智慧云测DPLS安全实验室

CC 体系下的芯片与零部件安全测试与整车信息安全合规协同

2025年5月

WWW.DPLSLAB.COM

公司地址：北京市门头沟区莲石湖西路98号院7号楼701

行业背景

万物互联，全球智能

物联网将使新技术得到爆炸性的发展（正如寒武纪大爆炸为地球带来了数千个新的物种那样）并将带来1万亿个物联网设备，而这会将人类导向奇点，届时机器智能将超越人类智能的总和。

金融物联，源自支付

金融行业是最早借助物联网技术作为大规模基础设施实现行业应用，惠及每一位用户

卡片、二维码、POS机、ATM机.....每一笔交易都是物联网的功劳

行业背景

OPLS Lab

终端数量

到了2021年，我们将会拥有18亿台PC，86亿台移动设备，157亿台物联网设备。在未来20年，物联网设备的数量将会超过1万亿台。

1

2

良莠不齐

很多传感器、终端、芯片只是具备某些功能，没有统一的标准和质量要求，设计方也不愿意投入。

3

开放式环境

开放式的网络环境、开放式的物理环境、甚至开放性的主机环境，带来的风险是显而易见的。

4

缺乏安全设计

产品设计单位缺乏安全设计理念，传统信息产品的设计理念，不愿意增加产品设计成本。

行业背景

安全风险

病毒攻击　账户滥用　DOS攻击
隐私泄露　窃听篡改　非法入侵
身份冒充　业务滥用

应用层

云端管理平台

智能电网 智能制造 智能水利 智能交通、
智慧城市……

阻塞干扰　跨网攻击　信息伪造
信息篡改　网络窃听/拦截
网络中断　DOS攻击

网络层

网关基站

NB-IOT/LoRA/ZigBee/Wi-Fi/
Bluetooth……

物理俘获　网络窃听　DOS攻击
节点欺骗　非授权访问
假冒攻击　节点信息窃取

感知层

物联网终端

温度计、烟感、光感、信号灯、门禁、
摄像头……

DPLSLAB

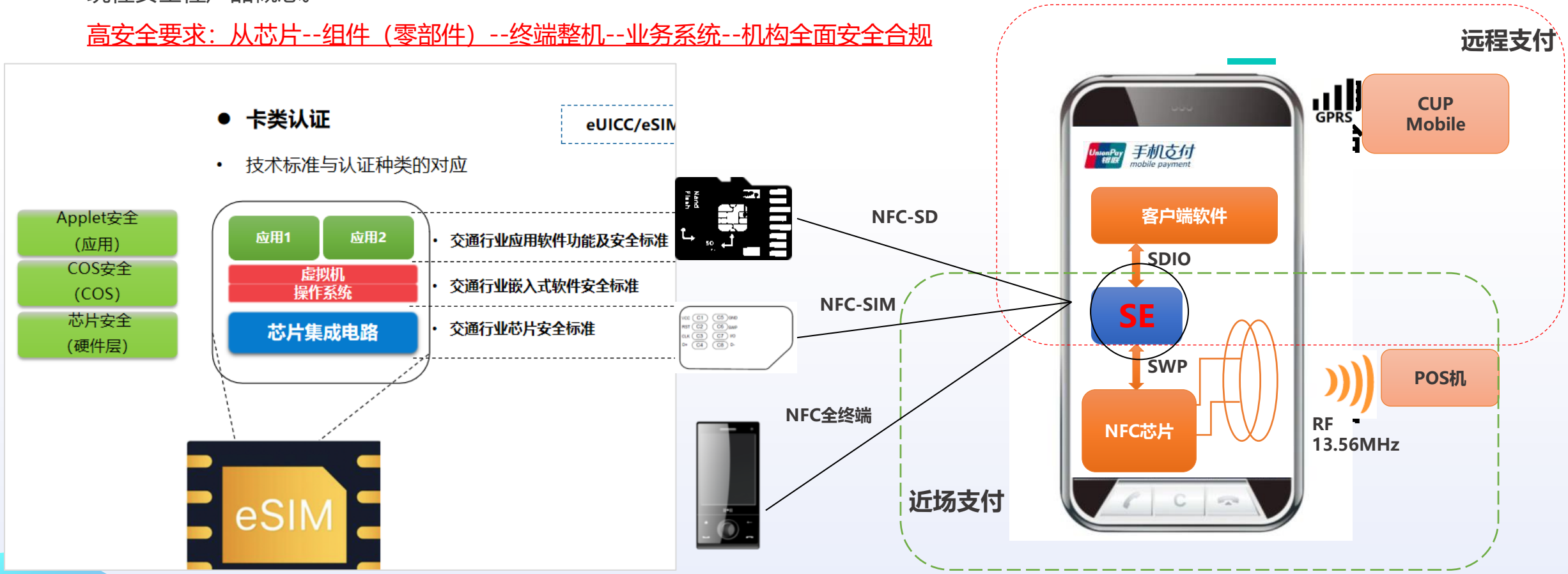
金融行业物联网安全合规

全面覆盖

金融行业安全解决方案：全面合规

金融物联网产品以智能化终端为载体，通过自动控制、计算机以及物联网等技术，将支付、远端控制、环境监控、信息管理、范金融服务等功能有机结合，为用户提供更具便捷性、舒适性、与安全性的金融服务环境。金融物联网产品不单指某一独立产品，而是一个广泛的系统性安全性产品概念。

高安全要求：从芯片--组件（零部件）--终端整机--业务系统--机构全面安全合规



金融行业安全解决方案：全面合规

金融物联网产品以智能化终端为载体，通过自动控制、计算机以及物联网等技术，将支付、远端控制、环境监控、信息管理、范金融服务等功能有机结合，为用户提供更具便捷性、舒适性、与安全性的金融服务环境。金融物联网产品不单指某一独立产品，而是一个广泛的系统性安全性产品概念。

高安全要求：从芯片--组件（零部件）--终端整机--业务系统--机构全面安全合规

- **终端类认证**

终端 银联认证 Certified by UnionPay

- 技术标准与认证种类的对应

《银联卡受理终端应用规范》
- 第1部分 销售点终端（POS）应用规范
- 第3部分 银联卡（IC卡）脱机受理终端规范
- 第4部分 密钥分发专用POS终端规范
- 第5部分 电话支付终端应用规范
- 第6部分 脚本POS技术规范
- 第7部分 智能销售点终端（POS）应用规范

《银联卡受理终端入网测试指引》

银联卡受理终端入网认证 → 直联、间联POS终端；电话支付终端；IC卡脱机受理终端

《银联卡受理终端安全规范》-UPTS2.0
- 第1卷 基础卷
- 第2卷 产品卷
  - 第1部分 销售点（POS）终端
  - 第2部分 无人值守（自助）终端
  - 第3部分 个人支付终端
  - 第4部分 独立部件
  - 第5部分 电话终端
  - 第6部分 智能销售点终端
  - 第7部分 mPOS通用技术安全
- 第3卷 检测卷
- 第4卷 辅助卷

银联卡受理终端安全认证 → POS终端；智能终端；PIN输入设备；电话支付终端；自助终端；个人支付终端；mPOS

《银联卡支付应用软件安全规范》
《银联卡受理商户信息系统安全规范》

银联卡受理商户信息系统（MIS）开发企业资质认证 → MIS系统开发企业资质

DPLSLAB

汽车行业车联网安全合规

趋势与探索

汽车行业背景

车联网攻击技术发展趋势

网络级安全攻击

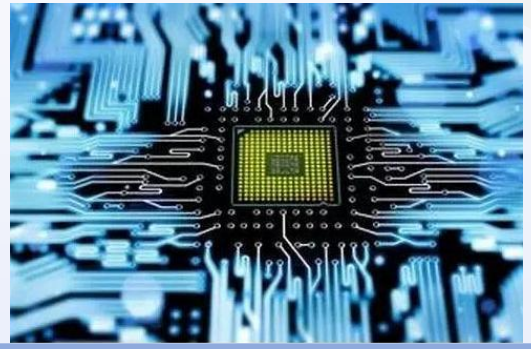
- 网络级安全攻击
- 应用级安全攻击
- 协议级安全攻击

物理硬件级安全攻击

- 电路逆向分析
- 固件提取及逆向分析
- 无线协议及端口攻击

芯片级密钥攻击

- 侧信道密钥分析
- 电磁故障注入密钥分析
- 激光攻击密钥分析
- 智能毛刺密钥分析

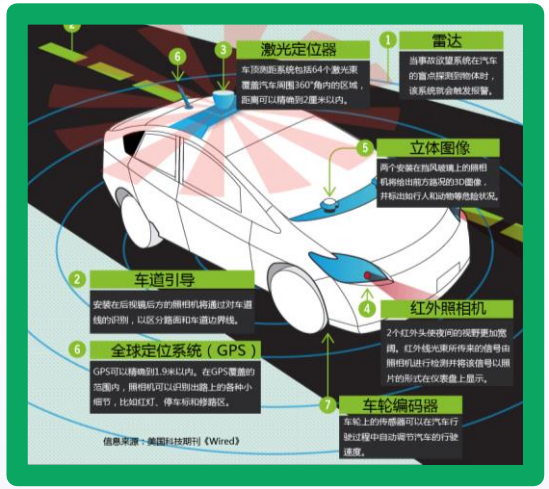


攻击面越来越接近底层硬件及芯片，攻击技术及设备门槛越来越高，黑客越来越跨学科，越来越团队化

汽车行业背景

开放式环境

- 进入万物互联时代
- 共享汽车、无人驾驶（无人值守资产）



芯片大量国外引进

- 大量芯片、传感器、甚至终端国外引进，对其背景和应用不深
- 拿来就用，没有统一的安全标准和安全质量要求
- 无法甄别是否有后门或者安全隐患

硬件安全分析及检测能力不足

- 网络安全，更多集中在上层网络及应用
- 涉及到硬件安全，投入大、门槛高
- 硬件安全一旦发生，极为致命

统一化验证手段难以建立

- 攻击面多，黑客单点攻击技术及深度甚至高于行业检测机构，黑客不愿意公开或分享其技术
- 相对碎片化，人工化，需要更多自动化，工具化技术

汽车行业国际安全合规

R155认证测试

整车R155认证测试

测试标准

UN R.155

ISO 21434: 2020

汽车整车信息安全技术要求

测试项目

外部连接安全	测试远控系统、第三方APP、外部接口是否安全
通信信道安全测试	测试车外网、车内网通信通道是否安全
软件升级安全测试	测试OTA升级是否安全
数据代码安全测试	测试数据和代码是否进行安全防护

测试案例

已为多家企业提供相关测试服务，具备丰富的测试经验

- 外部连接安全测试

远控系统安全测试

第三方应用安全测试

外部接口安全测试

- 通信信道安全测试

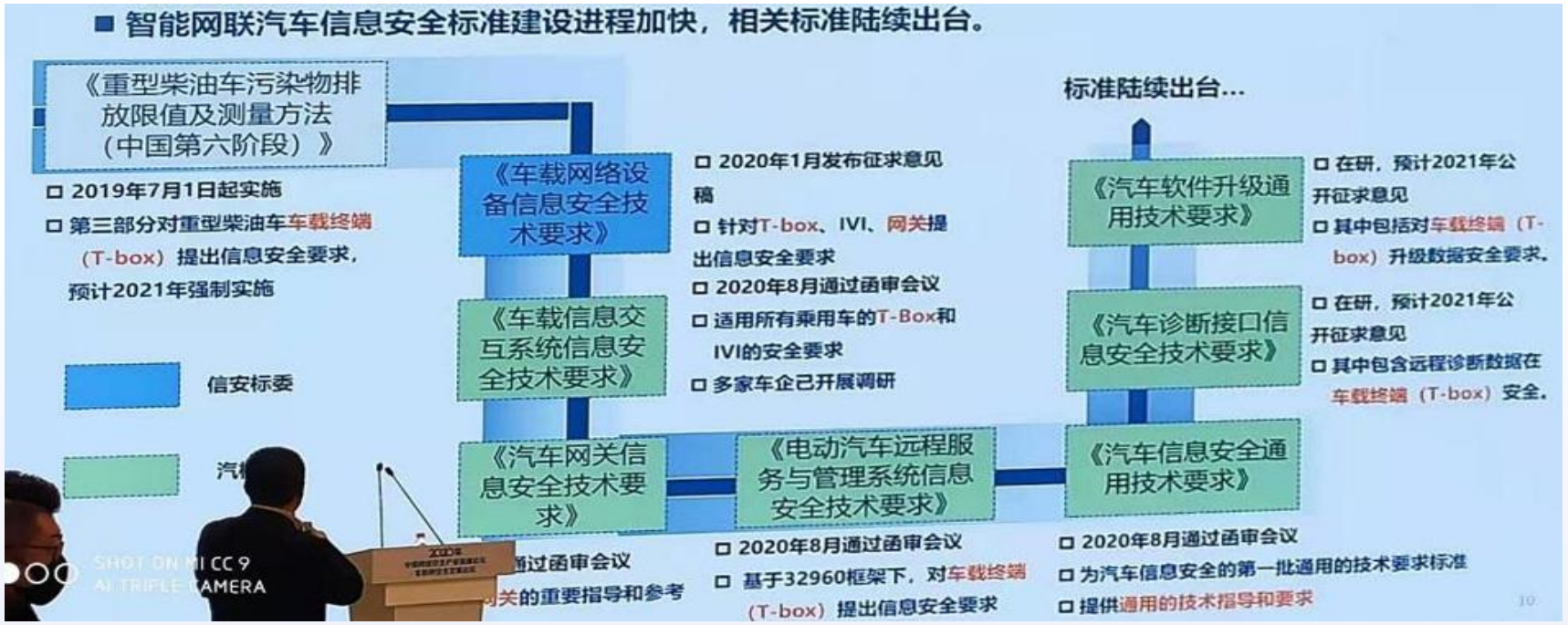
防欺骗测试

防未授权执行测试

通信消息真实性、完整性、有效性测试

汽车行业国内安全合规

国内汽车信息安全的伊始及逐步展开



2019年7月1日发布《HJ 1239.1-2021 重型车排放远程监控技术规范》首次对车辆信息传输提出数据加密要求

汽车行业国内安全合规

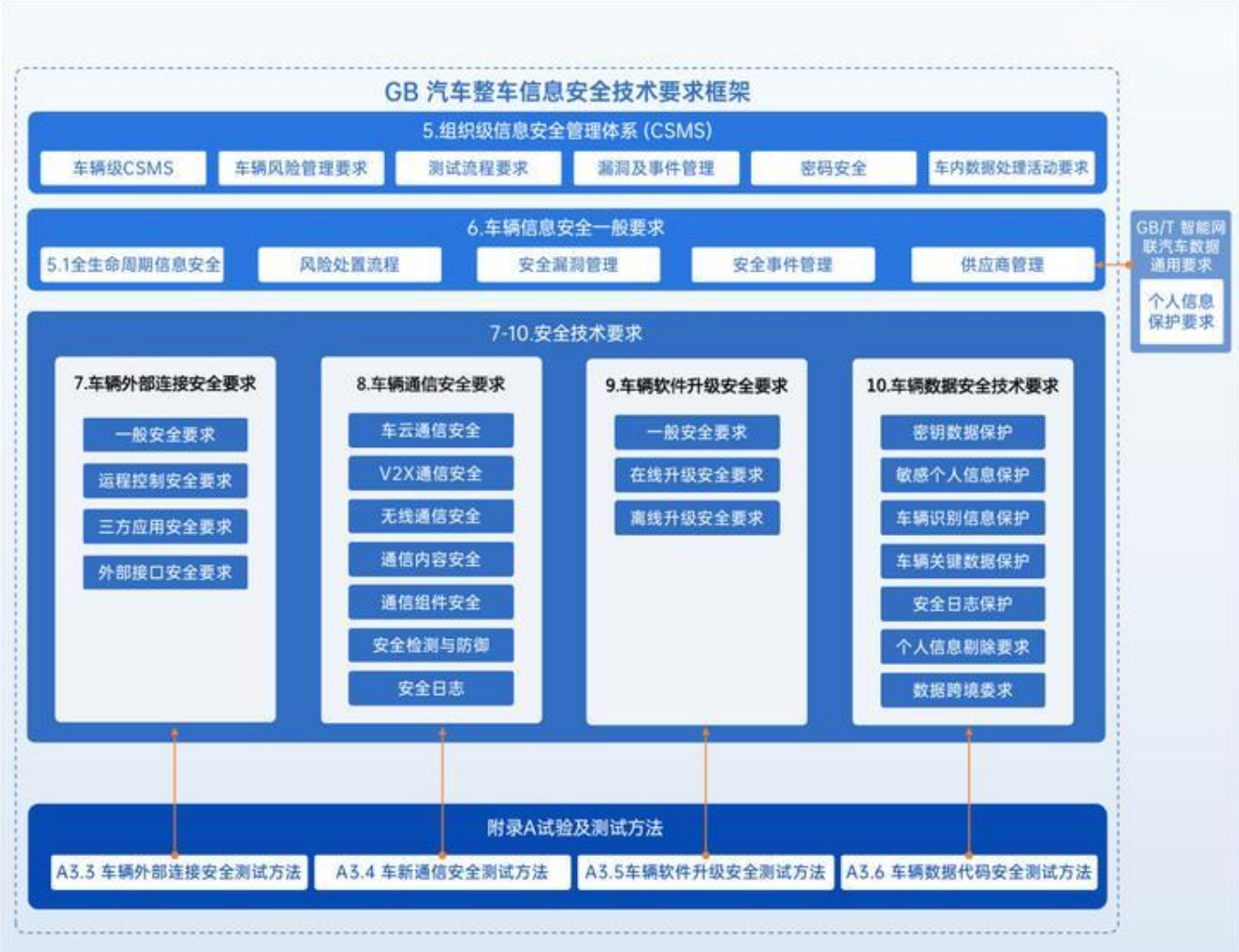
即将实施的国家标准（强制标准）

《汽车整车信息安全技术要求》

GB标准正式发布：2024年6月 1 日执行

《汽车芯片信息安全技术规范》
《汽车密码技术要求》

等标准正在制定落地中



汽车行业安全合规挑战

整车信息安全和体系合规
汽车超长供应链

零部件安全如何保证？

第一阶段

传统交通代步工具

- 功能安全
- 可靠性安全

第二阶段

智能车联网

- 功能安全
- 信息安全
- 隐私安全

第三阶段

自主可控&体系化安全

- 芯片国产化，技术国产化
- 抵抗住主动攻击的无人驾驶等技术
- 体系化、标准化安全保障机制

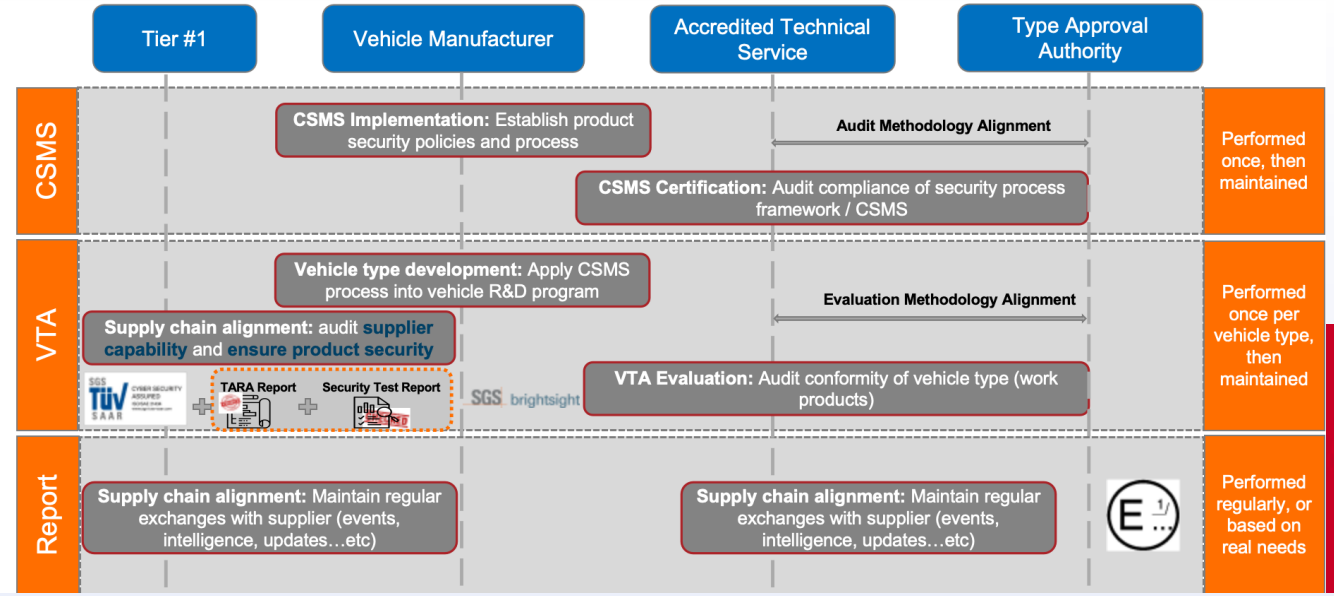
DPLSLAB

汽车行业车联网安全合规

国际趋势

国际合规探索

- 机会与挑战
- 面对 IoT 复杂供应链的安全挑战
- 面对整车信息安全国内外合规要求挑战
- 面向整车TRAR分析要求如何实现整车到子系统再到芯片的安全闭环，如何实现供应链安全合规
- 是否仿照传统金融安全复用 CC 体系实现从芯片-组件/终端（COS/Applet/POS/ATM)-应用系统全面合规?



国际 CC

CC作为全球产品安全合规发端，最早被期待适配IoT场景，并指导国内外金融物联网合规探索与落地，全形态产品覆盖

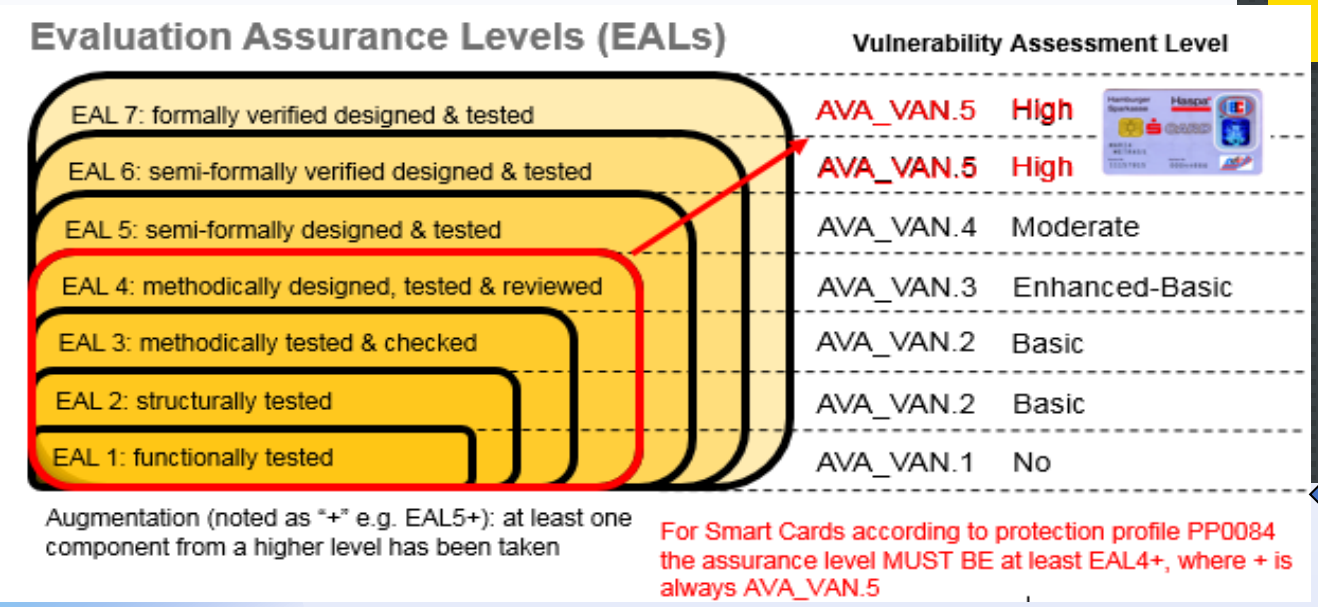
优劣：

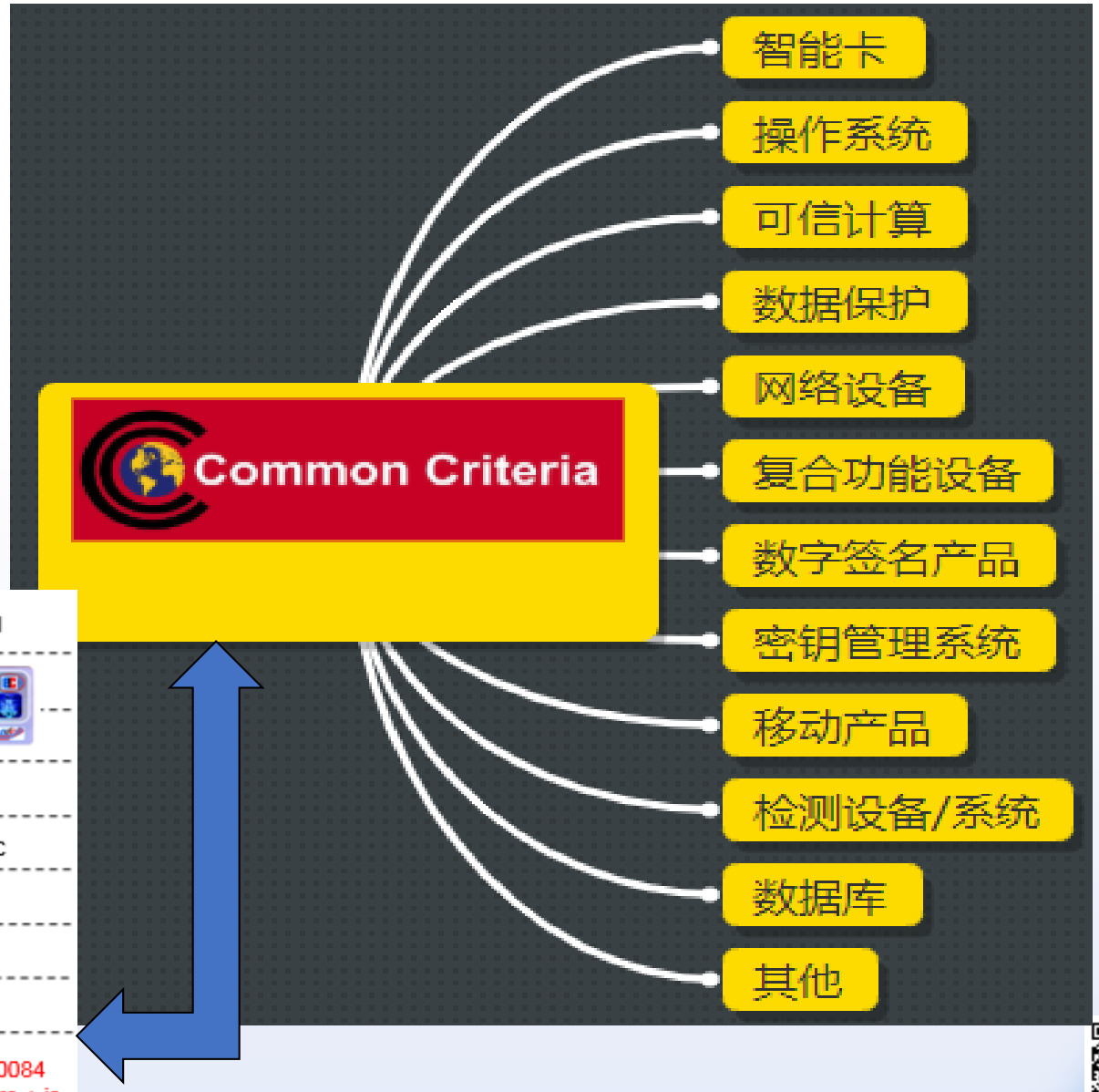
1复杂度高：形式化语言

2成本高：动辄百万+人民币

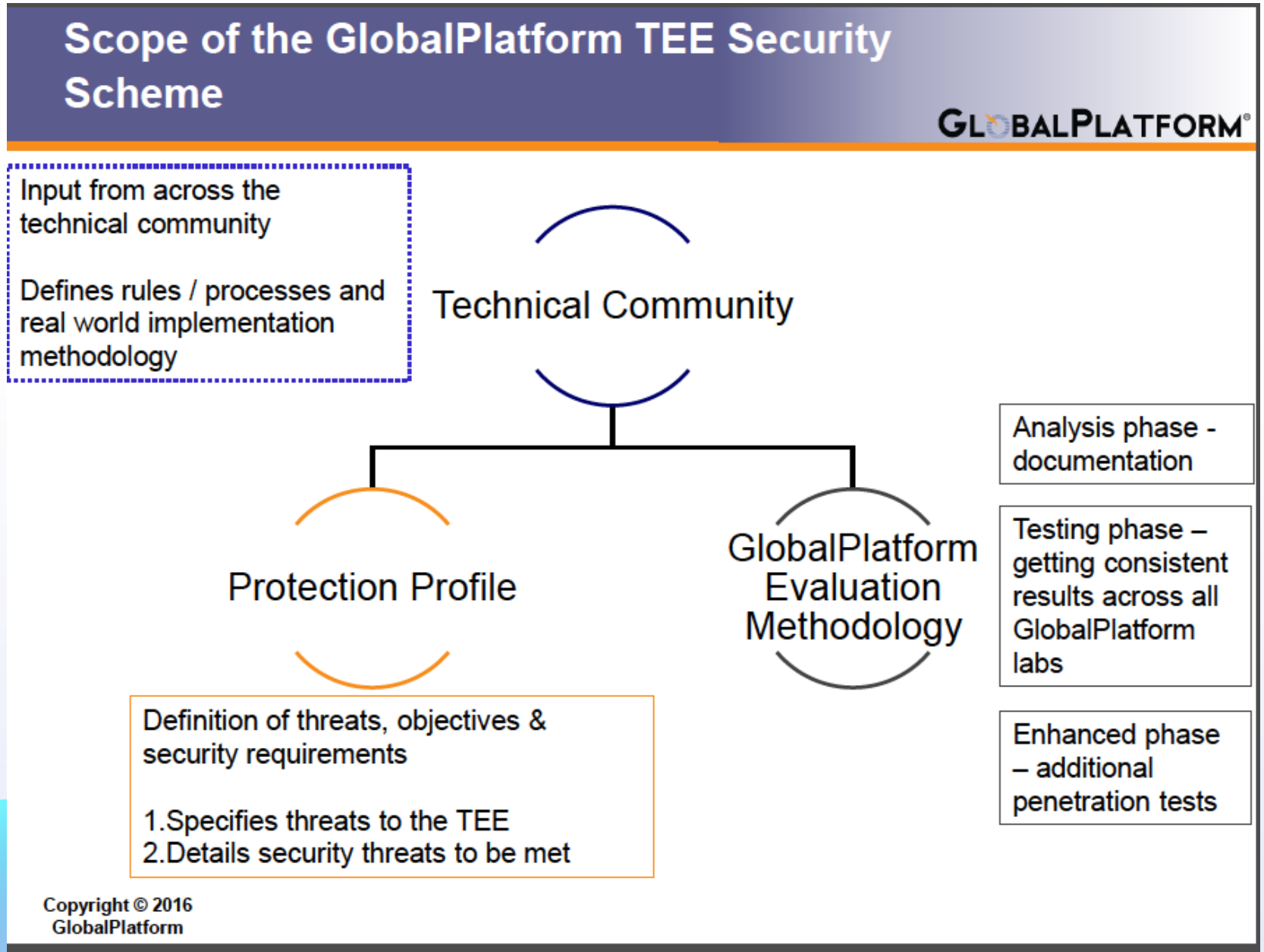
3周期长：12-24个月评估周期

4 全产品形态覆盖，欧美通行





国际 GP TEE



面向车载大芯片机片上操作系统OS 安全

主要匹配中控 IVI 机车载网关

EAL2+级别

优劣：

1仅适合车载复杂子系统

2成本较高，百万级

3国际认可度高，OS 可单独送检

4 无需审厂，周期端

5 兼容 ARM/RISC-V/Intel 多架构

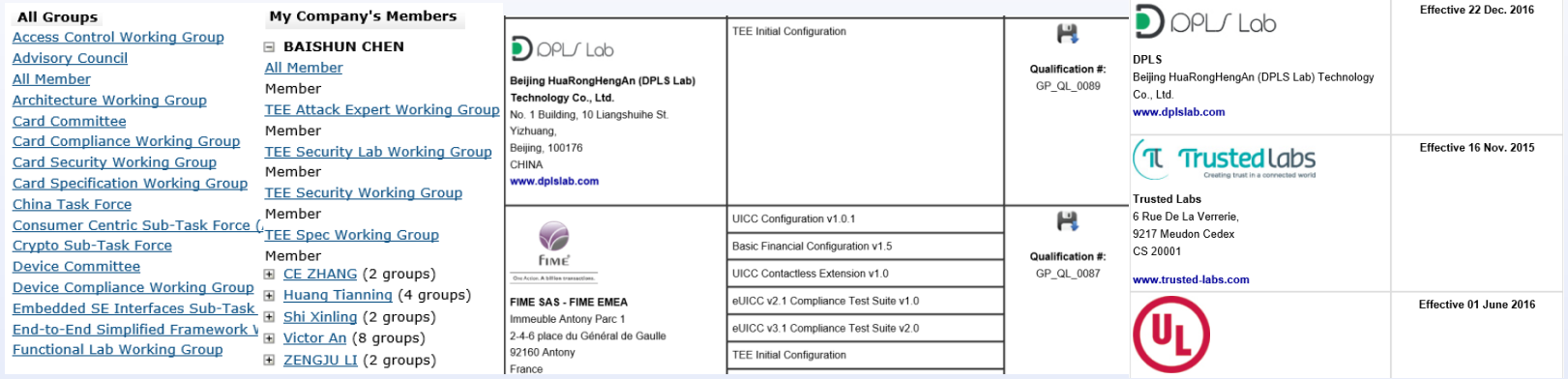
国际 GP TEE

TEE产品安全

- GP Device Committee成员
- 加入实验室安全工作组：

  TEE Security Lab Working Group

  TEE Attack Expert Working Group
- 定期参加GP组织的工作组会议，承担GP 实验室AP（攻击案例）文档编写
- 与GP就测试案例、攻击案例编写有良好沟通
- 是GP认可的功能符合性测试实验室
- GP TEE安全测试，已获得GP预授权



All Groups

Access Control Working Group
Advisory Council
All Member
Architecture Working Group
Card Committee
Card Compliance Working Group
Card Security Working Group
Card Specification Working Group
China Task Force
Consumer Centric Sub-Task Force (
Crypto Sub-Task Force
Device Committee
Device Compliance Working Group
Embedded SE Interfaces Sub-Task
End-to-End Simplified Framework V
Functional Lab Working Group

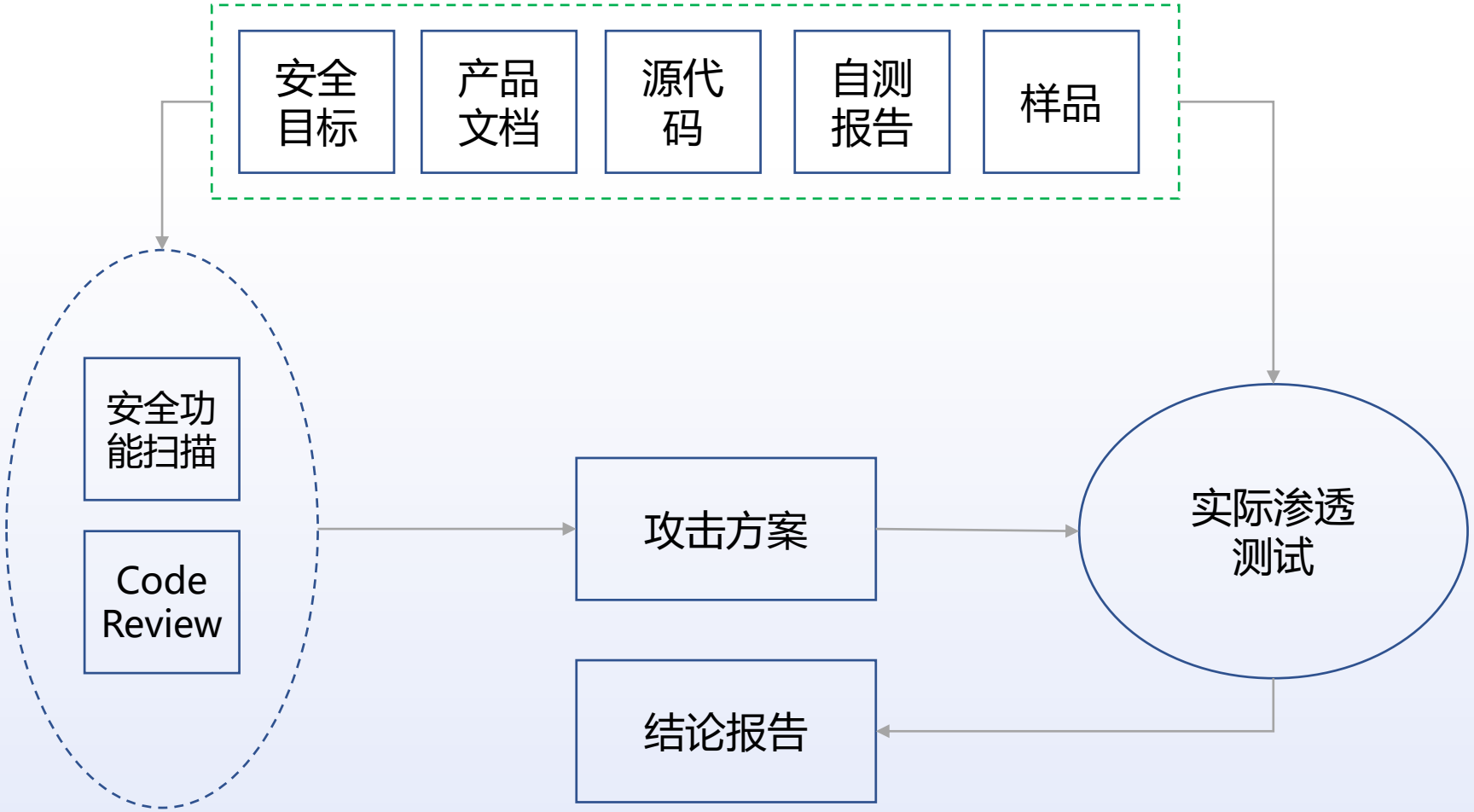
My Company's Members

BAISHUN CHEN
All Member
Member
TEE Attack Expert Working Group
Member
TEE Security Lab Working Group
Member
TEE Security Working Group
Member
TEE Spec Working Group
Member
CE ZHANG (2 groups)
Huang Tianning (4 groups)
Shi Xinling (2 groups)
Victor An (8 groups)
ZENGJU LI (2 groups)

DPLS Lab **Beijing HuaRongHengAn (DPLS Lab) Technology Co., Ltd.** No. 1 Building, 10 Liangshuihe St. Yizhuang, Beijing, 100176 CHINA **www.dplslab.com**	TEE Initial Configuration	**Qualification #:** GP_QL_0089
FIME **FIME SAS - FIME EMEA** Immeuble Antony Parc 1 2-4-6 place du Général de Gaulle 92160 Antony France	UICC Configuration v1.0.1 Basic Financial Configuration v1.5 UICC Contactless Extension v1.0 eUICC v2.1 Compliance Test Suite v1.0 eUICC v3.1 Compliance Test Suite v2.0 TEE Initial Configuration	**Qualification #:** GP_QL_0087

brightsight your partner in security approval **Brightsight BV** Delftechpark 1, 2628 XJ, Delft The Netherlands **www.brightsight.com**	**Effective 15 Nov. 2015**
DPLS Lab **DPLS** Beijing HuaRongHengAn (DPLS Lab) Technology Co., Ltd. **www.dplslab.com**	**Effective 22 Dec. 2016**
Trusted Labs Creating trust in a connected world **Trusted Labs** 6 Rue De La Verrerie, 9217 Meudon Cedex CS 20001 **www.trusted-labs.com**	**Effective 16 Nov. 2015**
UL	**Effective 01 June 2016**

TEE测试流程



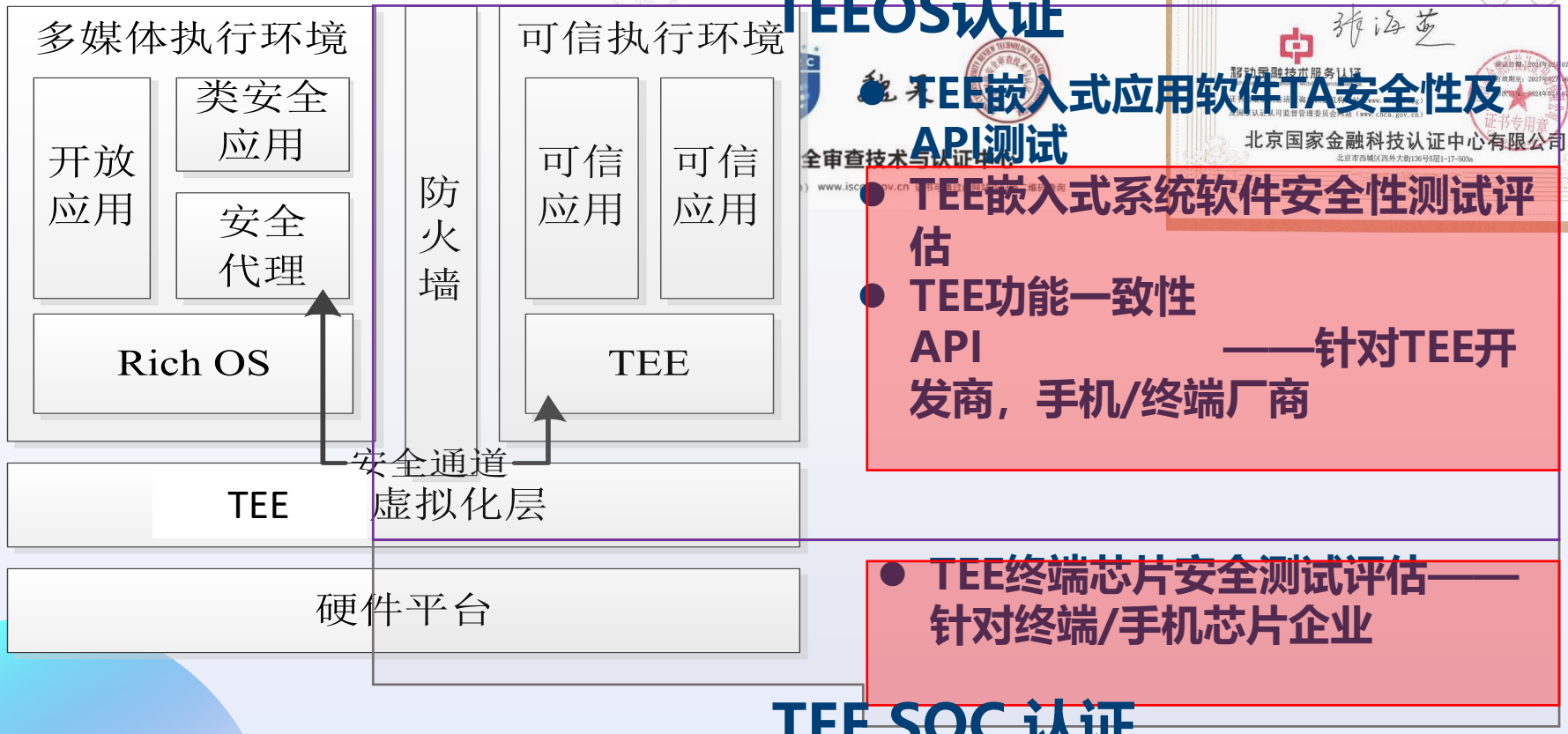
国际 GP TEE

检测服务内容


IT产品信息安全认证证书
评估保障级（EAL）

证书编号：CCRC-2023-VP-1189
委托人名称及所在地
小米通讯技术有限公司
北京市海淀区西二旗中路33号院6号楼9层019号
生产者（制造商）名称及所在地
小米通讯技术有限公司
北京市海淀区西二旗中路33号院小米科技园6栋11层
生产企业名称及所在地
小米通讯技术有限公司
北京市海淀区西二旗中路33号院小米科技园6栋11层
产品名称和型号、规格、版本
小米智能终端可信执行环境操作系统 2.0
评估保障级
EAL5增强级：AVA_VAN.5
产品标准和技术要求
GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》 CCRC-EAL-TR-052-2023《智能终端可信执行环境操作系统安全技术要求》
上述产品符合产品认证实施规则（CCRC-IR-033:2019）的要求，特发此证。
颁证日期：2023年05月31日 有效期至：2026年05月30日
证书有效期内本证书的有效性依据发证机构的定期监督获得维持。


服务认证证书
移动金融技术服务认证
注册号：NFTC202402910052
兹证明：
杭州中天微系统有限公司
（注册地址：浙江省杭州市滨江区长河街道网商路699号5号楼2楼201室）
申请的移动终端可信执行环境（TEE）《JR/T 0156-2017 移动终端支付可信环境技术规范》、《移动金融技术服务认证实施规则-移动终端可信执行环境（TEE）》（V2.1）的相关要求，特发此证。。
名称和版本型号：
产品名称：Xuantie VirtualZone TEE
型号版本号：TH1520 v1.0
芯片型号：TH1520
研发中心、生产中心名称及地址：
杭州中天微系统有限公司
浙江杭州市西湖区三墩镇灯彩街1008号云谷园区
北京国家金融科技认证中心有限公司

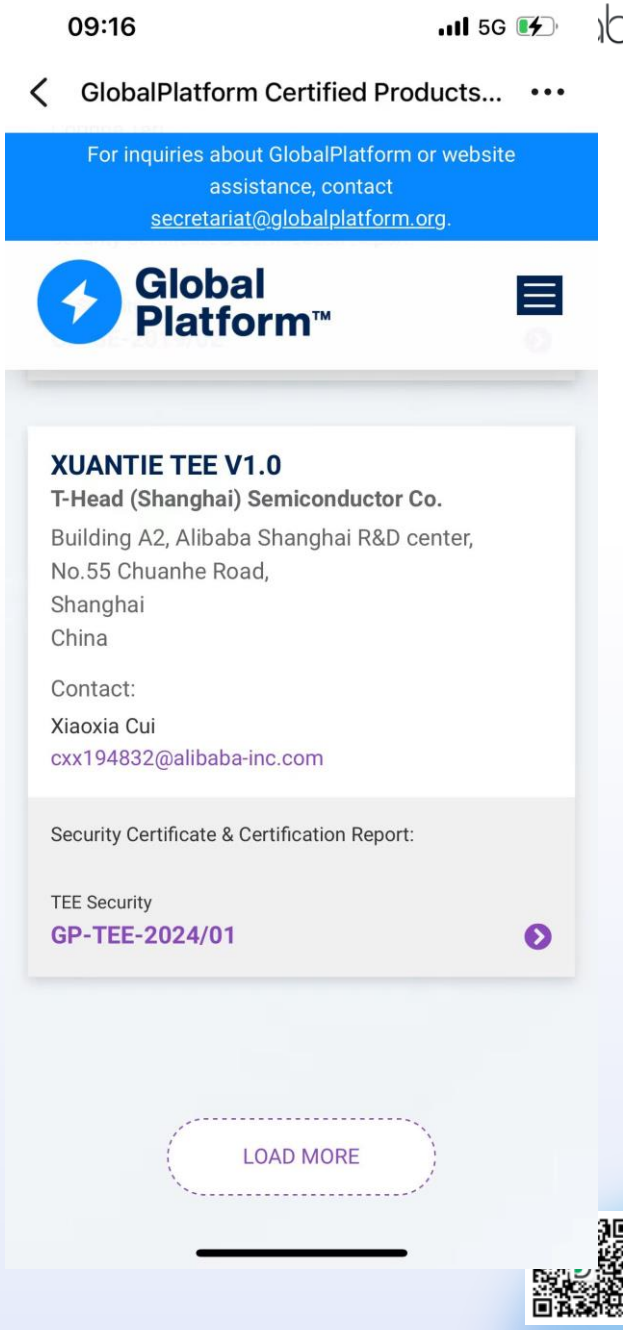


TEEOS认证

- **TEE嵌入式应用软件TA安全性及API测试**
- **TEE嵌入式系统软件安全性测试评估**
- **TEE功能一致性API ——针对TEE开发商，手机/终端厂商**

- **TEE终端芯片安全测试评估——针对终端/手机芯片企业**

TEE SOC 认证



国际 GP 车载零部件合规

从 ISO/SAE 21434到

SAEJ3101 Hardware Protected Security

再到 SESIP 简化 CC 零部件安全认证

SESIP Compliance to ISO/SAE DIS 21434

Rachel Menda-Shabat

Director of Security Solution Certification Division, Winbond

SAE INTERNATIONAL

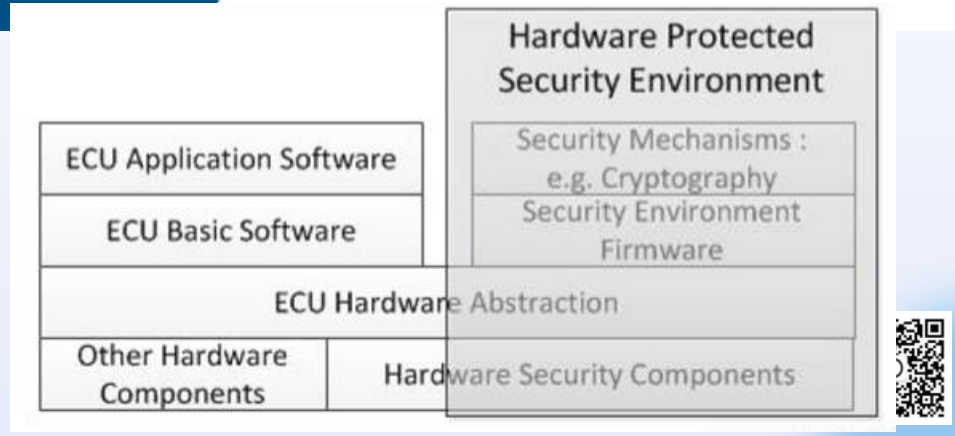
SURFACE VEHICLE RECOMMENDED PRACTICE	J3101™	FEB2020
	Issued 2020-02	
Hardware Protected Security for Ground Vehicles		

RATIONALE

Automotive computer systems are required to establish trustworthiness through device identity, sealing, attestation, data integrity, and availability. These systems must be resilient to a wide range of attacks that cannot be thwarted through software-only security mechanisms. A hardware root of trust and the hardware-based security primitives are fundamentally necessary to satisfy demands of connected and highly or fully automated vehicles. This document provides a comprehensive view of security mechanisms supported in hardware for automotive use cases, along with best practices for using such mechanisms.

GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES



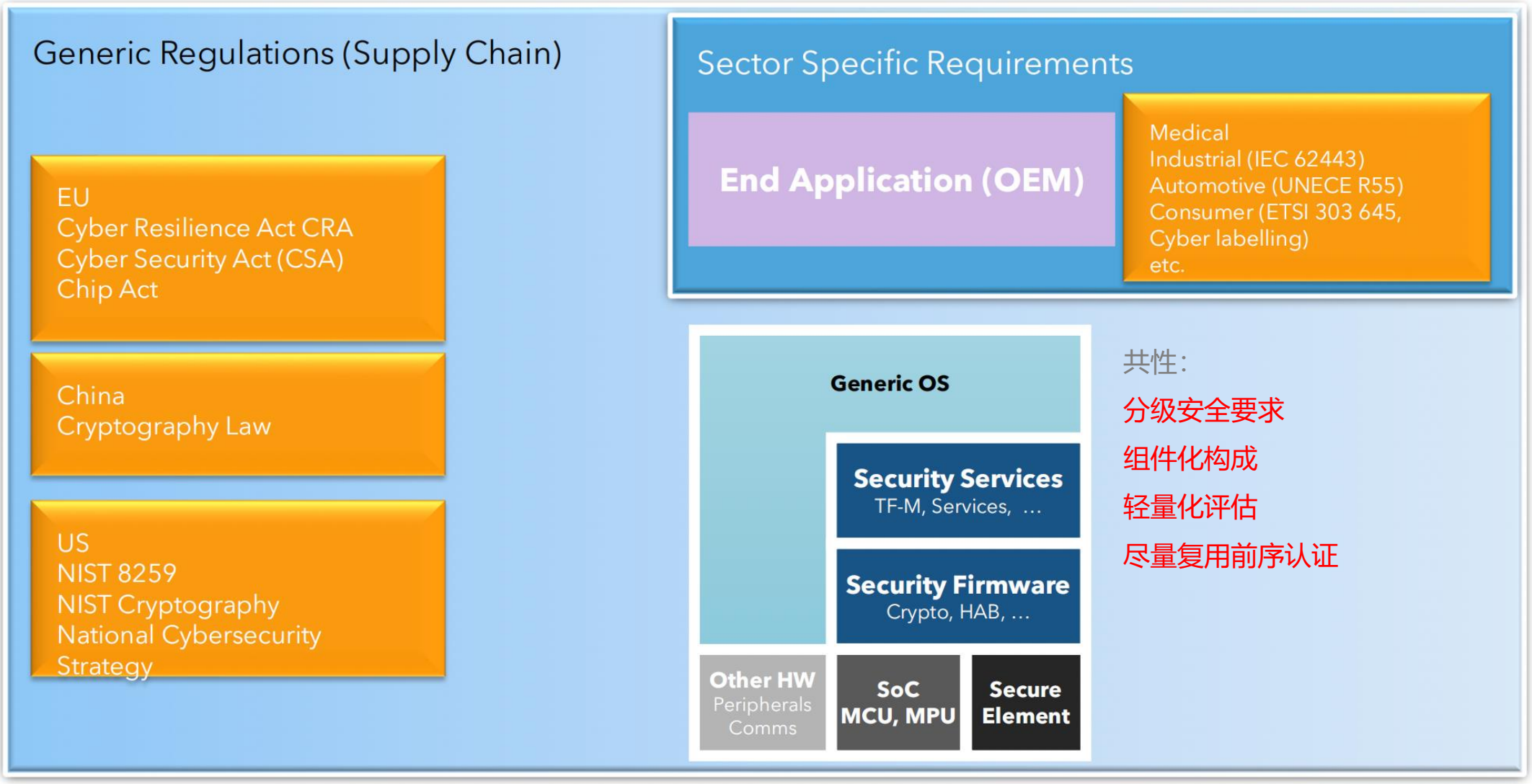
国际 GP 车载零部件合规

MCU/MPU PROFILE – GENERIC PRODUCT TYPE THREAT ANALYSIS (GENERIC TARA -1)

Assets	Threats	MCU/MPU profile coverage
Sensitive data End-user information (identity, other personal information, related keys/password) Environment data (e.g. road traffic information, environment measurements) Internal sensitive data (configuration data, keys, life cycle state)	**Modification [and disclosure] of sensitive data while stored** ➔ Impersonation leading e.g. to access to internal or external restricted services ➔ Privacy concerns ➔ Diffusion of wrong environment information ➔ Access to sensitive data and/or restricted services	Secure [Confidential/External] Storage – protections of sensitive data Secure KeyStore – protections of user crypto data e.g. keys, password Secure Debugging – protection of data access through debug interfaces Residual Information Purging – ensures erasure of sensitive data when needed (e.g. to ensure privacy in case of Field Return, Factory Reset, Decommissioning of the device) [Physical Attacker Resistance – protection against physical intrusions as simple probing]
	Modification [and disclosure] of sensitive data during manipulation ➔ Same potential impacts as above	All features – each claimed feature include the protection of assets related to the security feature [Software Attacker Resistance: Isolation of Platform – additional protections against software attacks using untrusted local code] [Physical Attacker Resistance – protections against local attacks]
	Modification [and disclosure] of sensitive data during exchanges with external entity (e.g. remote server, secure element of the integrating SoC) ➔ Diffusion of wrong environment information	Secure Communications – protections of the overall establishment of communications including related keys (generation/derivation, exchange, storage, binding, etc.)
Code	**Modification or replacement of stored code** ➔ Deletion of parts of original code ➔ Execution of attacker code replacing original code ➔ Disabling of part or all security features, access to sensitive data	Secure Initialization of Platform / Secure Update – check code authenticity and integrity before running Secure Update – allow security breaches fix All features – protection of security features execution
	Modification code at execution ➔ Bypass of parts of the code ➔ Execution of attacker code illegally loaded in memory ➔ Disabling of part or all security features, access to sensitive data and/or restricted services	[Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code] [Physical Attacker Resistance – protections against local attacks disrupting code execution e.g. HW fault injections]

SESIP兴起

中美欧为主要标准，难点在于供应链安全风险传递



SESIP兴起

中美欧为主要标准，难点在于供应链安全风险传递

SESIP总览

SESIP ≈ Common Criteria

SESIP: Security Evaluation Standard for IoT Platforms 物联网平台安全评估标准

适用于物联网组件的测评框架，如：
- 安全单元、片上系统、安全子系统、可信启动固件、信任根、操作系统等

采用**脆弱性分析**及渗透测试
- 测试活动却决于产品实现方式
- 没有预先固定的、清单式的测试内容

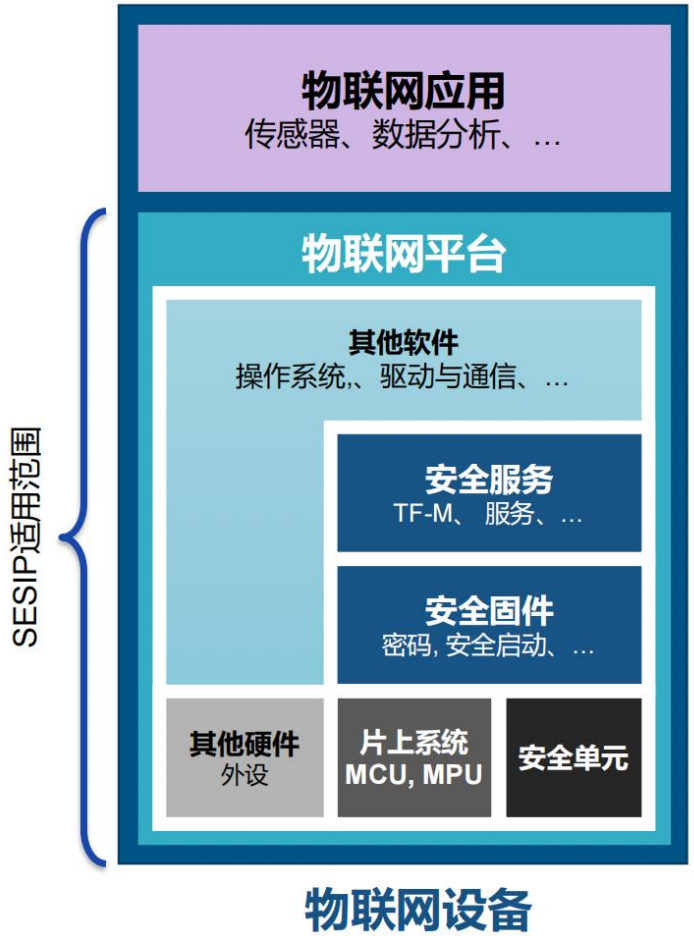
直观的安全声明
- 采用正常语言编写

测评结果的复用 – 自下而上的认证与复合认证

五个保障等级SESIP1 – SESIP5

三个攻击者轮廓
- 远程攻击
- 软件攻击
- 本地/物理攻击

最大化复用安全芯片已获取的安全认证，
以安全单元为核心搭建整套IoT应用平台

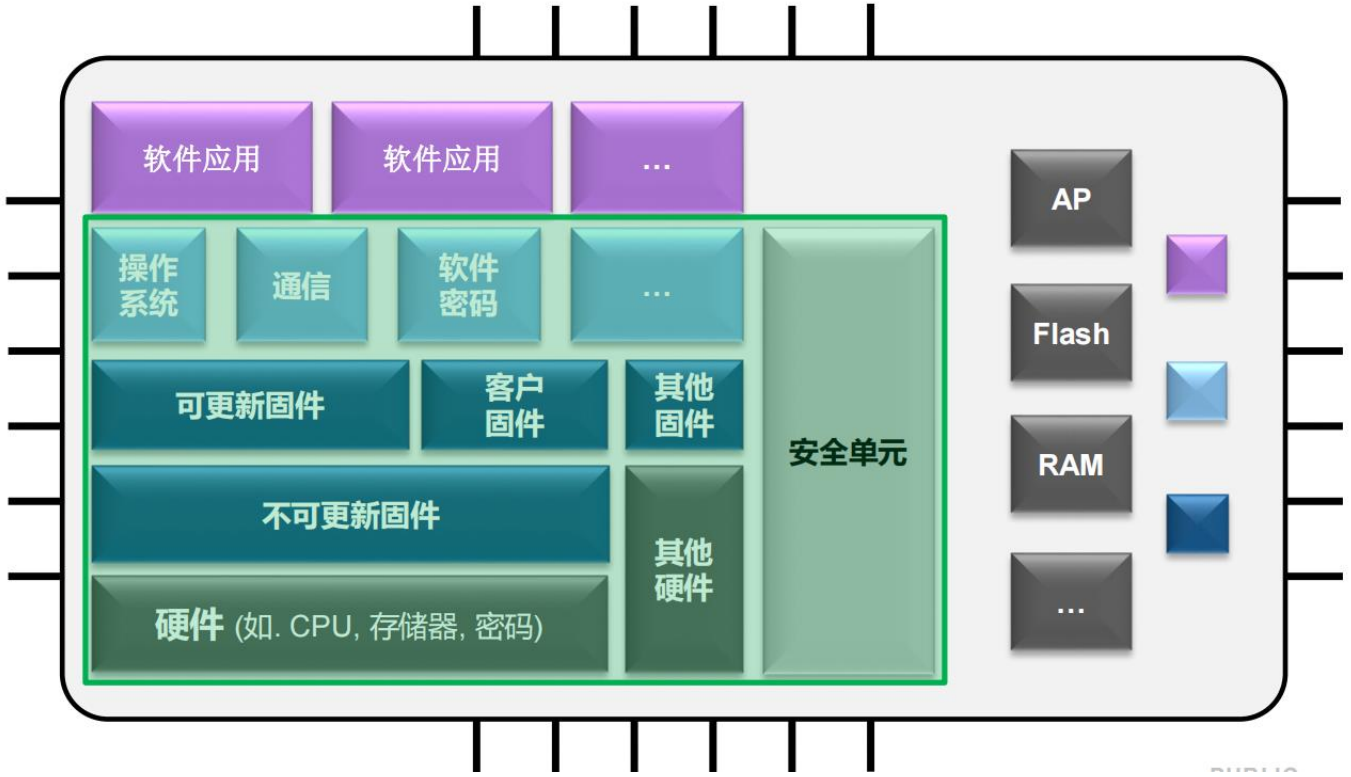


SESIP兴起

中美欧为主要标准，难点在于供应链安全风险传递

- **物联网平台安全评估标准**
  - 测评子组件& 任意子组件的组合
  - 测评结果可复用于组合测评
  - 测评结果可复用以达到物联网标准合规

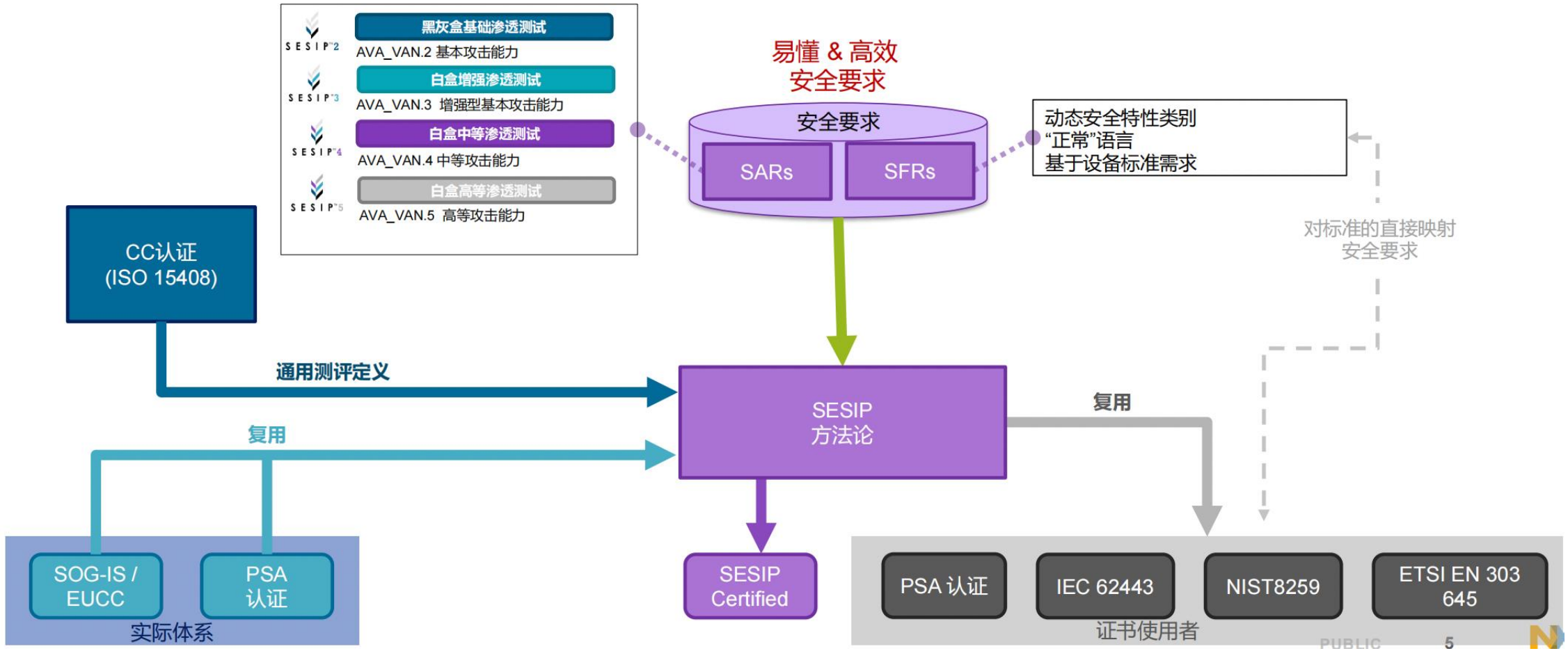
逐步覆盖全平台的安全分析



SESIP分级

中美欧为主要标准，难点在于供应链安全风险传递

- SESIP方法论模型与ISO15408 CC相似
- 基于SESIP与认证标准的“映射”，复用认证证书，避免额外工作，降低认证成本



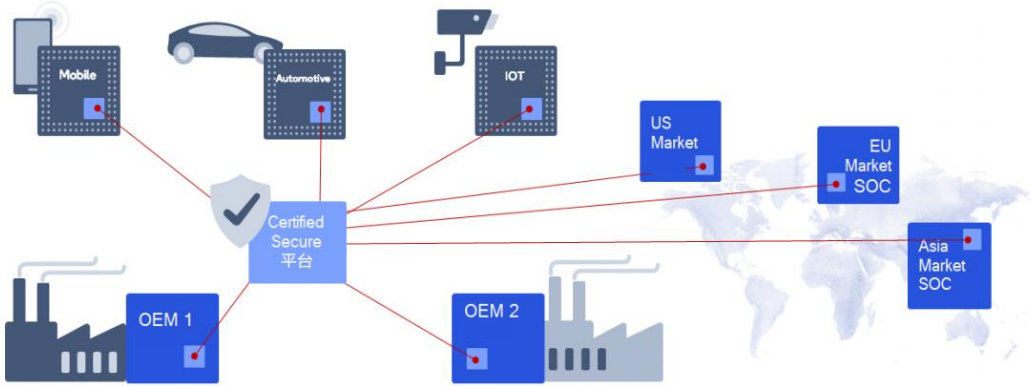
SESIP组合

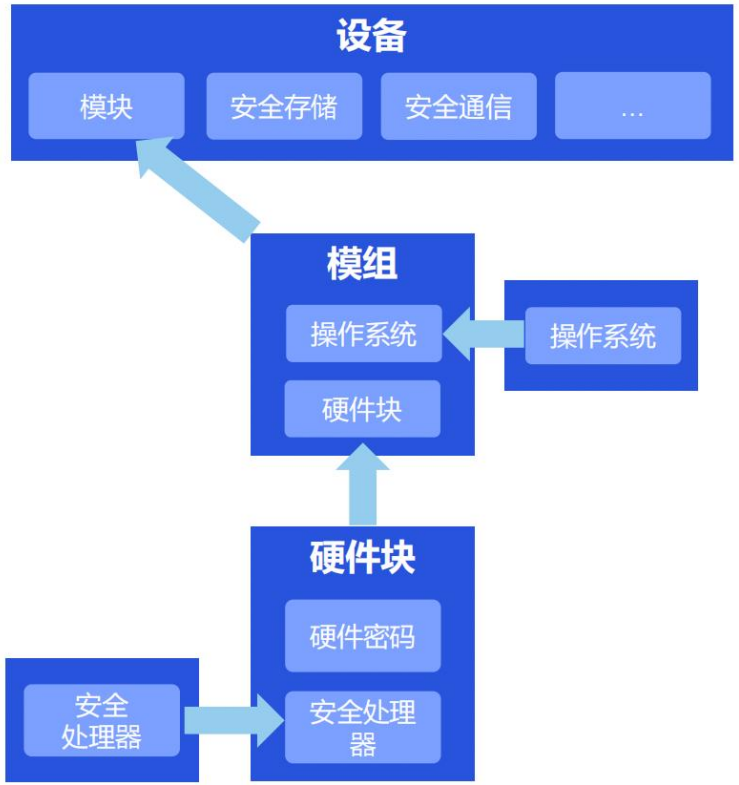
按需定义 恰当的SFR可以根据需求定义

识别和验证	产品生命周期	密码功能	安全通信	合规功能	额外的攻击者防御
平台身份验证	恢复平台出厂设置	密码运算	安全通信支持	安全存储	有限的物理攻击者防御
平台实例身份验证	平台停用	密码随机数生成	安全通信强制	安全加密存储	物理攻击防御
平台正版性验证	平台现场返修	密钥存储		安全外部存储	软件攻击者防御：平台隔离
应用程序正版性验证	平台的安全更新	密钥生成		残余信息清除	软件攻击者防御：平台部件隔离
平台状态验证	应用程序的安全安装			审计日志的生成和存储	软件攻击者防御：应用程序部件隔离
应用程序状态验证	应用程序的安全更新			安全调试	
平台的安全初始化	应用程序的安全卸载			可靠指标	

多行业匹配

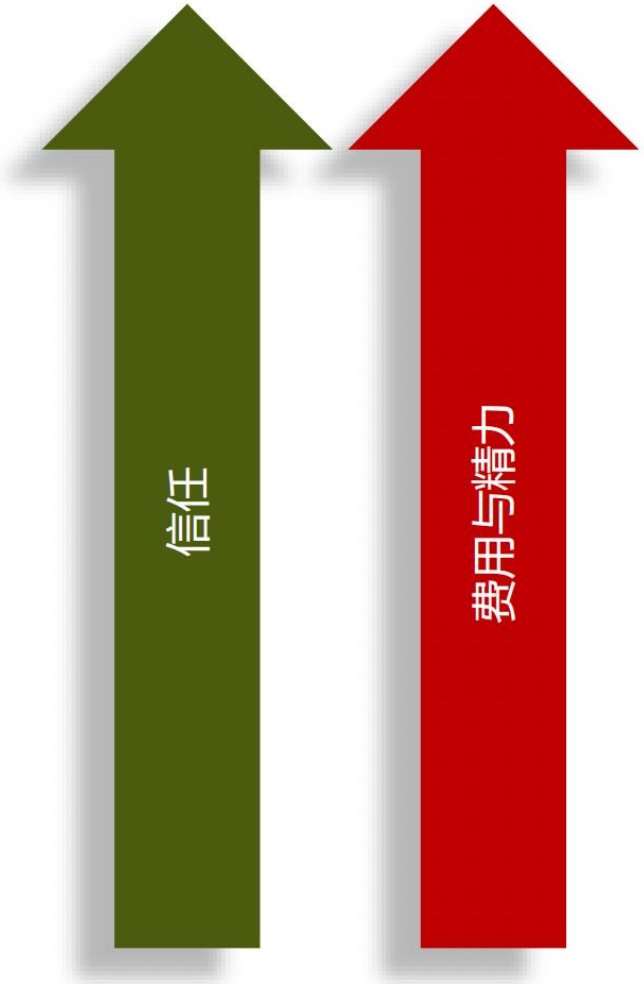
- 组件集成于多个产品
- 迭代复合的认证模式





多行业匹配

根据产品形态、行业属性、应用类型选取合适级别，抵抗适度风险



DPLSLAB

汽车行业车联网安全合规

国内探索

国内合规对标

国际标准

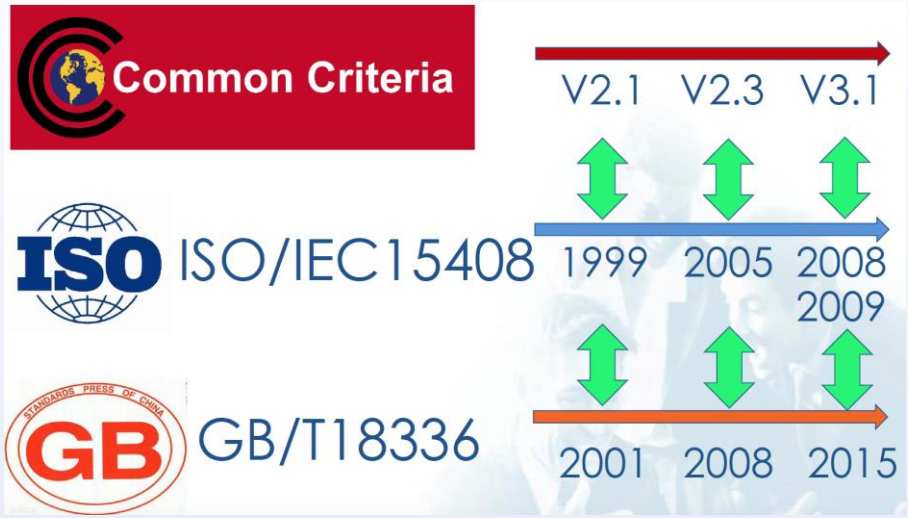
EMVCo
Chip Security

Common Criteria
ISO 15408

国内标准

JR/T 0098.2
中国金融移动支付检测规范

GB/T 18336
信息技术安全评估准则
GB/T 22186
信息安全技术具有中央处理器的IC卡芯片安全技术要求



成本显著下降（20W-50W人民币）

但仍然对于物联网领域过重

很难推广

China CC


中国网络安全审查认证和市场监管大数据中心
CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER
返回首页 | 网站地图 | ENGLISH
GO
信息公开 · 新闻快讯 · 网络安全审查 · 云安全评估 · 数据安全 · 产品认证 · 体系认证 · 服务认证 · 人员认证与培训 · 检验检测 · 法律法规 · 资源下载 · 联系我们
使认证制度
成为保障信息安全的有效机制
IT产品信息安全认证公告 更多
IT产品信息安全认证书暂停、撤..
关于部分产品依据新标准实施认证的..
关于部分产品依据新标准实施认证的..
关于部分产品依据新标准实施认证的..
产品认证FAQ 更多
暂无内容
联系方式
产品认证二处
电 话：010-82260938
电子邮件：isv@isccc.gov.cn
IT产品信息安全认证
中国网络安全审查技术与认证中心开展的IT产品信息安全认证业务，是依据信息技术安全评估准则和相关技术要求，对IT产品的安全性进行评价，旨在保护用户信息安全，维护用户利益。生产企业的IT产品获得信息安全认证证书，表明该产品符合相应的标准和技术要求。
产品认证业务
工控产品认证
物联网终端产品认证
云计算安全防护产品认证
智能卡类产品认证
评估保障级（EAL）认证
其他IT产品认证
产品认证申办系统
服务认证业务管理系统
体系认证业务管理系统
电子招标投标系统
认证申办系统
APP安全认证申办系统
人员认证业务管理系统
数据安全认证申办系统
申投诉
查询专区
强制性产品认证证书查询
产品认证证书查询
体系认证证书查询
服务资质认证证书查询


认证机构
(CCRC)
型式试验
检测机构
(DPLSLab)
质量体系评定
获证后监督
送样检测
送检企业

China CC

参考标准

GB/T 18336
信息技术安全评估准则

GB/T 22186
信息安全技术具有中央处理器的IC卡芯片安全技术要求

分级认证级别

EAL1--EAL5+

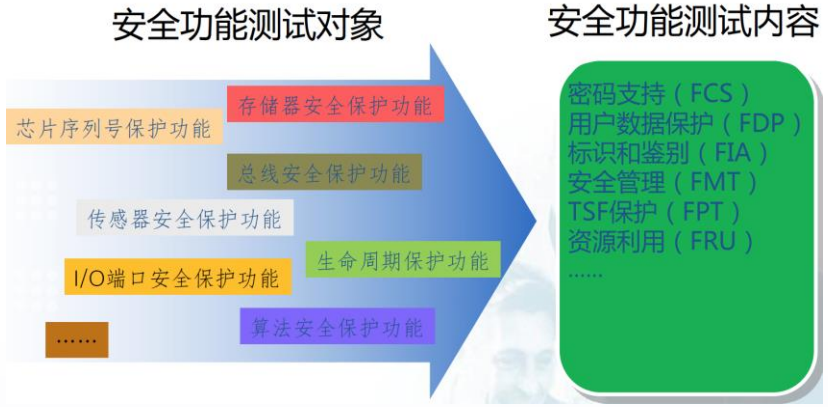
可适配芯片、TEE、零部件产品全覆盖

提交材料要求

- ✓ 申请方情况（基本信息、资质证明、质量体系文件等）
- ✓ 产品相关说明（说明书/使用手册、标准适用性说明、自测设备人员及设备说明、差异说明及自测报告、密码检测证书等（如果有的话））
- ✓ 安全保证要求说明（安全目标、功能规范、高层设计、低层设计、对应性分析、安全策略模型、指导性文档、脆弱性分析、开发者的测试报告、开发者的测试分析、开发安全、开发工具和技术、生命周期定义、交付和运行、配置管理文档、实现表示等）

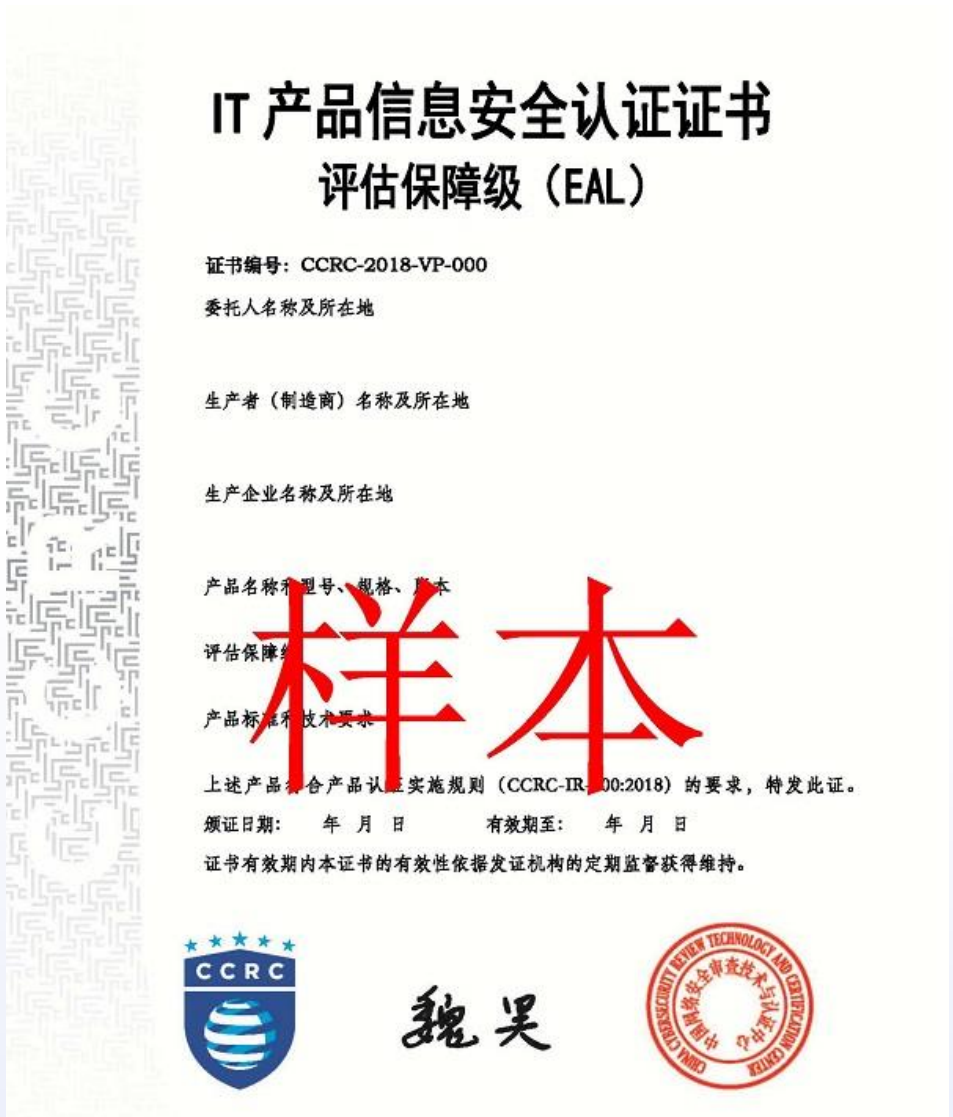
China CC

型式化试验内容



穿透性测试

编号	测试项目
Test01	物理攻击
Test02	克服探测器和过滤器
Test03	干扰攻击
Test04	利用DFA获取密钥
Test05	SPA/DPA
Test06	高阶DPA
Test07	EMA攻击
	……
Test15	中间人攻击
Test16	重放攻击
Test17	旁路鉴别或访问控制
Test18	缓存溢出或堆栈溢出
	……



IT 产品信息安全认证证书

评估保障级（EAL）

证书编号：CCRC-2018-VP-000

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称、型号、规格、版本

评估保障级

产品标准和技术要求

样本

上述产品符合产品认证实施规则（CCRC-IR-[illegible]00:2018）的要求，特发此证。

颁证日期：　年　月　日　　有效期至：　年　月　日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

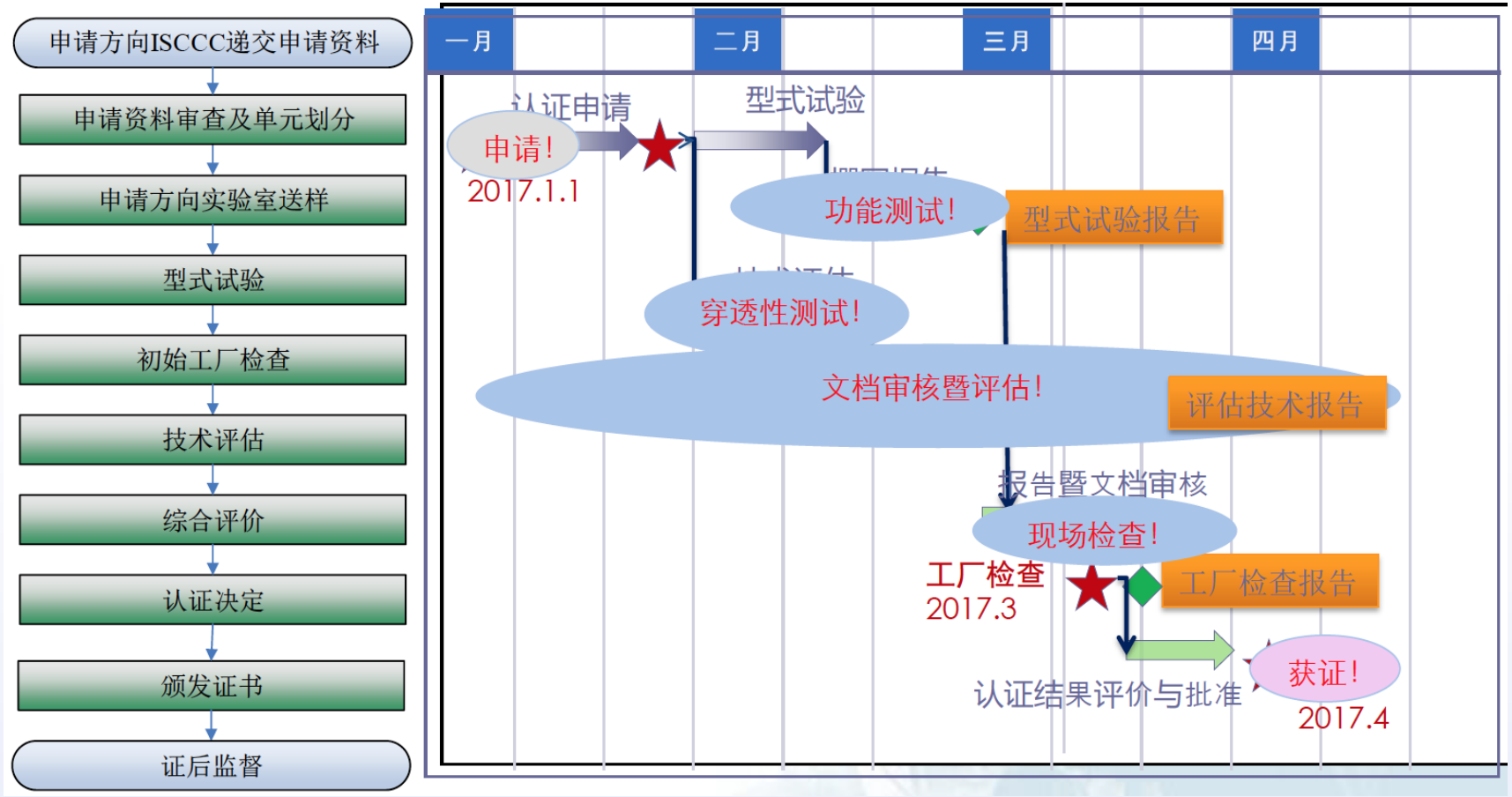
CCRC

魏 吴

中国网络安全审查技术与认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

测试流程



对于新客户/产品的测试时间预计大于6个月!

China CC

已有认证项目（PP）涉及

- 车钥匙卡
- 车载 Tbox
- 车载网关
- 车载防火墙产品
- 汽车数字钥匙
- 充电桩

4.4.2 认证单元及检测依据

序号	认证单元		检测依据	备注
1	智能卡芯片		GB/T 22186《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》	
2	智能卡产品	一般智能卡	GB/T 22186《信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求》 GB/T 20276《信息安全技术 具有中央处理器的 IC 卡嵌入式软件安全技术要求》	
		JAVA 智能卡	ISCCC-TR-041《Java 卡通用安全技术要求(EAL4+级)》 GB/T 18336 《信息技术 安全技术 信息技术安全评估准则》	
3	JAVA COS		ISCCC-TR-041《Java 卡通用安全技术要求	需测试 java

序号	产品类别	标准编号或标准号	产品依据标准
1	物联网感知终端	GB/T 36951-2018	《信息安全技术 物联网感知终端应用安全技术要求》其中 5.1 和 6.1 的物理安全要求不适用。
2	物联网感知层网关	GB/T 37024-2018	《信息安全技术 物联网感知层网关安全技术要求》其中 6.1 和 7.1 的物理安全要求不适用
3	智能家居产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-088-2022	《智能家居产品安全技术要求及测试评价方法》
4	智能门锁产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-098-2021	《智能门锁产品安全技术要求及测试评价方法》
5	道路交通信号控制机	GB 25280-2016	《道路交通信号控制机》中 5.7 节和 6.8 节。
6	车载 TBOX	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-102-2020	《智能车载终端 TBOX 安全技术要求和测试评价方法》
7	车载网关	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-101-2020	《车载网关安全技术要求和测试评价方法》
8	智能印章产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-104-2020	《智能印章产品安全技术要求和测试评价方法》
9	车载防火墙产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-109-2020	《车载防火墙产品安全技术要求和测试评价方法》
10	汽车数字钥匙	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-110-2020	《汽车数字钥匙安全技术要求和测试评价方法》
11	可穿戴产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-112-2021r1	《可穿戴产品安全技术要求和测试评价方法》
12	智能录音笔产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-114-2021	《智能录音笔产品安全技术要求和测试评价方法》
13	电动汽车充电桩产品	GB/T 18336-2015	《信息技术 安全技术 信息技术安全评估准则》
		CCRC-TR-120-2022	《电动汽车充电桩产品安全技术要求和测试评

China CC

已有认证项目（PP）涉及

- 车机操作系统
- 车联网产品
- ADAS 芯片
- 车载 TEE OS等

多个门类

且还可定制化增加

序号	产品	级别	依据标准	标准名称	增强组件
	复产品			息技术安全评估准则	
			CCRC-EAL-TR-010-2018	数据备份与恢复产品安全技术要求（评估保障级 3+级）	
10	入侵防御产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-011-2019	网络型入侵防御产品安全技术要求（评估保障级 3 增强级）	AVA_VAN.3
			CCRC-EAL-TR-017-2019	网络型入侵防御产品安全技术要求（评估保障级 4 增强级）	AVA_VAN.4
11	入侵检测系统产品	EAL3+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-012-2019	网络入侵检测系统安全技术要求（评估保障级 3 增强级）	AVA_VAN.3
12	多级安全隔离系统	EAL4	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-013-2019	多级安全隔离系统安全技术要求（评估保障级 4 级）	
13	数据泄露防护产品	EAL3+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-014-2019	数据泄漏防护产品安全技术要求（评估保障级 3+级）	AVA_VAN.3
14	用于消费类设备的嵌入式 UICC 产品	EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-015-2019	用于消费类设备的嵌入式 UICC 产品安全技术要求（评估保障级 EAL4+）	ALC_DVS.2 AVA_VAN.5
15	可下载条件接收系统硬件安全模块	EAL3	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-016-2019	可下载条件接收系统硬件安全模块安全技术要求（评估保障级 3 级）	
16	车机操作系统安全防护产品	EAL3 EAL4	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-018-2019	车机操作系统安全防护产品安全技术要求	
17	移动智能终端操作系统	EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-019-2021	移动智能终端操作系统安全技术要求（评估保障级 4 增强级）	ALC_FLR.1
18	网络隔离产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-020-2020	网络隔离产品安全技术要求（评估保障级 EAL3+、EAL4+）	AVA_VAN.3、AVA_VAN.4

序号	产品	级别	依据标准	标准名称	增强组件
	联产品		CCRC-EAL-TR-042-2021	移动智能终端与车载终端互联产品安全技术要求（评估保障级 EAL4+级）	
41	运维监控产品	EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-043-2021	运维监控产品安全技术要求（评估保障级 4 增强级）	ALC_FLR.1
42	面向辅助驾驶的车载计算芯片	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-044-2022	面向辅助驾驶的车载计算芯片安全技术要求	AVA_VAN.3 AVA_VAN.4
43	主机型入侵检测产品	EAL3+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-045-2022	主机型入侵检测产品安全技术要求（评估保障级 3 增强级）	AVA_VAN.3
44	智能终端分布式操作系统	EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-046-2022	智能终端分布式操作系统安全技术要求（评估保障级 4 增强级）	ALC_FLR.1
45	代码安全审计产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-047-2022	代码安全审计产品安全技术要求	AVA_VAN.3 AVA_VAN.4
46	交互式应用程序测试产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-048-2022	交互式应用程序安全测试产品安全技术要求	AVA_VAN.3 AVA_VAN.4
47	开源软件分析产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-049-2022	开源软件分析产品安全技术要求	AVA_VAN.3 AVA_VAN.4
48	模糊测试产品	EAL3+ EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-050-2022	模糊测试产品安全技术要求	AVA_VAN.3 AVA_VAN.4
49	网络管理与控制系统	EAL4+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-051-2022	网络管理与控制系统安全技术要求（评估保障级 4 增强级）	ALC_FLR.1
50	智能终端可信执行环境操作系统	EAL4+ EAL5+	GB/T 18336-2015	信息技术 安全技术 信息技术安全评估准则	
			CCRC-EAL-TR-052-2023	智能终端可信执行环境操作系统安全技术要求	AVA_VAN.4 AVA_VAN.5

产品认证证书查询

产品名称 Product Name | 车 | 验证码 | VuNpW | 搜索 | 注：如需根据证书编号进行查询，请输入完整的证书编号

证书编号	产品名称、型号规格、版本号	申请级别	认证委托人	生产企业	制造商	认证标准	发证日期	有效期至	首次发证日期
CCRC-2023-VP-1249	车载操作系统信息安全子系统 / V1.0	EAL4	亿咖通(湖北)技术有限公司 ECARX (Hubei) Technology Co., Ltd.	亿咖通(湖北)技术有限公司 ECARX (Hubei) Technology Co., Ltd.	亿咖通(湖北)技术有限公司 ECARX (Hubei) Technology Co., Ltd.	GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》 CCRC-EAL-TR-018-2019《车机操作系统安全防护产品安全技术要求》	2023-08-21	2026-08-20	2023-08-21
CCRC-2023-VP-1231	MizarU车载安全芯片 TTMU	EAL5增强级：ALC_DVS.2, AVA_VAN.5	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	GB/T 22186-2016《信息安全技术 具有中央处理器的IC卡芯片安全技术要求》	2023-07-24	2026-07-23	2023-07-24
CCRC-2022-VP-1068	车载计算芯片征程5 （面向辅助驾驶的车载计算芯片）	EAL3增强级：AVA_VAN.3	北京地平线机器人技术研发有限公司	地平线（上海）人工智能技术有限公司	地平线（上海）人工智能技术有限公司	GB/T 18336-2015《信息技术			
CCRC-2022-VP-1021	电动汽车直流充电机 NRKJ9300 /		南京能瑞电力科技有限公司 Nanjing Nengrui Electric Power Technology Co.Ltd	南京能瑞电力科技有限公司 Nanjing Nengrui Electric Power Technology Co.Ltd	南京能瑞电力科技有限公司 Nanjing Nengrui Electric Power Technology Co.Ltd				
CCRC-2022-VP-987	ZEEKRPower电动汽车交流充电桩 HH-A-ZK01/7K /		浙江浩瀚能源科技有限公司 Zhejiang Haohan Energy Technology Co., Ltd.	科大智能(合肥)科技有限公司 CSG SCIENCE &TECHNOLOGY CO.,LTD. HEFEI	浙江浩瀚能源科技有限公司 Zhejiang Haohan Energy Technology Co., Ltd.	GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》 CCRC-TR-120-2022《电动汽车充电桩产品安全技术要求和测试评价方法》	2022-07-26	2025-07-25	2022-07-26
CCRC-2020-VP-644	Mizar车载安全芯片 Mizar	EAL4增强级：AVA_VAN.4	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	上海芯钛信息科技有限公司 Shanghai Thinktech Information Technology Co., Ltd.	GB/T 22186-2016《信息安全技术 具有中央处理器的IC卡芯片安全技术要求》（EAL4增强级：AVA_VAN.4）	2020-07-01	2023-06-30	2020-07-01
CCRC-2020-VP-587	车机管家 / V2	EAL4	北京百度网讯科技有限公司 Beijing Baidu Netcom Science Technology Co.,Ltd.	北京百度网讯科技有限公司 Beijing Baidu Netcom Science Technology Co.,Ltd.	北京百度网讯科技有限公司 Beijing Baidu Netcom Science Technology Co.,Ltd.	GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》; CCRC-EAL-TR-018-2019《车机操作系统安全防护产品安全技术要求》（EAL4）	2020-01-09	2023-01-08	2020-01-09

标准	标准名称	增强组件
C-EAL-TR-042-2021	移动智能终端与车载终端互联产品安全技术要求（评估保障级 EAL4+ 级）	
Γ 18336-2015	信息技术 安全技术 信息技术安全评估准则	ALC_FLR.1
C-EAL-TR-043-2021	运维监控产品安全技术要求（评估保障级 4 增强级）	
Γ 18336-2015	信息技术 安全技术 信息技术安全评估准则	AVA_VAN.3 AVA_VAN.4
C-EAL-TR-044-2022	面向辅助驾驶的车载计算芯片安全技术要求	
Γ 18336-2015	信息技术 安全技术 信息技术安全评估准则	AVA_VAN.3
C-EAL-TR-045-2022	主机型入侵检测产品安全技术要求（评估保障级 3 增强级）	
Γ 18336-2015	信息技术 安全技术 信息技术安全评估准则	ALC_FLR.1
C-EAL-TR-046-2022	智能终端分布式操作系统安全技术要求（评估保障级 4 增强级）	
Γ 18336-2015	信息技术 安全技术 信息技术安全评估准则	AVA_VAN.3

18	网络隔离产品	EAL3+ EAL4+	GB/T 18336-2015	
			CCRC-EAL-TR-020-2020	EAL3+、EAL4+）

系统	CCRC-EAL-TR-052-2023

商密认证

认证机构

商密检测中心

授权检测机构

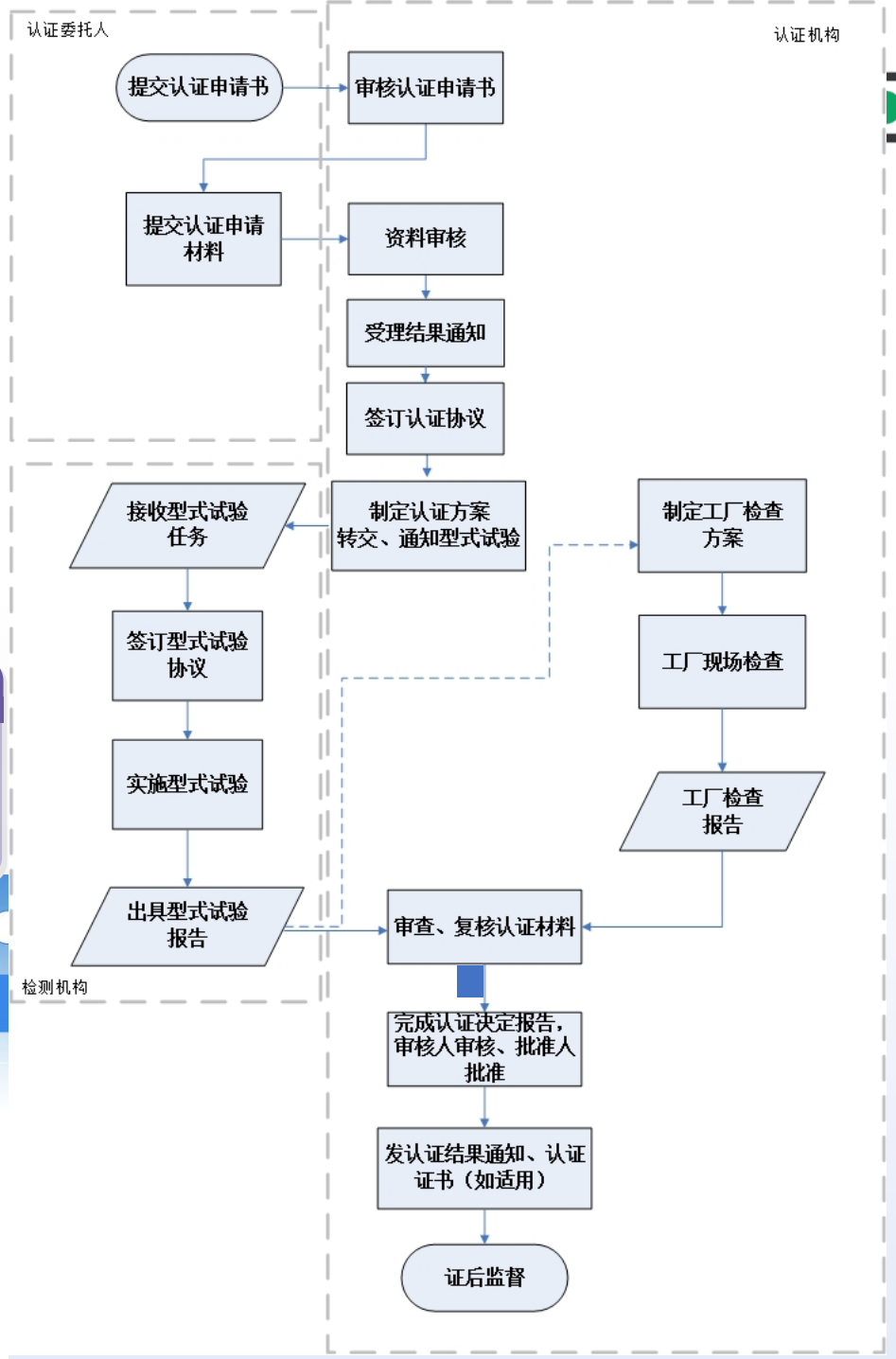
商密检测中心
（可受理28类产品）

授权检测机构

深圳鼎铉等6 家
（可受理X类产品）

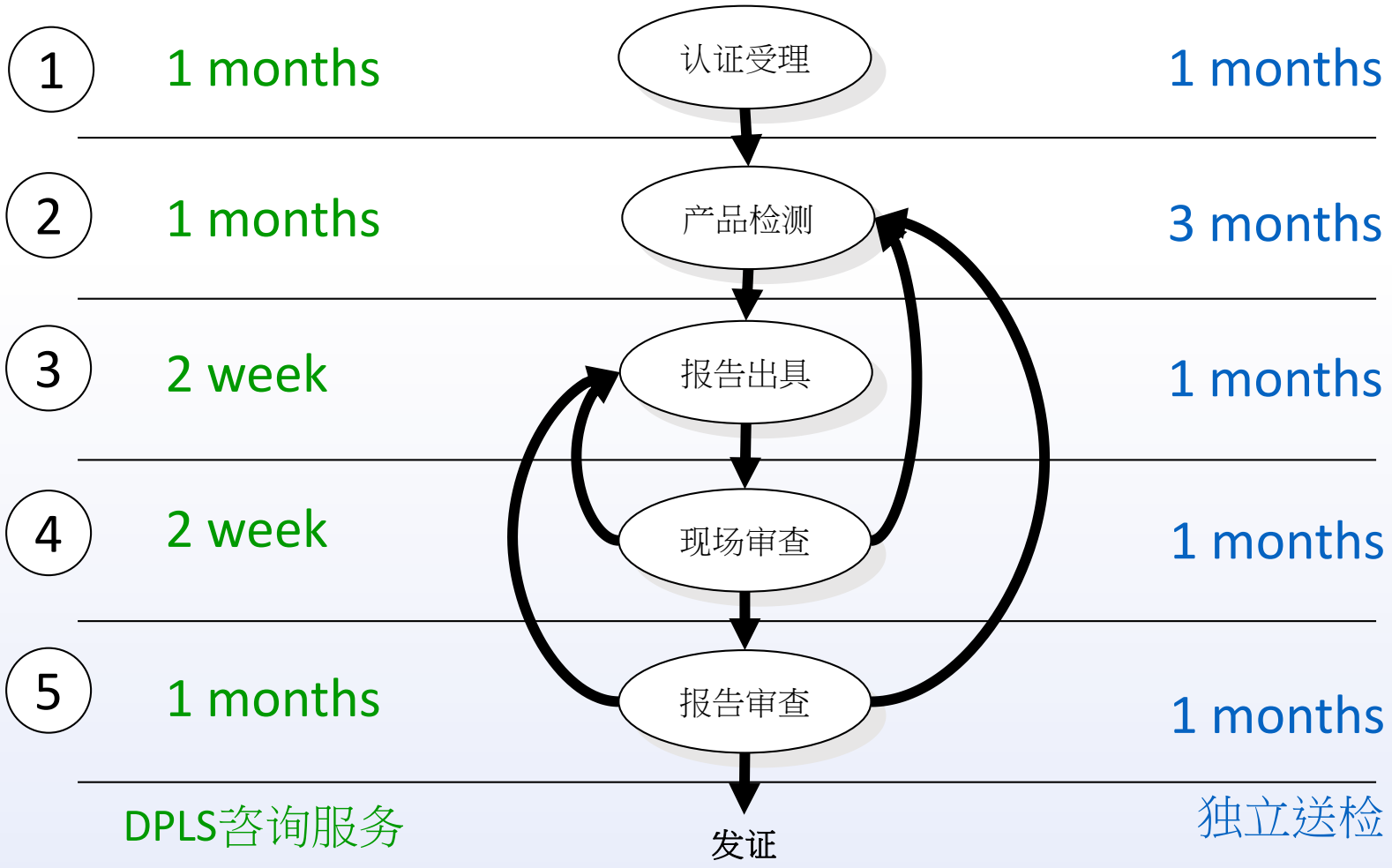
授权检测机构

汽车行业
中汽研软评
（可受理2类产品）



商密认证

检测周期


1
1 months
认证受理
1 months
2
1 months
产品检测
3 months
3
2 week
报告出具
1 months
4
2 week
现场审查
1 months
5
1 months
报告审查
1 months
DPLS咨询服务
发证
独立送检

商密&FIPS认证

超过40家企业协助咨询

申请方
密码产品厂商

测试反馈

检测中咨询
陪同答辩
检测问题解答

检测中咨询
演示样品适配
测试脚本开发

提交样品及送检材料

送检前咨询
培训
样品预测试
文档模板提供及梳理

提交通过报告

授权检测机构
FIPS/OSCCA
密码Lab

认证机构
密码检测中心
FIPS/OSCCA

现场审查咨询
预审查服务

OSCCA
Consulting

咨询项目	服务项目	服务内容	预计时间
	算法正确性验证 CAVP	针对SM2算法实现正确性及鲁棒性验证Correction and robustness verification for SM2 algorithm	3Week
		针对SM3算法实现正确性及鲁棒性验证Correction and robustness verification for SM3 algorithm	
		针对SM4算法实现正确性及鲁棒性验证Correction and robustness verification for SM4 algorithm	
	TRNG实现质量 Achieve quality	针对TRNG实现原理及随机数质量检测For TRNG implementation principle and random number quality detection	1Week
	文档准备辅导	送检材料梳理，使之符合技术处和检测中心对材料的要求，包括提交当地监管机构和提交检测机构二套材料	8Week
	测试过程中配合	与检测机构沟通测试进度，协助回复检测机构问题，给出整改指导方案，提前了解答辩专家情况设计针对性的答辩方案（如有），服务时间到当款产品获取证书为止	X
	预测试	送客户送检前的所有功能和安全相关测试项进行预测试，确认材料和方案测试都已准备完毕，出具预测结果及整改意见，配合生成自测报告，针对问题指导整改	3Week
	审查	针对设计和生产环境进行现场审查，配合资质审核。包括物理环境准备、制度材料准备，专家现场审核内容及评分机制，技术人员的国密基础知识考试。	2Day
	小计		
	培训	针对安全芯片测试点开展深入培训，专注检测评估标准和内容，包括送检流程、材料编写、规范、检测案例及答辩注意事项	2Day
	文档模板	提供文档编写模板	1Day

关于我们
ABOUT US

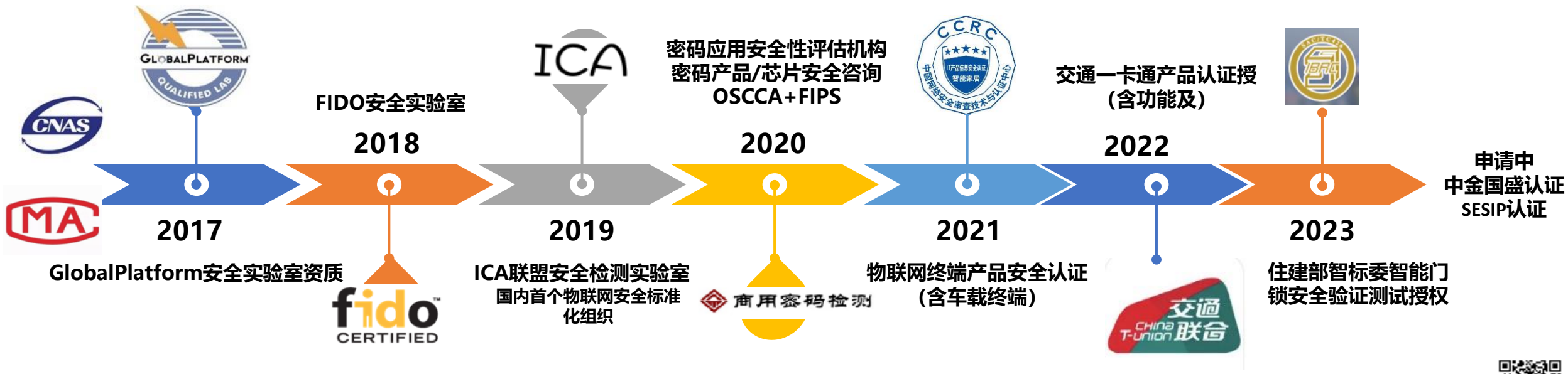
智慧云测公司的技术团队成员由博士、硕士以及归国留学人员等组成，核心技术人员均获得过国家部委级别的科技特等奖、一等奖，参与国家标准和行业标准等的制修订工作，是中国合格评定国家认可委员会CNAS认可授权实验室、CMA检验检测机构资质认定等资质。

公司成立以来，稳步成长，在国际、国内的信息安全行业享有较高知名度和声誉的全流程服务的综合性安全实验室，依据国际国内行业安全标准，提供专业的合规认证、检测服务、咨询服务及更广泛的安全领域配套服务。服务领域涉及金融、交通、广播电视、公安、电力、质量监督、高校等行业领域。

资质能力

技术及行业深耕+民营独立第三方身份，获得国际国内芯片安全类检测资质

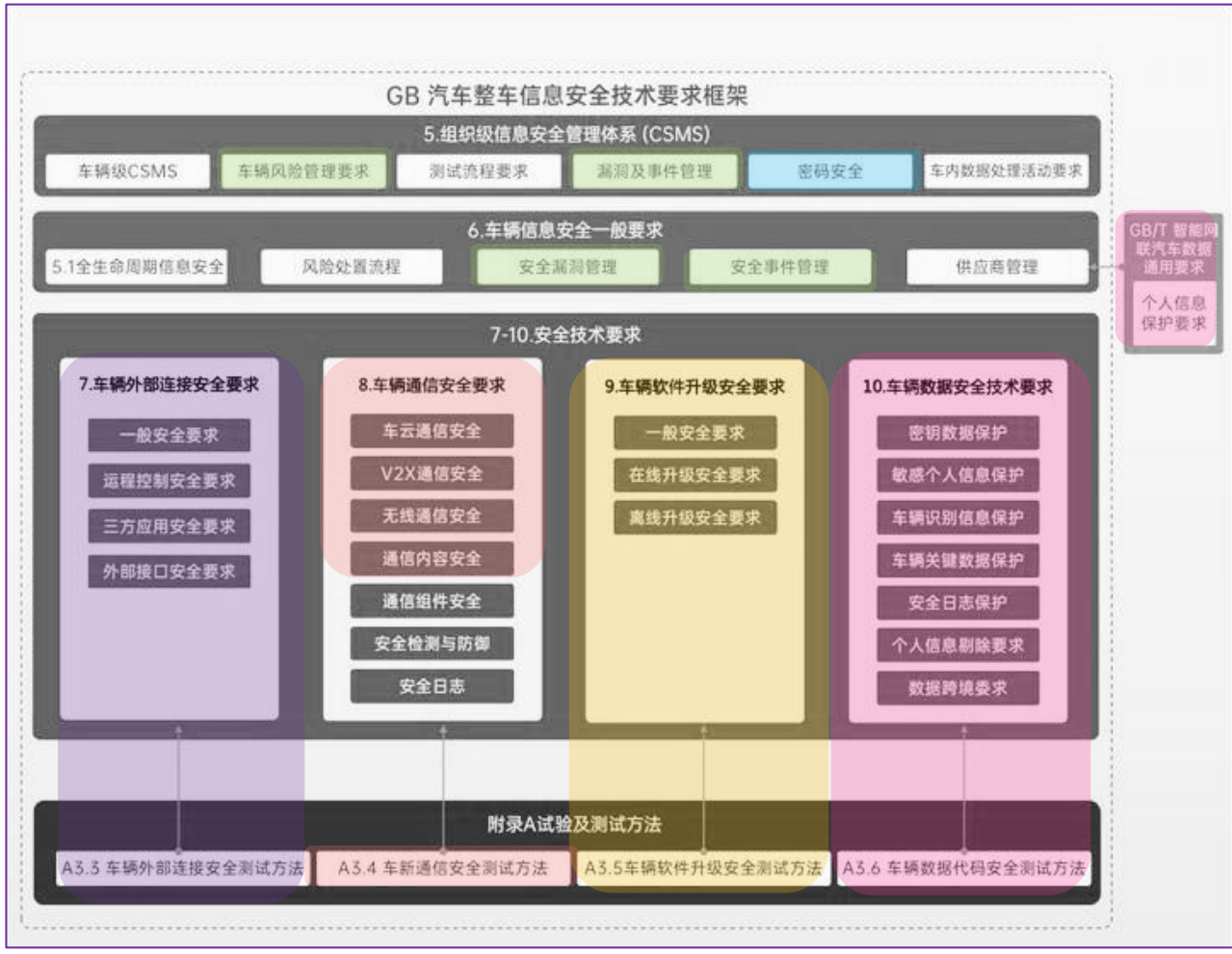
- 国内第1家GlobalPlatform安全实验室资质（全球共3家），完成全国首款，全球第2款TEE产品安全测试
- 国内第1家国际生物识别安全标准化组织FIDO授权安全实验室（全球共8家），完成全国第1款生物识别安全产品测试
- 国家密码管理局授权密码应用安全性评估机构，在近百家被考察机构中技术考核全国第4名
- 国内第1个物联网安全标准化组织ICA联盟安全检测工作组组长单位，国内首批在物联网安全领域内开展芯片及产品安全检测实验室
- 工信部唯一授权人工智智能及物联网安全检测公共服务平台企业。



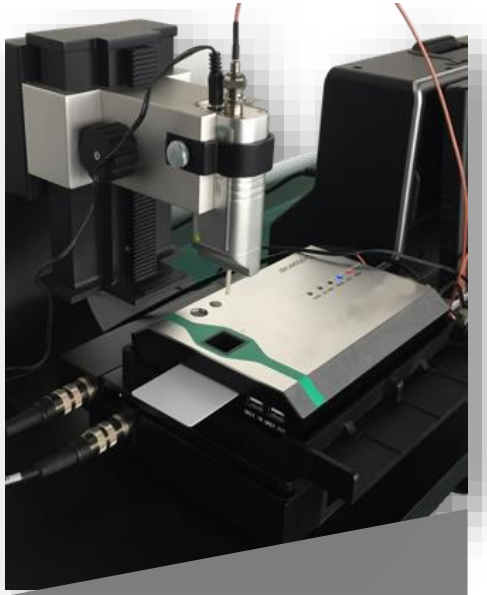
数据来自：GP、FIDO、中交信联、国家密码管理局、DPLSLAB等官网

汽车信息安全检测能力建设

标准化检测工具矩阵与GB对应关系



检查设备及服务 非侵入，半侵入芯片检测设备



侧信道测试平台

支持多种常用攻击算法
内建多种对齐 / 滤波算法
支持国密算法
内建多种分析处理算法

单点激光测试平台

支持多种波长激光注入
激光脉冲宽度 / 能量可调
支持国密算法
支持多种芯片接口

电磁操纵测试平台

电磁注入能量可调
电磁最小脉冲宽度10纳秒
支持国密算法
支持多种芯片接口

智能电压毛刺平台

支持多种芯片接口
电压毛刺最小宽度4纳秒
支持国密算法
支持任意位置攻击

检查设备及服务 侵入式芯片检测设备

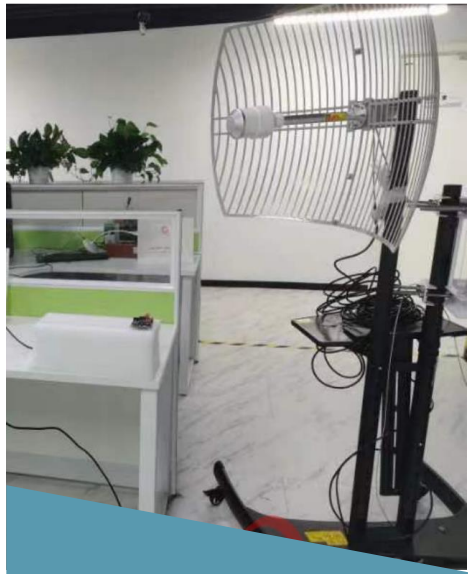
多维故障注入平台

支持多种故障源组合攻击攻击

一体化集成设计

支持红外透视

汽车芯片领域率先适配



侧信道拓展平台

远场侧信道分析拓展组件

深度学习侧信道拓展组件

多源侧信道拓展组件

汽车行业台架适配

激光开封平台

基于激光攻击产品线延伸

自主可控国产替代方案

软件支持二次开发

视觉定位高可靠性

激光切割平台

基于激光攻击产品线延伸

支持红外/绿/紫外多种波长激光源

高精度切割

芯片失效分析平台

X-Ray芯片无损失效分析

集成日本滨松X射线源

可编辑的检测程序

IN BEIJING, CHINA

中国·北京

分享完毕

THANK YOU FOR YOUR WATCHING

感 谢 您 的 观 赏 聆 听

公 司 地 址 ： 北 京 市 门 头 沟 区 莲 石 湖 西 路 9 8 号 院 7 号 楼 7 0 1