Microchip汽车安全简介

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

王敏，汽车产品部应用工程师

2021年01月26日

SMART | CONNECTED | SECURE

攻击面持续扩大

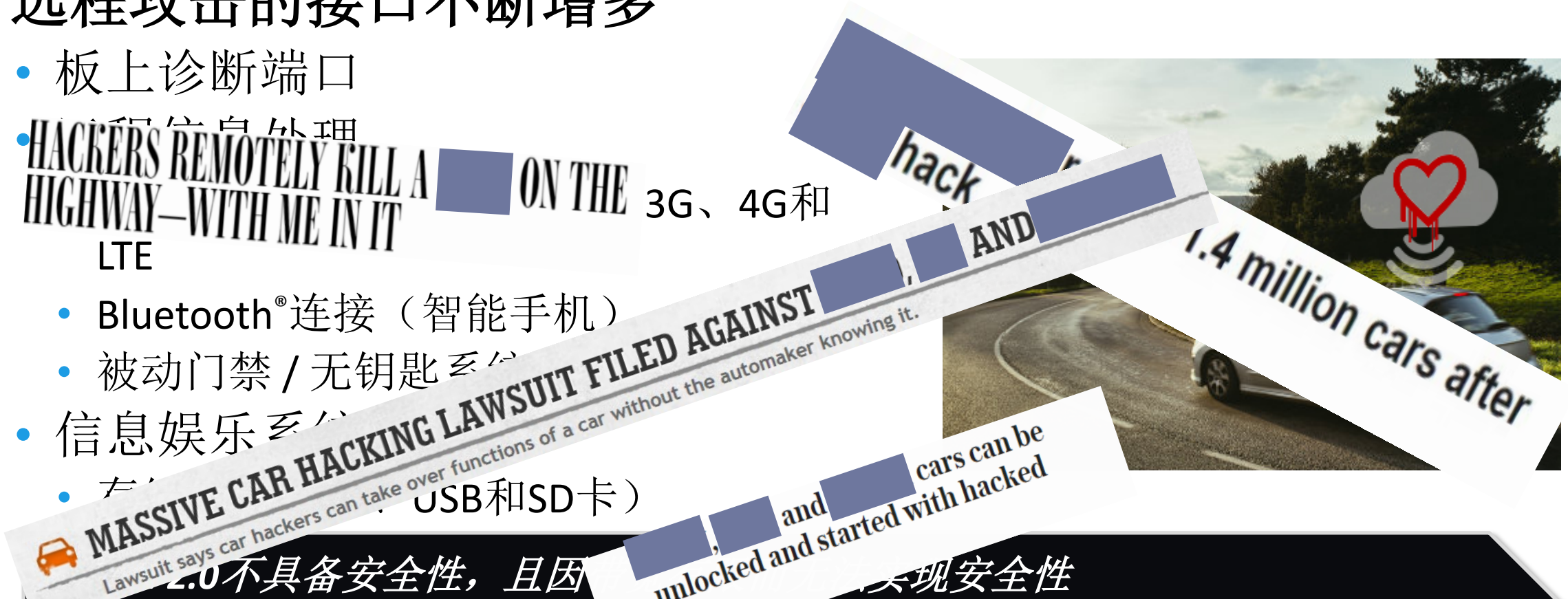
- 远程攻击的接口不断增多
  - 板上诊断端口
  - 远程信息处理
    - Wi-Fi®热点和远程无线连接，3G、4G和LTE
    - Bluetooth®连接（智能手机）
    - 被动门禁 / 无钥匙系统
  - 信息娱乐系统
    - 存储媒介（CD、USB和SD卡）

- ***CAN 2.0不具备安全性，且因带宽有限而无法实现安全性***
- ***以太网VLAN用于流量隔离而非安全性***

MICROCHIP

攻击面持续扩大

- 远程攻击的接口不断增多
  - 板上诊断端口
  - 远程信息处理
    - 3G、4G和LTE
    - Bluetooth®连接（智能手机）
    - 被动门禁 / 无钥匙系统
  - 信息娱乐系统
    - 有线（USB和SD卡）



- *2.0不具备安全性，且因[redacted]实现安全性*
- *以太网VLAN用于流量隔离而非[redacted]性*

MICROCHIP

对新型汽车安全标准的影响因素

ISO/IEC 9797-1/ISO 26262
ISO 27001/IEC 62443
J3061/J3101

汽车安全

NHTSA

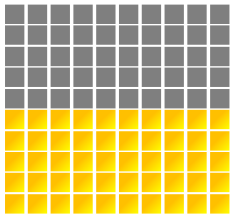
美国国家公路交通安全管理局

CAN

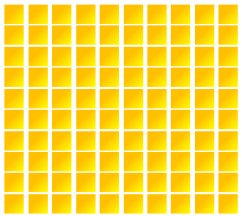
CAN FD

OEM

安全规范



More than 50% of vehicles sold worldwide in 2015 to be connected (either embedded, tethered or smartphone integration)



Every new car to be connected in multiple ways by 2025

MICROCHIP

市场趋势：
标准的部分列表

- ISO/IEC 9797-1：安全技术——报文验证代码
- ISO/IEC 11889：可信平台模块
- IEC61508：电子系统的功能安全
- ISO 12207：系统和软件工程——软件生命周期过程
- ISO 15408：IT安全评估准则
- ISO 26262：道路车辆的功能安全
- ISO 27001：信息安全管理体系
- ISO 27002：实用规则——安全
- ISO 27018：实用规则——处理PII/SPI（隐私）
- ISO 27034：应用安全技术
- ISO 29101：隐私架构框架
- ISO 29119：软件测试标准
- IEC 62443：工控网络和系统安全
- 国际自动机工程师学会（SAE International）正在制定或已经发布的一些标准：
  - J2945：专用短距离通信（DSRC）最低性能要求
  - J3061：信息物理车辆系统网络安全指南
  - ISO 21434：道路车辆——网络安全工程
  - J3101：地面车辆应用的硬件保护安全要求
  - WP.29：车辆法规协定

MICROCHIP

网络安全规范审查服务

- **Microchip提供安全规范审查**
  - Microchip在规范开发期间直接与OEM合作
  - 为Tier-1客户进行逐行审查
    - 帮助回答RFI/RFQ
    - 帮助制定架构安全策略以支持规范
  - 支持风险评估审查和攻击树分析

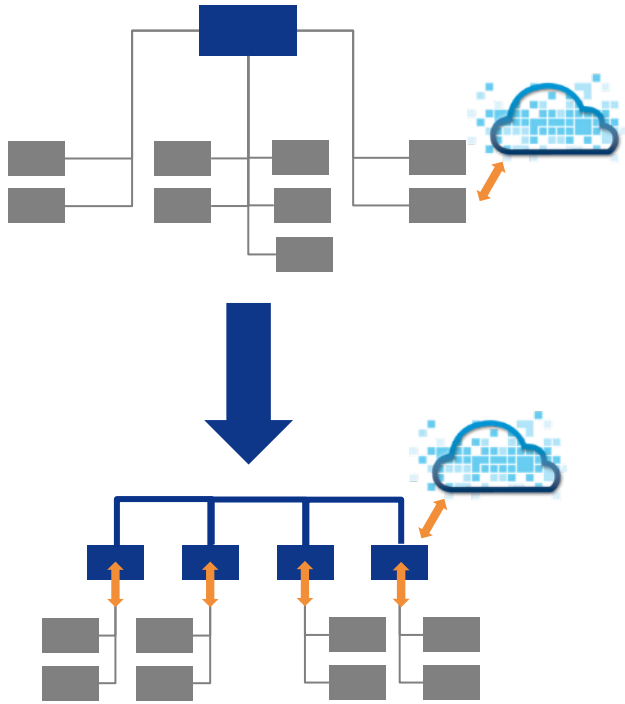
MICROCHIP

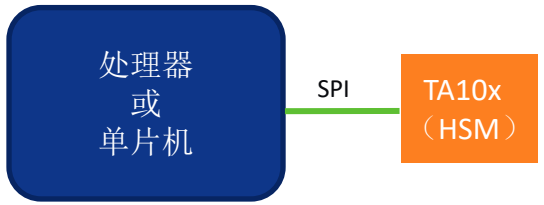
那么，目前的计划是什么？

- （缓慢）迁移到充当防火墙的集中式域控制单元

- 使用安全双核单片机在受控环境中运行“安全”软件……这是一次成本高昂的升级，可能无法满足安全密钥存储要求
  - 相反，应保留现有的MCU、MPU或FPGA解决方案，并使用安全配套HSM器件升级安全性

- 不论采用什么总线，均添加报文验证
  - CAN 2.0或CAN FD报文验证
  - 射频智能电池包——经过验证的BMS



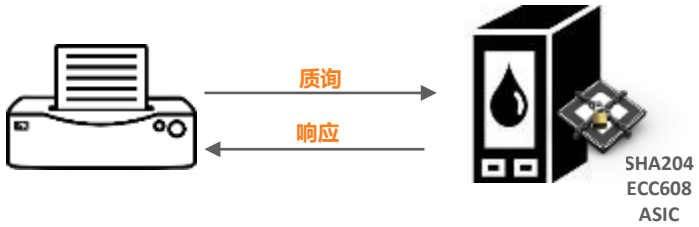


MICROCHIP

SPG产品细分

配件

配件或一次性用品验证
- 接触式或非接触式验证

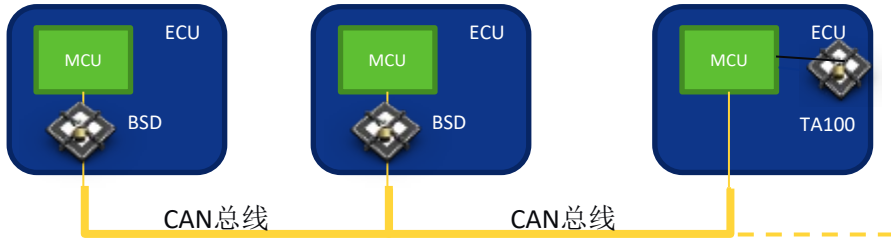


物联网

已连接节点
- 可轻松对任何IoT节点进行安全升级
- 无缝密钥和证书预配置
- 节点认证
- 通信加密

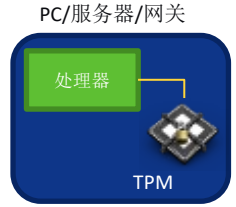
汽车级\工业级

车载网络安全
- 安全引导和固件更新
- 报文验证
- TLS/HDCP/USB-C安全
- 简单的ECU安全升级



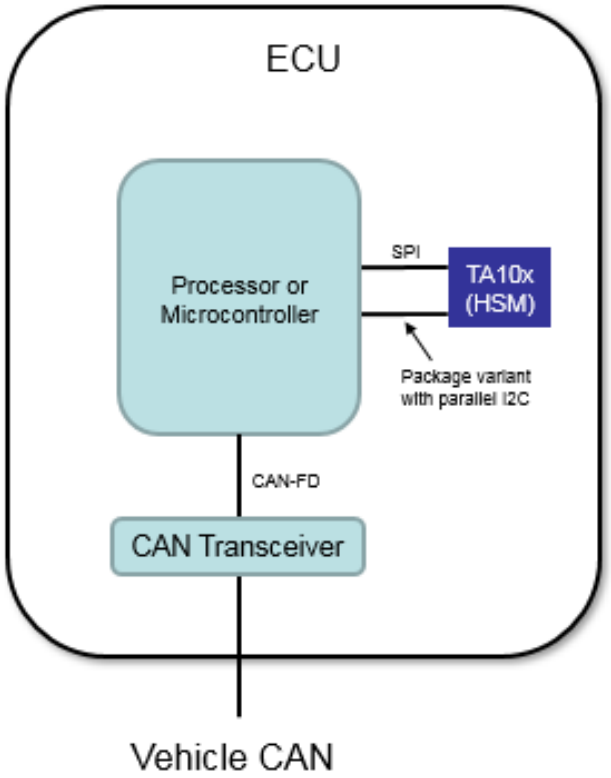
企业级

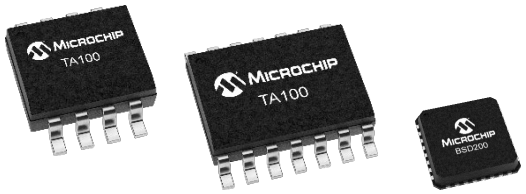
可信平台模块（TPM）
- 平台完整性测量
- 远程认证

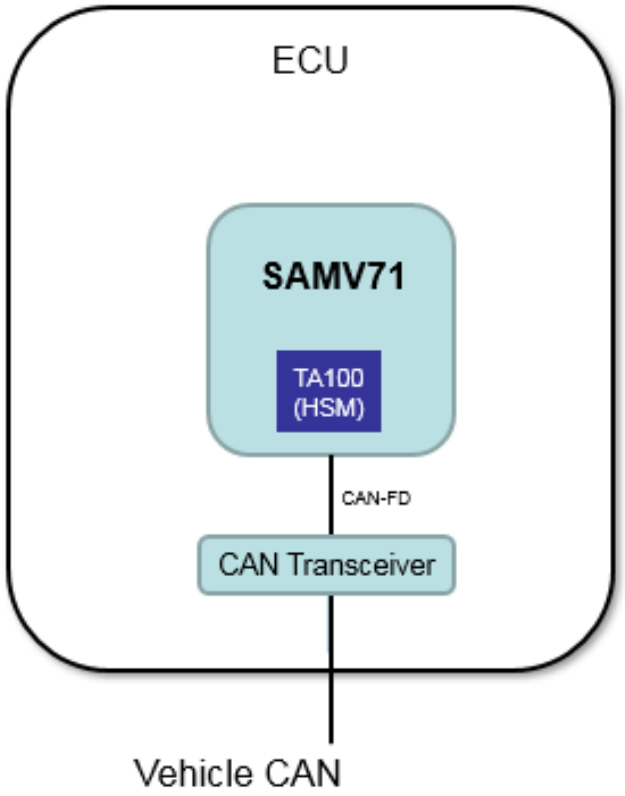


MICROCHIP

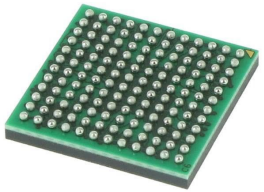
信任锚HSM外形







BU	产品
MCU32	SAMV71
MCU32	新一代SAMV71
MCU32	C21
MCU32	PIC32CM
MCU32	全新E54
MCU16	dsPIC33CK



- **多个MCU/TA100 SiP（即MCM）BGA**

MICROCHIP

解决方案概述：信任锚和边界安全器件

	TA10x	BSD20x

主要特性和应用场景	• CAN报文过滤和车辆总线防火墙
	• 可配置安全引导
	• X.509证书验证和存储
	  • USB-C的轻量级版本
	• 安全的私钥/秘钥存储
	• RSA和ECC签名生成和验证
	• RSA/ECC会话建立和密钥协议
	• 命令授权和协议加密
	• RSA/ECC/AES/SHA验证
	• AES/ECC密钥生成
	• 高质量RNG（SP 800-90 A/B/C）
	• 可选的WPC、TLS和高带宽数字内容保护（HDCP）
	  • 3k RSA验证
	  • 1k RSA加密/解密
	• **CAN报文验证，与支持CAN-FD的MCU配套使用**
		• CAN报文过滤和车辆总线防火墙
		• 可配置安全引导
		• X.509证书验证和存储
		  • USB-C的轻量级版本
		• 安全的私钥/秘钥存储
		• RSA和ECC签名生成和验证
		• RSA/ECC会话建立和密钥协议
		• 命令授权和协议加密
		• RSA/ECC/AES/SHA验证
		• AES/ECC/RSA密钥生成
		• 高质量RNG（SP 800-90 A/B/C）
		• 可选的WPC、TLS和高带宽数字内容保护（HDCP）
		  • 3k RSA验证
		  • 1k RSA加密/解密
		• **CAN报文验证，与不支持CAN-FD的MCU配套使用**
		  • **CAN-2.0 <<<>>> CAN-FD报文转换**

I/O	I2C和SPI	I2C、SPI、CAN 2.0和CAN-FD

MICROCHIP

信任锚灵活存储器

安全密钥存储 > 64个密钥

Target Qty	Unit Size	Total Size	Name	Description
32	16	512	Symmetric Key	Symmetric keys used for AES-128 message authentication/encryption.
4	256	1024	Private Key	RSA-2048 Private keys
4	32	128	Private Key	ECC P256 Private keys
5	256	1024	Public Keys	RSA-2048 Public keys
5	64	256	Public Keys	ECC P256 Public keys
1	296	296	Root	RSA-2048 Root public key
1	104	104	Root	ECC Root public key
4	272	2176	Extracted Certs	Extracted RSA-2048 certs – Public Keys and identity digest for extracted certificates that have been validated. Full certificates stored in host memory
8	80	640	Extracted Certs	Extracted ECC certs – Public Keys and identity digest for extracted certificates that have been validated. Full certificates stored in host memory
32	24	768	Revocation List	Revocation list, each 24 bytes long
1	512	512	Key Group	Thirty-two AES keys each 16 bytes long that can be used by the Fast Crypto engine. All keys have the same attributes and share a single handle.
32	40	1280	Partial Digests	List of partial code digests to be used for partial secure boot

MICROCHIP

信任锚灵活存储器

完整的证书存储

Target Qty	Unit Size	Total Size	Name	Description
16	16	256	Symmetric Key	Symmetric keys used for AES-128 MAC/ encryption.
3	256	768	Root	RSA-2048 public keys + 1 root
3	64	192	Root	ECC P256 public keys + 1 root
3	1000	3000	Full Certs	Full RSA-2048X.509 certificates
3	616	1848	Full Certs	Full ECC X.509 certificates
3	272	2176	Extracted Certs	Parsed RSA certificate elements to be used for validation
3	80	320	Extracted Certs	Parsed ECC certificate elements to be used for validation
2	256	512	Private Key	RSA-2048 Private key
2	32	64	Private Key	ECC P256 Private key
24	40	960	Partial Digests	List of partial code digests to be used for partial secure boot
1	320	320	Key Group	20 AES-128 keys to be used by Fast Crypto engine

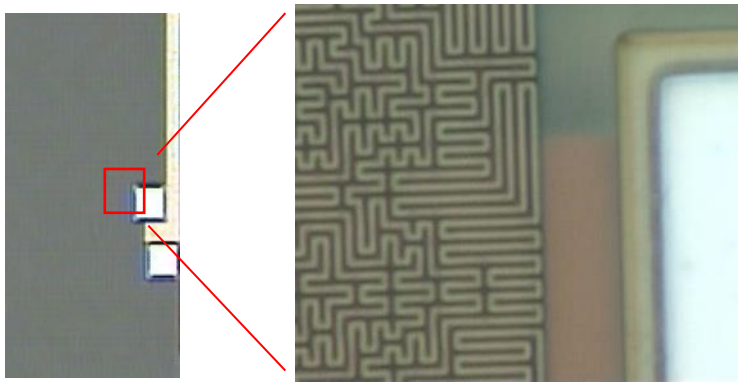
MICROCHIP

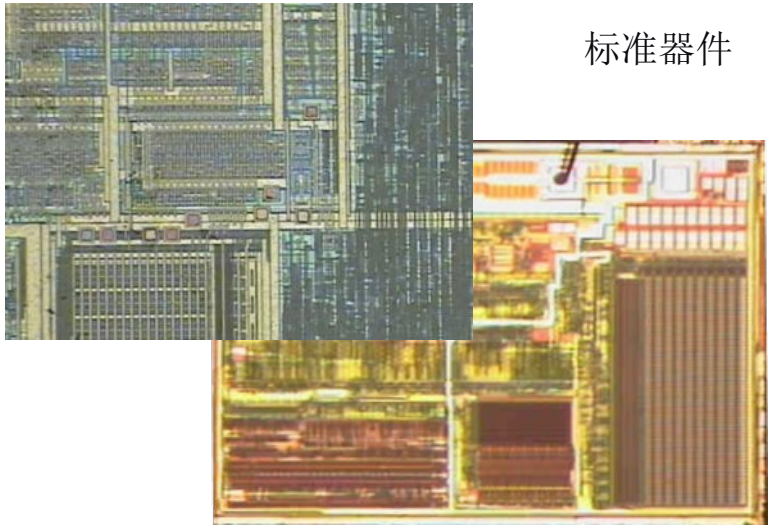
密钥的保护方式至关重要！

- **强大的多级硬件安全**
  - 在整个芯片内进行主动屏蔽
  - 所有存储器均内部加密
  - 加密执行与数据无关
  - 随机数学运算
  - 内部状态一致性检查
  - 电压和温度篡改
  - 内部时钟生成
  - 安全测试方法，无需JTAG
  - 无调试探测点，无测试焊盘

- **经设计可抵御**
  - 微探针攻击
  - 时序攻击
  - 辐射分析攻击
  - 故障和无效命令攻击
  - 掉电再上电和时钟差错

硬件加密器件





标准器件

MICROCHIP

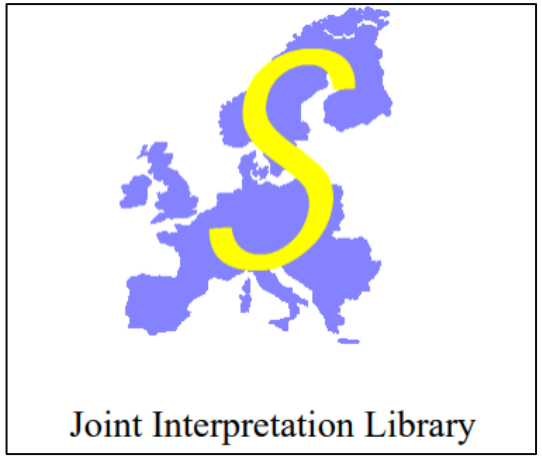
联合解释库（JIL）

- **JIL是全球认可的安全评估评分系统**
- **根据攻击难度获得分值**
  - 实验室可以自由使用任何攻击方法，具体取决于他们认为对器件最有效的攻击方式
  - 在法国，我们使用**Serma Safety and Security**。效果非常不错。
  - 综合各种标准得出分值，请参见下一页

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

TA100高级加密引擎算法的JIL评分为高

Algorithm
ECDSA P256
ECDH
RSA 2048
AES 128 GCM (ACE module)
HMAC SHA 256
ECDB P224



MICROCHIP

漏洞测试

- 破解算法需要多长时间？
- 攻击者必须具备何种水平的技能？
- 要成功进行攻击，需要掌握TOE的哪些知识？
- 获得TOE样片有多困难，需要多少片？
- 要成功进行攻击，需要什么类型的设备？
- 实验室是否需要使用开放的工程样片来加快攻击成功？

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

MICROCHIP

FIPS 140

- 美国和加拿大政府对加密模块的标准
- 版本2是最新版本（FIPS 140-2）

- 加密模块验证程序

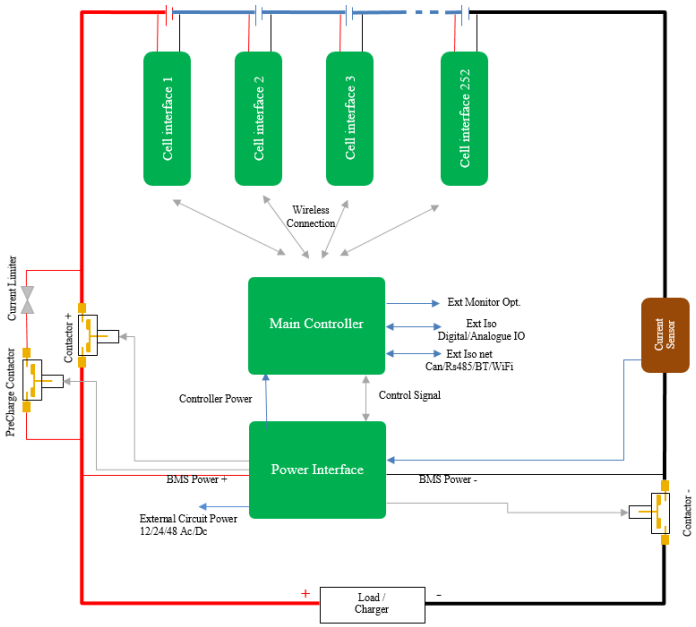
- 验证加密模块是否符合联邦信息处理标准（FIPS）140-2
  - 完整的FIPS认证包括许多不同方面，而不仅仅是算法
  - 与通用标准一样，该工作由独立实验室完成，然后由政府机构批准

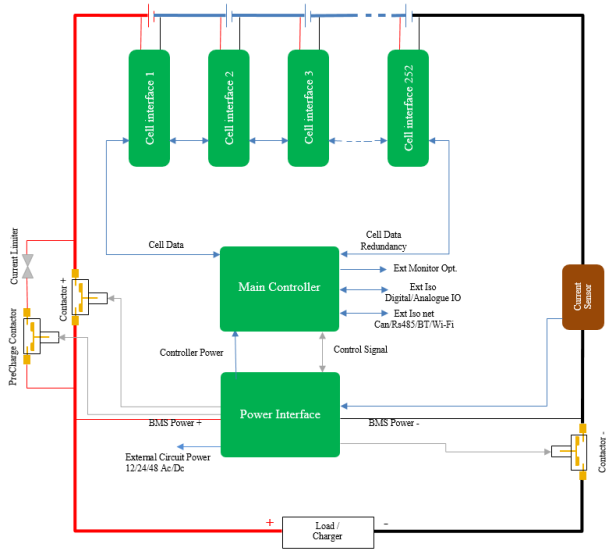
TA100将达到FIPS 140-2模块级别2和硬件保护级别3

电动汽车电池管理

安全电池/模块验证

- **单个电池将状态传输到BMS网关**
  - 通过X.509证书对每个模块进行验证
  - 验证模块的制造来源
  - 可选报文验证
    - 有线或无线



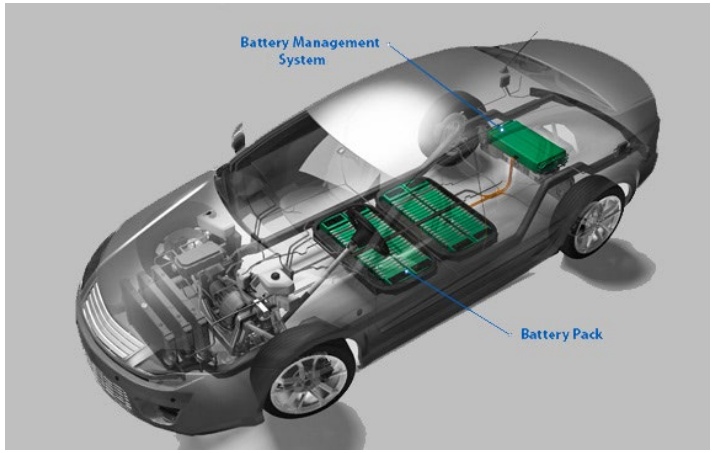


MICROCHIP

电动汽车电池管理系统

网关安全

- **BMS >> 网关 >> 云**
  - 安全引导
  - 安全固件更新
  - TLS云会话建立
  - 提供的已签名健康状态
  - X.509证书
    - 验证模块的制造来源



MICROCHIP

WPC安全状态

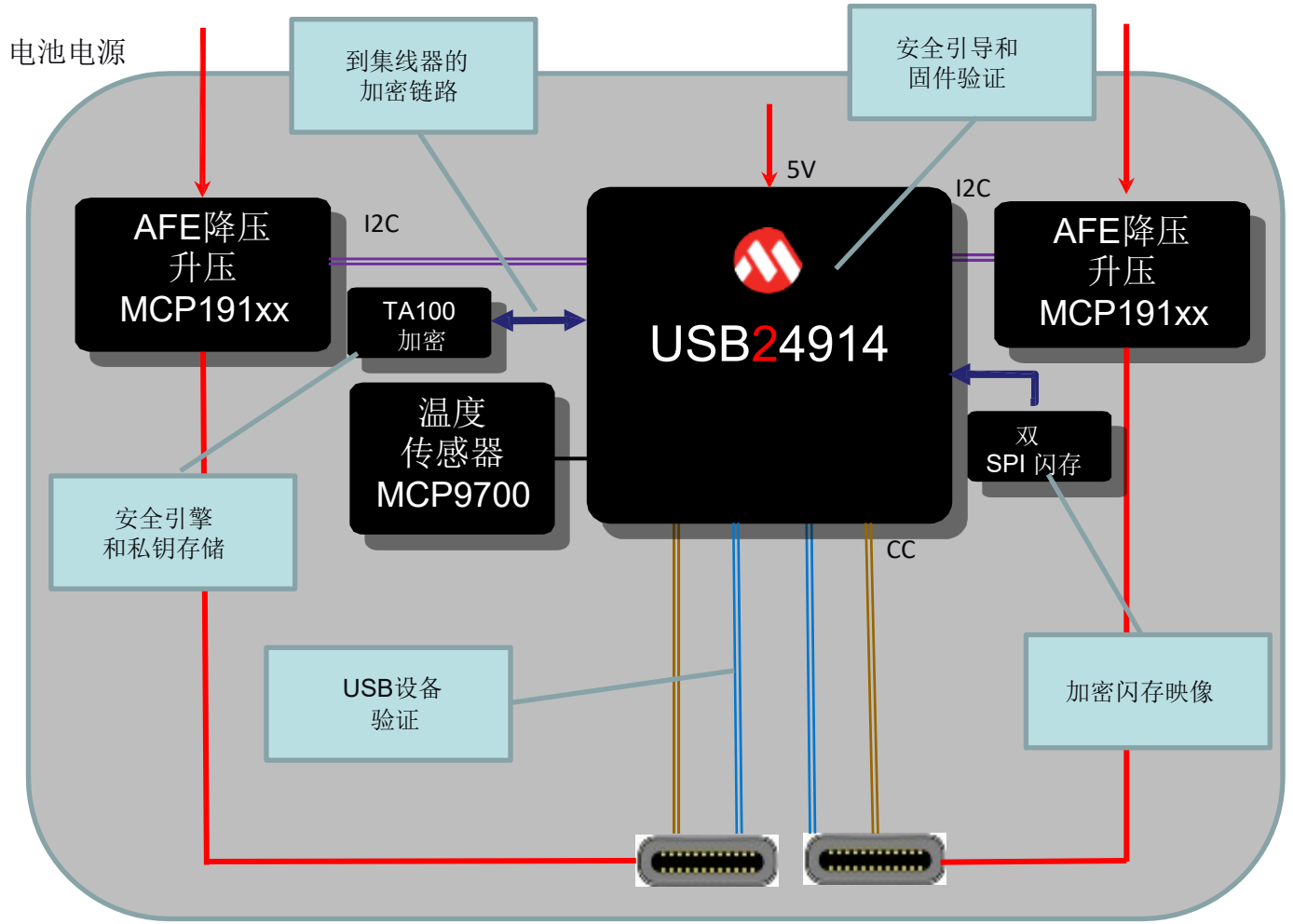
- **TA100轻松支持充电器WPC加密功能**
- **WPC委员会在双向验证问题上来回摇摆**
  - 目前他们正处于需要单向验证的“回退”阶段
- **TA100已添加用于扩展压缩公钥的特殊功能，以便能够支持充电器对电话进行验证**
  - 不仅仅是电话对充电器进行验证
- **WPC预计将使用标准格式的x.509证书**
  - Microchip支持完整x.509证书格式

WIRELESS POWER CONSORTIUM

MICROCHIP

新一代集线器（带模拟前端AFE）

完全“安全”USB PD系统拓扑



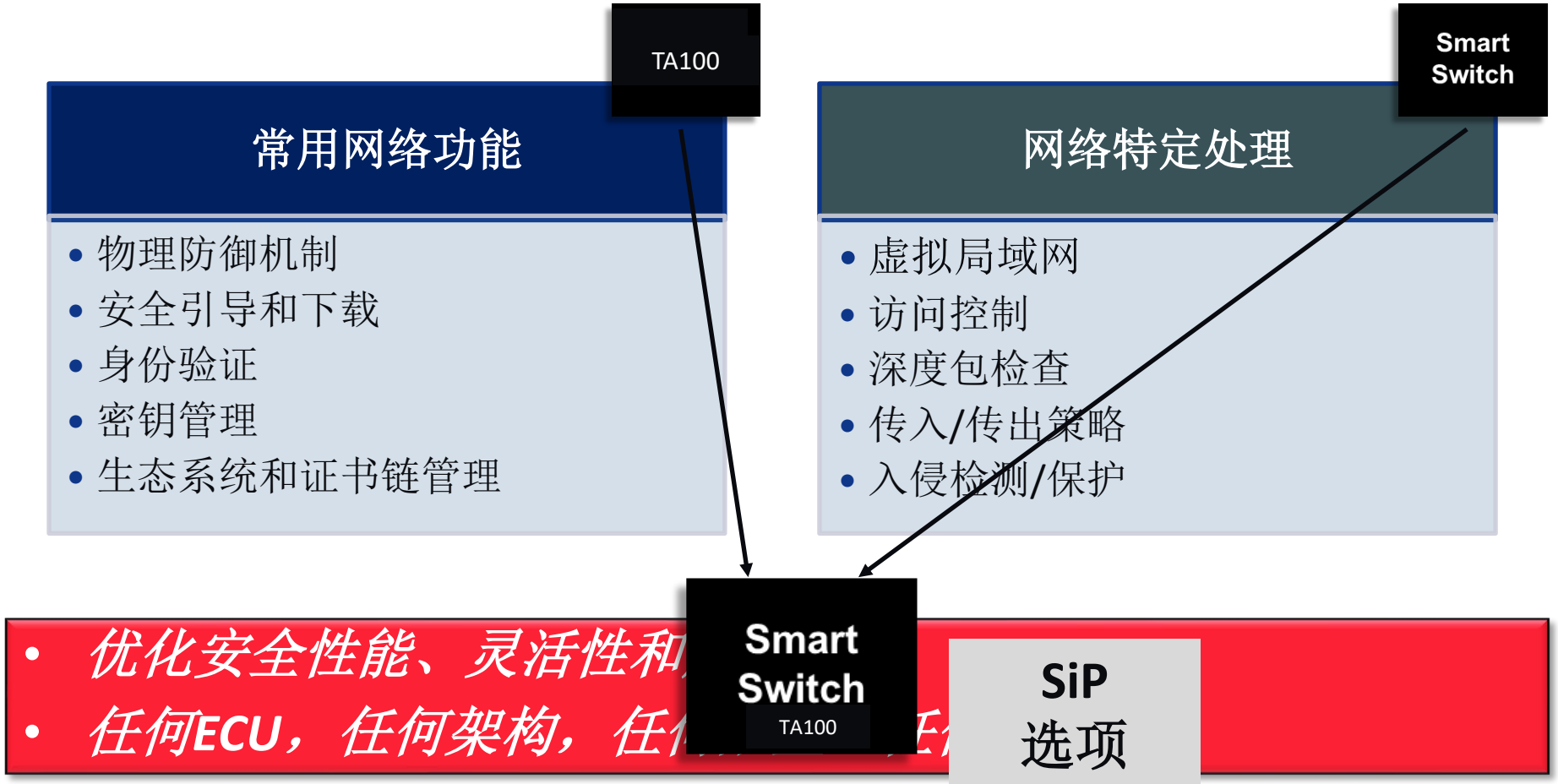
安全供电

- **TA100加密密钥存储**
  - Microchip加密预配置服务
  - 非对称公钥/私钥加密和验证
- **硬件控制的电源协商**
  - 软件改写需要“密钥”
  - 提供100W
- **固件通过DFP自主更新**
  - 需要“密钥”
- **支持SPI闪存映像加密**
- **支持UFP上的媒体集线器到HEU的验证**
- **支持DFP上的USB-C验证**

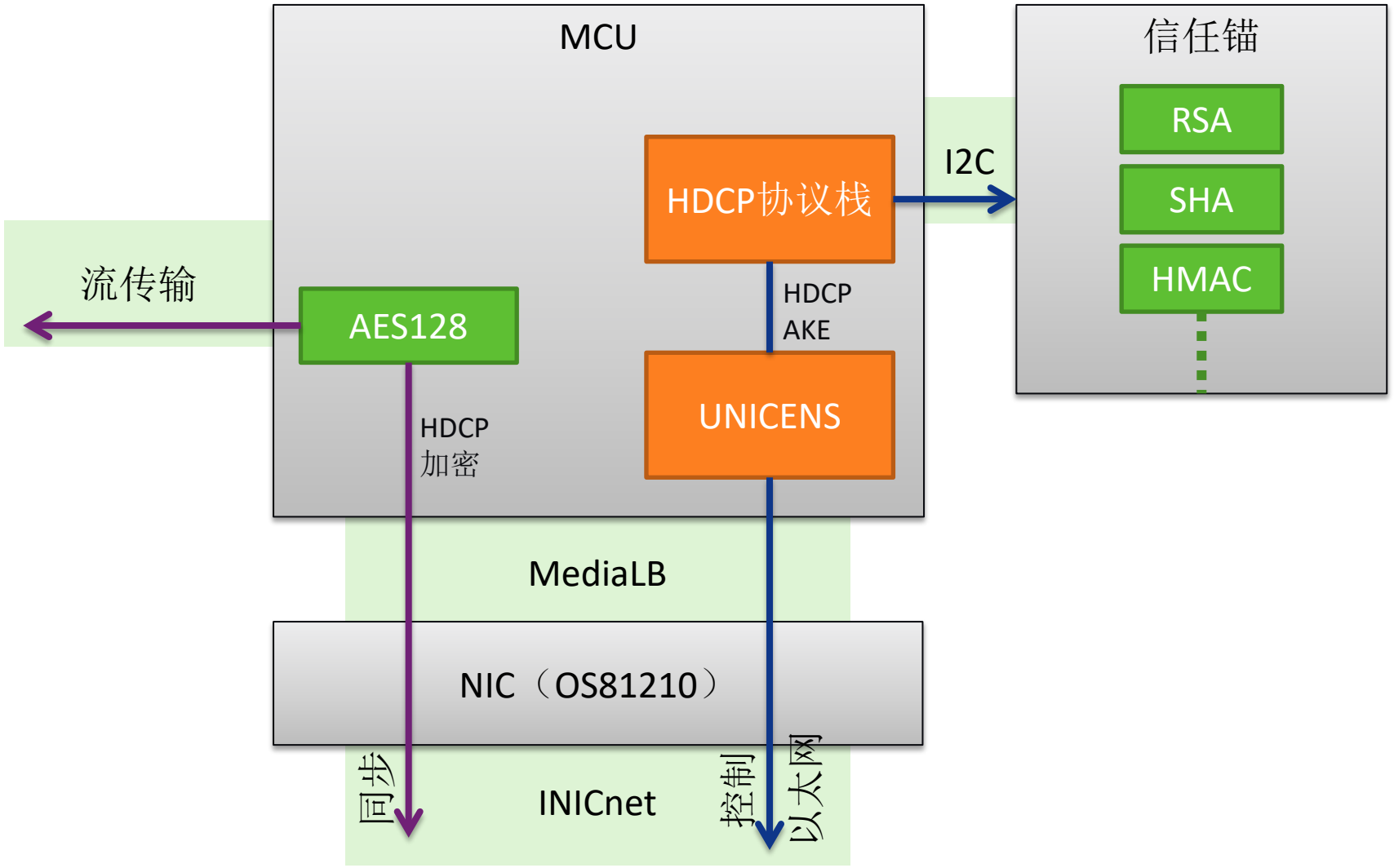
MICROCHIP

采用TA100的UNG以太网开关

- 将常用网络安全与数据通信处理分开

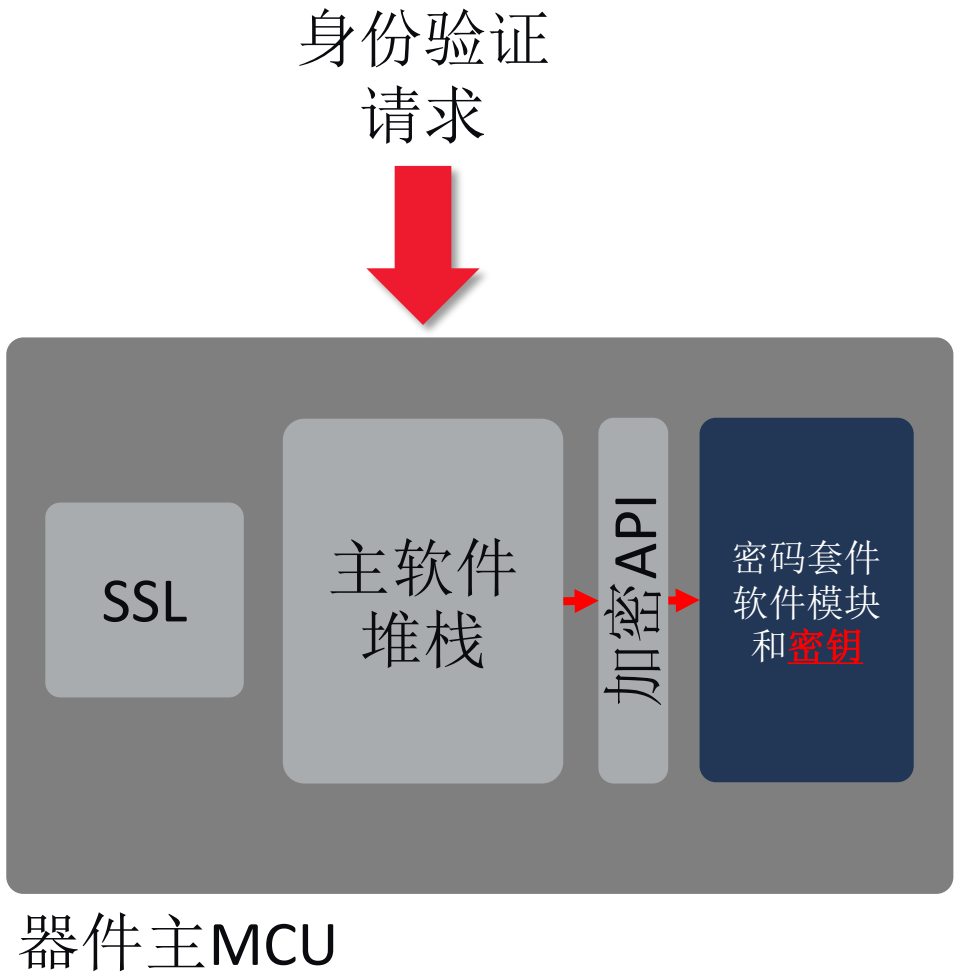


HDCP解决方案



MICROCHIP

纯软件TLS
身份验证



- 在器件MCU中的软件中执行加密功能
  - 需要更多代码空间
  - 需要更多处理负载
  - *将密钥存放在软件和未加密的存储器中*
- 采用低端处理器的小型节点速度太慢

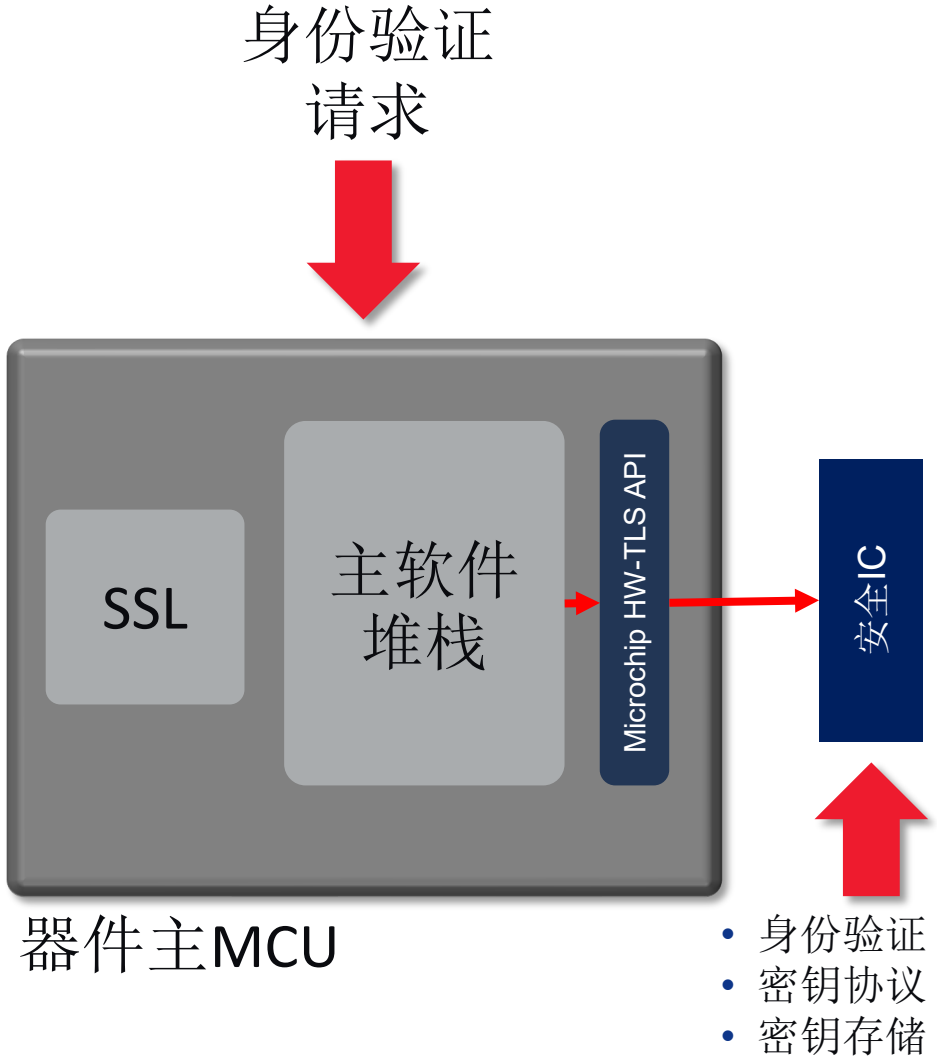
纯软件TLS容易受到攻击！

TLS = 传输层安全

MICROCHIP

硬件安全TLS

身份验证



- **硬件TLS将加密功能从器件MCU卸载**
  - 通过HW-TLS API访问
  - 安全IC处理所有计算
  - 最小的代码空间和计算负载
  - *在安全的硬件中生成和保护密钥*

密钥是安全的！

MICROCHIP

安全引导概念

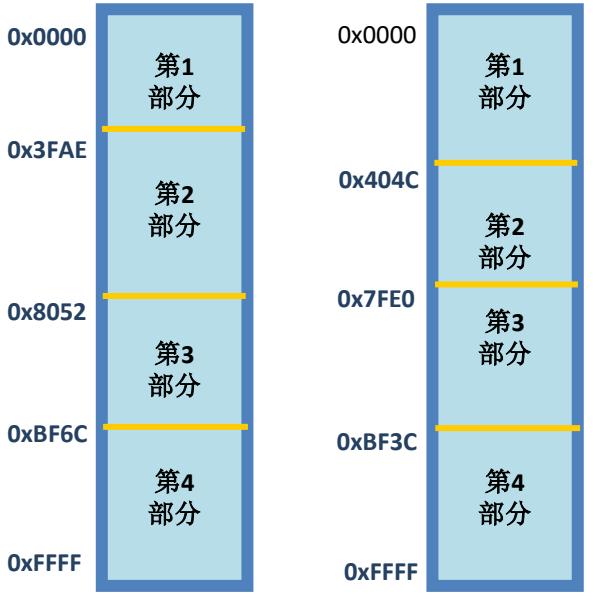
- **仅允许ECU安装（工厂端）或更新（应用端）“正版”软件**
  - 基于非对称签名验证确保真实性
- **识别/仅执行未经篡改的ECU软件**
  - 通过程序/恒定数据的Hash验证软件完整性
  - ECU上电时
  - 可选择在其他时间——例如定期
- **需要安全存储密钥、Hash值……**
- **对ECU启动时间的影响**
  - 权衡安全要求与启动时间
  - 取决于主机MCU性能

MICROCHIP

身份验证模式配置

- **验证模式选项：**
  1. 全部
     - 在主机MCU执行之前验证整个程序
     - 延迟启动以验证整个程序
  2. 部分
     - 验证程序的一部分后，主机MCU开始执行这一部分，同时验证程序的其余部分
     - 启动延时缩短
     - 可配置部分数量（最多50个）
     - 在程序安装/更新（下载）时，部分边界地址被随机化≈ ± 10%
       - 反重放：并非所有器件实例都具有相同的部分地址
       - 在一个ECU上捕捉主机MCU响应的做法可能不适用于另一个ECU
     - 部分验证顺序随机化

图示
64 KB程序存储器
4部分



安全启动N顺序：
2, 1, 3, 4

安全启动N+1顺序
4, 2, 3, 1

MICROCHIP

频率和响应配置

- **验证频率选项**
  - 上电/复位
  - 通过主机MCU请求
  - 定时——从上次安全引导操作开始

- **对非可信程序的响应选项**
  - 让主机MCU复位
  - 禁止在TA中使用（指定的）密钥
  - 重试（包括重试计数器）

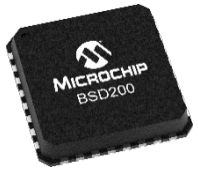
MICROCHIP

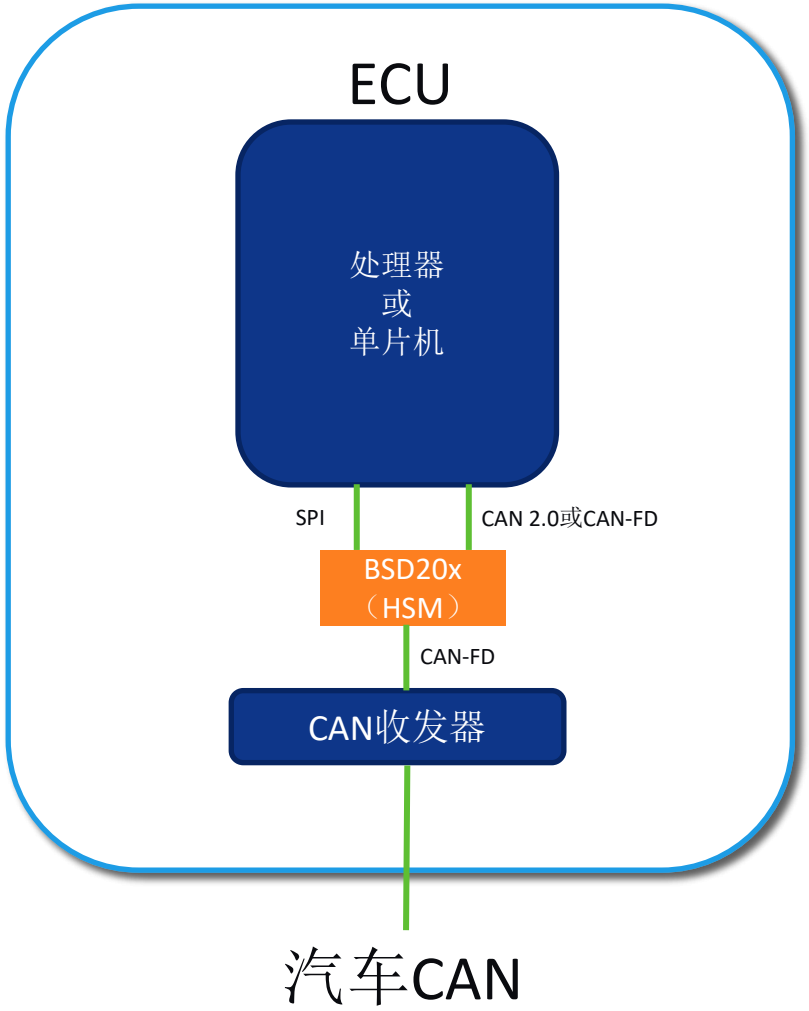
ECU框图

BSD20x伙伴HSM

信任锚功能超集

- **安全密钥存储**
  - CAN通信密钥和证书存储
  - CAN通信会话密钥存储
- **ECU验证和密钥协议**
  - 内置自定义ECU验证和密钥协议方案
  - 加密和认证的命令会话
- **硬件加密加速器**
  - RSA2048和ECC P256
    - 有HDCP选项的3k RSA验证
  - DH和ECDH密钥协议
  - 串行接口中的硬件SHA256加速器
  - 符合NIST的RNG
  - 用于串行通信保护的HMAC和CMAC
- **用例：**
  - 安全引导
  - 增强型TLS和内容保护方案
  - 对具有CAN2.0功能的MCU的MAC支持
    - CAN2.0到CAN-FD报文转换
- **接口：**
  - 串行接口：16 MHz SPI、1 MHz I2C和CAN 2.0
  - 能够通过CAN 2.0运行所有MCU通信
  - 1条中断线
  - CAN-FD总线接口
- **汽车1级**
- **封装：QFN 5x5**





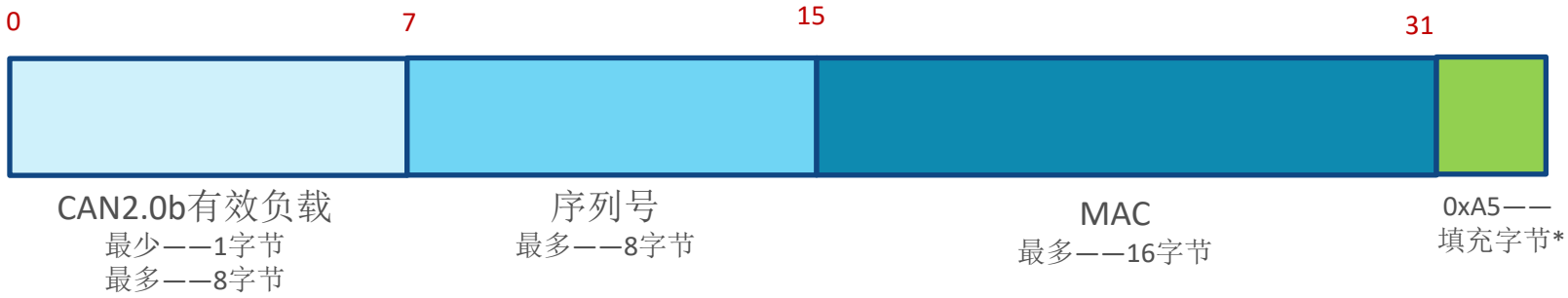
MICROCHIP

CAN报文验证

- 将MAC附加到CAN报文 -> CAN-FD帧
- 通过CAN 2.0连接到主机MCU（无收发器）
- 查找表以确定需要在没有干预的情况下传送的报文
  - 只要支持CAN-FD，便允许混合使用多种ECU

MICROCHIP

示例CAN-FD帧详细信息



AUTOSAR帧格式

CAN-FD报文大小：32字节

随着MAC/序列号减小，可以减小大小

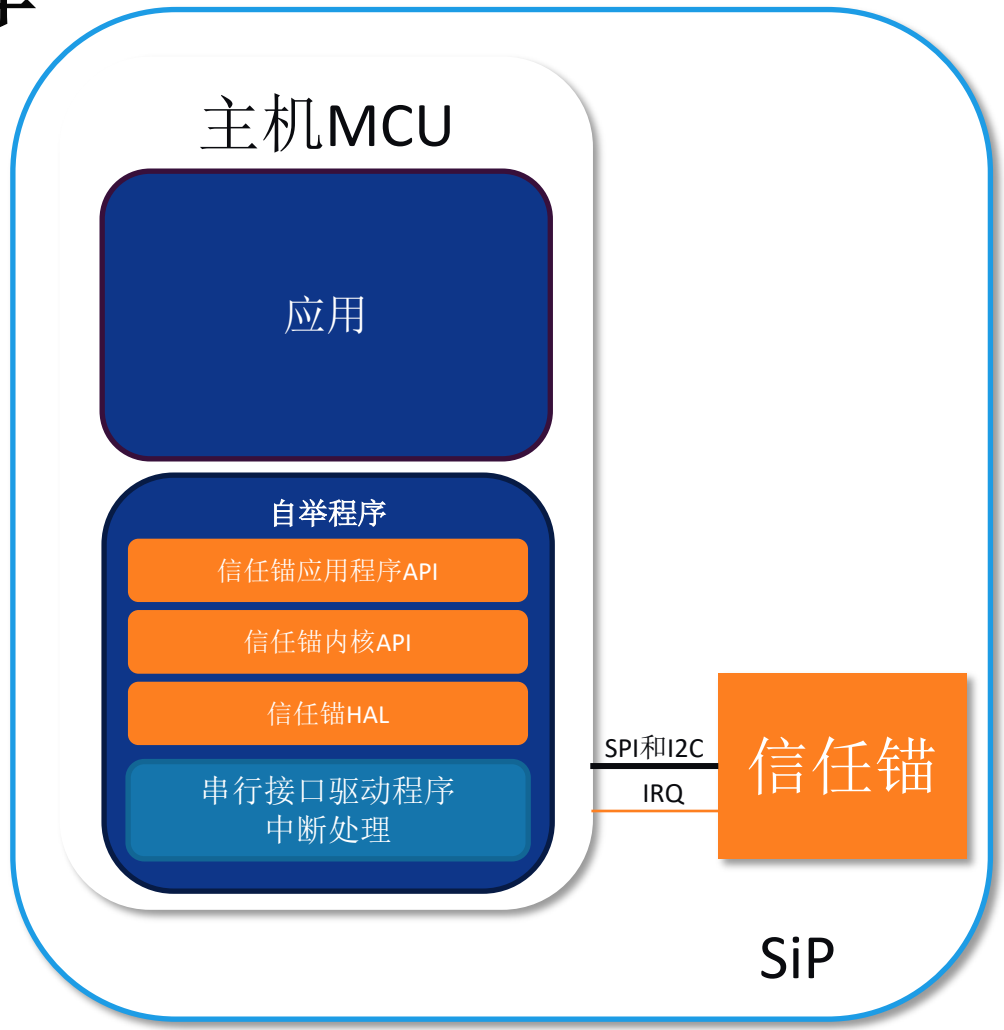
- 24字节
- 20字节

填充字节——添加0xA5以获得有效的CAN-FD帧大小

MICROCHIP

信任锚库

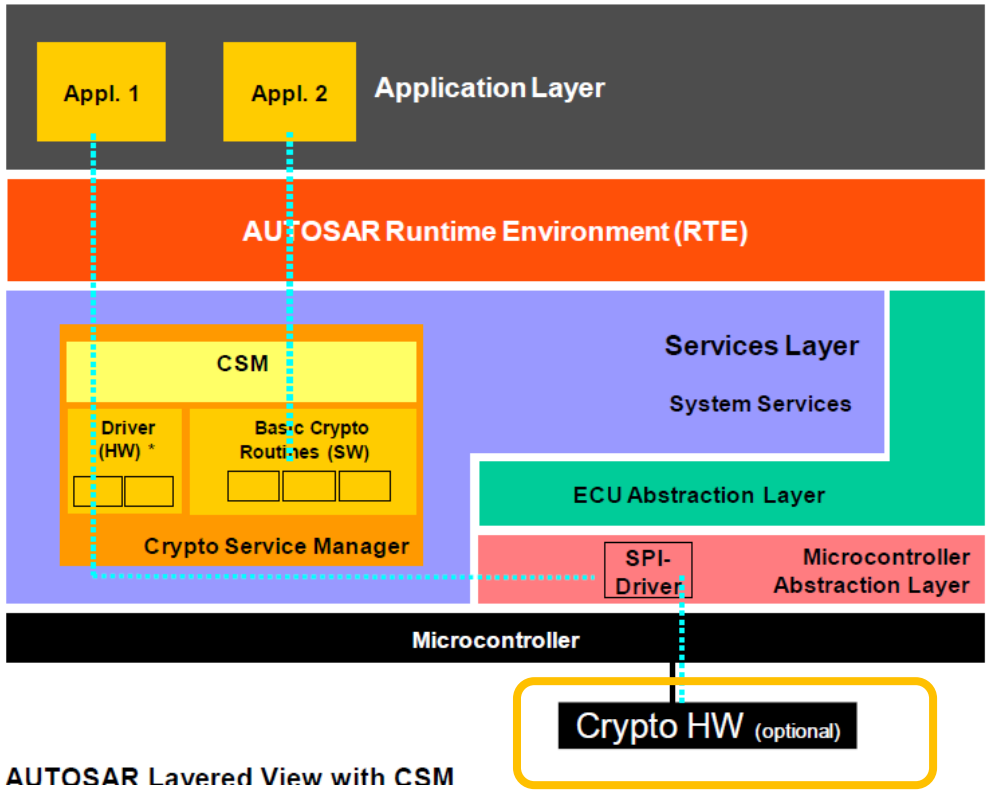
- **模块化、可扩展且可移植的库**
  - 以C源代码形式提供
  - *对HSM集成的AUTOSAR支持*
- **硬件抽象层（HAL）**
  - 串行接口命令抽象
- **内核API**
  - 信任锚命令集
- **应用程序API**
  - 应用程序级安全引导函数



MICROCHIP

Autosar v4.3外部硬件安全模块

- CSM服务通过可在“外部”硬件模块上实现的加密基元（CRY）使用加密算法
- 外部硬件模块的加密基元（CRY）通过硬件驱动程序/库（HW DRV）提供
- TA100等加密硬件模块可放置在通过SPI访问的MCU之外
- TA100可以满足CSM中指定的需求——Hash、MAC、RNG、ECDSA和KDF



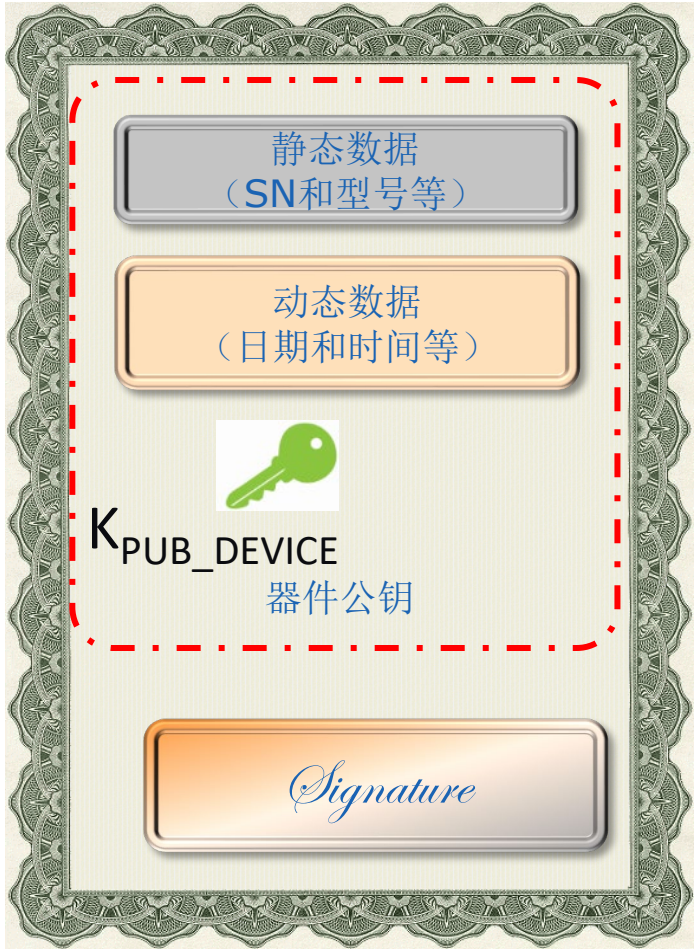
AUTOSAR Layered View with CSM

MICROCHIP

数字证书

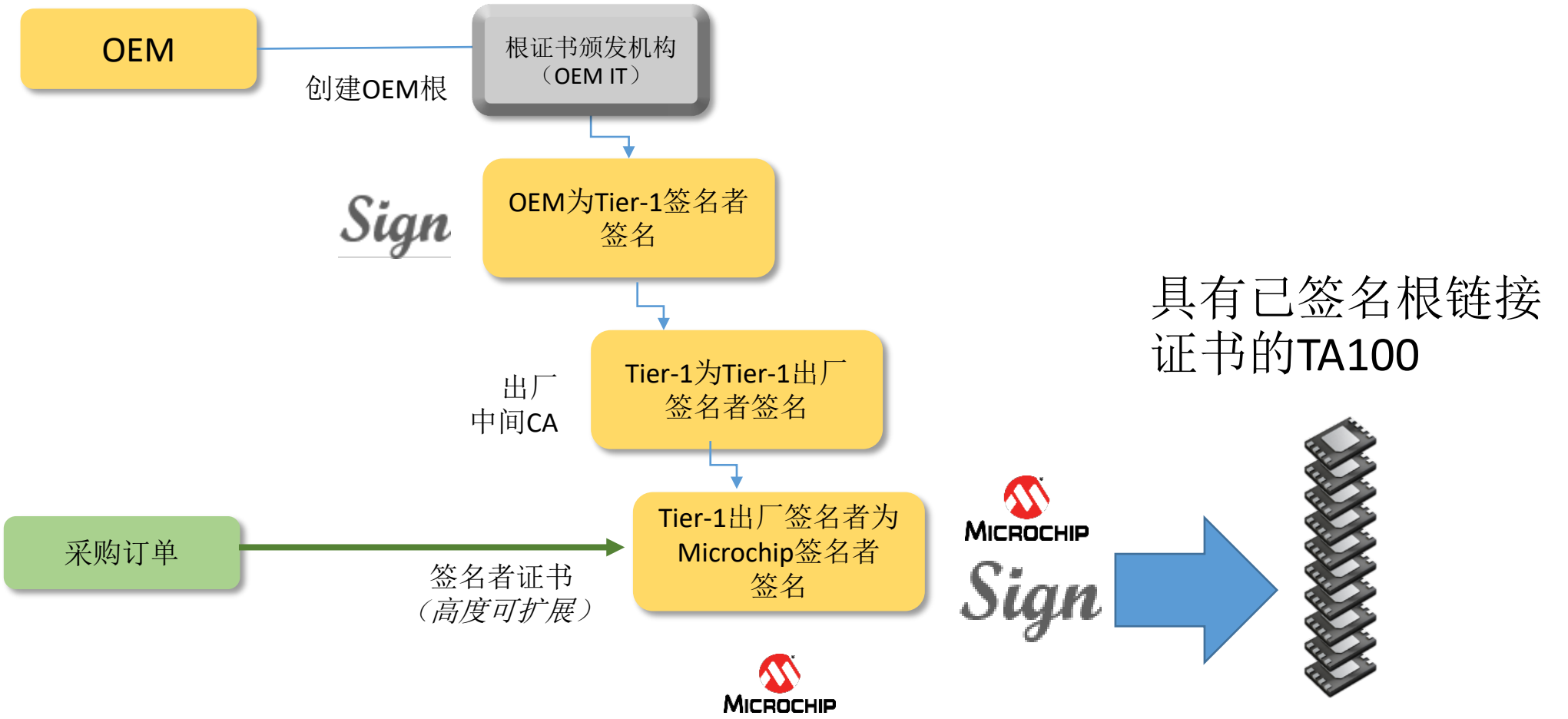
对USB-C支持X.509、WPC和轻量级版本

- 数字证书是节点*唯一可验证*的身份形式
- 它包括三个主要部分：
  - 器件公钥
  - 可验证真实性的签名
  - 捕捉所有者希望作为身份一部分的任何属性的数据
- 证书是互联网的标准驱动身份形式



MICROCHIP

证书链设置

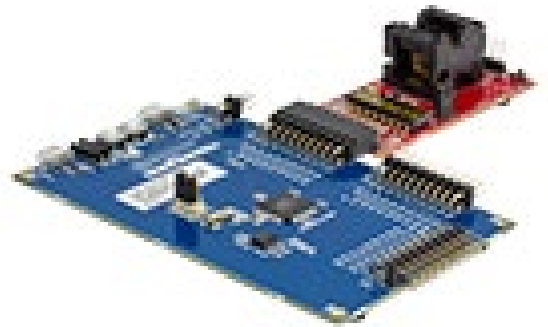


MICROCHIP

TA/BSD开发工具包

- **TA100 MikroBus™兼容插座板现已上市**
  - 8-SOIC和14-SOIC
  - ATMBusAdapter开发板支持XPRO

- **广泛用于客户培训和OEM的PoC**
- **可配置安全引导方案**
- **CAN报文验证**
- **支持任何主机MCU**
- **允许模拟安全引导时间**
- **可用的主机MCU库源代码**
  - 8/16/32位主机MCU的示例项目
- **自学视频培训模块即将推出**



MICROCHIP

TA/BSD培训模块

9:30 am - 11:30 am	**Crypto Primer (Optional Session)** Mark Lowden
11:30 am - 1:00 pm	**Lunch / PC Software Prep**
1:00 pm - 1:30 pm	**Solutions Update** Todd Slack
1:30 pm - 3:30 pm	**Kit Deep Dive: Secure Boot** Sven Semmler
3:30 pm - 3:45 pm	**Break**
3:45 pm - 5:00 pm	**Kit Deep Dive: CAN MAC** Bill Stuart

- 采用模块化结构，可灵活地开展客户培训
  - 可以分成多个主题

MICROCHIP
Technical Training

示例项目启动动手实验TA100培训

- **9:00-9:10 开场**
- **9:10-9:30 培训概述（安全引导和CAN-MAC）**
- **9:30-11:30 安全引导/固件更新**
  - GUI配置（40分钟）
  - 将使用**动态预配置的**TA
  - 自举程序编译/签名/编程/刷写
  - 通过CAN进行应用程序编译/签名/编程/更新
- **午休**
- **13:00-15:00 CAN-MAC**
  - GUI配置（40分钟）
  - 将使用**动态预配置的**TA
- **15:00-15:30 源代码介绍**
- **15:30-16:30 数据手册/功能介绍**

MICROCHIP

问题？

问答环节

MICROCHIP

谢谢！

Microchip汽车创新系列研讨会

2021年02月02日（周二）——触摸式HMI解决方案

MICROCHIP