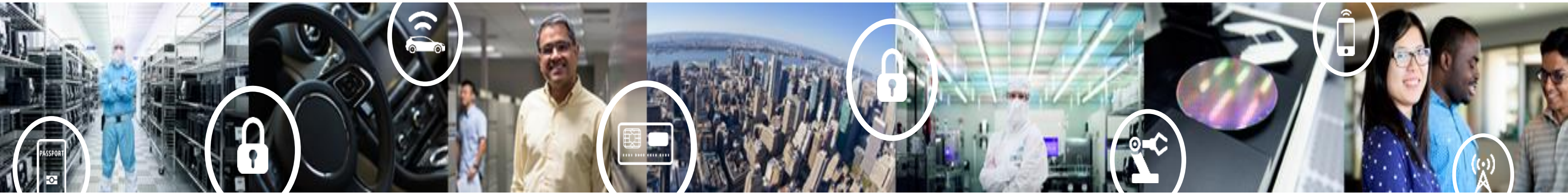
物联网系统中的安全需求与软硬件解决方案

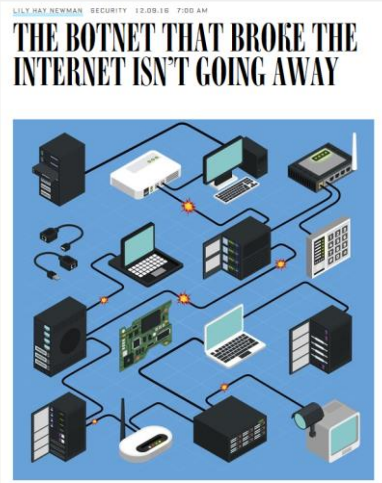
莫志豪
恩智浦半导体资深应用工程师
2020.09



PUBLIC

NXP SECURE CONNECTIONS FOR A SMARTER WORLD

物联网缺乏安全性在当前显而易见



LILY HAY NEWMAN SECURITY 12.09.16 7:00 AM

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

Mirai botnet

Disruption of major Internet services

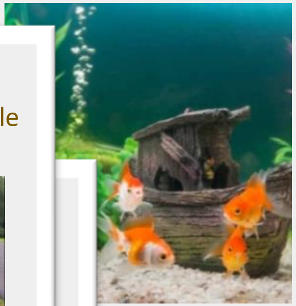
Software bug makes Nest Cams vulnerable to hacks

Nest Hack

Security camera shut down by a simple click on a phone

Jeep hack

Loss of control over vehicle via WiFi connection



Casino hack

Overview of high-rollers extracted via thermostat of a fish-aquarium in the lobby

Target Hack

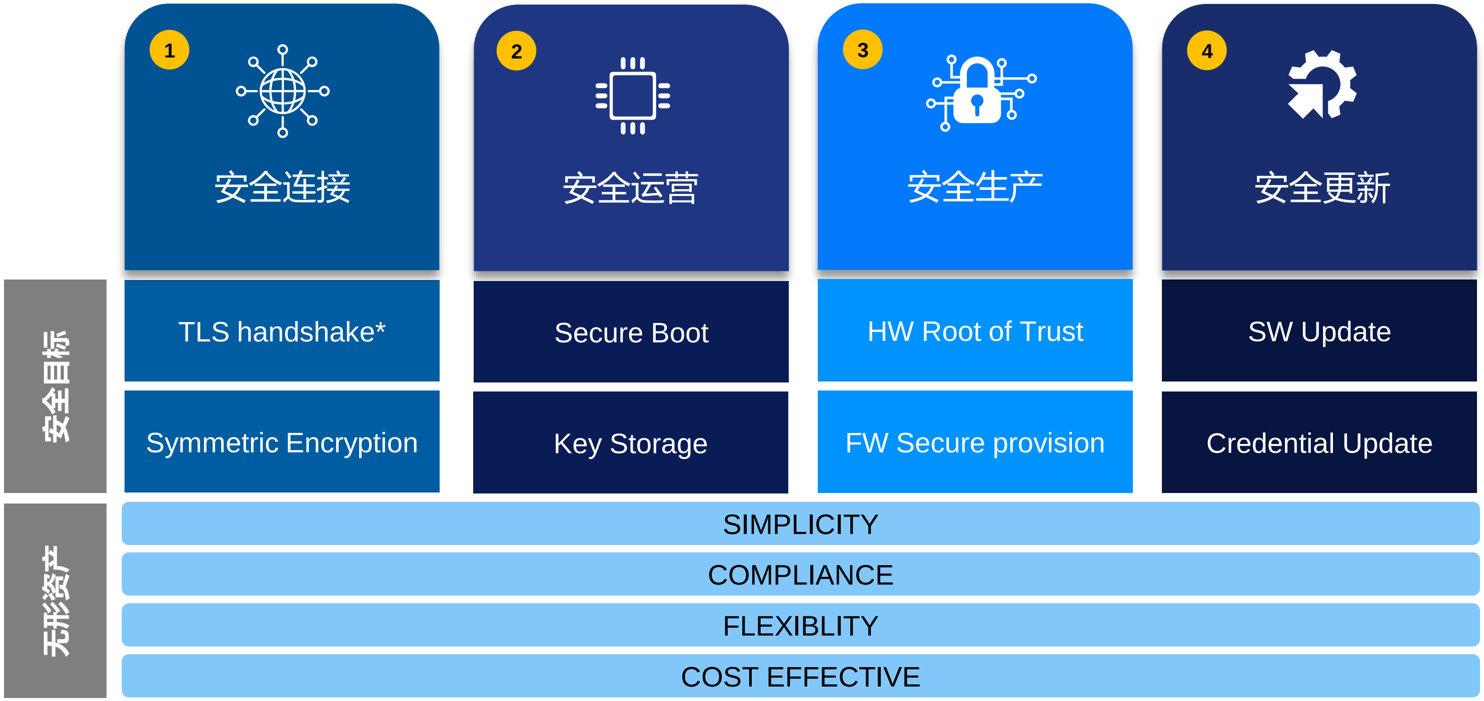
Target declared that the total cost of the data breach had been $202M *NBC news, May 24, 2017*

TARGET

SEPTEMBER 20, 2017 by Mamta Badkar in New York

Parcel delivery company **FedEx** said on Tuesday that a June **cyber attack** on its **TNT Express** unit **cost** the company **$300m in the first quarter**, … the **NotPetya cyber attack**, which originated from tax preparation software in Ukraine and resulted in the disruption of communications systems at TNT Express.

物联网设备的主要安全挑战
解决这四个挑战使OEM能够对应主要的物联网攻击



	1 安全连接	2 安全运营	3 安全生产	4 安全更新
安全目标	TLS handshake*	Secure Boot	HW Root of Trust	SW Update
	Symmetric Encryption	Key Storage	FW Secure provision	Credential Update
无形资产	SIMPLICITY			
	COMPLIANCE			
	FLEXIBLITY			
	COST EFFECTIVE			

TLS handshake* : HW pre-integration of common SSL stacks e.g OpenSSL, mbedTLS..

联网智能设备在其整个生命周期中都容易受到攻击

产品生命周期

开发，制造和分销

本地攻击 (逻辑 和 物理)

- Extract keys/certificates
- Overproduction of original device
- False certificate/private key injection
- Malicious image loading
- Counterfeits of devices
- IP Theft

设备未连接，无法进行远程攻击

机载，操作和更新

本地攻击 (逻辑 或 物理) – Device level scale

- Tamper the IC to obtain access to data and SW and re-use for remote attacks (Trojan horse, DoS on Cloud, …)
- Especially dangerous for non-diversified Symmetric key protection: “Break one, Break all”

远程攻击 – All products are the attack surface

- Create unauthorized connection to extract data, abuse functionality or inject malware to turn device into a bot
- Perform malicious software update to do the same

作废

本地攻击 (逻辑 和 物理)

- Extract credentials (user data, keys, certificates)
- Inject malware to network

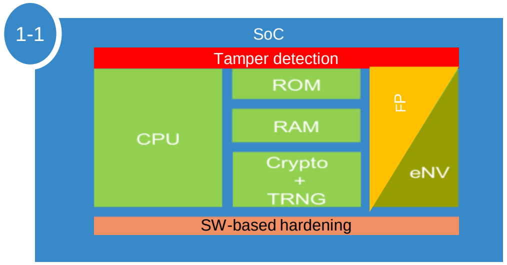
通过重新调试设备以攻击网络或云，可以进行远程攻击

当前发布的恩智浦产品支持的安全架构

Add Trusted Execution based on ARM TrustZone® and/or isolation features[1] on the SoC

Add SE to architecture

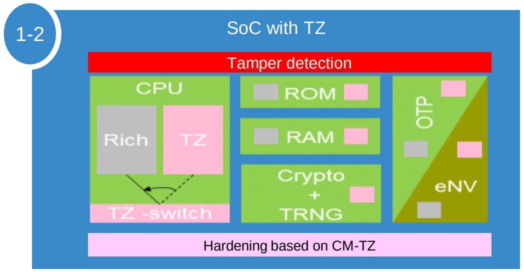
Standard SoC with basic security hardening



Allows for

- *Secure Boot*
- *Secure Debug*
- *Cryptographic Operations*
- *Tamper Detection*

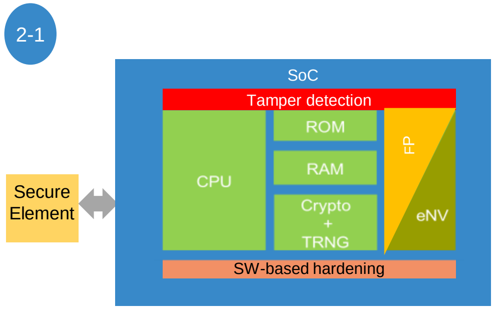
SoC with basic security hardening & TrustZone



Additional features:

- *Secure execution environment (“Trusted”)*
- *Rich execution environment (“Non-trusted”)*

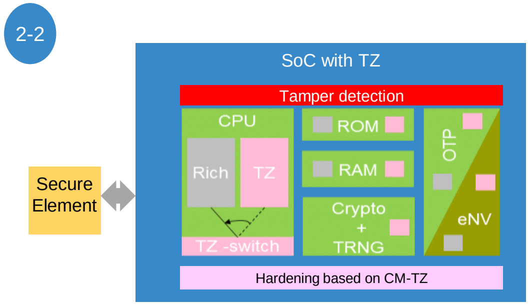
SoC with basic security hardening and a SE



Additional features:

- *Tamper Resistant Protection of root keys*
- *Credentials can be securely injected in SE*
- *Provisioned keys are delivered directly to the customer through a secure channel*

SoC with basic security hardening, TZ & SE



Additional features:

- *Combined features of architecture 1-2 and 2-1*

[1] Features like RDC (Resource Domain Controller) on i.MX

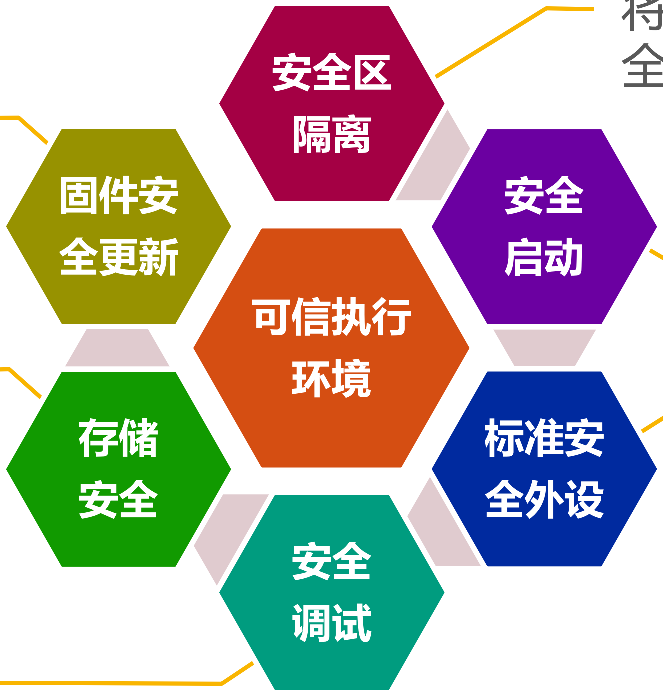
MCU产品安全特性概览：i.MX RT / LPC54S/55S / K(L)81/21

特性	i.MX RT10xx	i.MX RT1170	i.MX RT600/500	LPC54S0xx	LPC55Sxx	K81/KL81	K21
对称和杂凑算法（DES/3DES, AES, SHA1/256）	✓- DES/3DES	✓+ SHA384/512	✓- DES/3DES	✓- DES/3DES	✓- DES/3DES	✓	✓
非对称算法 ECDSA (up to P521/B571) RSA (up to 4096)	x	✓CAAM	✓Casper	x	✓Casper	✓LTC	x
随机数产生器SA-TRNG	✓	✓RNG	✓	✓	✓	✓	✓RNGA
隔离安全应用 Isolated security applications (e.g. TFM)	x	✓	✓	x	✓	x	x
安全启动 (RSA up to 4096)	✓HAB	✓HAB	✓	✓	✓	✓Flash	✓Flash
加密启动Encrypted Boot	✓	✓	✓	✓	✓	x	x
安全调试Secure Debug	✓	✓	✓	x	✓	x	x
物理不可克隆模块SRAM PUF	x	✓	✓	x	✓	x	x
Always ON domain	✓	✓	x	x	x	✓	✓
安全存储Secure Storage (non-volatile)	✓	✓	✓OTP	✓OTP	✓PFR	✓	✓
防篡改Tamper Detection Signal	x	✓ Active	x	x	x	✓Active	✓Active
电压/温度/频率检测Volt/Temp/Freq Detection	x	✓	x	x	x	✓	✓
在线加密保护Bus Encryption (BEE, OTFAD)	✓	✓ + IEE	✓	x	✓ PRINCE	✓K81 only	x
量产保护Manufacturing Protection	x	✓	✓	x	✓	x	x
资源域隔离Resource Domain Isolation	✓CSU	✓RDC	✓TZ	x	✓TZ	✓SysMPU	✓SysMPU
数字内容保护Content Protection	x	✓	x	x	x	x	x

MCU安全模块提供的安全服务:
i.MX RT / LPC54S/55S / K(L)81/21

安全服务类型	相关的安全模块	抵御的安全威胁
真实性（对信息的来源进行判断，能对伪造来源的信息予以鉴别）	• HAB, CAAM, SRTC, secure ROMBoot, LTC, Casper	假冒,重放
保密性（保证机密信息不被窃听，或窃听者不能了解信息的真实含义）	• DryICE, Tamper detection, CAAM, DCP, LTC secure RAM, TRNG, ZMK, BEE, IEE, OTFAD, PRINCE, HashCrypto, SRAM PUF	信息泄露,窃听,业务流分析,旁路控制,媒体废弃,物理侵入
完整性（保证数据的一致性，防止数据被非法用户篡改）	• CAAM, RTIC, SRTC, HashCrypto, eFuse, PFR	破坏信息的完整性,
可用性（保证合法用户对信息和资源的使用不会被不正当地拒绝）	• TrustZone, (X)RDC, CSU, CAAM, SysMPU, Secure AHB Controller	拒绝服务
不可抵赖性（建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的）	• CAAM, eFuse, unique ID. LTC, Casper, SRAM PUF	抵赖,业务欺骗
可控制性（对信息的传播及内容具有控制能力，阻止未经授权的访问）	• TrustZone, CSU, MPU, (X)RDC, Secure Debug, Secure JATG, CAAM, eFuse, unique ID, SRTC, sysMPU, Secure AHB controller, SRAM PUF	非法使用, 授权侵犯,特洛伊木马,陷阱门,计算机病毒,人员不慎,窃取

可信安全执行环境 – TEE



将系统资源隔离为安全和非安全两个区域

OTA固件更新、 撤销密钥、固件防回滚

仅执行经过认证的固件

密钥、代码和数据安全

哈希、加密解密外设

仅允许有授权的开发者进行调试

MCU上的安全子系统 —— 以LPC55S00为例

安全启动管理

- 来自“可信计算工作组”的基于ROM的设备标识符组合引擎（DICE）

具有专用安全密钥访问权限的加密引擎

- CASPER非对称（RSA / ECC）引擎，可加速WolfSSL / mbedTLS（256位密钥）
- 恩智浦的实时解密引擎（**PRINCE**），用于加密内部闪存代码
- 对称（AES-256）和哈希（SHA-256）引擎
- 具有256位的真随机数生成器（RNG）

256位硬件保护的安全存储

- 先进的SRAM **PUF**提供了一个不变的，唯一的设备根密钥
- 带设备密钥存储区的受保护的闪存区域（PFR）

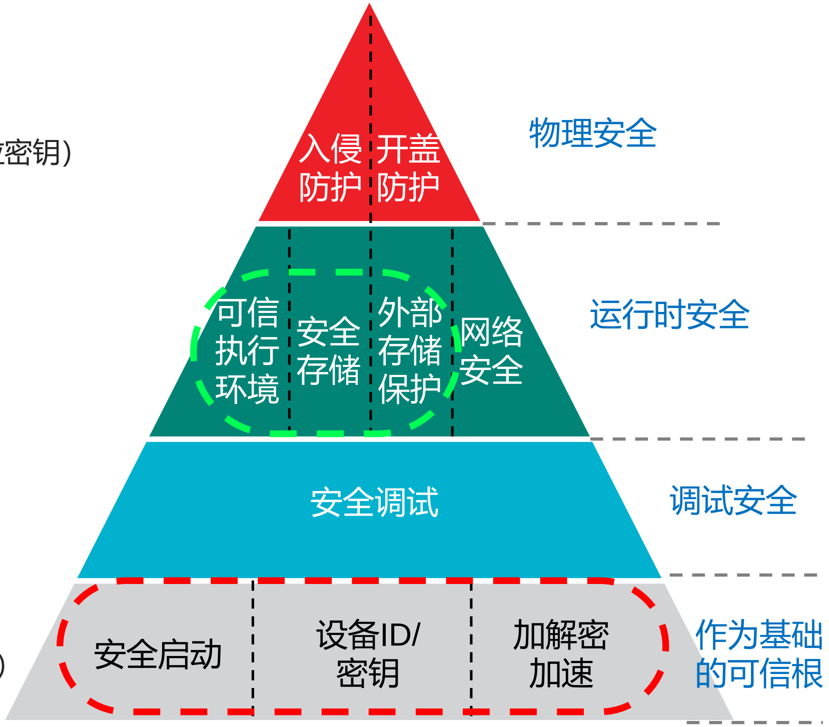
  +符合行业标准的128位通用唯一标识符（UUID）

  +现场和工厂可编程空间，可提供唯一的设备根密钥和密钥哈希

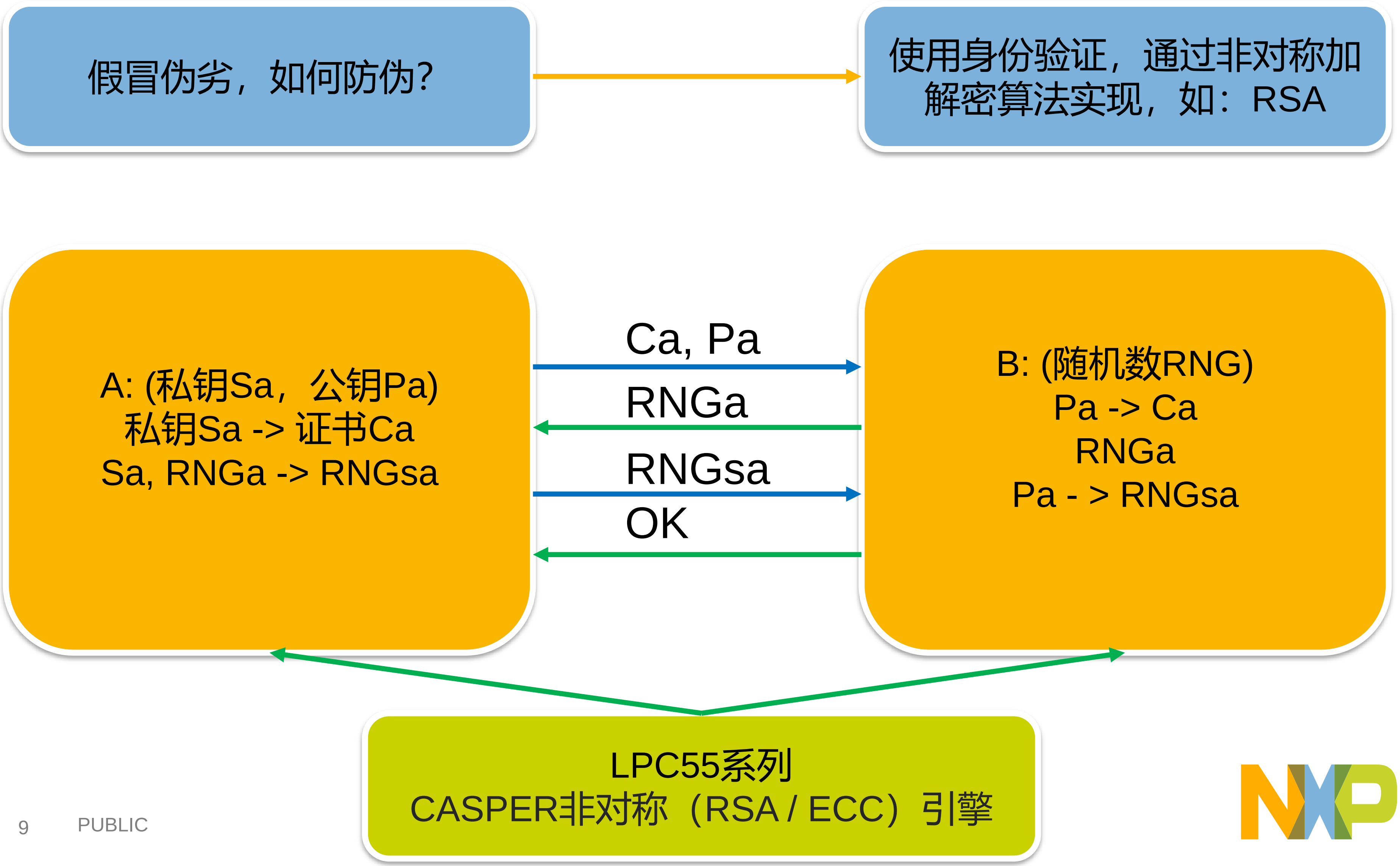
安全调试身份验证

物理保护和运行时安全

- Armv8-M **TrustZone**，安全归因单元（SAU）和安全内存保护单元（MPU）
- 与恩智浦定义的归因单元和安全总线/ GPIO / DMA控制器结合使用



MCU上安全示例 – LPC55



假冒伪劣，如何防伪?

使用身份验证，通过非对称加解密算法实现，如：RSA

A: (私钥Sa，公钥Pa)
私钥Sa -> 证书Ca
Sa, RNGa -> RNGsa

Ca, Pa

RNGa

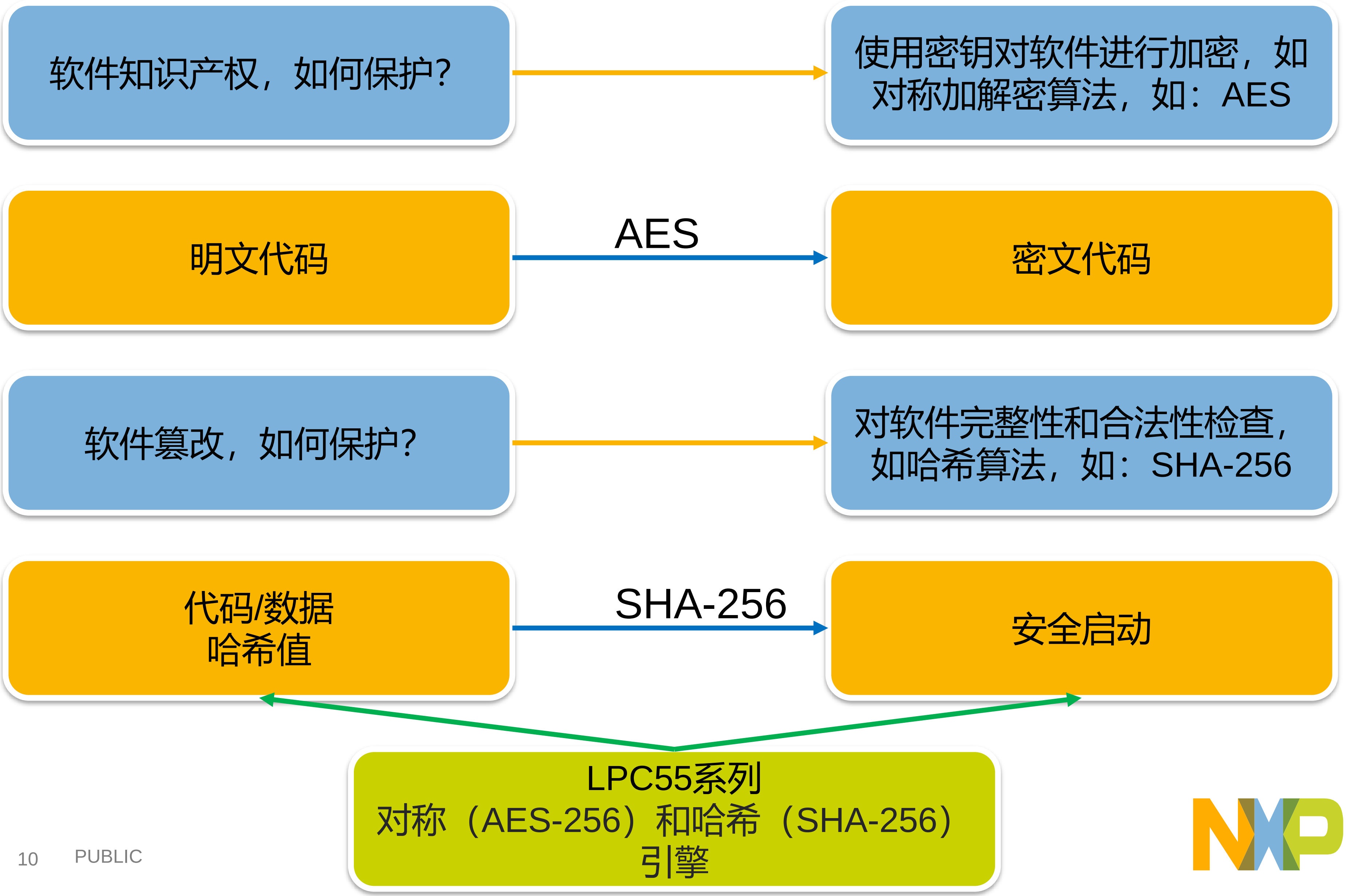
RNGsa

OK

B: (随机数RNG)
Pa -> Ca
RNGa
Pa - > RNGsa

LPC55系列
CASPER非对称（RSA / ECC）引擎

MCU上安全示例 – LPC55



软件知识产权，如何保护?

使用密钥对软件进行加密，如对称加解密算法，如：AES

明文代码

AES

密文代码

软件篡改，如何保护?

对软件完整性和合法性检查，如哈希算法，如：SHA-256

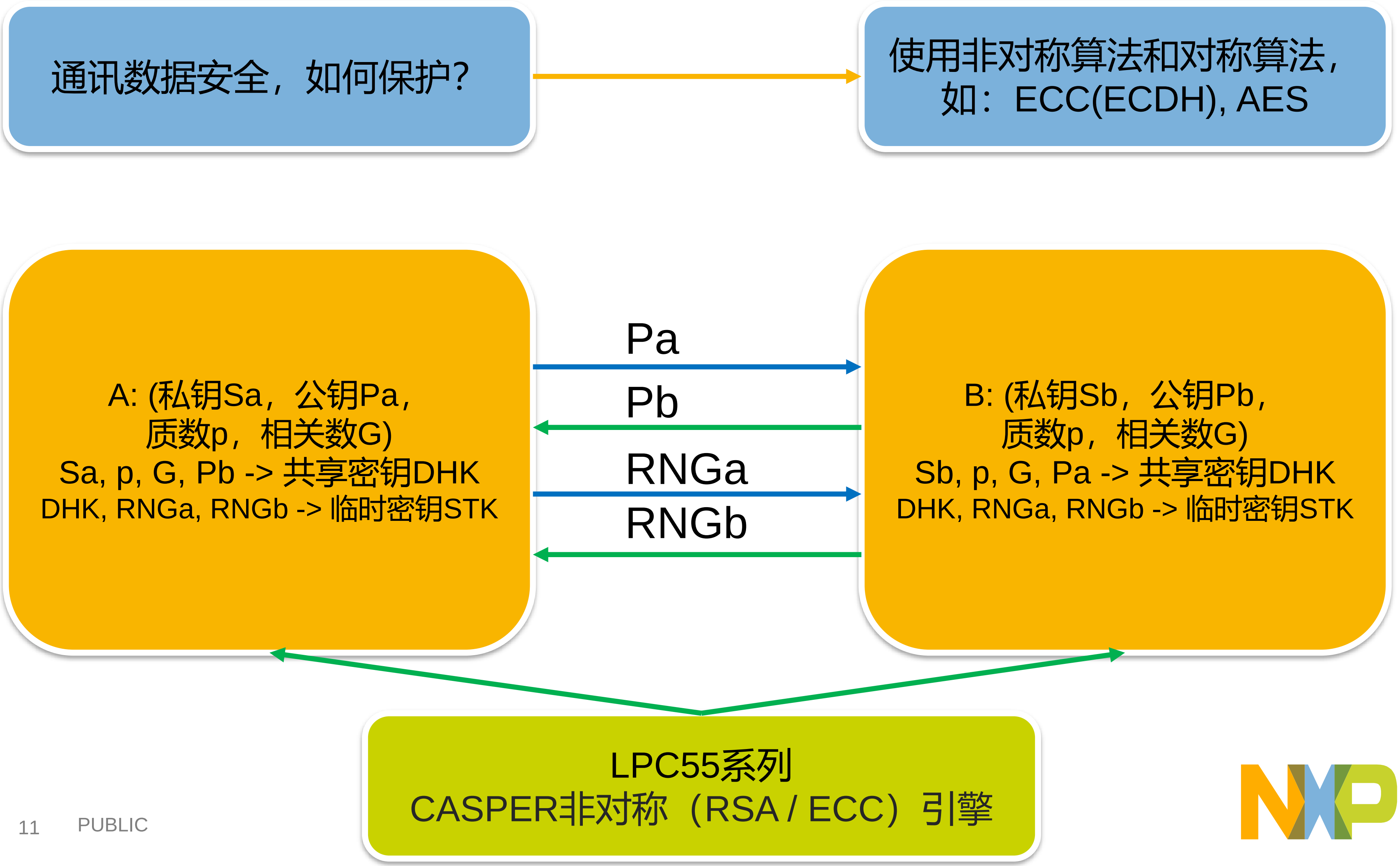
代码/数据
哈希值

SHA-256

安全启动

LPC55系列
对称（AES-256）和哈希（SHA-256）
引擎

MCU上安全示例 – LPC55



通讯数据安全，如何保护?

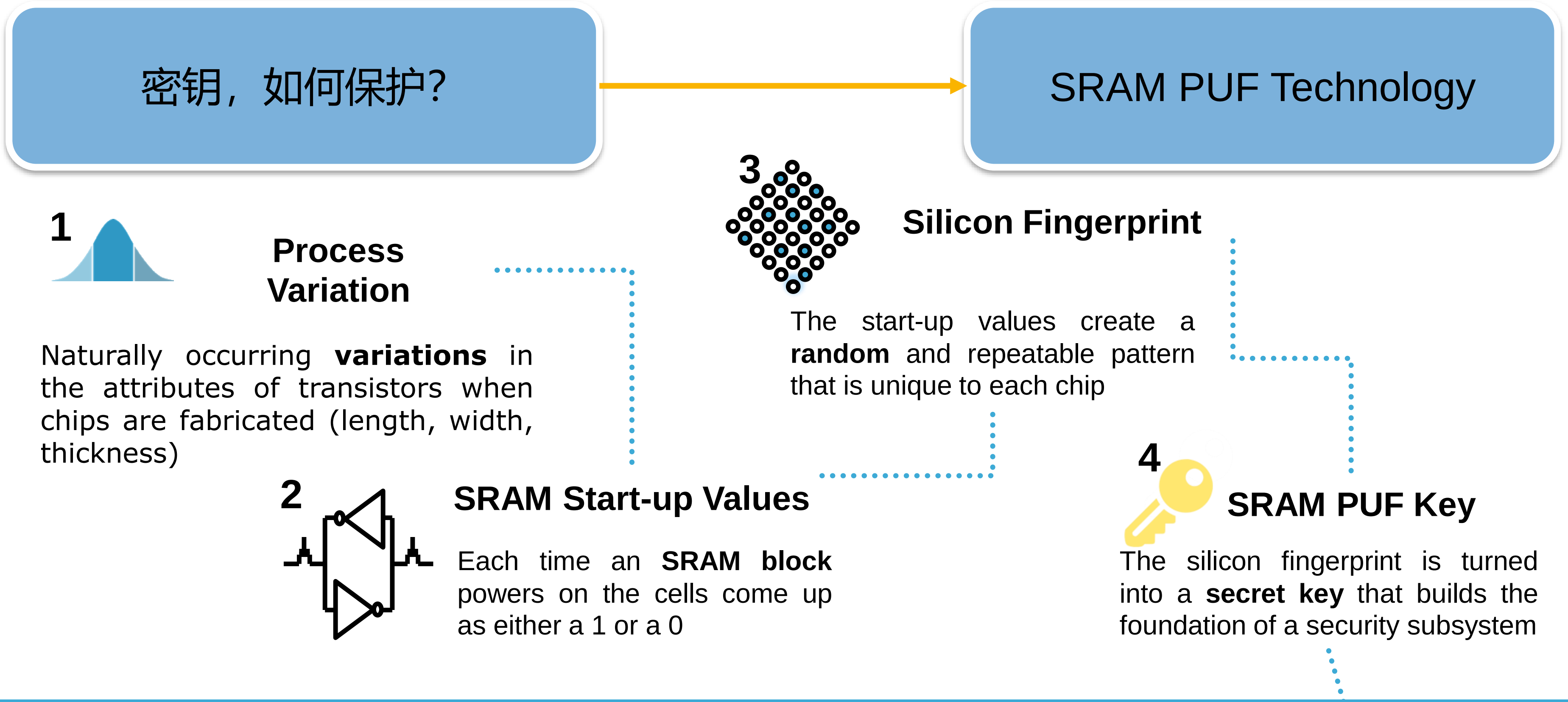
使用非对称算法和对称算法，
如：ECC(ECDH), AES

A: (私钥Sa，公钥Pa，
质数p，相关数G)
Sa, p, G, Pb -> 共享密钥DHK
DHK, RNGa, RNGb -> 临时密钥STK

B: (私钥Sb，公钥Pb，
质数p，相关数G)
Sb, p, G, Pa -> 共享密钥DHK
DHK, RNGa, RNGb -> 临时密钥STK

LPC55系列
CASPER非对称（RSA / ECC）引擎

MCU上安全示例 – LPC55



密钥，如何保护?

SRAM PUF Technology

1

Process Variation

Naturally occurring **variations** in the attributes of transistors when chips are fabricated (length, width, thickness)

2

SRAM Start-up Values

Each time an **SRAM block** powers on the cells come up as either a 1 or a 0

3

Silicon Fingerprint

The start-up values create a **random** and repeatable pattern that is unique to each chip

4

SRAM PUF Key

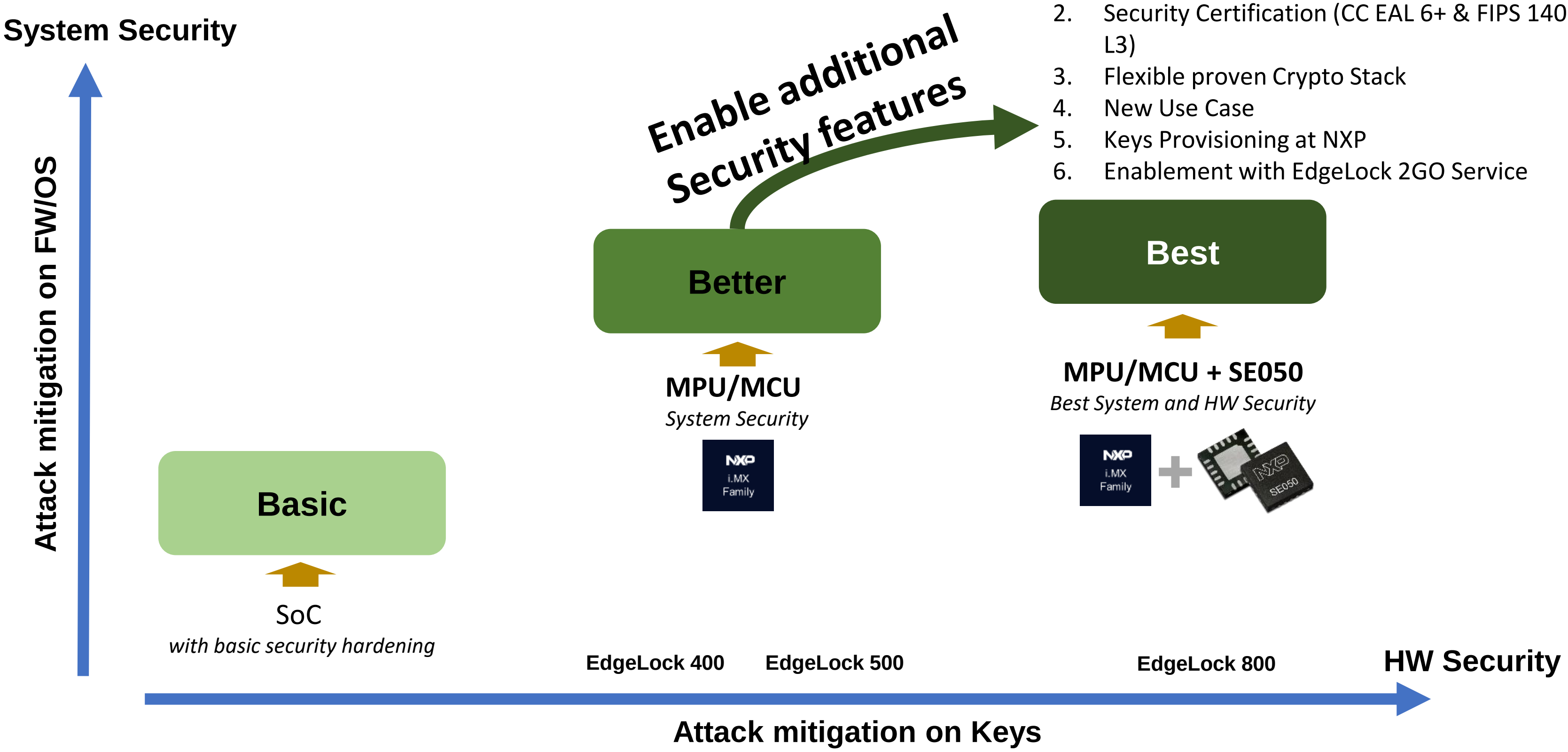
The silicon fingerprint is turned into a **secret key** that builds the foundation of a security subsystem

SRAM PUF Benefits

- Device-unique, unclonable fingerprint
- Leverages entropy of mfg. process
- No key material programmed

安全体系结构选项简介

1. HW Tampering Resistance
2. Security Certification (CC EAL 6+ & FIPS 140-2 L3)
3. Flexible proven Crypto Stack
4. New Use Case
5. Keys Provisioning at NXP
6. Enablement with EdgeLock 2GO Service



System Security

Attack mitigation on FW/OS

Enable additional Security features

Basic

SoC
with basic security hardening

Better

MPU/MCU
System Security

Best

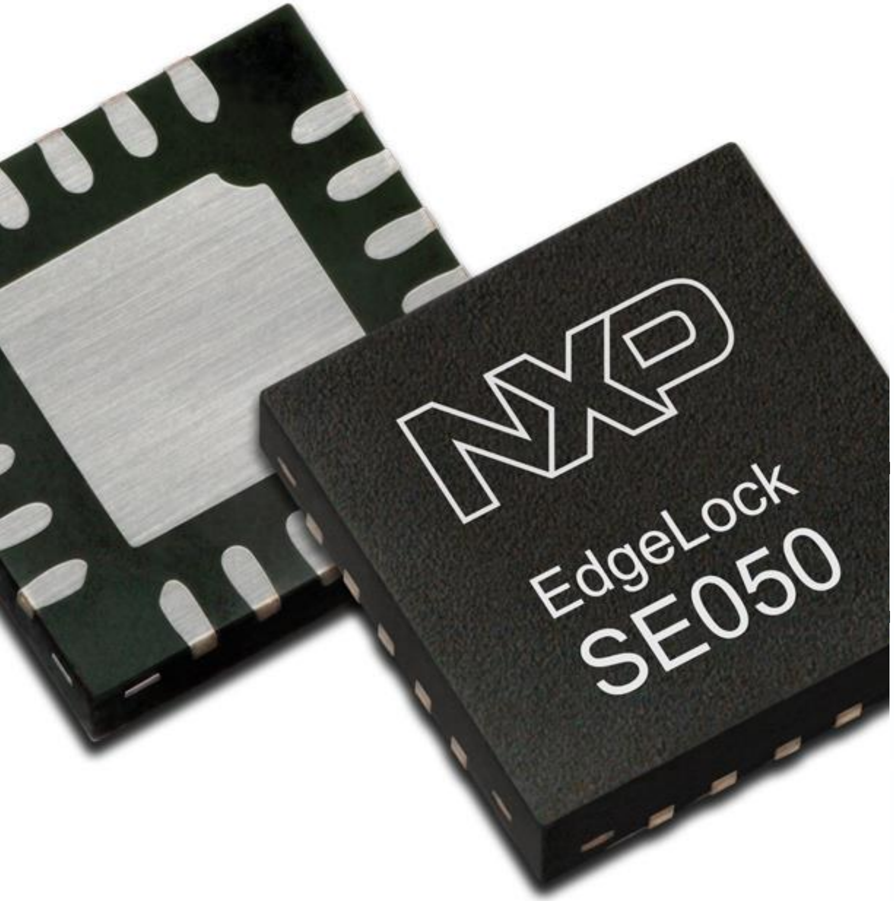
MPU/MCU + SE050
Best System and HW Security

EdgeLock 400 EdgeLock 500 EdgeLock 800

HW Security

Attack mitigation on Keys

EdgeLock SE050



PLUG&TRUST

5 POINTS TO HAVE IN MIND FOR CHOOSING EDGELOCK SE050 ON TOP OF NXP MPU/MCU

1. HW Tampering Resistance
2. Security Certification – CC EAL 6+ & FIPS 140-2 L3
3. Flexible Crypto Stack
4. New Use Cases
5. Enabled with EdgeLock 2GO

安全开发及配置工具

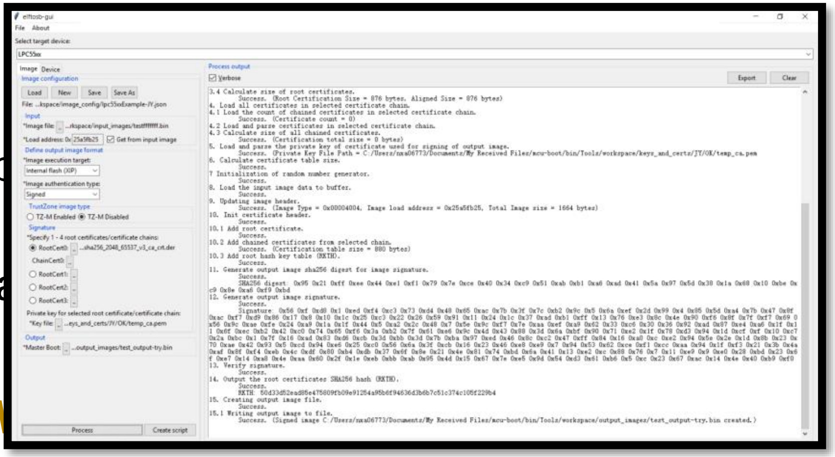
安全应用文档和软件安全

Application Notes	Document Linker	Software Liner
AN12445	Asymmetric Cryptographic Accelerator CASPER	NA
AN12278	LPC55S69 Security Solutions for IoT	NA
AN12324	LPC55Sxx usage of the PUF and Hash Crypt to AES coding	Application note software for AN12324
AN12326	LPC55S6x Secure GPIO and Usage	Application software for AN12326
AN12283	LPC55Sxx Secure Boot	…\SDK_2.6.2_LPCXpresso55S69\middleware\mcu-boot\bin\Tool\elftosb-gui(win).exe

Reference Code	KSDK Position, Request to be selected by downloader when building your SDK
mbedTLS	…\SDK_2.x.x_LPCXpresso55S6x\middleware\mbedtls
Flashloader	…\SDK_2.x.x_LPCXpresso55S6x\middleware\mcu-boot
safeRTOS	https://www.highintegritysystems.com/partners/nxp/
ARM TF-M	…\SDK_2.6.2_LPCXpresso55S6x_MDK\middleware\tfm

安全启动和配置小工具

- **Secure Boot Tool**
  - Part type: LPC55xx, RT6xx, K32W0x
  - Boot type: signed boot, encrypted boot, CRCed b +signed boot
  - Signed/Encrypted/XIP/SB bootable image genera
  - eFuse/OTP/FPR configuration
  - **…\SDK_2.6.2_LPCXpresso55S69\middleware\ gui(win).exe**
- **TEE Config Tool (CM33 TZ)**
  - Memory (RAM and Flash)
  - Master / Slave IP
  - Interrupt
  - Pins
  - MCUXpresso Config Tools - Pins



Select target device: LPC55xx

Image configuration

File: ...kspace/image_config/lpc55xxExample-JY.json

Input

*Image file: ...rkspace/input_images/testffffffff.bin

*Load address: 0x 25a5fb25 ☑ Get from input image

Define output image format

*Image execution target: Internal flash (XIP)

*Image authentication type: Signed

TrustZone image type

○ TZ-M Enabled ● TZ-M Disabled

Signature

*Specify 1 - 4 root certificates/certificate chains:

● RootCert0: ...sha256_2048_65537_v3_ca_crt.der

ChainCert0:

○ RootCert1:

○ RootCert2:

○ RootCert3:

Private key for selected root certificate/certificate chain:

*Key file: ...eys_and_certs/JY/OK/temp_ca.pem

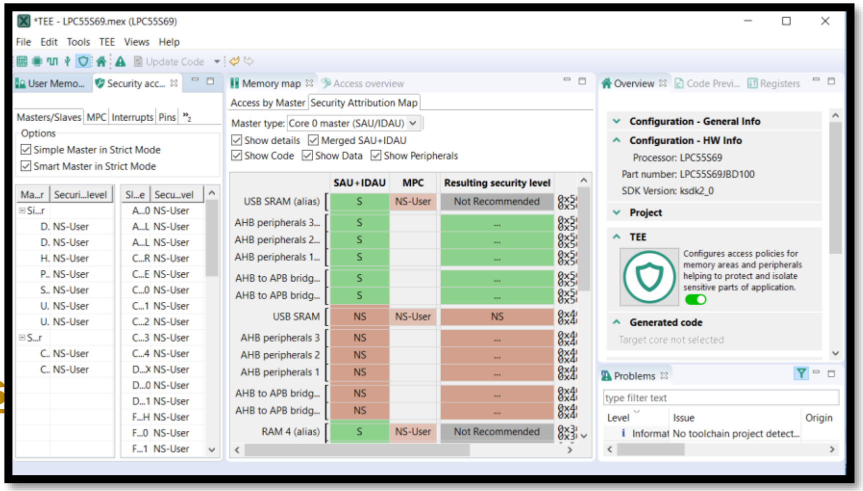
Output

*Master Boot: ...output_images/test_output-try.bin

Process output

☑ Verbose

```
3.4 Calculate size of root certificates.
        Success. (Root Certification Size = 876 bytes. Aligned Size = 876 bytes)
4. Load all certificates in selected certificate chain.
4.1 Load the count of chained certificates in selected certificate chain.
        Success. (Certificate count = 0)
4.2 Load and parse certificates in selected certificate chain.
4.3 Calculate size of all chained certificates.
        Success. (Certification total size = 0 bytes)
5. Load and parse the private key of certificate used for signing of output image.
        Success. (Private Key File Path = C:/Users/nxa06773/Documents/My Received Files/mcu-boot/bin/Tools/workspace/keys_and_certs/JY/OK/temp_ca.pem
6. Calculate certificate table size.
        Success.
7 Initialization of random number generator.
        Success.
8. Load the input image data to buffer.
        Success.
9. Updating image header.
        Success. (Image Type = 0x00004004, Image load address = 0x25a5fb25, Total Image size = 1664 bytes)
10. Init certificate header.
        Success.
10.1 Add root certificate.
        Success.
10.2 Add chained certificates from selected chain.
        Success. (Certification table size = 880 bytes)
10.3 Add root hash key table (RKTH).
        Success.
11. Generate output image sha256 digest for image signature.
        Success.
        SHA256 digest: 0x95 0x21 0xff 0xee 0x44 0xe1 0xf1 0x79 0x7e 0xce 0x40 0x34 0xc9 0x51 0xab 0xb1 0xa6 0xad 0x41 0x5a 0x97 0x5d 0x38 0x1a 0x68 0x10 0xbe 0x
c9 0x8e 0xa6 0xf9 0xbd
12. Generate output image signature.
        Success.
        Signature: 0x56 0xf 0xd8 0x1 0xed 0xf4 0xc3 0x73 0xd4 0x48 0x65 0xac 0x7b 0x3f 0x7c 0xb2 0x9c 0x5 0x6a 0xef 0x2d 0x99 0x4 0x85 0x5d 0xa4 0x7b 0x47 0x8f
0xac 0xf7 0xd9 0x86 0x17 0x8 0x10 0x1c 0x25 0xc3 0x22 0x26 0x59 0x91 0x11 0x24 0x1c 0x37 0xad 0xb1 0xff 0x13 0x76 0xe3 0x8c 0x4e 0x90 0xf6 0x8f 0x7f 0xf7 0x69 0
x56 0x9c 0xae 0xfe 0x24 0xa9 0x1a 0x1f 0x44 0x5 0xa2 0x2c 0x48 0x7 0x5e 0x9c 0xf7 0x7e 0xaa 0xef 0xa9 0x62 0x33 0xc6 0x30 0x36 0x92 0xad 0x87 0xe4 0xa6 0x1f 0x1
1 0x6f 0xec 0xb2 0x42 0xc0 0x74 0x65 0xf6 0x3a 0xb2 0x7f 0x61 0xe6 0x9c 0x4d 0x43 0x88 0x3d 0x6a 0xbf 0x90 0x71 0xe2 0x1f 0x78 0xd3 0x94 0x1d 0xcf 0xf 0x10 0xc7
0x2a 0xbc 0x1 0x7f 0x16 0xad 0x83 0xd6 0xcb 0x3d 0xbb 0x3d 0x7b 0xba 0x97 0xed 0x46 0x8c 0xc2 0x47 0xff 0x84 0x16 0xa0 0xc 0xe2 0x94 0x5e 0x2e 0x1d 0x8b 0x23 0x
70 0xae 0x42 0x93 0x5 0xcd 0x94 0xe6 0x25 0xc0 0x56 0x6a 0x3f 0xcb 0x16 0x23 0x46 0xe8 0xe9 0x7 0x94 0x53 0x62 0xce 0xf1 0xcc 0xaa 0x94 0x1f 0xf3 0x21 0x3b 0x4a
0xaf 0x8f 0xf4 0xeb 0x4c 0xdf 0x80 0xb4 0xdb 0x37 0x6f 0x8e 0x21 0x4e 0x81 0x74 0xbd 0x6a 0x41 0x13 0xe2 0xc 0x88 0x76 0x7 0x11 0xe9 0x9 0xe0 0x28 0xbd 0x23 0x6
f 0xe7 0x14 0xa8 0x4e 0xaa 0x60 0x2f 0x1e 0xeb 0xbb 0xab 0x95 0x4d 0x15 0x67 0x7e 0xe5 0x9d 0x54 0xd3 0x61 0xb6 0x5 0xc 0x23 0x67 0xac 0x14 0x4e 0x40 0xb9 0xf0
13. Verify signature.
        Success.
14. Output the root certificates SHA256 hash (RKTH).
        Success.
        RKTH: 50d33d52ead85e475809fb09e91254a95b6f94636d3b6b7c51c374c105f229b4
15. Creating output image file.
        Success.
15.1 Writing output image to file.
        Success. (Signed image C:/Users/nxa06773/Documents/My Received Files/mcu-boot/bin/Tools/workspace/output_images/test_output-try.bin created.)
```



Options

☑ Simple Master in Strict Mode

☑ Smart Master in Strict Mode

Ma...r	Securi...level
⊟ Si...r	
D.	NS-User
D.	NS-User
H.	NS-User
P..	NS-User
S..	NS-User
U.	NS-User
U.	NS-User
⊟ S...r	
C..	NS-User
C..	NS-User

Sl...e	Secu...vel
A...0	NS-User
A...L	NS-User
A...L	NS-User
C...R	NS-User
C...E	NS-User
C...0	NS-User
C...1	NS-User
C...2	NS-User
C...3	NS-User
C...4	NS-User
D...X	NS-User
D...0	NS-User
D...1	NS-User
F...H	NS-User
F...0	NS-User
F...1	NS-User

Master type: Core 0 master (SAU/IDAU)

☑ Show details ☑ Merged SAU+IDAU

☑ Show Code ☑ Show Data ☑ Show Peripherals

	SAU+IDAU	MPC	Resulting security level	
USB SRAM (alias)	S	NS-User	Not Recommended	0x5 0x5
AHB peripherals 3...	S		...	0x5 0x5
AHB peripherals 2...	S		...	0x5 0x5
AHB peripherals 1...	S		...	0x5 0x5
AHB to APB bridg...	S		...	0x5 0x5
AHB to APB bridg...	S		...	0x5 0x5
USB SRAM	NS	NS-User	NS	0x4 0x4
AHB peripherals 3	NS		...	0x4 0x4
AHB peripherals 2	NS		...	0x4 0x4
AHB peripherals 1	NS		...	0x4 0x4
AHB to APB bridg...	NS		...	0x4 0x4
AHB to APB bridg...	NS		...	0x4 0x4
RAM 4 (alias)	S	NS-User	Not Recommended	0x3 0x3

Configuration - General Info

Configuration - HW Info

Processor: LPC55S69

Part number: LPC55S69JBD100

SDK Version: ksdk2_0

Project

TEE

Configures access policies for memory areas and peripherals helping to protect and isolate sensitive parts of application.

Generated code

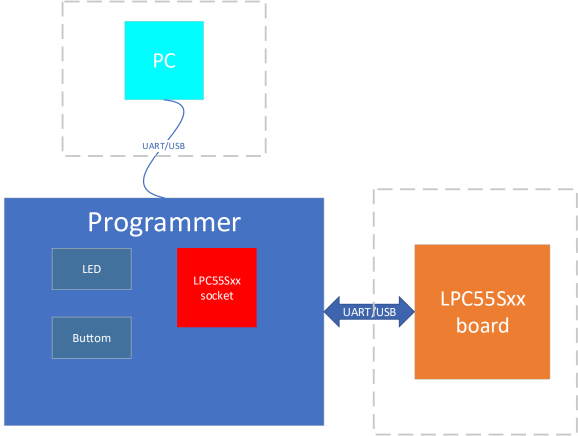
Target core not selected

type filter text

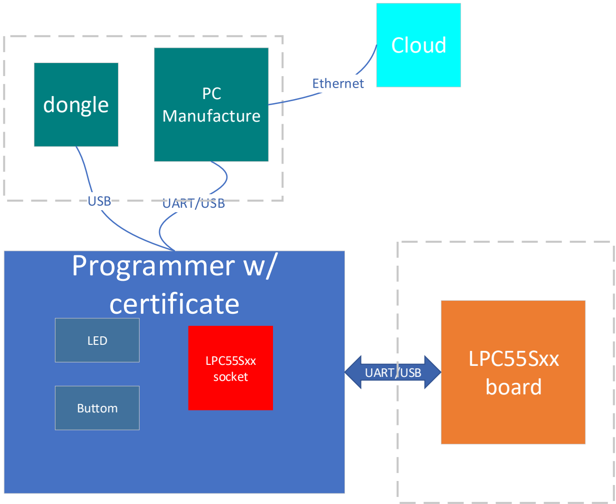
Level	Issue	Origin
i Informat	No toolchain project detect...	

安全编程器

- 通用编程器
  - Program encrypted image/Key/config info
  - Support chip and board programming
  - Programming count

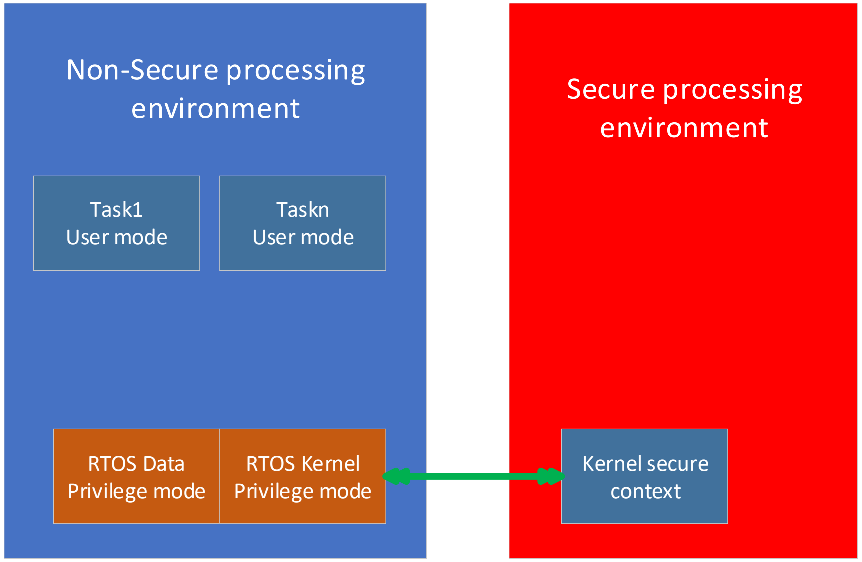


- 具有认证功能的编程器
  - Secure communication
  - Control/protect key by cloud end
  - Support dongle encryption
  - Support chip and board programming
  - Programming count



安全操作系统

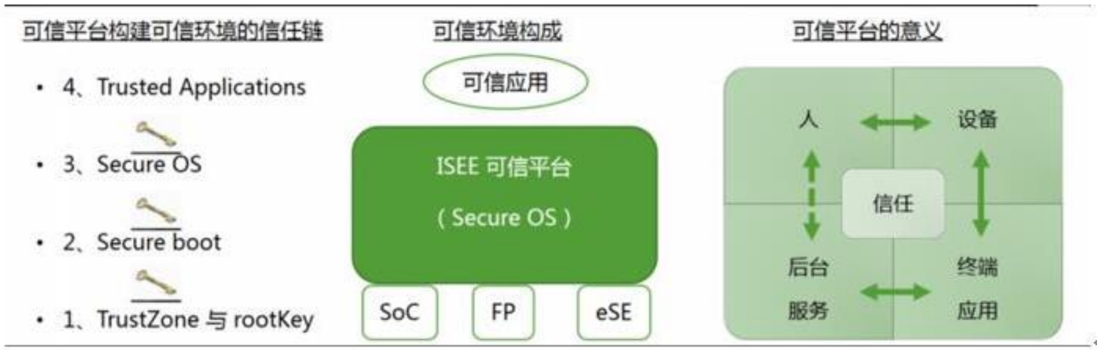
- SafeRTOS
  - Tasks run in Non-secure processing environment
  - Spatial Separation with MMU and Trustzone
  - Key context runs in secure processing environment
  - Demo from https://www.highintegritysystems.com/partners/nxp/



TEE完整解决方案

豆荚 Beanpod

青莲云

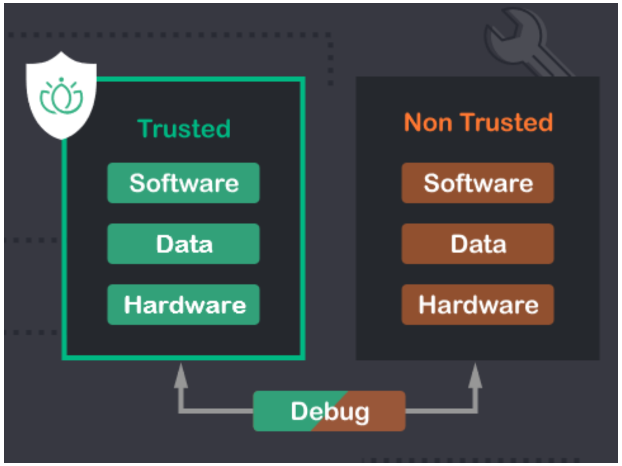


可信平台构建可信环境的信任链

- 4、Trusted Applications
- 3、Secure OS
- 2、Secure boot
- 1、TrustZone 与 rootKey

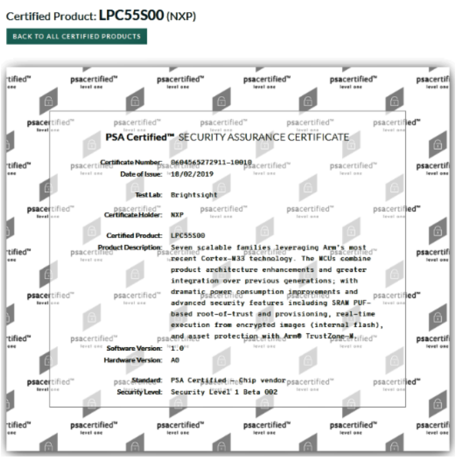
可信环境构成

可信平台的意义



安全认证

- ARM PSA Certified: building trust in IoT
- SESIP Certified: building trust in IoT
- BCTC Certified: building security in Personal Payment
- TrustedLabs pre-Certified: building trust in POS/IoT/Smart Meter

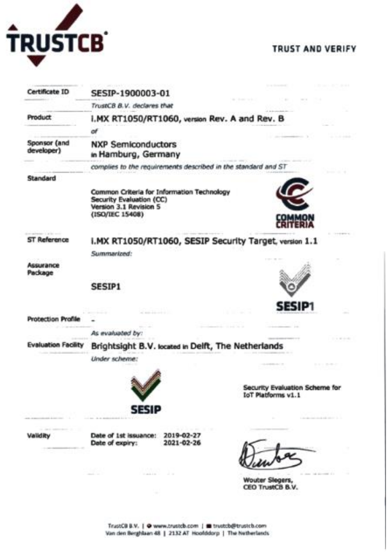


Certified Product: **LPC55S00** (NXP)

BACK TO ALL CERTIFIED PRODUCTS

PSA Certified™ SECURITY ASSURANCE CERTIFICATE

Certificate Number:	0604565272911-10010
Date of Issue:	18/02/2019
Test Lab:	Brightsight
Certificate Holder:	NXP
Certified Product:	LPC55S00
Product Description:	Seven scalable families leveraging Arm's most recent Cortex-M33 technology. The MCUs combine product architecture enhancements and greater integration over previous generations; with dramatic power consumption improvements and advanced security features including SRAM PUF-based root-of-trust and provisioning, real-time execution from encrypted images (internal flash), and asset protection with Arm® TrustZone-M.
Software Version:	1.0
Hardware Version:	A0
Standard:	PSA Certified - Chip vendor
Security Level:	Security Level 1 Beta 002



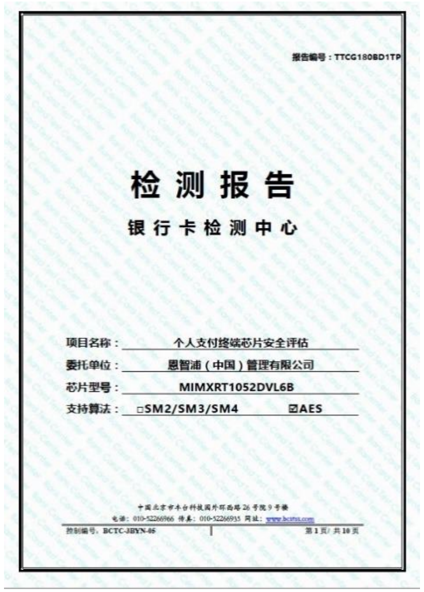
TRUSTCB

TRUST AND VERIFY

Certificate ID	SESIP-1900003-01
	TrustCB B.V. declares that
Product	I.MX RT1050/RT1060, version Rev. A and Rev. B
	of
Sponsor (and developer)	NXP Semiconductors in Hamburg, Germany
	complies to the requirements described in the standard and ST
Standard	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1 Revision 5 (ISO/IEC 15408)
ST Reference	I.MX RT1050/RT1060, SESIP Security Target, version 1.1
	Summarized:
Assurance Package	SESIP1
Protection Profile	-
	As evaluated by:
Evaluation Facility	Brightsight B.V. located in Delft, The Netherlands
	Under scheme:
	SESIP — Security Evaluation Scheme for IoT Platforms v1.1
Validity	Date of 1st issuance: 2019-02-27 Date of expiry: 2021-02-26

Wouter Slegers,
CEO TrustCB B.V.

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com
Van den Berghlaan 48 | 2132 AT Hoofddorp | The Netherlands



报告编号：TTCG180BD1TP

检测报告

银行卡检测中心

项目名称：个人支付终端芯片安全评估

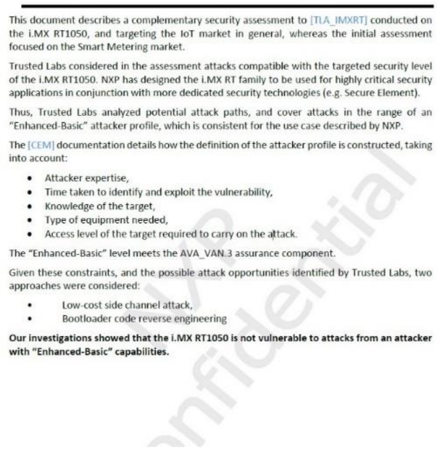
委托单位：恩智浦（中国）管理有限公司

芯片型号：MIMXRT1052DVL6B

支持算法：□SM2/SM3/SM4 ☑AES

中国北京市丰台科技园外环西路26号院9号楼
电话：010-52266966 传真：010-52266935 网址：www.bctest.com

控制编号：BCTC-JBYN-05 | 第1页/ 共10页



This document describes a complementary security assessment to [TLA_IMXRT] conducted on the i.MX RT1050, and targeting the IoT market in general, whereas the initial assessment focused on the Smart Metering market.

Trusted Labs considered in the assessment attacks compatible with the targeted security level of the i.MX RT1050. NXP has designed the i.MX RT family to be used for highly critical security applications in conjunction with more dedicated security technologies (e.g. Secure Element).

Thus, Trusted Labs analyzed potential attack paths, and cover attacks in the range of an "Enhanced-Basic" attacker profile, which is consistent for the use case described by NXP.

The [CEM] documentation details how the definition of the attacker profile is constructed, taking into account:

- Attacker expertise,
- Time taken to identify and exploit the vulnerability,
- Knowledge of the target,
- Type of equipment needed,
- Access level of the target required to carry on the attack.

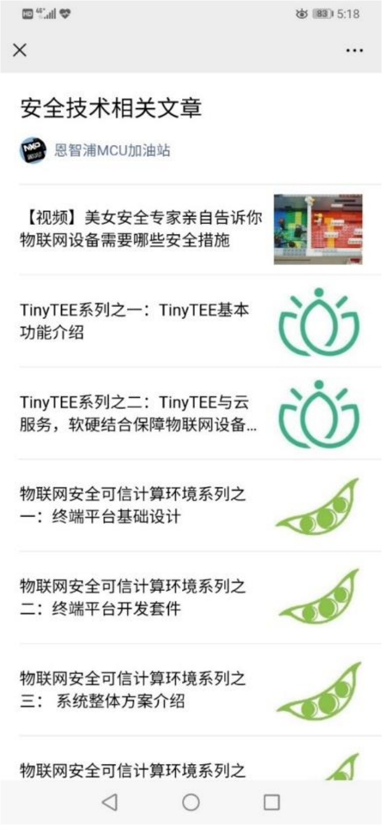
The "Enhanced-Basic" level meets the AVA_VAN.3 assurance component.

Given these constraints, and the possible attack opportunities identified by Trusted Labs, two approaches were considered:

- Low-cost side channel attack,
- Bootloader code reverse engineering

Our investigations showed that the i.MX RT1050 is not vulnerable to attacks from an attacker with "Enhanced-Basic" capabilities.

安全技术相关文章与视频



安全技术相关文章

恩智浦MCU加油站

【视频】美女安全专家亲自告诉你物联网设备需要哪些安全措施

TinyTEE系列之一：TinyTEE基本功能介绍

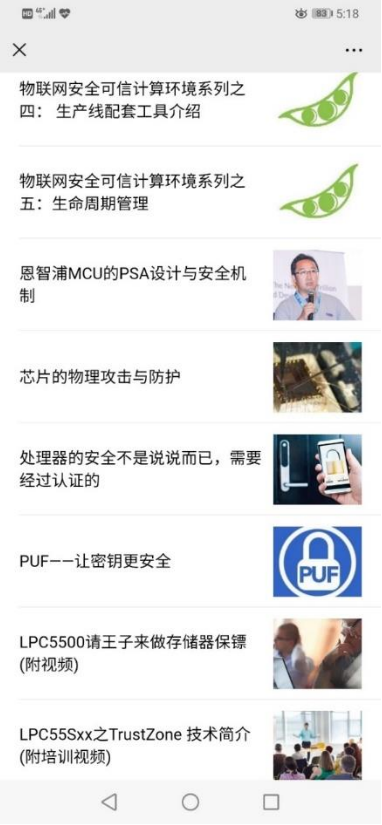
TinyTEE系列之二：TinyTEE与云服务，软硬结合保障物联网设备...

物联网安全可信计算环境系列之一：终端平台基础设计

物联网安全可信计算环境系列之二：终端平台开发套件

物联网安全可信计算环境系列之三：系统整体方案介绍

物联网安全可信计算环境系列之



物联网安全可信计算环境系列之四：生产线配套工具介绍

物联网安全可信计算环境系列之五：生命周期管理

恩智浦MCU的PSA设计与安全机制

芯片的物理攻击与防护

处理器的安全不是说说而已，需要经过认证的

PUF——让密钥更安全

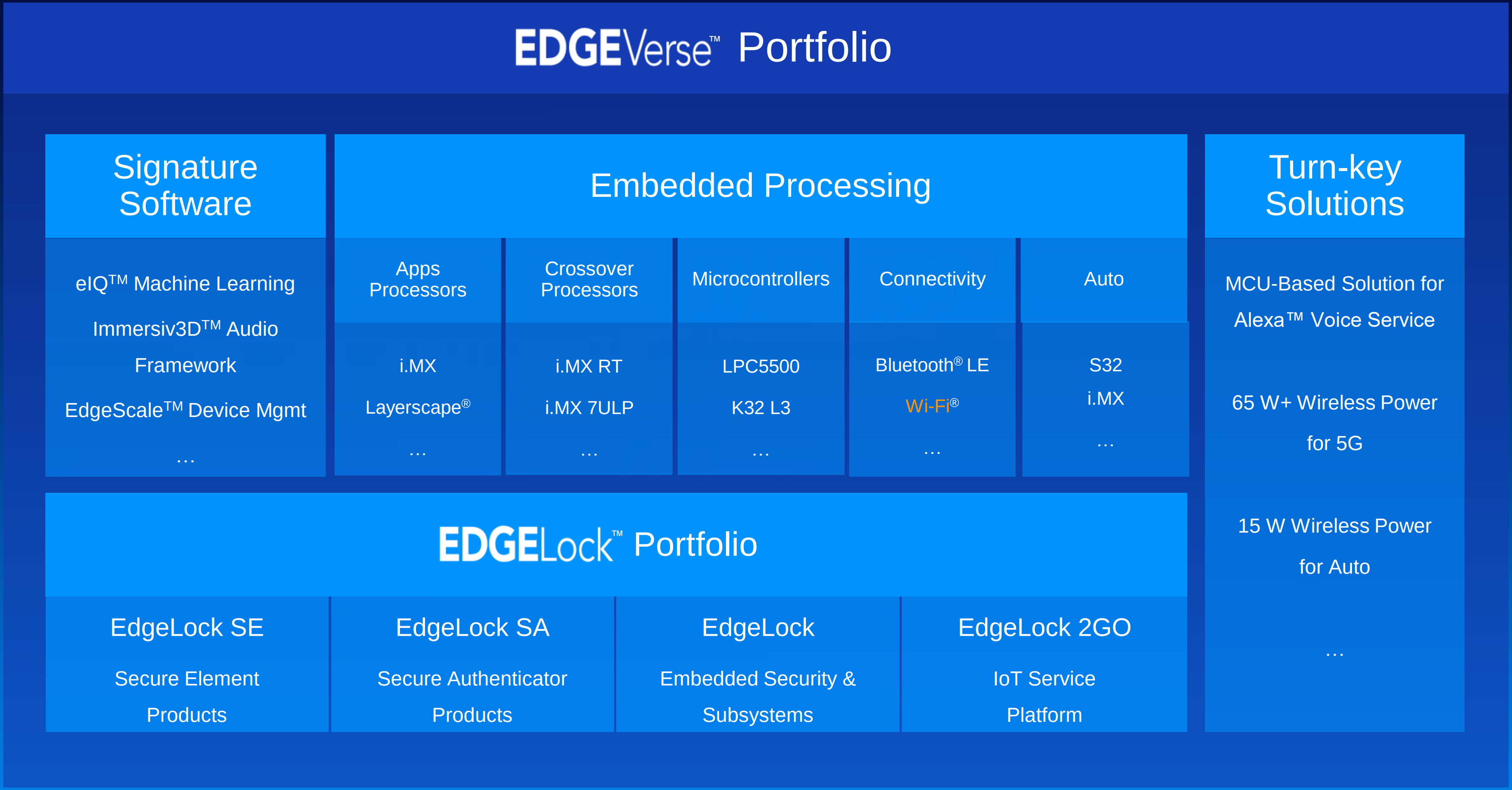
LPC5500请王子来做存储器保镖(附视频)

LPC55Sxx之TrustZone 技术简介(附培训视频)

EDGEVerse

NXP全面的边缘计算和安全平台

https://www.nxp.com.cn/applications/solutions/enabling-technologies/edgeverse:EDGE-COMPUTING?cid=wechat_iot_004311



EDGEVerse™ Portfolio

Signature Software

eIQ™ Machine Learning

Immersiv3D™ Audio Framework

EdgeScale™ Device Mgmt

…

Embedded Processing

Apps Processors	Crossover Processors	Microcontrollers	Connectivity	Auto
i.MX	i.MX RT	LPC5500	Bluetooth® LE	S32
Layerscape®	i.MX 7ULP	K32 L3	Wi-Fi®	i.MX
…	…	…	…	…

Turn-key Solutions

MCU-Based Solution for Alexa™ Voice Service

65 W+ Wireless Power for 5G

15 W Wireless Power for Auto

…

EDGELock™ Portfolio

EdgeLock SE	EdgeLock SA	EdgeLock	EdgeLock 2GO
Secure Element Products	Secure Authenticator Products	Embedded Security & Subsystems	IoT Service Platform

SECURE CONNECTIONS
FOR A SMARTER WORLD