基于处理器和微控制器的芯片安全技术及在金融支付系统中的应用

恩智浦半导体
张小平

NOV 2016

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

恩智浦：智慧生活 安全连接

节点形成网络，网络传递信息，互联形成智慧

Everything **Connected**

10亿以上的实时在线用户数，
300亿以上的互联设备

连接

Everything **Smart**

2020年，预计有400亿台以上的智能设备或终端接入网络

处理

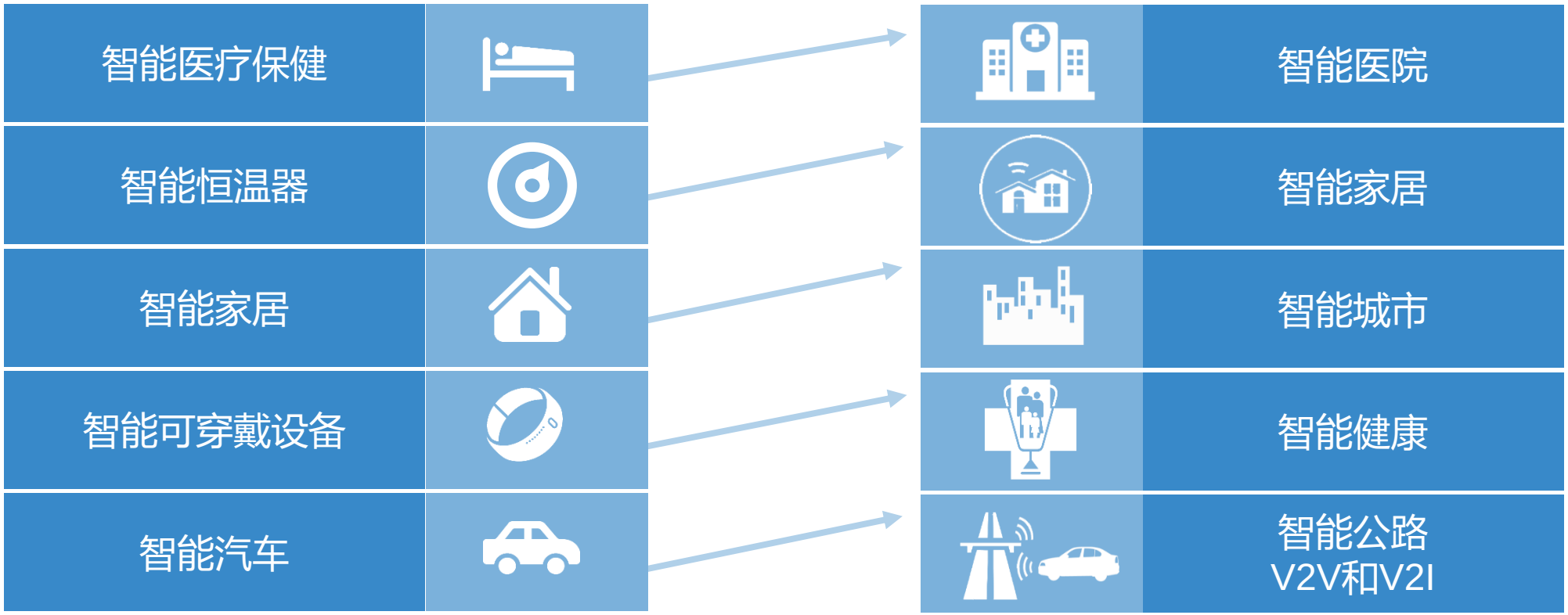
Everything **Secure**

节省上亿美元的成本

安全

Source: Euromonitor; Gartner; ARM Holdings; UBS; Center for Strategic and International Studies; McAfee, NXP analysis, International Telecommunications Union

未来互联网 → 智能、连接和安全



提升数据收集和处理的复杂度以便提供增值的信息。

我们面临的安全风险

接口访问

固件更新

资源限制

增加价值

攻击者
能力提高

风险评估

- 坚不可摧的安全性
  - 有了足够的时间、精力、资源和动力，可以突破安全实现方案
  - 突破安全性所做的努力与可能花费的费用之间的临界点在哪里？

- 安全应以特定的威胁为基础
  - 需要保护什么？
  - 为何加以保护？
  - 保护对象是谁？

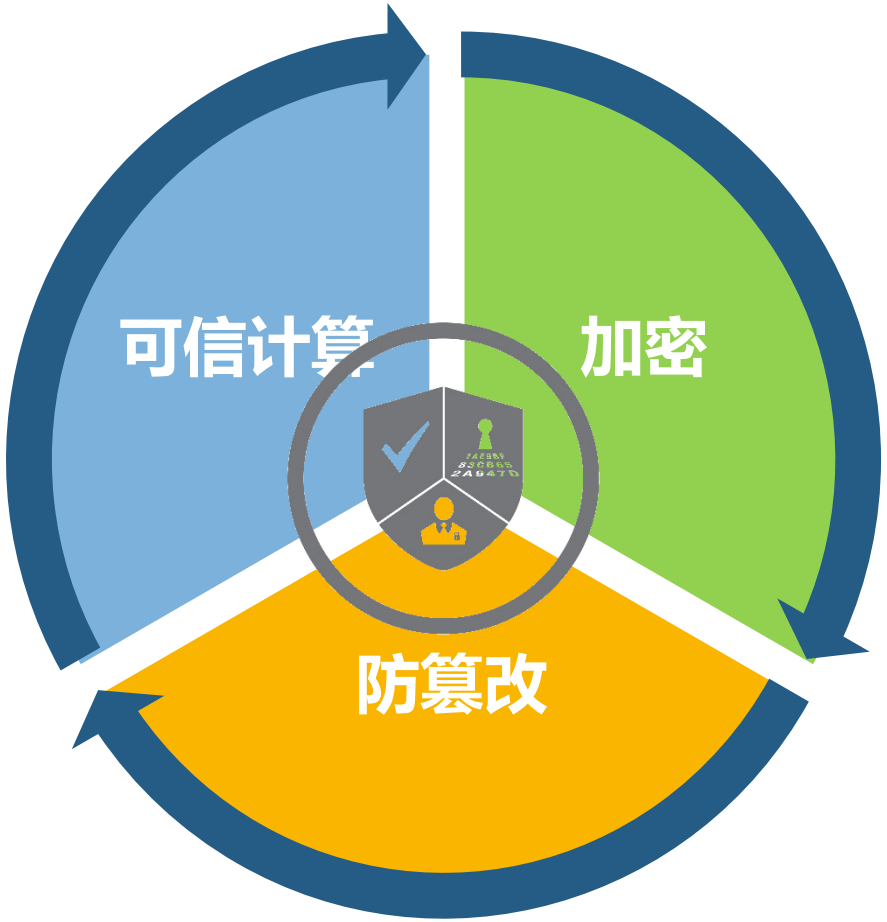
安全规划——攻击

- 内部攻击
  - 财务收益/欺诈
  - 报复/回报
  - 勒索
- 午夜攻击
  - 在短时间内发生
- 集中攻击
  - 时间、金钱和资源并不是构成攻击的因素

安全规划——攻击者

- 局外人（富有好奇心的黑客）
  - 聪明，但具有有限的系统知识
  - 尝试利用现有的安全漏洞
- 业内人士（专业人士/学者）
  - 具有丰富的专业技术经验
  - 能够获得先进的工具和仪表
- 组织机构（犯罪集团/政府）
  - 掌握大量资金资源的专家
  - 具备先进的分析工具，能够进行深入的分析和攻击

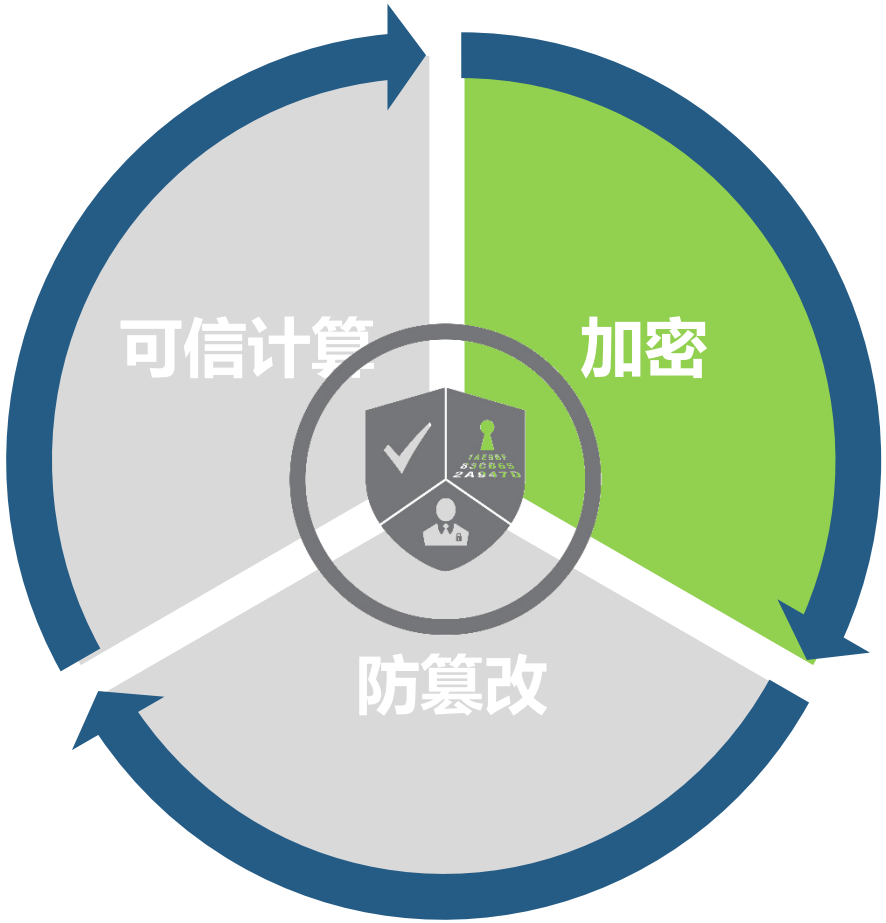
恩智浦芯片级安全技术



加密技术

- 通过编码和解码来保护数据的技术

- 对称加密
  - DES/DES3、AES
- 不对称加密
  - RSA、ECC
- 哈希
  - CRC、MD5、SHA
- 真正的随机数生成
- 安全协议
  - SSL、HomeKit、Thread



防篡改

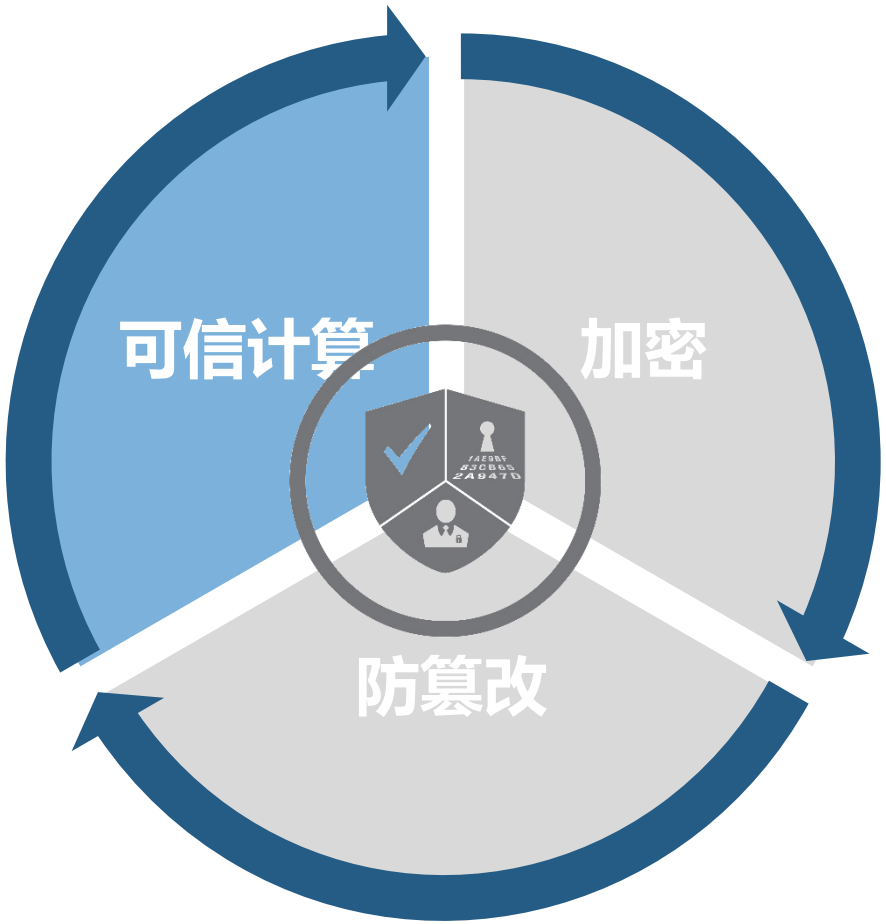
- 主动监控物理和环境系统攻击

- 篡改检测
  - –物理
    - 壳体入侵
    - 钻孔和探测
  - –环境
    - 电压
    - 温度
    - 频率
- 安全存储

可信计算

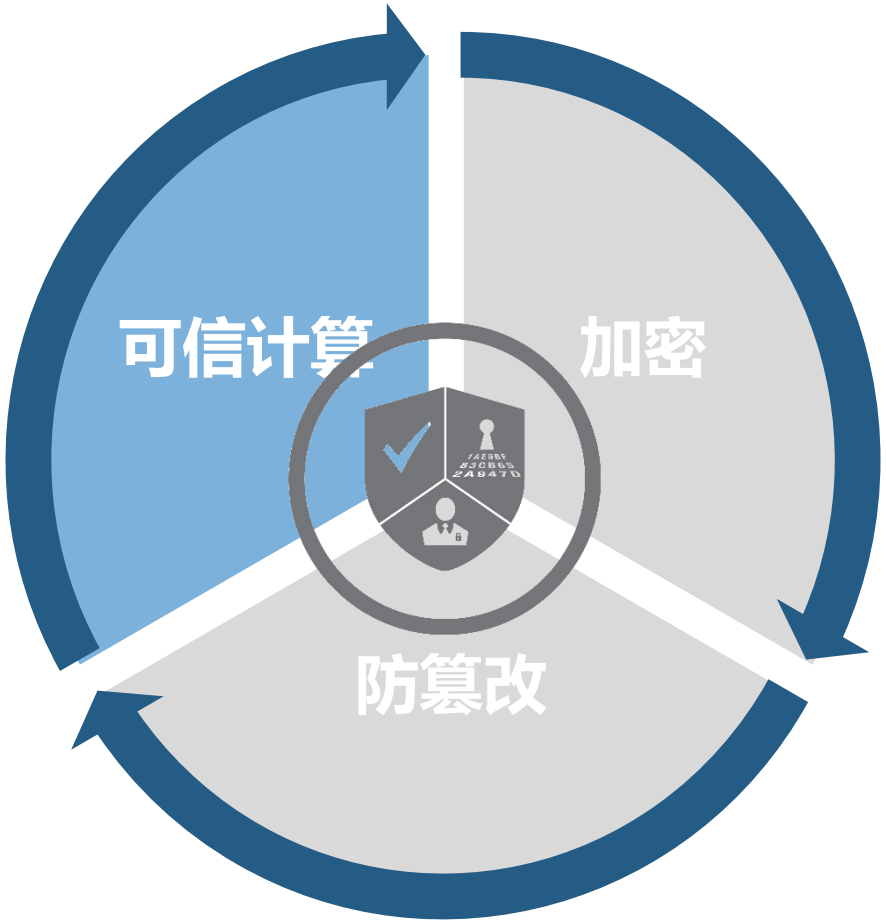
- 确保只从可靠来源进行访问

- 代码I/P保护
  - 内部存储器保护
  - 外部存储器保护
- 调试端口保护
- 身份验证
  - 软件更新
  - 设备验证
- 安全启动



芯片级安全技术的实现

可信计算：确保从可靠来源操作



可信计算：所有Kinetis设备支持

特性	优势	详情	支持
片内Flash安全和保护机制	防止固件盗窃和应用克隆	能够防止对处理器进行调试访问。能够设置64位密钥以便重获调试访问	**AN4507：** *“利用Kinetis安全和Flash保护功能”*
调试端口配置	阻止外部访问到调试或flash重新编程	Flash安全可禁用调试端口。JTAG引脚还可通过软件禁用	**AN4507：** *“利用Kinetis安全和Flash保护功能”*
唯一ID	软件可用于唯一识别MCU作为可信设备	**Kinetis L系列：**80位唯一ID **所有其他：**128位唯一ID	
仅从内部存储器启动	受控启动条件可避免使用外部存储器的攻击	仅从片内闪存或ROM启动	

可信计算：部分Kinetis设备支持

特性	优势	详情	支持
仅执行和超级用户访问	软件IP保护	非易失性控制寄存器，可设置片内闪存资源的访问权限。可为多达64个不同的区段设置仅超级用户或执行访问	**AN5112：** “*使用Kinetis Flash仅执行访问控制功能*”
加密的固件更新	防止固件盗窃和应用克隆	ROM支持对内部flash或外部串行NOR进行加密的图像下载。代码直接存储在设备上	KBOOT
即时AES解密(OTFAD)	防止固件盗窃和应用克隆	外部串行NOR flash中的代码能以加密形式存储在外部存储器中，且仅在处理器读取时解密	KBOOT

Flash安全和保护功能

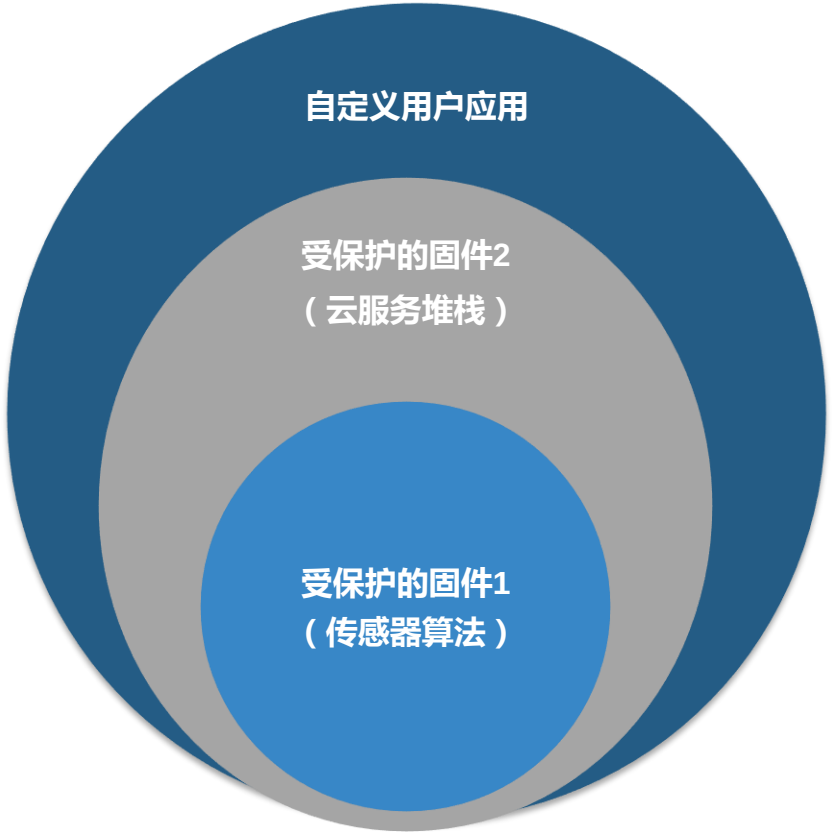
- 所有Kinetis设备均具有flash安全和保护功能

- 安全特性
  - Kinetis MCU提供几个flash安全级别
  - Flash安全是一项系统级特性
    - 当flash处于安全状态时，其功能齐全（如果常驻固件已安装以便对flash进行编程，仍可进行固件更新）
    - 安全效应确实是个系统级问题。安全设置可确定SoC允许的操作
  - 软件IP是一项很大的投资。支持安全功能有助于保护IP投资

- 保护特性
  - Flash保护可用于防止意外删除或编程
  - 初始保护值在重置时从flash配置字段中加载

仅执行应用代码

- 仅执行应用代码的概念是：
- 主要开发人员（例如，恩智浦或第三方软件提供商）为指定的MCU或MPU创建有用的增值应用。提供入口点和使用信息（例如，API详细信息），但未提供源代码。该代码假定为“可信”。
- 通过一种方法将此软件加载到器件中并标记为“仅执行”，而在加载过程中不公开该软件。
- 其他开发人员和/或用户向这些器件中添加更多软件并使用这些应用程序。
- 应用程序用户将无法看到或公开任何受保护的仅执行代码。
- 可能已添加多层“仅执行”应用代码，而之前添加的所有层均受保护。
- 新型Kinetis设备支持该功能，并通过Flash FTF寄存器组进行控制。

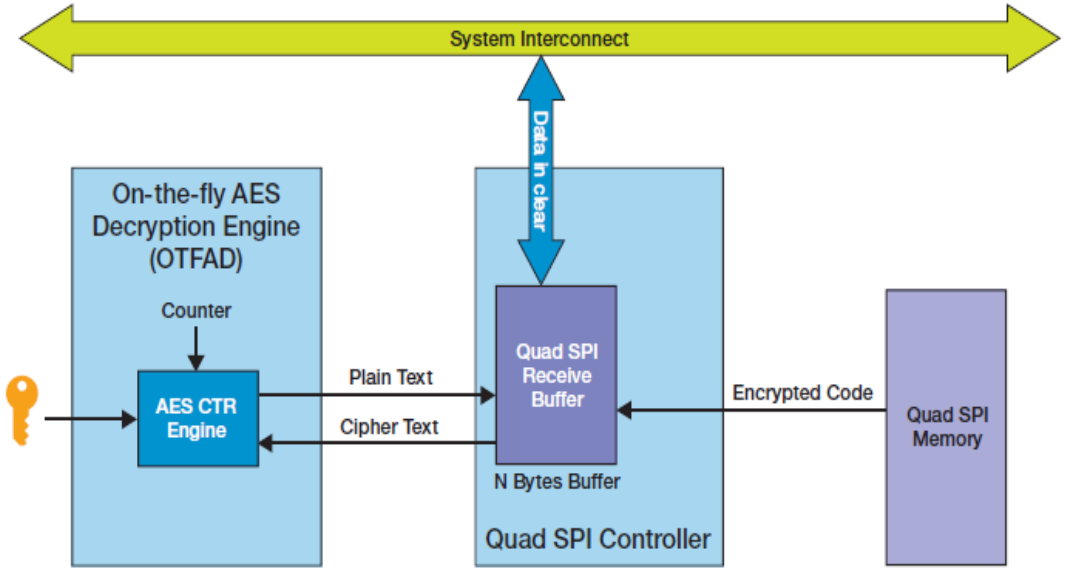


加密的二进制文件下载（Kinetis K8x MCU系列）

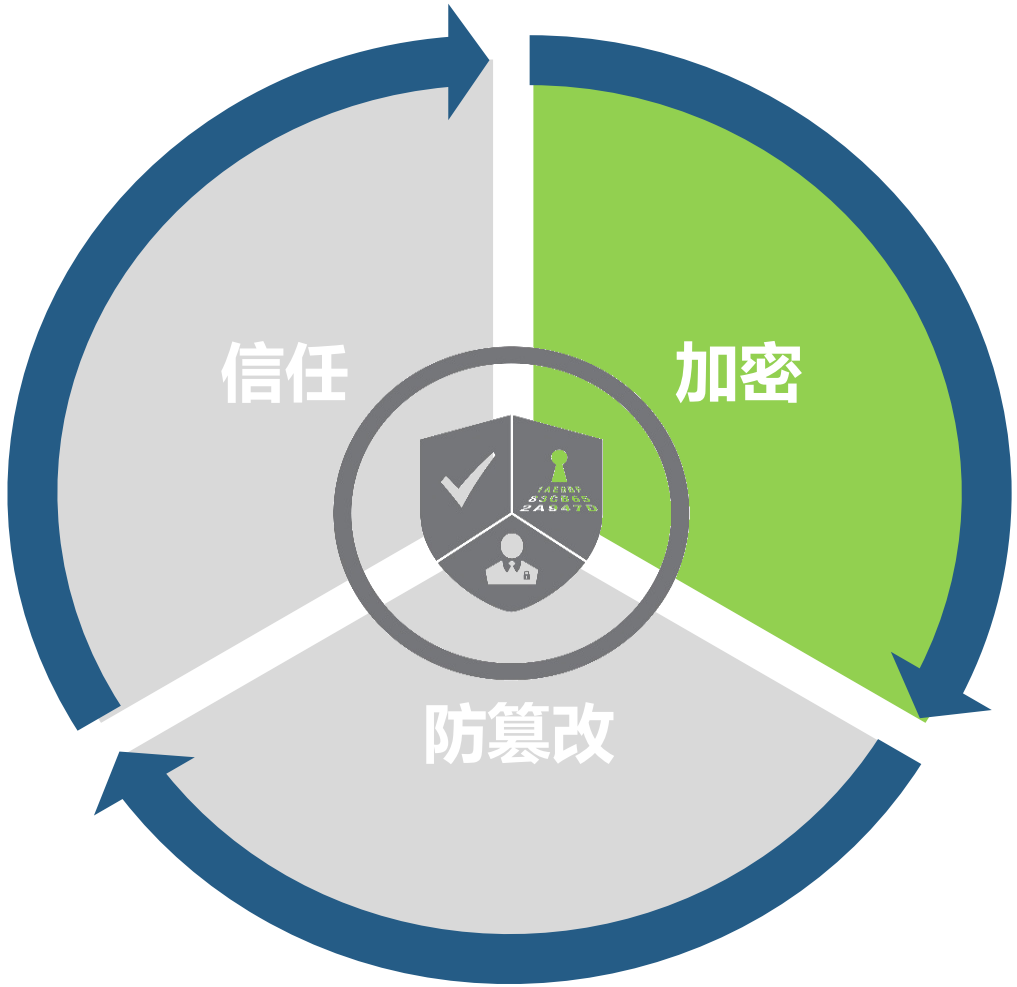
- ROM支持下载安全二进制(SB)文件格式的加密二进制文件（使用AES-128加密）
- 下载加密的应用程序，但以解密的状态存储到内部flash中（也可以选择将加密文件下载到外部串行NOR flash中）
- 预编程到flash“一次可擦程序”空间中的密钥值用于解密
- 当设备处于安全或非安全状态时，可以下载加密的SB文件；但是如果设备是安全的，ROM将禁用所有内存读取和写入，而加密的SB文件除外。
- 因此，如启用安全性，加密的二进制文件是ROM用于更新固件的唯一方式
- KBOOT软件提供用于生成加密二进制文件的工具
- 在Kinetis K81/K82设备上，LP可信密码(LTC)模块用于解密二进制文件
- 在Kinetis K80设备上，存储器映射加密提速单元(mmCAU)用于解密二进制文件

即时AES解密功能（Kinetis K8x MCU系列）

- 允许对四通道SPI中的加密代码进行即时解密
- 允许从四通道SPI就地运行加密代码
- 基于AES128-CTR对称算法
- OTFAD引擎后解密将数据直接传输回到随后可供系统使用的QuadSPI Rx缓冲器中
- 通过确保客户终端产品代码和数据安全来提供*防克隆*和*IP保护*功能
- 硬件支持4个独立的解密段，称为存储器上下文
- 每个上下文具有唯一的128位密钥、64位计数器和64位存储区域描述符



加密：通过编码保护数据



加密：算法/协议

	要求	使用
OTA安全固件更新 安全启动	RSA-2048验证 SHA-256通过固件映像	每次更新时 每次启动时
HomeKit	SRP-3072 Ed22519签名/验证 曲线-25519 基于SHA-512的KDF ChaCha20加密 多1305 MAC SHA-256	首次设备配对时 首次设备配对时 每次与配件连接时 每次与配件连接时
Thread	EC-JPAKE (NIST-P256) AES-128 CCM (TLS) 基于HMAC-SHA256的KGF SHA-256	首次设备配对时
AllJoyn	ECDHE-PSK ECDHE-ECDSA ECDHE-NULL NIST-P256 X509证书 SHA-256	每次连接时

Kinetis MCU硬件

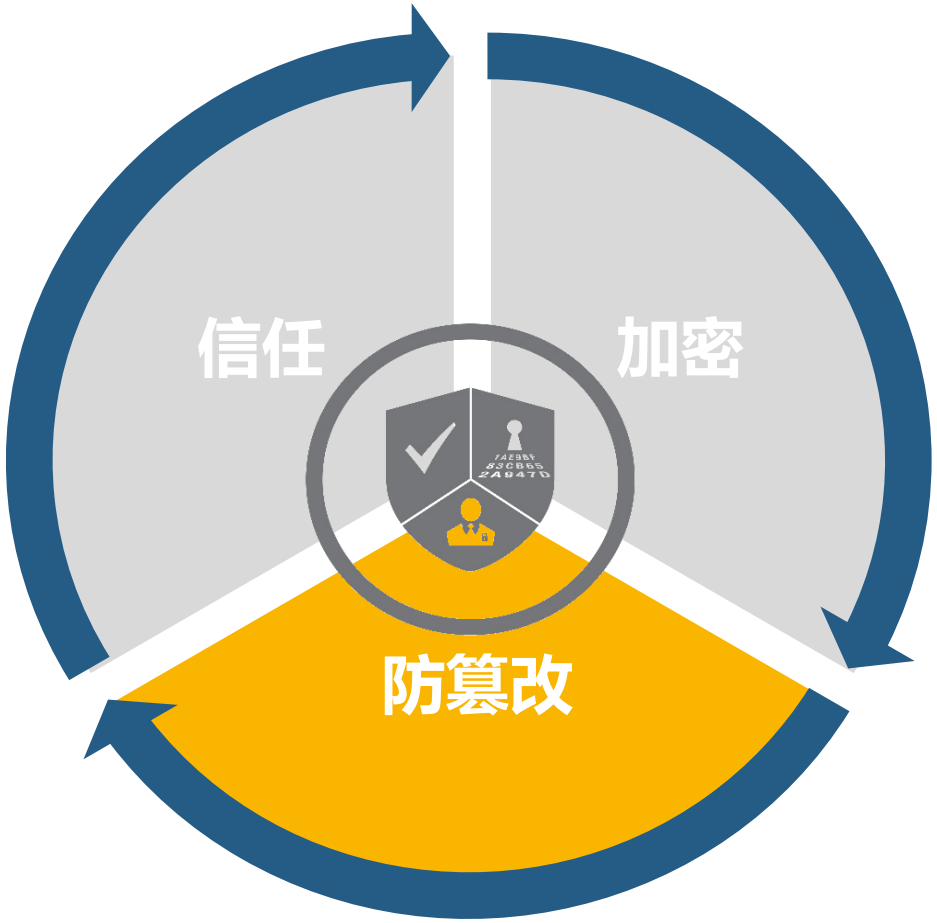
- 软件
  - 任何Kinetis设备可以使用公开可用的加密库用于执行加密、解密和哈希操作
- 存储器映射加密提速单元(mmCAU)
  - 将硬件协处理器连接至专用外设总线(PPB)，用于加速基于软件的加密算法
- LP可信密码(LTC)
  - DMA从机加速引擎为受支持的每个安全算法配有专用硬件

硬件加密与软件优势

	LTC	MMCAU
AES-CBC	15.4x	5.5x
AES-GCM	39.0x	1.5x
AES-CTR	13.4x	N/A
AES-CCM	15.8x	7.0x
Footprint	~10 KB smaller	~10 KB smaller
	LTC	MMCAU
3DES-CBC	81.8x	13.1x
Footprint	~ 2 KB smaller	~ 2.7 KB smaller

	LTC
RSA encryption	6.3x
RSA decryption	4.7x
Footprint	~ 5.5 KB smaller
	LTC
ECC 256 key generation	18.5x
EC-DHE key agreement	19.4x
EC-DSA sign	15.8x
EC-DSA verify	17.1x
Footprint	~ 2 KB smaller

防篡改：检测攻击并作出反应

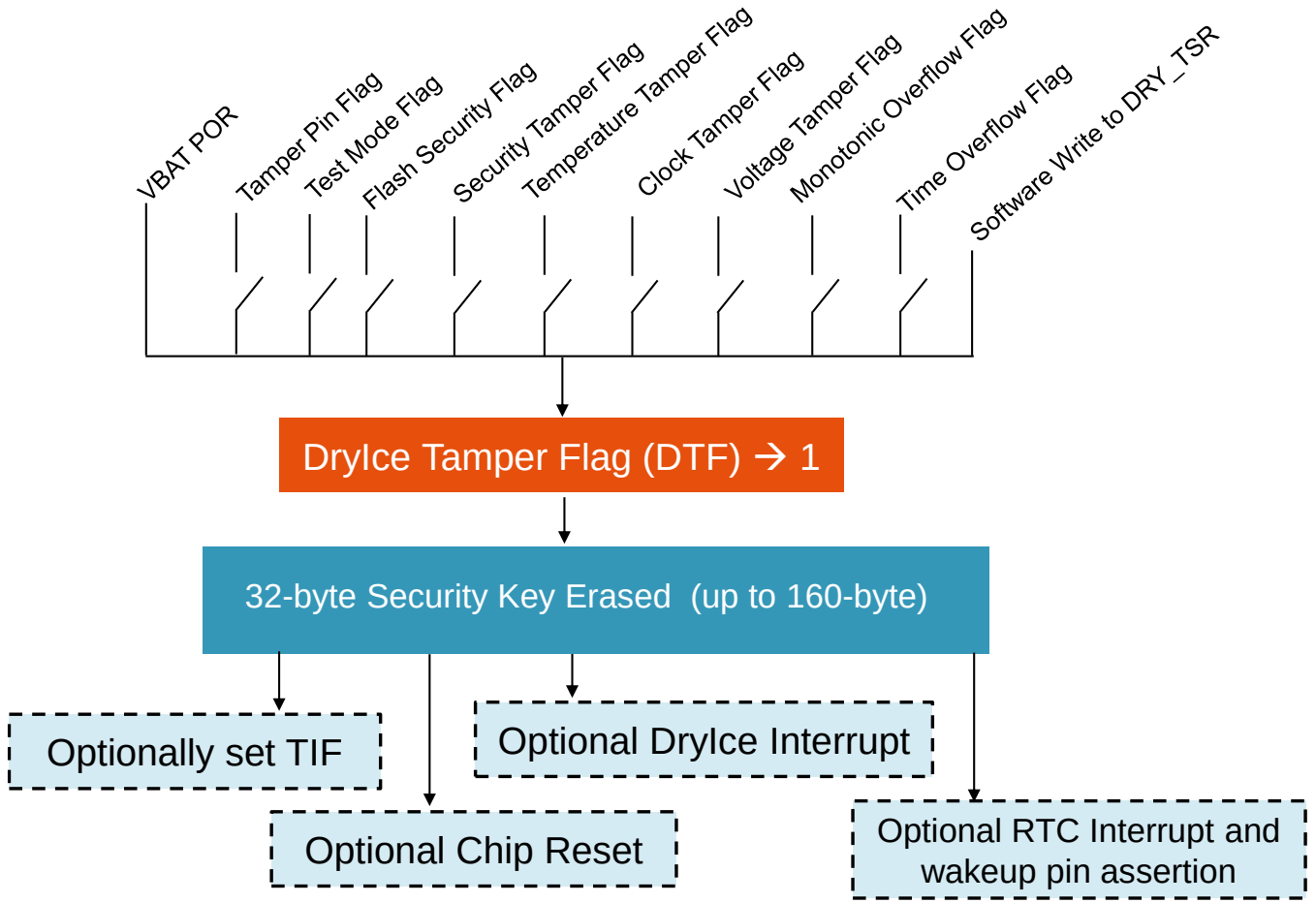


防篡改：一系列Kinetis支持

特性	优势	特性详情	支持
篡改检测模块具有多达8个篡改引脚	减少所需的外部电路以支持防篡改机制	针对引脚、温度、电压和时钟的篡改检测。以及主动篡改	适用于NDA客户的应用笔记
安全存储	篡改时可自动擦除的密钥存储（无需软件干预）	当发生外部篡改事件时支持异步擦除功能的安全密钥存储空间	适用于NDA客户的应用笔记

DryIce篡改事件

可设置DryIce篡改标志的事件 (DRY_SR[DTF])
外部
VBAT上电复位(POR)
DryIce篡改引脚x标志(TPFx)置位[多达8个引脚]
内部
DryIce测试模式标志(TMF)置位
DryIce Flash安全标志(FSF)置位
DryIce安全篡改标志(STF)置位*
DryIce温度篡改标志(TTF)置位
DryIce时钟篡改标志(CTF)置位
DryIce电压篡改标志(VTF)置位
DryIce单调溢出标志(MOF)置位
DryIce时间溢出标志(TOF)置位
软件启动写入DRY_TSR（无标志）

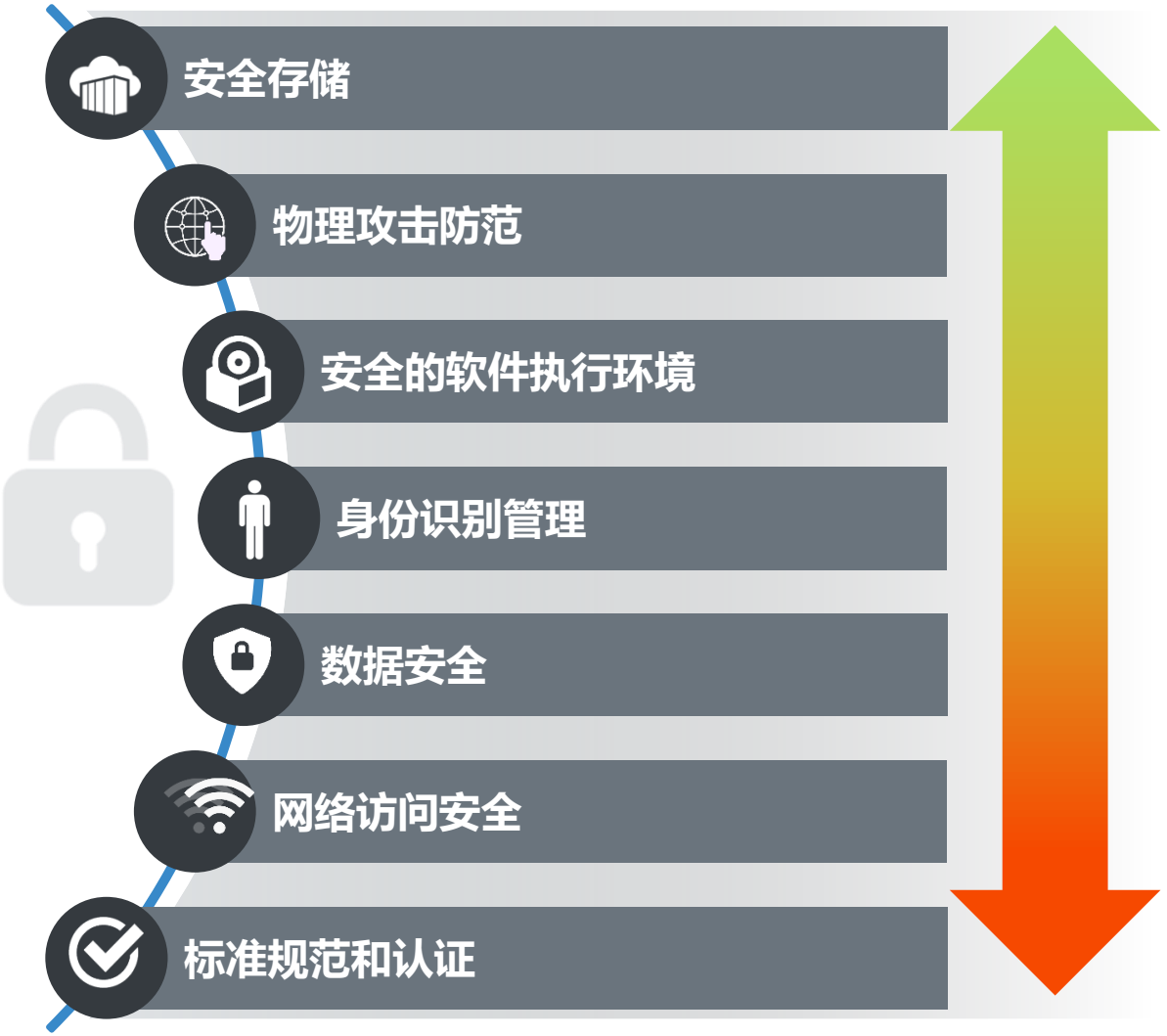


安全存储

- 与DryIce模块有关的安全存储量因设备而异

- 最新Kinetis K8x MCU设备支持：
  - 32字节安全密钥存储在DryIce模块中，在篡改时会擦除（电池支持）
  - 128字节VBAT寄存器文件（电池支持的存储器，在篡改时可选择擦除，这DRY_CR[SRF]设置决定）
  - 2KB安全会话RAM，在篡改和系统复位时会擦除

安全处理器/微控制器的技术发展方向



在线加密 (memory)

生产制造保护

授权调试和加载

实时完整性检测

可信区域设置和读写访问

安全存储

可归零化的RAM

可信重启

加解密加速引擎

对称和非对称算法引擎.

真随机数产生器

攻击保护

主动攻击防护 (物理)

DPA 保护(侧路攻击)

安全的软件执行环境

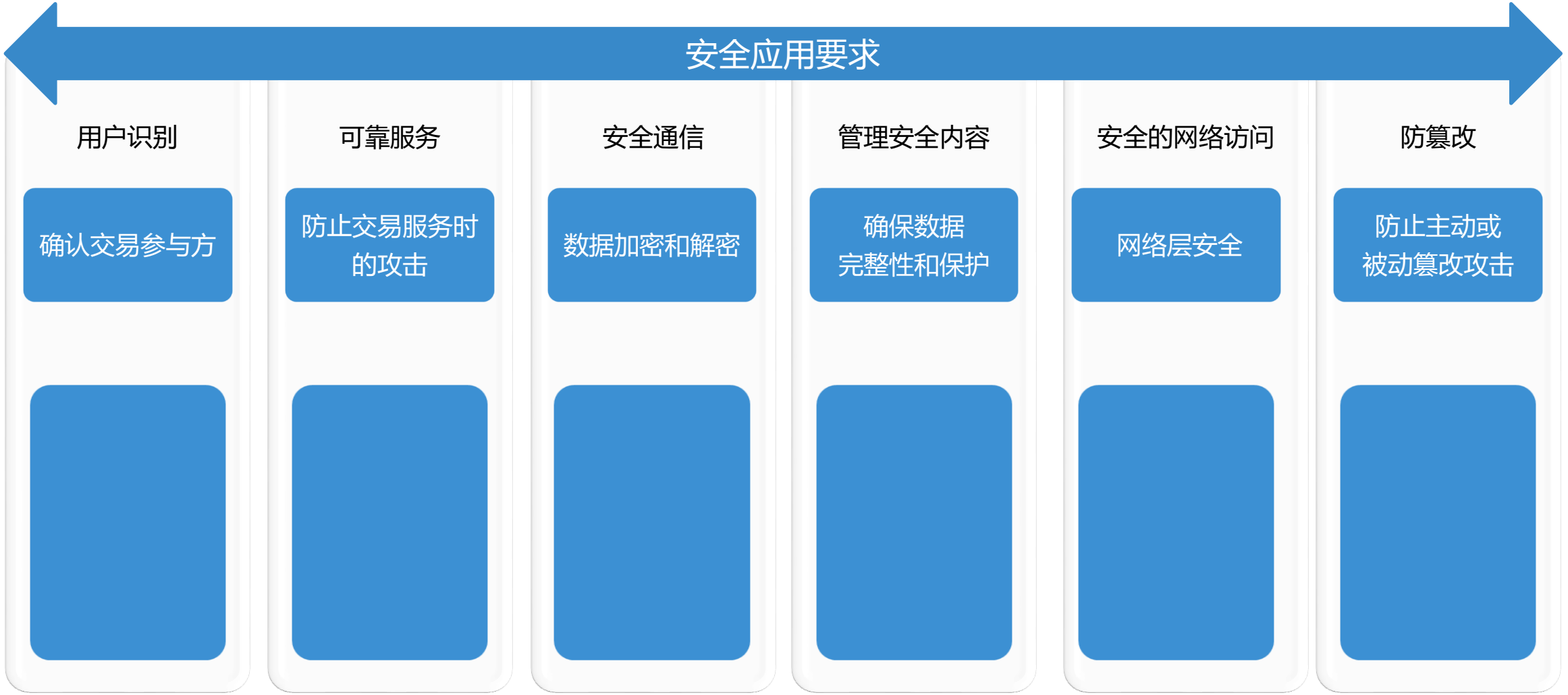
资源域控制

系统存储器单元保护

OTF加解密机制(代码)

在金融支付领域的应用

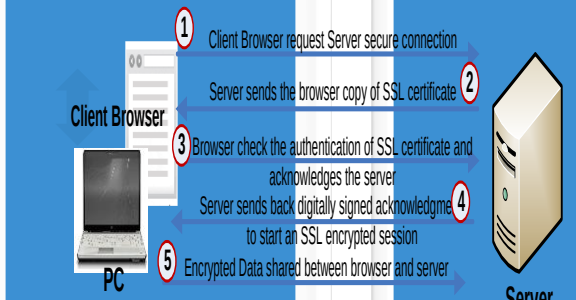
金融支付应用


安全应用要求
用户识别
确认交易参与方
可靠服务
防止交易服务时的攻击
安全通信
数据加密和解密
管理安全内容
确保数据完整性和保护
安全的网络访问
网络层安全
防篡改
防止主动或被动篡改攻击

金融支付应用

安全应用要求

用户识别	可靠服务	安全通信	管理安全内容	安全的网络访问	防篡改
确认交易参与方	防止交易服务时的攻击	数据加密和解密	确保数据完整性和保护	网络层安全	防止主动或被动篡改攻击



支付要求概况

- 资料来源：https://usa.visa.com/dam/VCOM/download/merchants/visa-PED-Requirements-2013.pdf
- 支付设备必须符合PCI（支付卡行业）标准
  - 这些标准每隔三年更新一次，如果存在重大威胁
    - 每当零售商购买新的POS设备时，都会建议其购买已通过最新标准的设备
  - 每隔7年，标准过时，建议零售商更换设备
- PCI安全会随着时间而变化

- **V1 PCI PED or EPP Security Requirements*** - Baseline security requirements with independent lab evaluation. Tamper evident controls required to easily detect unauthorized access to the device.
- **V2 PCI PED or EPP Security Requirements** - Improved tamper evident controls by requiring tamper responsive controls that detect intrusion attempts and subsequently destroys the content, including encryption keys.
- **V3 PCI PTS POI Security Requirements** (includes PED and EPP combined) Introduced secure read and exchange of data (SRED) capabilities that ensures cardholder account data is encrypted at the point of acceptance. (Note: Visa has no mandates for the use of SRED but implementation is a best practice)
- **V4 PCI PTS POI Security Requirements** (includes PED and EPP combined) - Improves testing evaluations and incorporates controls that address communication vulnerabilities that can be remotely exploited to gain access to sensitive data or resources within the device.

**Note there are also V1 HSM and UPT security requirements. Currently these requirements are designated as best practices for their use.*

金融支付终端的标准和认证需求

- PCI PTS（PIN交易安全）——PCI安全标准委员会是一个开放的全球论坛，致力于帐户数据保护安全标准的持续开发、完善、存储、传播与实施。[2]这包括软硬件的系统级要求。通过为安全的PED建立最低设计与制造标准，遵守PCI PTS安全要求可降低PIN泄露的可能性并限制其潜在影响。PCI PTS安全要求适用于ATM和终端机中使用的销售点(POS)设备和加密密码键盘(EPP)。[1]

- EMV (Europay、Mastercard、Visa)——EMVCo旨在促进安全支付交易在全球范围内实现互操作性和认可。它通过管理和发展EMV®规范和相关测试流程来完成这一任务。这包括但不限于卡片和终端评估、安全评估与互操作性问题管理。[2]

  -第三方实验室认证——PCI安全标准委员会建立了一套紧密的（但不是限制性的）且地理分布趋于分散的第三方认证实验室。每次提交时，这些实验室要求提供详细的支持文件以及对硬件进行全面的测试。这一流程可以及时、经济有效地完成。

[1] https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories
[2] https://www.emvco.com/

PCI安全要求：相关ISO标准

出版物
ISO 9564：个人识别号管理和安全
ISO 11568：银行业务 – 密钥管理（零售）
ISO 11770–2：信息技术 – 安全技术 – 密钥管理，第2部分：使用对称密钥管理技术的机制
ISO 13491：银行业务 – 安全加密设备（零售）
ISO 16609：银行业务 – 使用对称技术的消息验证要求
ISO/IEC 18033-3：信息技术 – 安全技术 – 加密算法 – 第3部分：块加密
ISO TR19038：三重DES操作模式指南

资料来源：https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

PCI安全要求：相关ANSI标准

出版物
ANSI X3.92：数据加密算法
ANSI X9.24（第1部分）：零售金融服务对称密钥管理第1部分：使用对称技术
ANSI X9.42：金融服务行业的公钥密码技术：使用离散对数密码技术的对称密钥协议
ANSI X9.44：使用整数因数分解密码系统的密钥确定
ANSI X9.62：金融服务ECDSA的公钥密码技术
ANSI X9.63：金融服务行业的公钥密码技术：使用椭圆曲线密码技术的密钥协议和密钥传输
ANSI X9.65：三重数据加密算法(TDEA)实施
ANSI TR-31：用于对称算法的互操作性安全密钥交换密钥块规范

资料来源：https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

PCI安全要求：相关FIPS、NIST、EMV和PCI标准

出版物
EMV：支付系统的集成电路卡规范，4.2版（2008年6月）——第2册：安全与密钥管理
FIPS PUB 140–2：密码模块的安全要求
NIST特种出版物800-22：针对密码应用的随机数和伪随机数生成器的统计测试套件
支付卡行业(PCI) PIN交易安全(PTS)交互点(POI)模块化安全要求
支付卡行业(PCI) PIN交易安全交互点模块化衍生测试需求
支付卡行业(PCI)硬件安全模块(HSM)安全要求
支付卡行业(PCI)硬件安全模块(HSM)衍生测试需求

资料来源：https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf

金融支付终端设备

可扩展的产品组合提供各种POS机解决方案

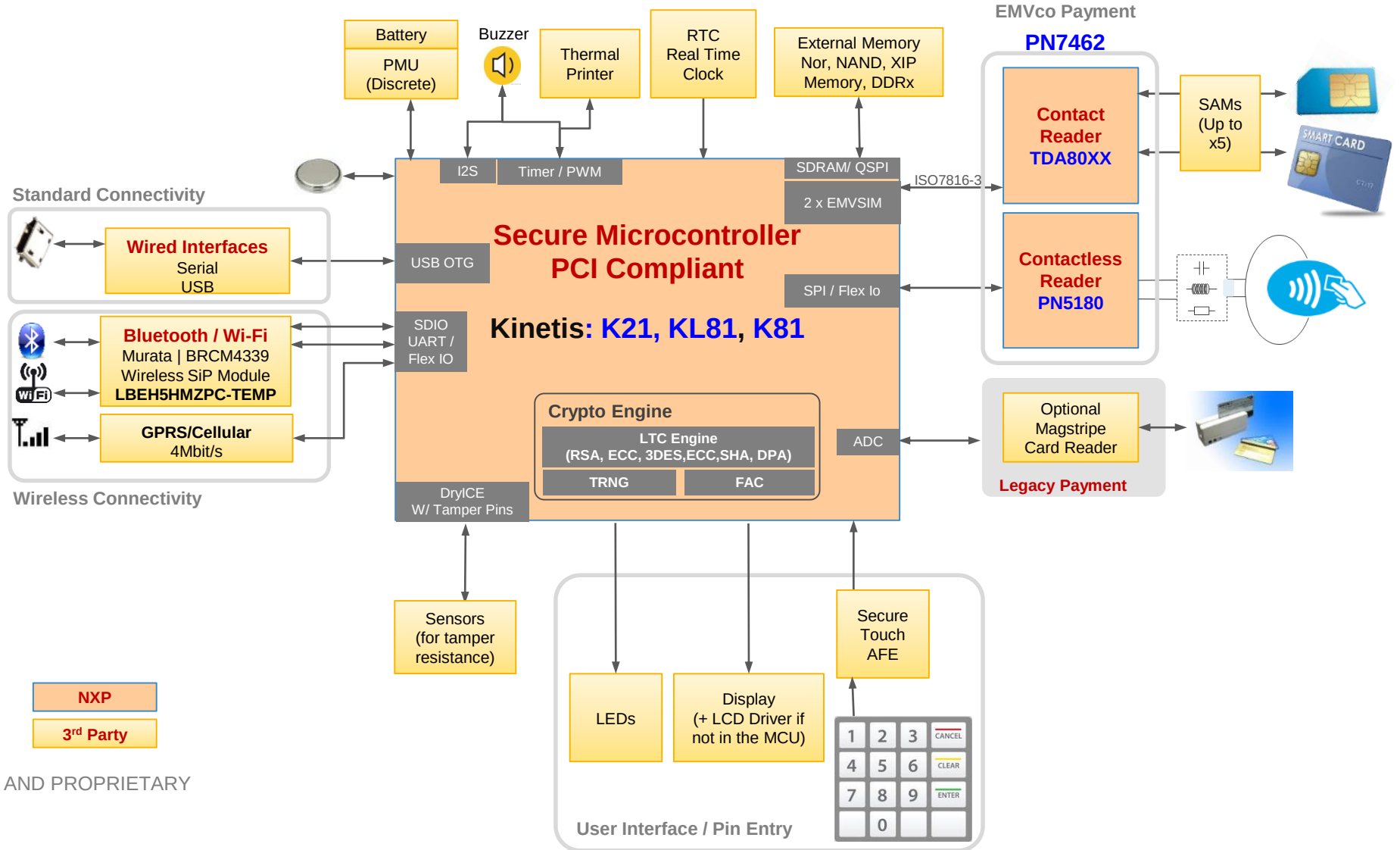
PinPad/mPOS	POS/智能POS	平板电脑/柜台POS	高端POS
 	 	 	
K21/K81/KL81	**i.MX 6** UL-3 **i.MX7** Solo	**i.MX 7**Dual；**i.MX** 8X系列 **i.MX** 6DL/D/Q + K81/KL81	**i.MX6** DQ Plus；i.MX 8X系列；8系列 + K81/KL81/A70CM

高效、安全和互联的解决方案

Payment Application Architectures

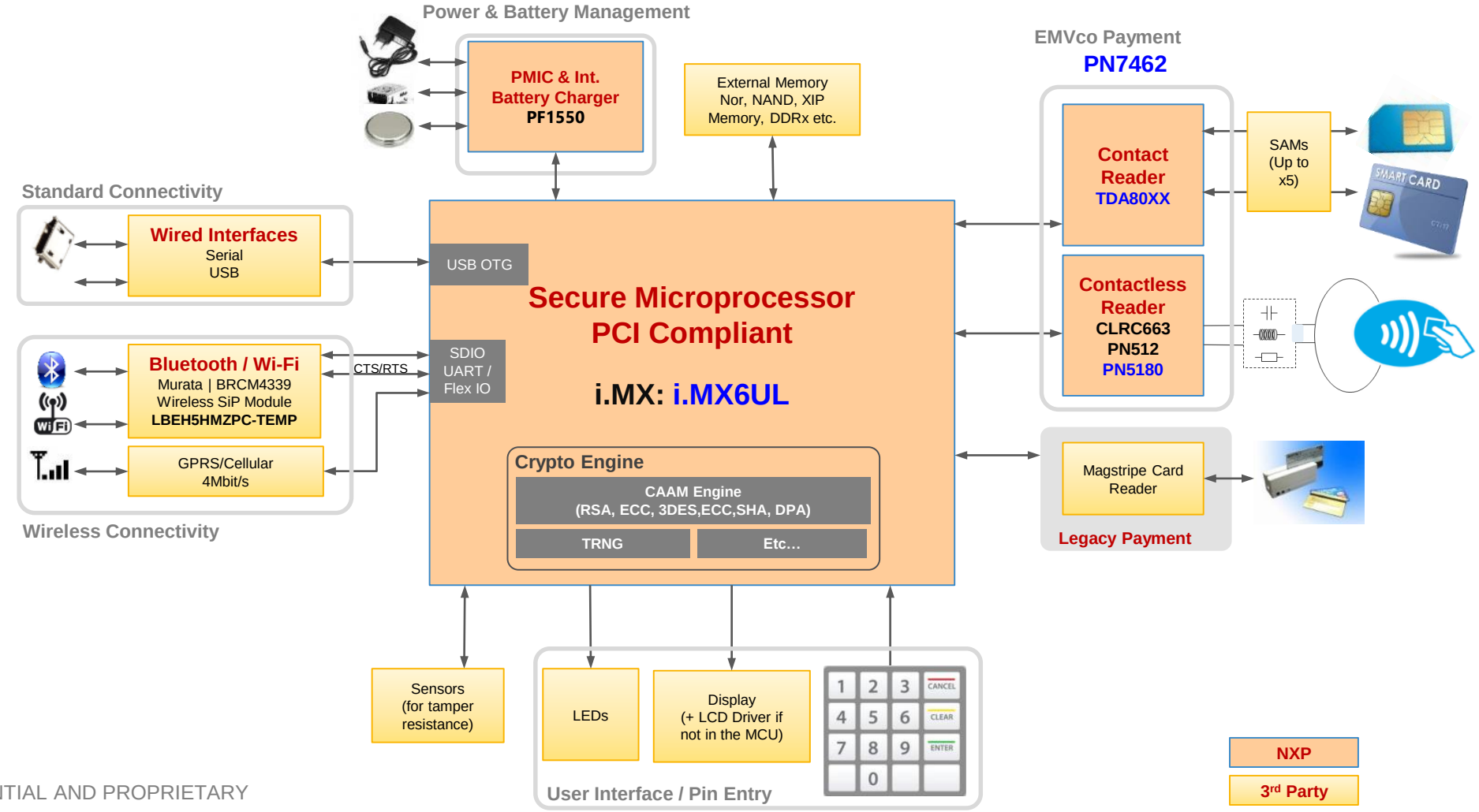
ARM Cortex-M

MCU/RTOS - PinPad, mPOS, Portable POS



ARM Cortex-A

MPU/Linux – mPOS, Portable POS



ARM Cortex-A

MPU/Android - Single Chip SmartPOS

Power & Battery Management

PMIC & Int. Battery Charger PF1550

External Memory Nor, NAND, XIP Memory, DDRx etc.

EMVco Payment

PN7462

Contact Reader TDA80XX

SAMs (Up to x5)

Contactless Reader CLRC663 PN512 PN5180

Standard Connectivity

Wired Interfaces Serial USB

USB OTG

Secure Microprocessor PCI Compliant

i.MX: i.MX7Solo/Dual

SDIO UART / Flex IO

CTS/RTS

Bluetooth / Wi-Fi Murata | BRCM4339 Wireless SiP Module LBEH5HMZPC-TEMP

GPRS/Cellular 4Mbit/s

Wireless Connectivity

Crypto Engine

CAAM Engine (RSA, ECC, 3DES,ECC,SHA, DPA)

TRNG

Etc…

Magstripe Card Reader

Legacy Payment

Sensors (for tamper resistance)

LEDs

Display (+ LCD Driver if not in the MCU)

User Interface / Pin Entry

NXP

3rd Party

MPU/Android - Split Architecture Smart POS and Kiosk

Battery Charger
BC3770
MC32PBC3770

PMIC
PF0100

Thermal Printer

RTC
Real Time Clock

External Memory
Nor, NAND, XIP Memory, DDRx etc.

Wired Interfaces
Serial
USB
Ethernet

Bluetooth / Wi-Fi
Murata | BRCM4339
Wireless SiP Module
LBEH5HMZPC-TEMP

Main Processing Unit
i.MX: i.MX6DL; D/Q; D/Q+; i.MX8

Secure Controller
Kinetis: KL81, K81

LEDs | Display | Secure Capacitive Touch Controller

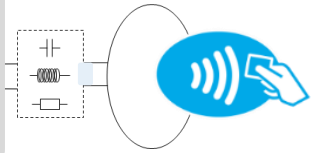
User Interface / Pin Entry

EMVco Payment
PN7462

Contact Reader
TDA80XX

SAMs (Up to x5)

Contactless Reader
CLRC663
PN512
PN5180



Magstripe Card Reader

Legacy Payment

NXP/FSL

3rd Party

结论

结论

- 每个产品都需要安全保障。嵌入式开发人员必须确定其实施方案所需的安全级别
  - **必须执行风险分析**：应对什么加以保护？为何加以保护？谁将发起攻击？
  - **三大安全支柱**：信任、加密和防篡改
  - **Kinetis MCU产品组合提供广泛的安全功能**：从简单的Flash保护到销售点设计和安全认证

安全技术可拓展的应用领域：ASIA

从传统的PC扩展到了更多的工业、消费、医疗等领域中

Access	Protection against denial of service attacks	Gateway, wireless module
Security	Encryption and decryption of data	POS, Security module Fingerprint…
Identification	Confirmation of the parties involved in a transaction	Payment, OTA Wearable device, IoT
Alarm	Detect attacks and send alarm to system	Wireless module

SECURE CONNECTIONS
FOR A SMARTER WORLD