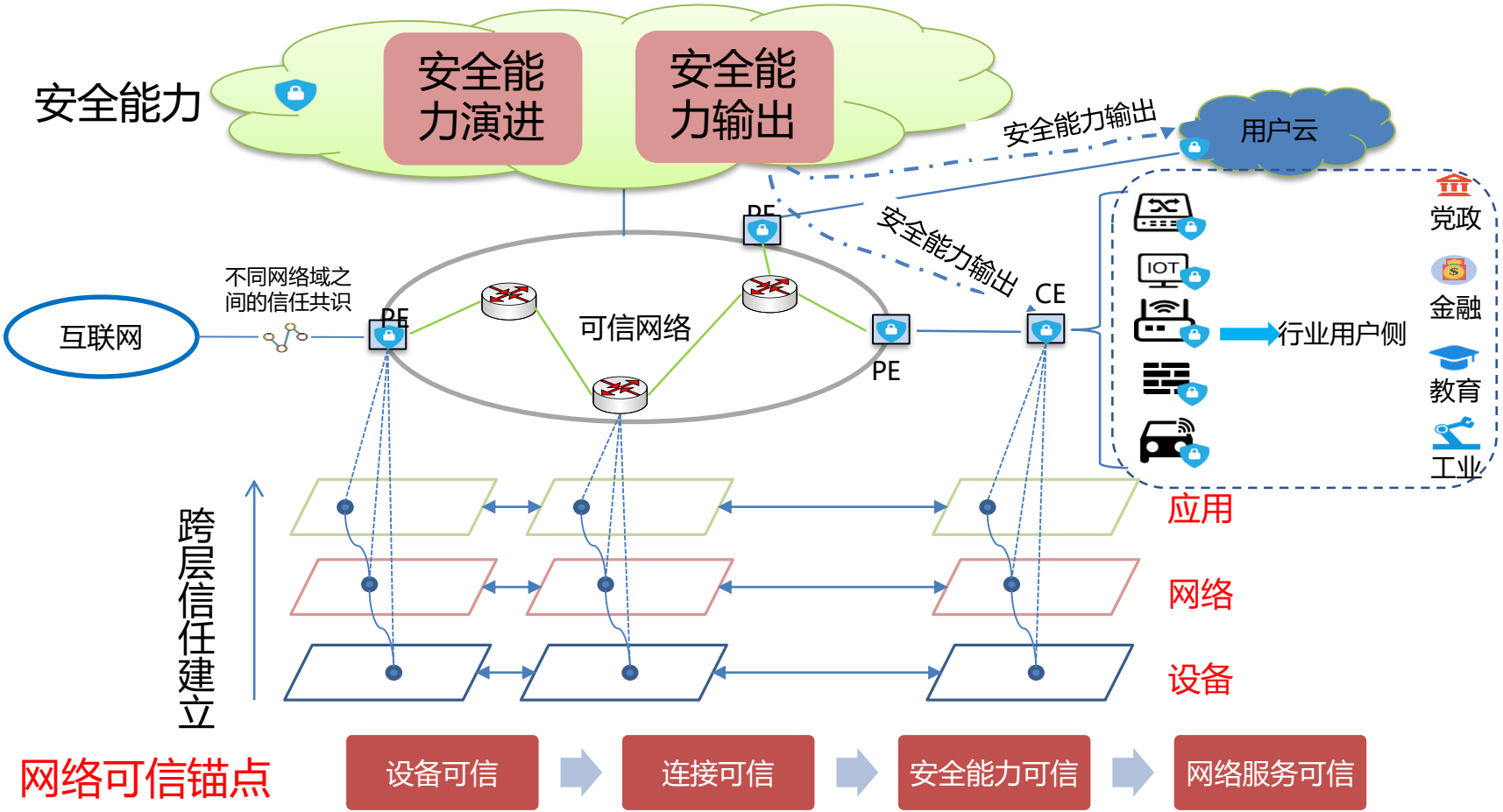
信任网络

- 应用/服务信任
- 网络信任
- 设备信任

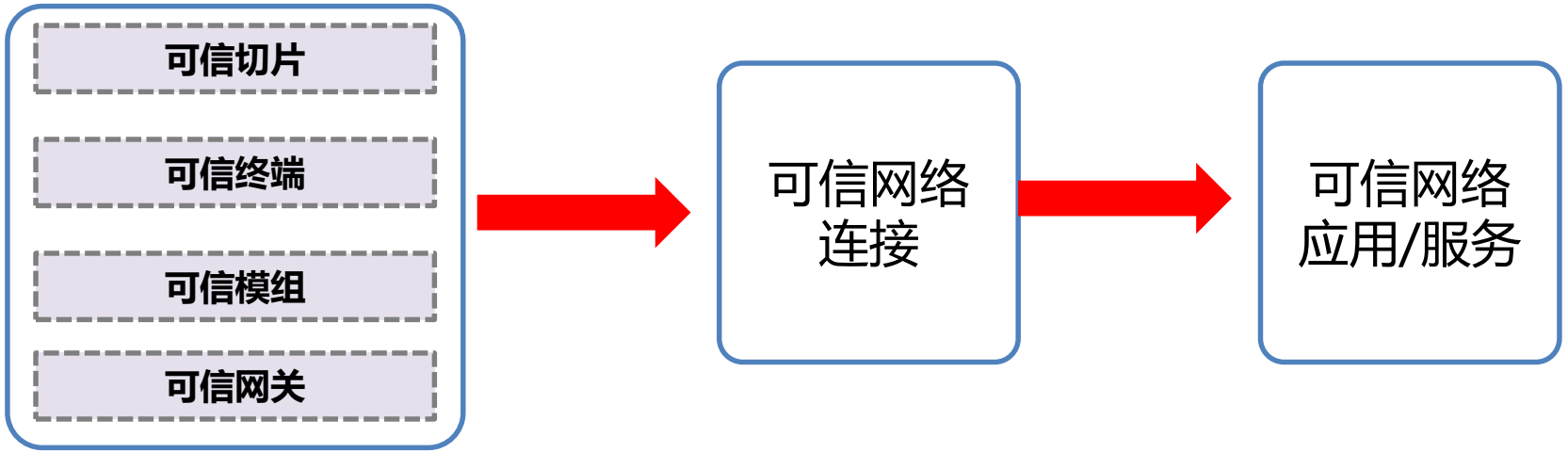
调用 / 积累

- 资产指纹库
- 情报库
- 规则库
- 风险库
- 算法库

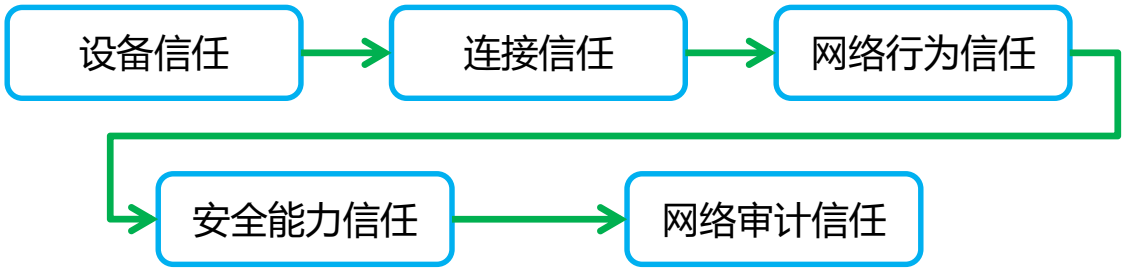
内生可信网络安全体系


安全能力
安全能力演进
安全能力输出
安全能力输出
用户云
PE
安全能力输出
CE
不同网络域之间的信任共识
互联网
PE
可信网络
PE
IOT
行业用户侧
党政
金融
教育
工业
跨层信任建立
应用
网络
设备
网络可信锚点
设备可信
连接可信
安全能力可信
网络服务可信

信任为网络基础

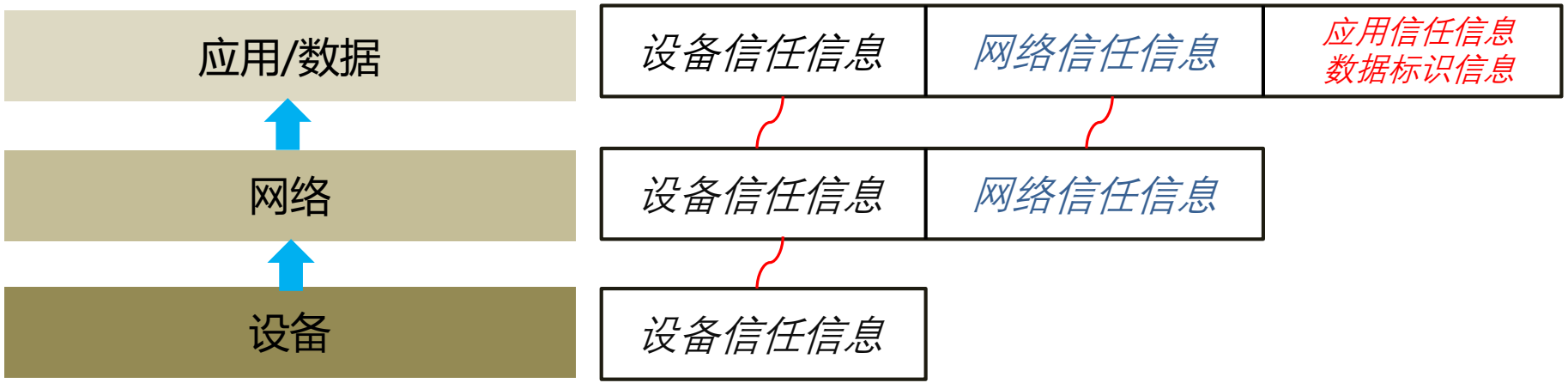


跨层次跨域的信任链条



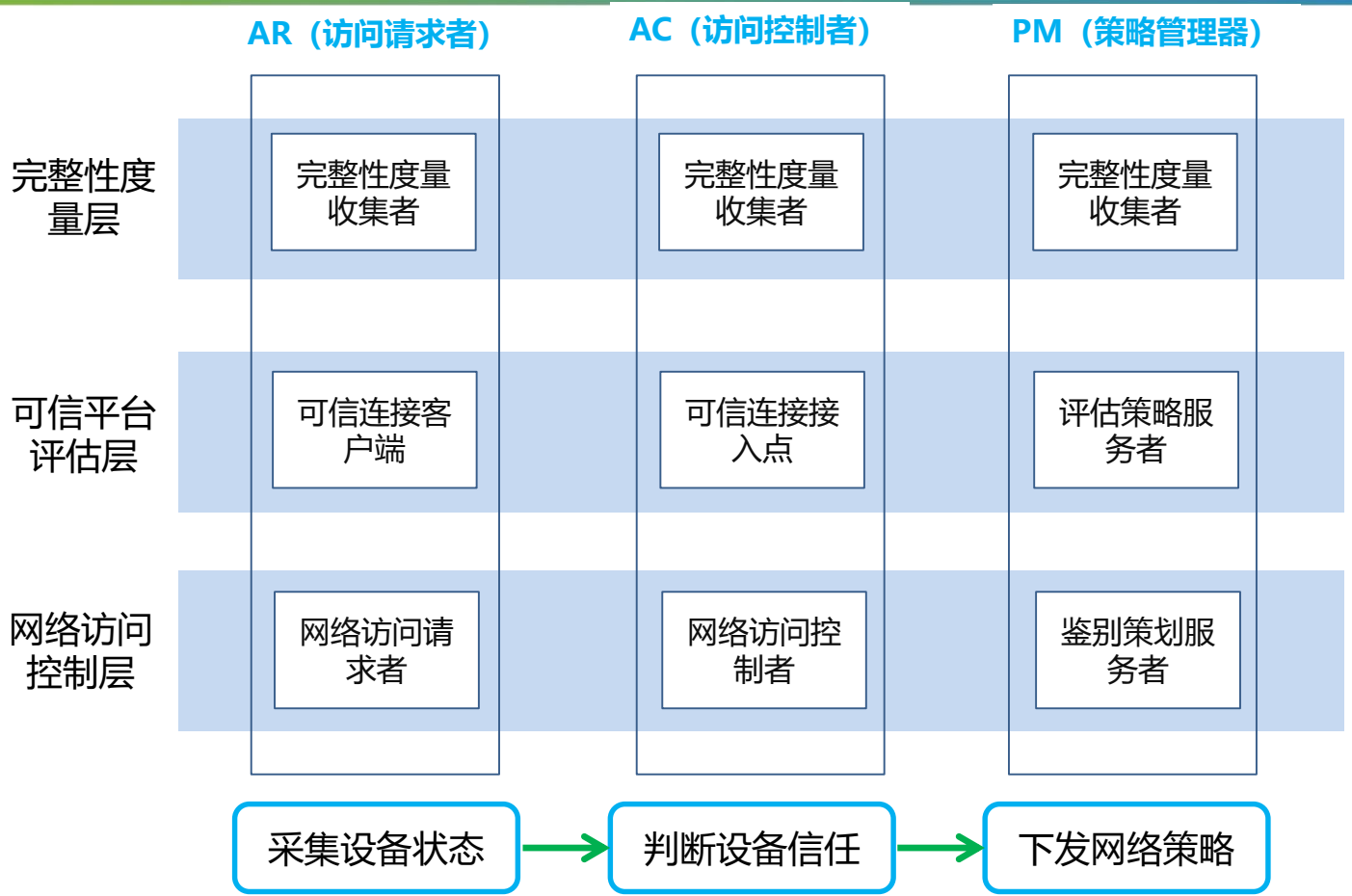
可传递信任链

可传递信任链：跨层的、多维度的信任信息传递，构建内生安全网络

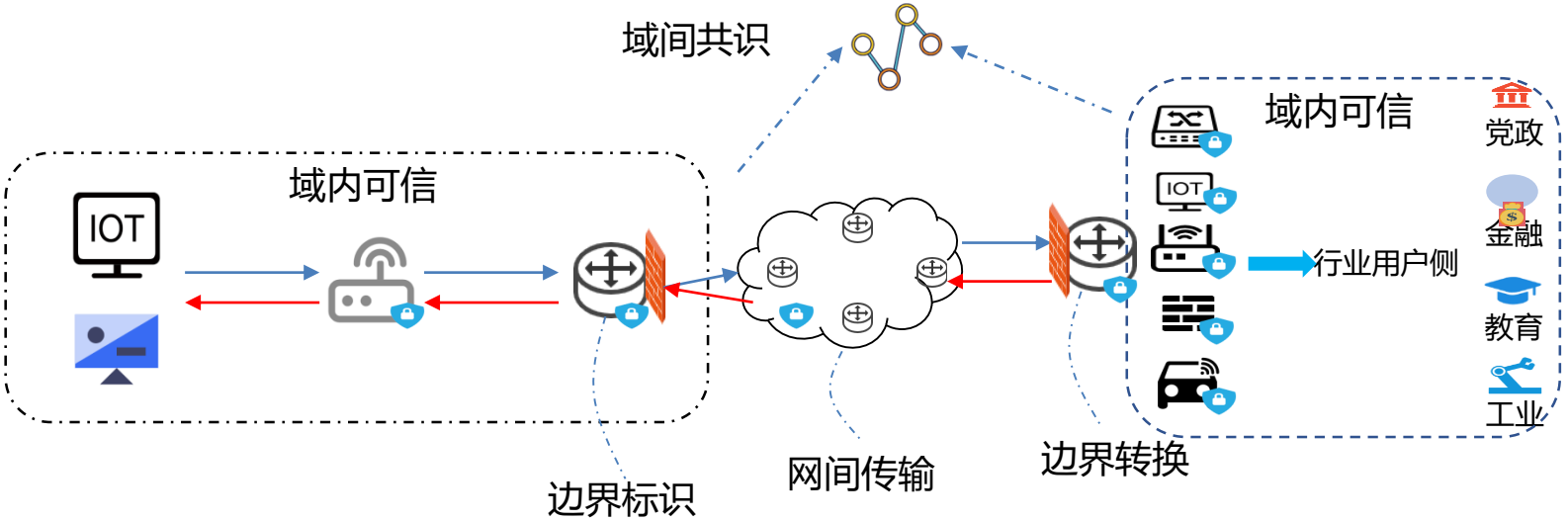


设备信任信息	通过可信计算技术描绘设备信任状态，建立设备信任关系
设备信任信息	通过可变长IP设置标签，实现域间追溯、域内解析
应用信任信息 数据标识信息	通过对应用和数据进行染色和标识，实现对应用和数据的认证和信任判断

设备信任


AR（访问请求者）
AC（访问控制者）
PM（策略管理器）
完整性度量层
可信平台评估层
网络访问控制层
完整性度量收集者
完整性度量收集者
完整性度量收集者
可信连接客户端
可信连接接入点
评估策略服务者
网络访问请求者
网络访问控制者
鉴别策划服务者
采集设备状态
判断设备信任
下发网络策略

网络信任



网络传输过程

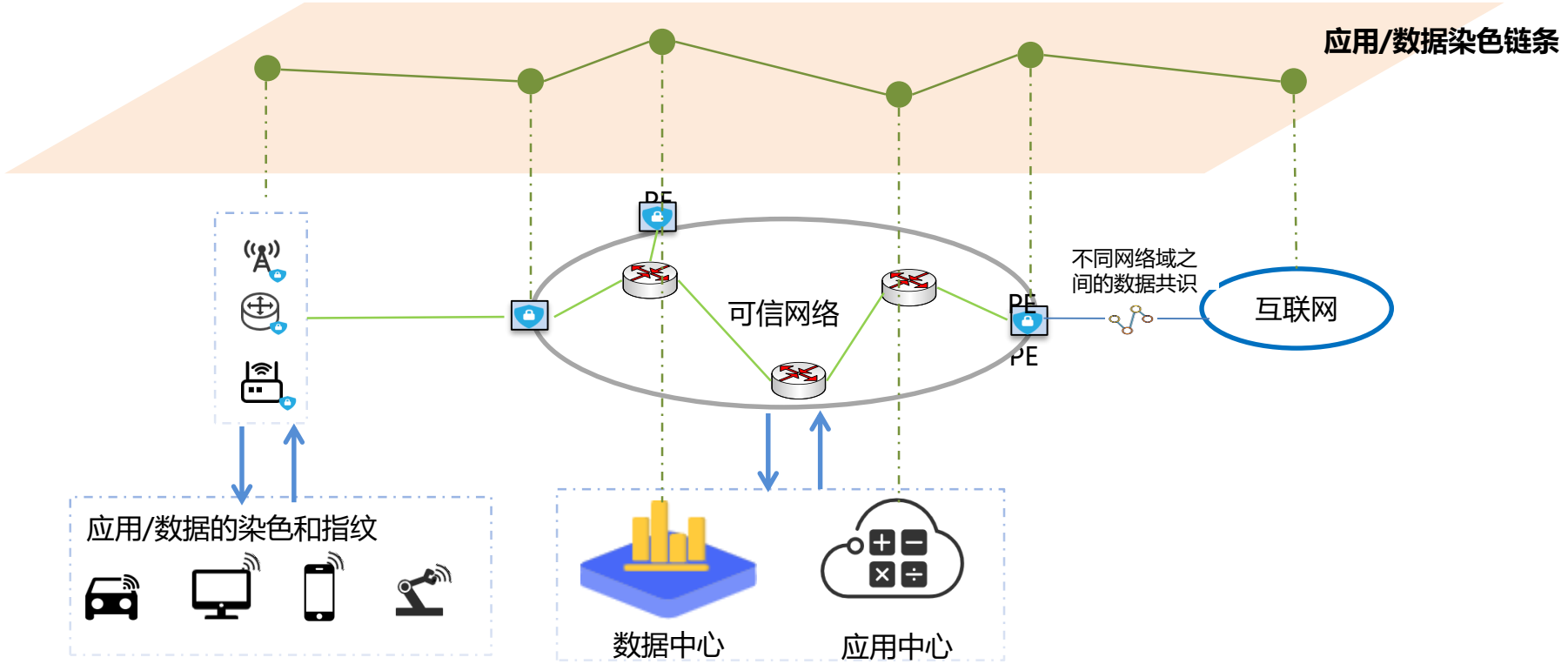
域内传输 → 边界标识 → 网间传输 → 目的解析

网络溯源过程

目的解析路由 → 网间回溯 → 源域边界 → 源域内部

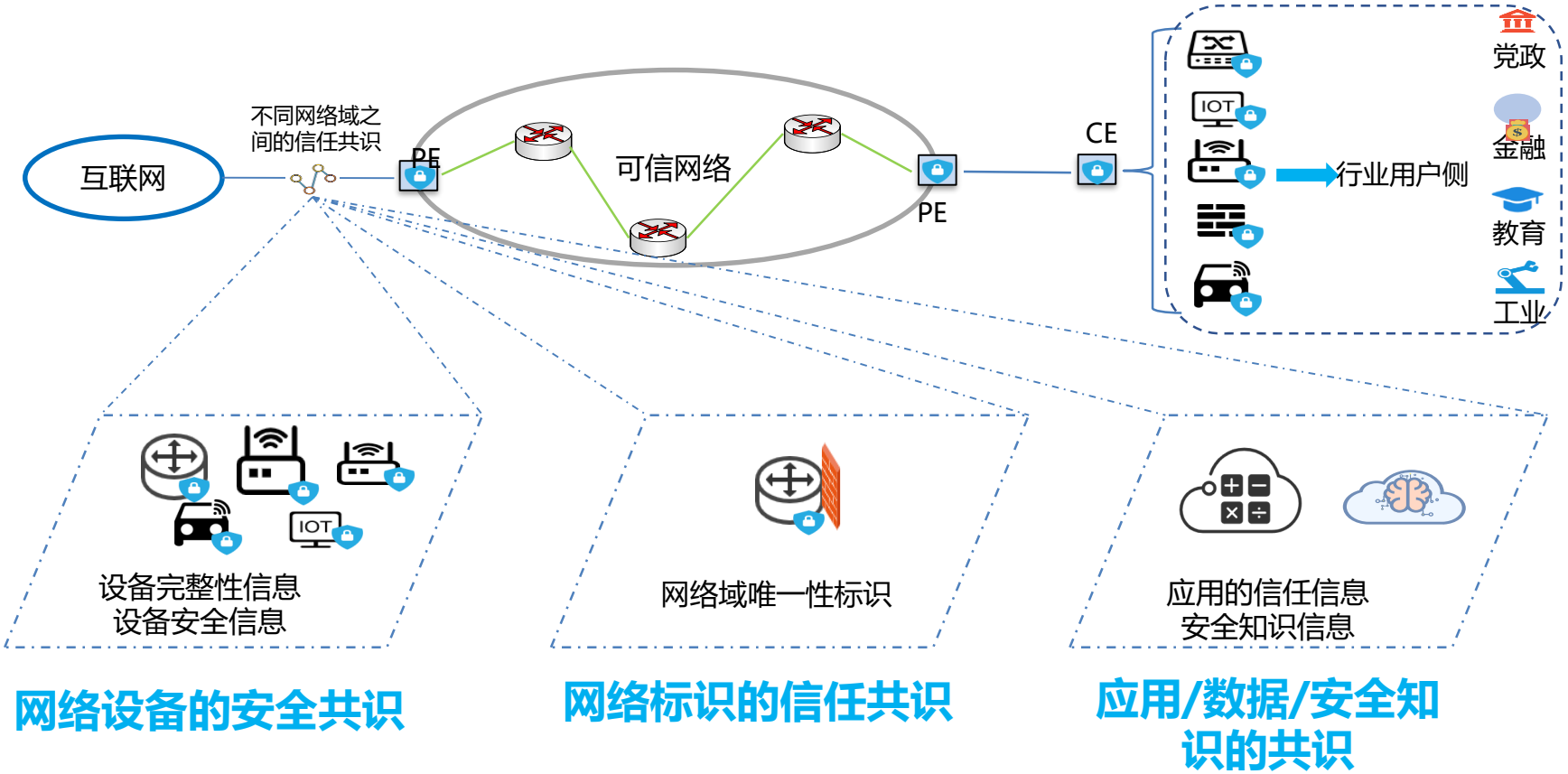
真实性&权限控制　隐私VS.可审计性　机密性&完整性　授权&可用性

应用信任



定义应用和数据指纹，对应用和数据进行唯一性标识，建立应用和数据的染色链条，识别和追踪应用/数据层安全

网络安全共识



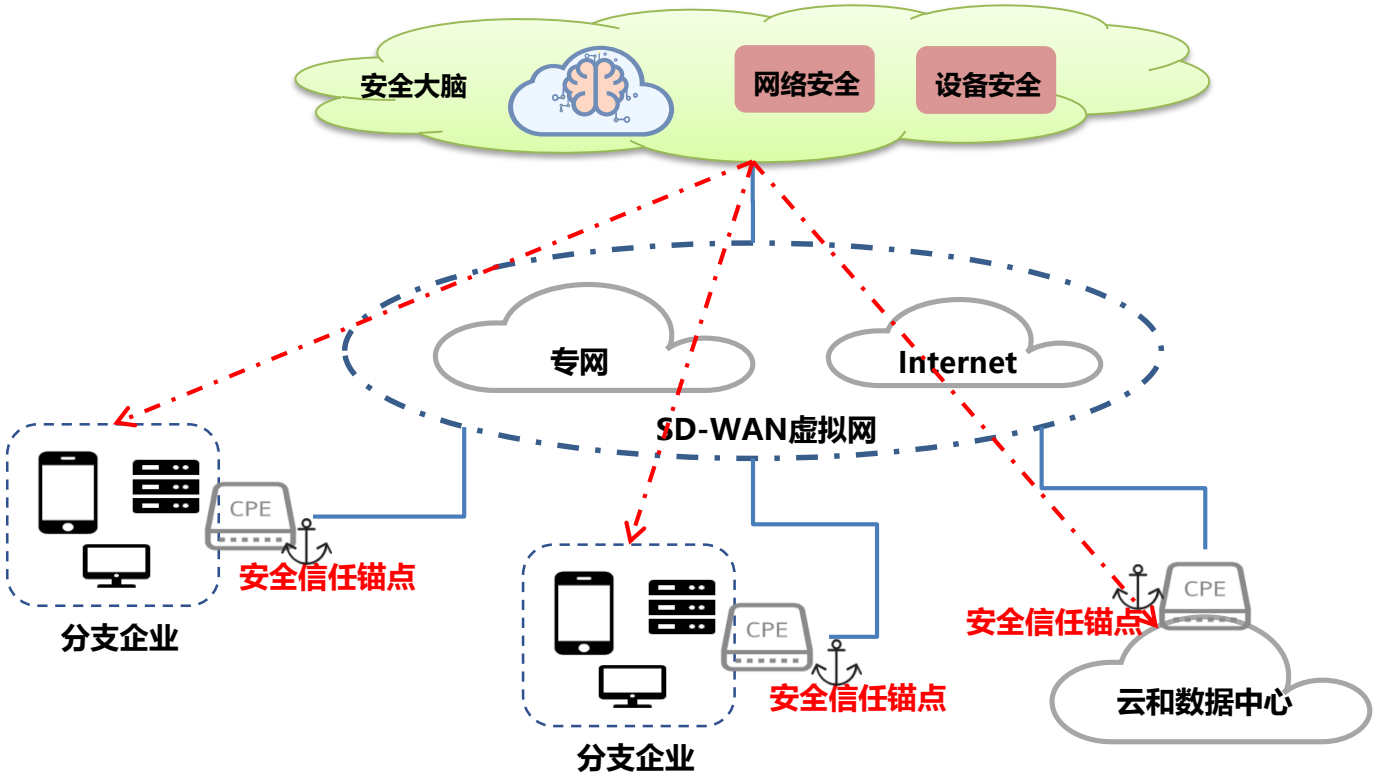
网络设备的安全共识

网络标识的信任共识

应用/数据/安全知识的共识

内生安全SD-WAN应用示例

以可信CPE为安全信任锚点，将安全能力输出到用户侧，实现内生安全网络的赋能体系。



（1）安全赋能

- 安全网络管控
- 网络安全技术：
  a. 下一代防火墙
  b. 入侵防护
  c. 入侵检测

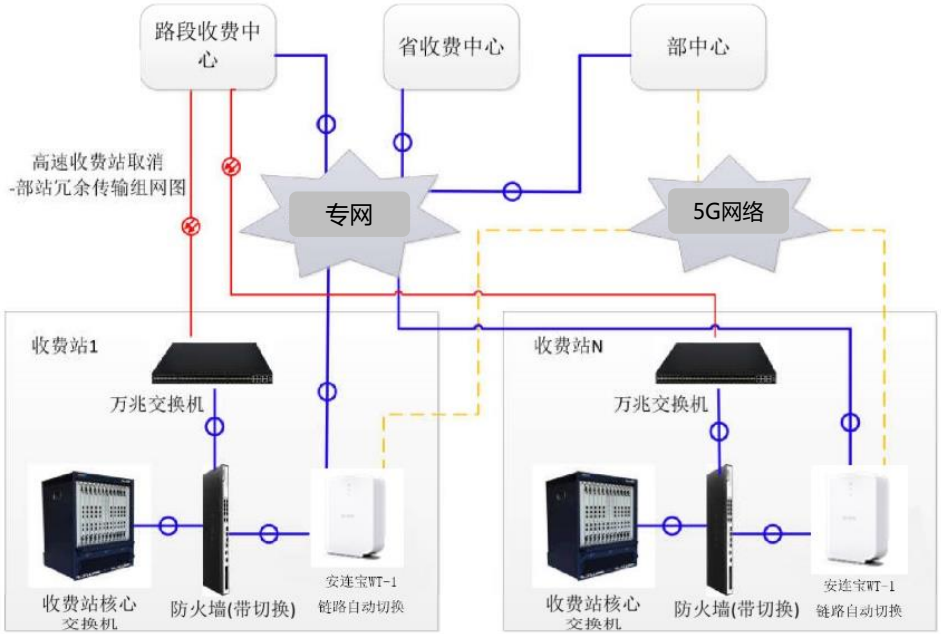
（2）可信连接

- 锚点为目标
- 双向可信验证

应用场景示范

市场背景

- **市场需求：**从各收费站到分中心，分中心到高速公路管理中心，需要稳定、可靠、有备份能力的网络安全传输。
- 已在广东全省十个市182个站点进行产品方案应用，后续向全国ETC行业推广。



采用物联网卡搭配安连宝可信接入网关组成无线专线链路，按照有线和无线链路1：1配置，并自动切换设备（安连宝WT-1)实现有线专线和无线专线（物联网专用APN卡）双链路互备，自动切换，确保高速ETC收费业务不中断。

谢　谢