LPC5500 MCU SERIES

INDUSTRIAL & IOT EDGE APPLICATIONS

CORTEX-M33 BASED MICROCONTROLLERS

MARC KUOCH – FAE MCU

JUNE 2019

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP's LPC55S6x Product Spotlight

Power Optimized Intelligence at the IoT Edge

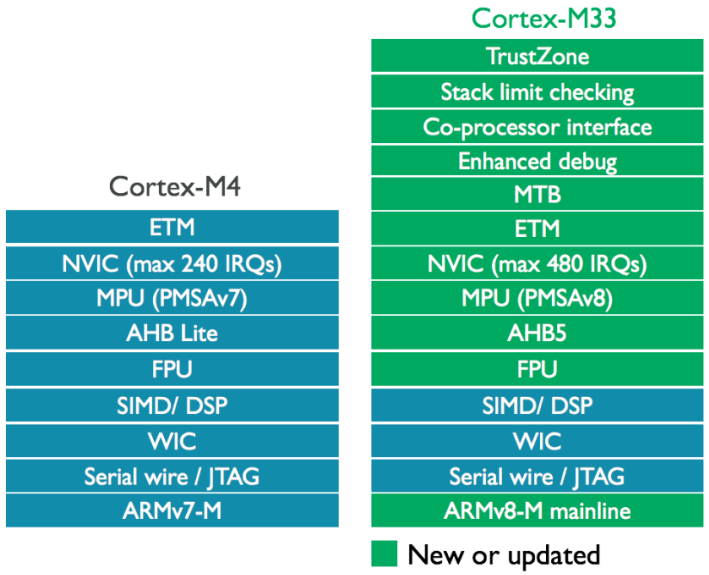
100 MHz Dual Cortex-M33-based MCU with TrustZone

- **Ultra-efficient processing**
  - As high as 755 CoreMarks[1] and as low as 32uA/MHz[2]
  - 10x improvement for signal processing & cryptography
- **Numerous interfaces to sense, connect, control**
- **Enhanced safety and security**
- **MCUXpresso developer ecosystem**

1: 2xCM33 @ 100MHz, **2:** 1xCM33 @ 100MHz

LPC5500 EFFICIENCY ADVANTAGES OVER COMPETITION

MARKET'S ONLY FULL ARMV8-M IMPLEMENTATION



Why Cortex-M33? Key Features and Comparisons

- **Nearly 20% performance improvement over Cortex-M3 based MCUs** (over 60% vs Cortex-M0) with redesigned pipeline - up to two instructions per clock cycle

	Cortex-M0+	Cortex-M23	Cortex-M3	Cortex-M4	Cortex-M33
DMIPS/MHz	**0.95**	0.98	1.25	1.25	**1.50**
CoreMark®/MHz	**2.46**	2.50	3.32	3.40	**3.86**

Prelim. Data from Arm for Cortex-M33 implementation at 40LP (9-track, typical 1.1v, 25°C)

- **TrustZone for system-wide, secure resource isolation** enabling trusted runtime execution and protection in embedded MCU applications

- **Tightly coupled accelerators with coprocessor interface & extensions,** including single precision FPU and NXP accelerators

NXP LPC5500 MCU SERIES

ROADMAP

Subject to Change

COMMON PLATFORM ARCHITECTURE FOR COMPLETE SCALABILITY

AREA & PERFORMANCE EFFICIENT

Advanced Efficiency & Integration

Balanced

Entry

LPC55S8x/8x
Rich Graphics

Up to 180 MHz Cortex-M33 (dual, PQ)
Up to 1.5MB Flash/512KB SRAM
Display Controller & Graphics Accel.
Trust Zone & Security ('S' version)

LPC55S7x/7x
Advanced Comms.

Up to 180 MHz Cortex-M33 (dual, PQ)
Up to 1.5MB Flash/512KB SRAM
100Mbps Ethernet, Dual CAN-FD, SDIO
Trust Zone & Security ('S' version)

LPC55S6x
High Efficiency

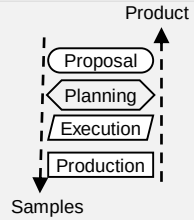
100 MHz Cortex-M33 (dual, PQ)
Up to 640KB Flash/320KB SRAM
SDIO
Trust Zone & Security ('S' version)

LPC55S2x/2x
Mainstream

100 MHz Cortex-M33
Up to 512KB Flash/256KB SRAM
SDIO
Security ('S' version)

LPC55S1x/1x
Baseline

100 MHz Cortex-M33
Up to 256KB Flash/80KB SRAM
Single CAN2.0



2018 2019 2020

Common features across families,

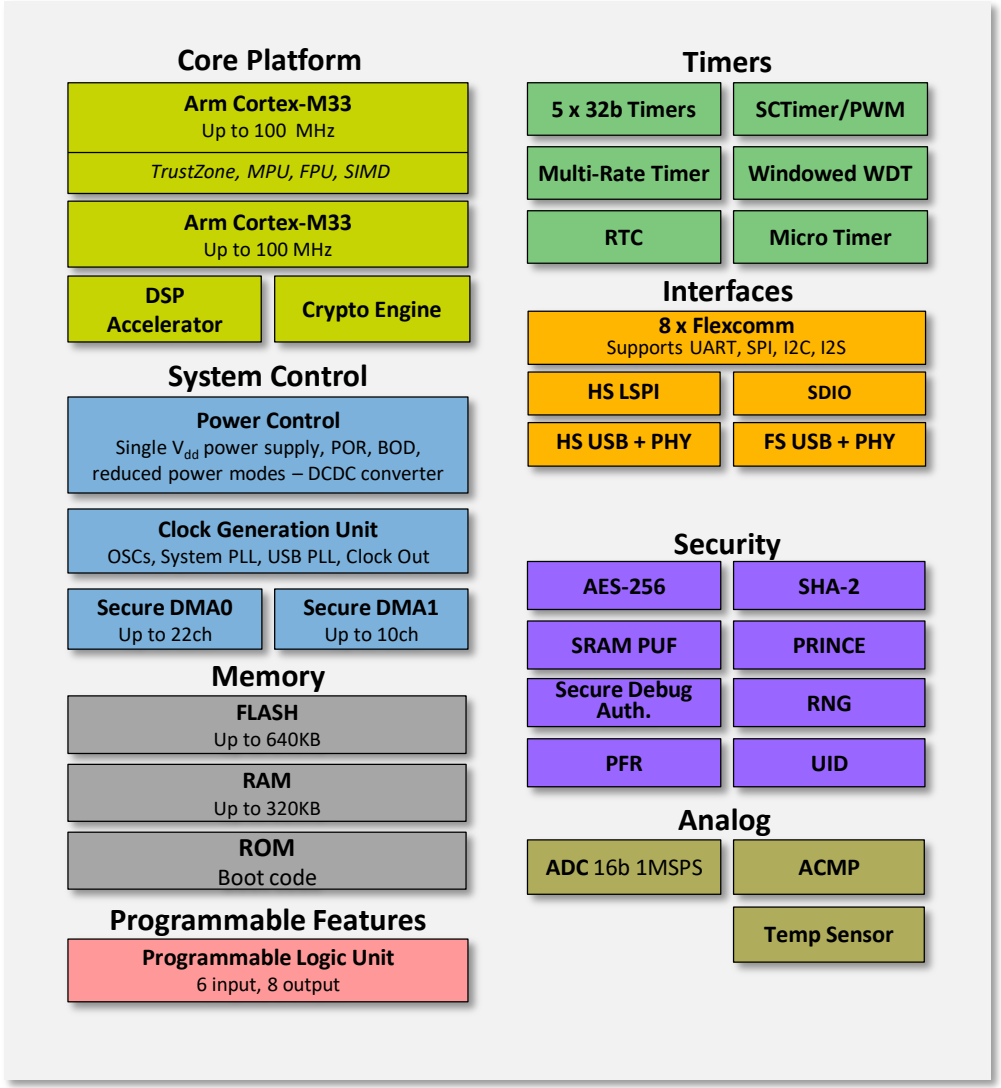
- FS USB (wo xtal)
- HS USB with PHY*
- 50MHz SPI,
- Up to 8/10 Serial Interfaces (FlexComm)
- I3C interface (LPC557x/8x families)
- Up to 2Msps 16-bit SAR ADC
- Comparator
- Temperature Sensor & RTC
- 1.8 to 3.6V
- -40 to 105 °C

**not available in all packages*

10Ku S/R is budgetary range; will vary for specific package/memory variants

LPC55S6X MCU FAMILY

- PERFORMANCE EFFICIENCY
- SIGNAL PROCESSING
- ENHANCED SECURITY FEATURES



Core Platform

- Up to 100MHz Cortex-M33
  - TrustZone, MPU, FPU, SIMD
- Up to 100MHz Cortex-M33
- Coprocessors
  - DSP Accelerator
  - Crypto Engine
- Multilayer Bus Matrix

Memory

- Up to 640KB FLASH (includes PFR)
- Up to 320KB RAM
- 128KB ROM

Timers

- 5 x 32b Timers
- SCTimer/PWM
- Multi-Rate Timer
- OS Timer
- Windowed Watchdog Timer
- RTC
- Micro Timer

Interfaces

- USB High-speed (H/D) w/ on-chip HS PHY
- USB Full-speed (H/D), Crystal-less
- SDIO, Support 2 cards
- 1 x High-Speed SPI up to 50MHz
- 8 x Flexcomms support up to 8x SPI, 8x I2C, 8x UART, 4x I^2S channels (total 8 instances)

Advanced Security Subsystem

- Protected Flash Region (PFR)
- AES-256 HW Encryption/Decryption Engine
- SHA-2
- SRAM PUF for Key Generation support
- PRINCE – On-The-Fly Encrypt/Decrypt for flash data
- Secure debug authentication
- RNG

Analog

- 16b ADC, 16ch, 1MSPS
- Analog Comparator
- Temperature Sensor

Packages

- LQFP100
- VFBGA98
- LQFP64

Other

- Programmable Logic Unit
- Buck DC-DC
- Operating voltage: 1.8 to 3.6V
- Temperature range: -40 to 105 °C

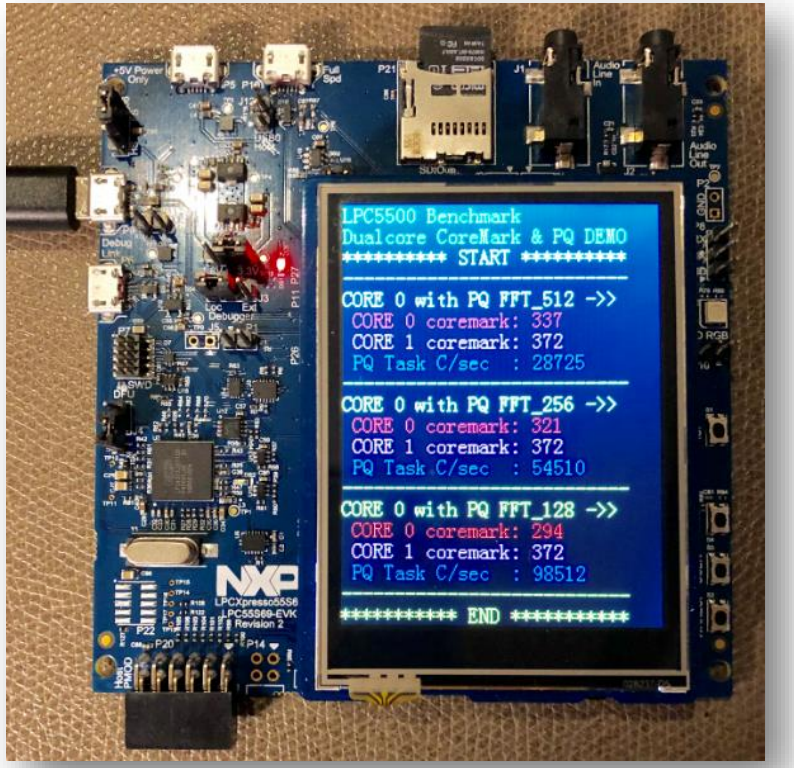
PERFORMANCE EFFICIENCY WITH DUAL CORE & POWERQUAD DSP

NXP's PowerQuad DSP

- **> 10x faster than CMSIS-DSP for most computing**
- **Energy Consumption Reduction for DSP Tasks**
- **4x 32b single-precision floating-point MAC**
- **Hardware accelerator for:**
  - FFT/IFFT/DCT/IDCT
  - FIR/Dual Biquad IIR
  - Convolution/Matrix
  - Trigonometric Functions/ CORDIC/Sqrt..

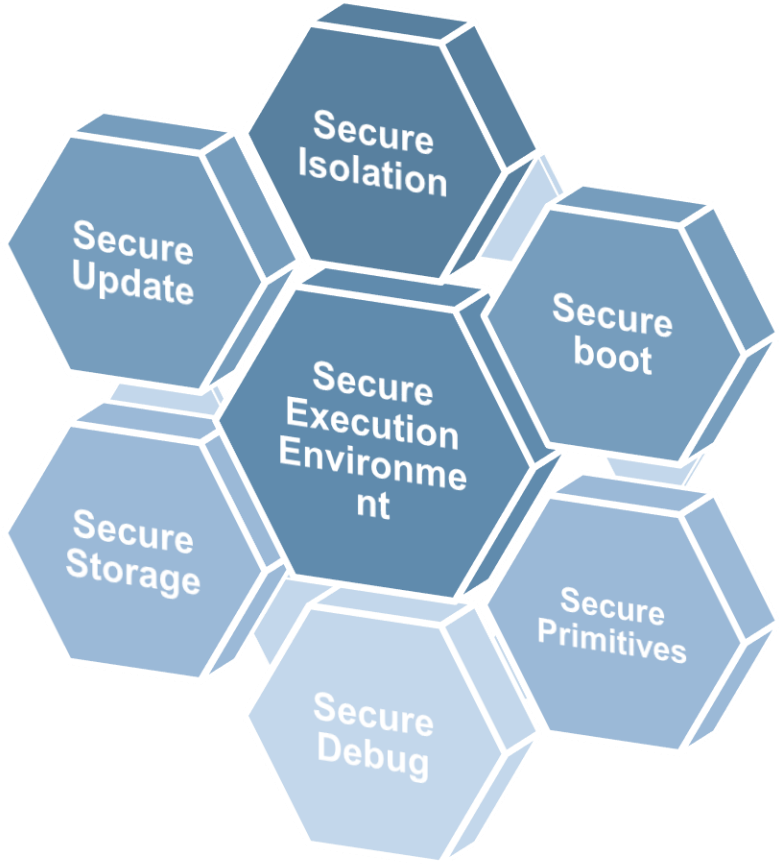
Mathematical Operation	Plain C FXP with -Ofast opt on Cortex M33	CMSIS DSP	PowerQuad DSP	HiFi4 DSP
FFT real N=32	6163	2295	**273**	586
FFT real inverse N=32	8951	2453	**329**	692
FFT real N=64	13856	5718	**465**	583
FFT real inverse N=64	20517	6009	**553**	657
FFT real N=128	30761	10798	**1066**	993

Demonstrating **>700 CoreMark** with dual Cortex-M33 and **simultaneous FFT computation**



SECURE EXECUTION ENVIRONMENT – SEE COMPONENTS

- Secure Isolation
  - Isolate secure and non-secure worlds
- Secure Boot
  - Execute only authorized firmware
- Secure Primitives
  - Cryptography Primitives – hashing, encryption, decryption, authentication
- Secure Storage
  - Secure Keys, Code and Data confidentiality
- Secure Update
  - OTA firmware update, revoke keys, anti-rollback
- Secure Debug
  - Only authenticated parties allowed to debug



NXP LPC5500 MCU SERIES

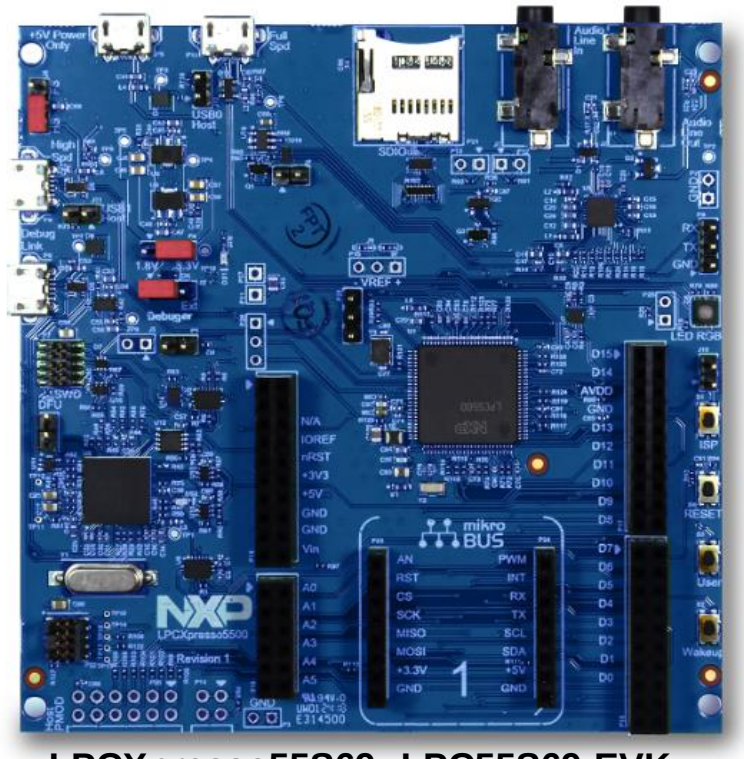
MCUXPRESSO SOFTWARE & TOOLS ECOSYSTEM

Complimentary with Extensive Support

- MCUXpresso SDK
- MCUXpresso IDE
- MCUXpresso Config Tools

Hardware Platform for Ease of Development

- On-board debug circuit
- PCB Layout, Schematic and Board Files Available



LPCXpresso55S69: LPC55S69-EVK

ARM KEIL Microcontroller Tools

IAR SYSTEMS

Simplify secure embedded development; Reduce time to market.

LPC5500 MCU Series

SERIES OVERVIEW & SCHEDULE

COMMON PLATFORM ARCHITECTURE FOR COMPLETE SCALABILITY

Common features across families,

- FS/HS USB with PHY, 50MHz SPI, up to 8/10 Serial Interfaces (FlexComm), plus I3C interface (LPC557x/8x families)
- Up to 2Msps 16-bit SAR ADC, Comparator, Temperature Sensor and RTC
- 1.8 to 3.6V, -40 to 105 °C

LPC5500 Family	Samples	Memory	CPU Freq	Dual Core	Security Features	DSP Accel.	FS&HS USB	SDIO	CAN-FD	10/100 ENET	Graphics Accel.	16-bit ADC & Comp.	Serial Interface
Graphics/HMI LPC558x/S8x	**Q1-20**	Up to 2MB Flash, 512KB SRAM	200 MHz Opt TZ	Yes	Opt.	Yes	Yes	Yes	2x	1x	Yes	Yes	10x FlexComm HS SPI, I3C
Large Memory LPC557x/S7x	**Q1-20**	Up to 2MB Flash, 512KB SRAM	200 MHz Opt TZ	Yes	Opt.	Yes	Yes	Yes	2x	1x	-	Yes	10x FlexComm HS SPI, I3C
Efficiency LPC55S6x	**Q4-18**	Up to 640KB Flash, 320KB SRAM	100 MHz Opt TZ	Yes	Yes	Yes	Yes	Yes	-	-	-	Yes	8x FlexComm, HS SPI
Mainstream LPC552x/S2x	**Q2-19**	Up to 512KB Flash, 256KB SRAM	100 MHz	-	-	-	Yes*	Opt.	-	-	-	Yes	8x FlexComm, HS SPI
Entry LPC551x/S1x	**Q3-19**	Up to 256KB Flash, 96KB SRAM	100 MHz Opt TZ	-	Opt.	-	Yes*	-	Yes*	-	-	Yes	8x FlexComm, HS SPI
Flashless MCU LPC550x	**Q2-20**	0KB Flash, 96KB SRAM	100 MHz Opt TZ	-	-	-	Yes	Yes	-	-	-	Yes	8x FlexComm, HS SPI

*HS USB/CAN-FD not available on all part numbers within the family, check data sheet for specific configurations

HIGHLIGHTS

- **Main Highlights of LPC5500**
  - World's First General Purpose Cortex-M33 based MCU in the market Today
  - Leading Performance Efficiency with 32uA/MHz in Active Mode
  - PowerQuad DSP for math intensive functions
  - Advanced security featuring TrustZone, SRAM PUF, real-time encryption/decryption, etc
  - Pin and Software Compatibility across the LPC5500 MCU Series
  - Robust Enablement with MCUXpresso Software & Tools

- **Start your Development Now!**
  - **www.nxp.com/LPC55S69-EVK**

Resources

LPC5500 MCU Series Homepage

LPC55S6x Product Summary Page

LPC55S6x Datasheet

Achieving Secure Execution Environments on Resource-Constrained, Low-Power MCUs

Reaching New Levels of Performance and Signal Processing with Arm Cortex-M33's Co-Processor Interfaces

Secure your Sensor with LPC5500 series

LPC55S69 Security Solutions for IoT

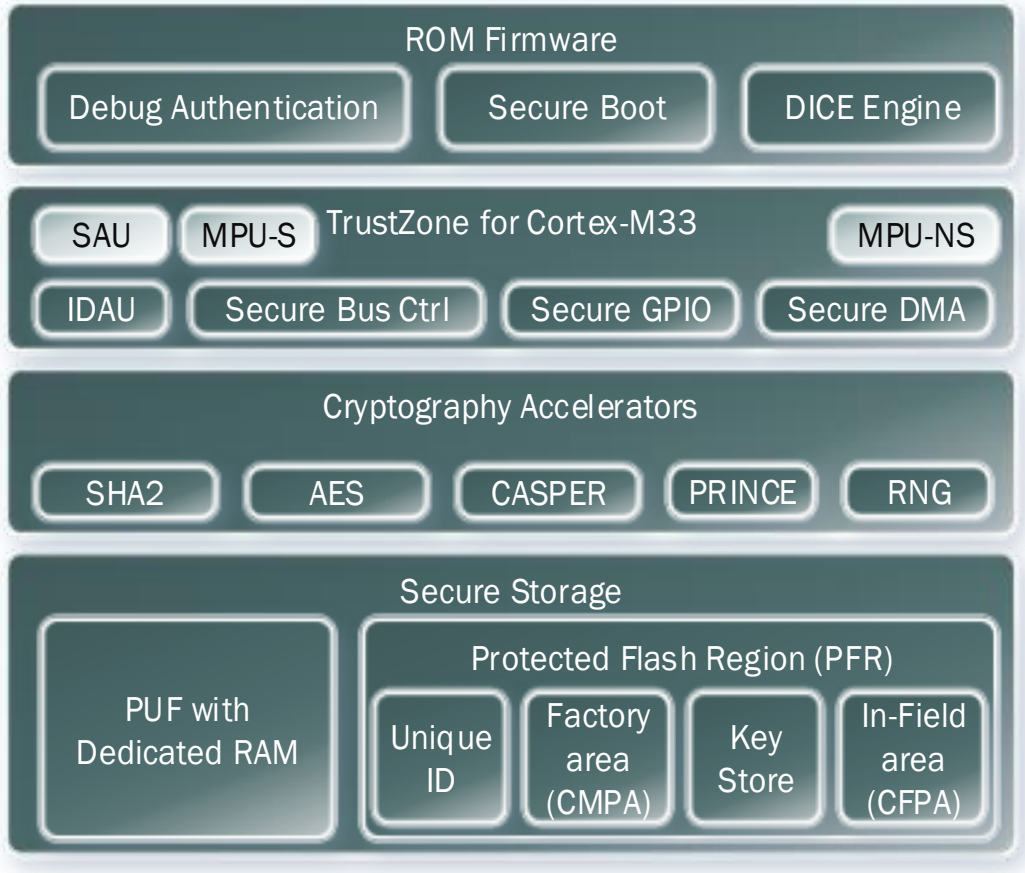
LPC55Sxx usage of the PUF and Hash Crypt to AES coding

LPC55Sxx Secure Boot

SECURITY

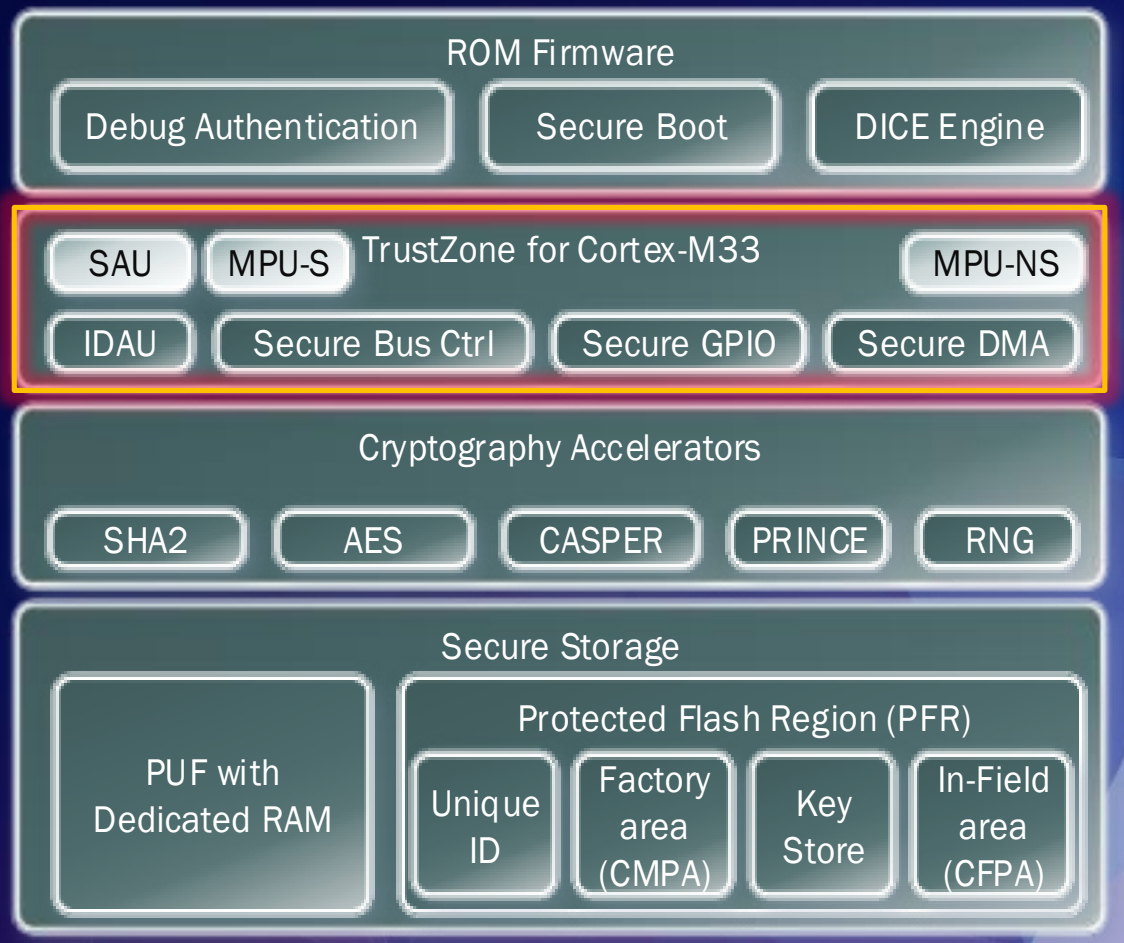
SECURITY SUBSYSTEM OVERVIEW

- **ROM supporting**
  - Secure Boot, Debug Authentication & DICE Engine
- **TrustZone for Cortex-M33**
  - Arm's Security Attribution Unit (SAU)
  - Arm's Memory Protection Unit (MPU): Secure & Non-Secure
  - NXP's Defined Attribution Unit (using IDAU interface)
  - NXP's Secure Bus, Secure GPIO & Secure DMA Controllers
- **Cryptography Accelerators**
  - Symmetric (AES-256) & Hashing (SHA2) engine
  - On-the-fly flash encryption/decryption engine (PRINCE)
  - Asymmetric engine for RSA and ECC (CASPER)
  - Random Number Generator (RNG)
- **Secure Storage**
  - Physically Unclonable Function (PUF)
    - Device unique root key (256 bit strength), 64-4096 bit key size
  - Protected Flash Region
    - RFC4122 compliant 128-bit UUID per device
    - PUF Key Store (Activation code, Prince region key codes, FW update key encryption key, Unique Device Secret)
    - Customer Factory Programable Area (Boot Configuration, RoT key table hash, Debug configuration, Prince configuration)
    - Customer In-Field Programable Area (Monotonic counter, Prince IV codes)



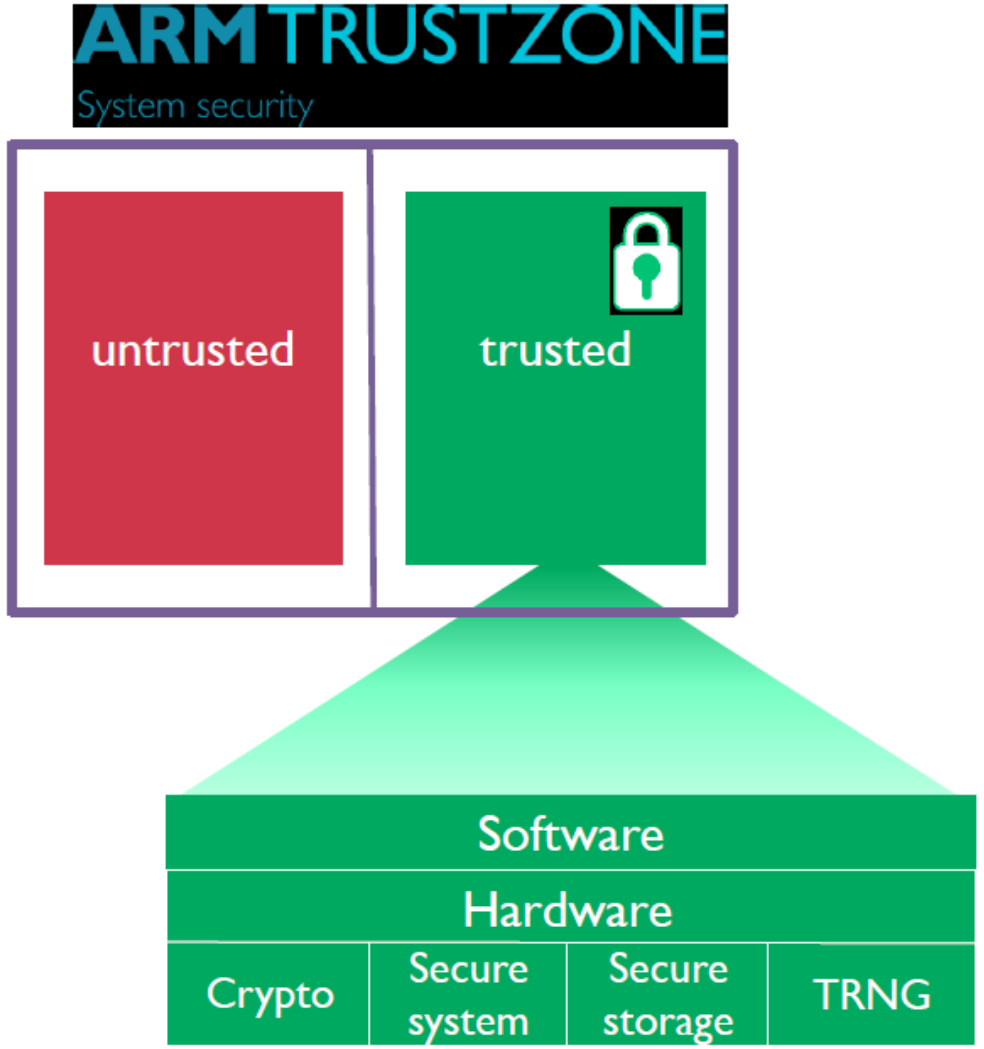
TrustZone-M Sub-system

- Secure Bus Controller
- Device Attribution Unit (IDAU)
- Secure GPIO
- Secure DMA

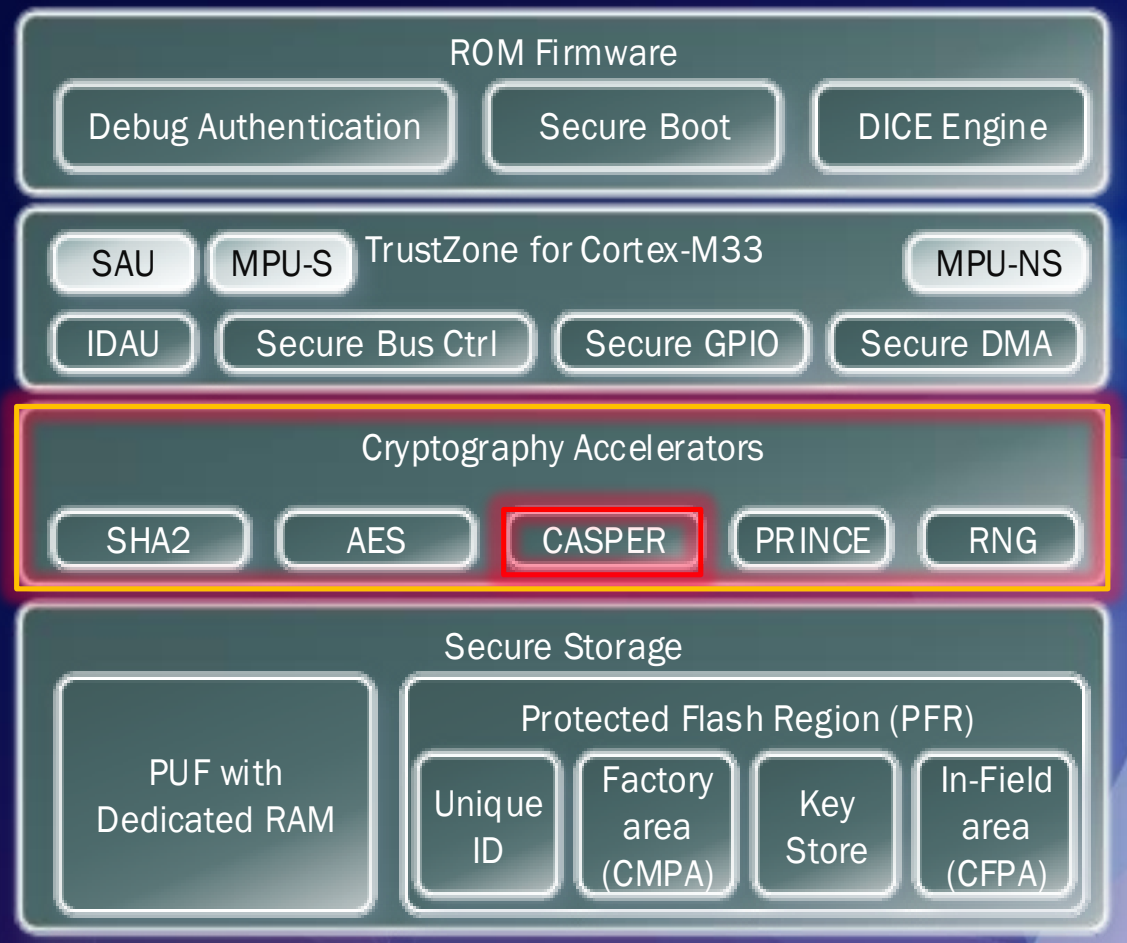


TrustZone for ARMv8-M Architecture M23/33 Core

- 2 Areas (trusted & untrusted)
- Separation and access control of your ROM code
- Isolate trusted software
- Trusted software placed in trusted Area
  - *Access only with 1 instruction possible*



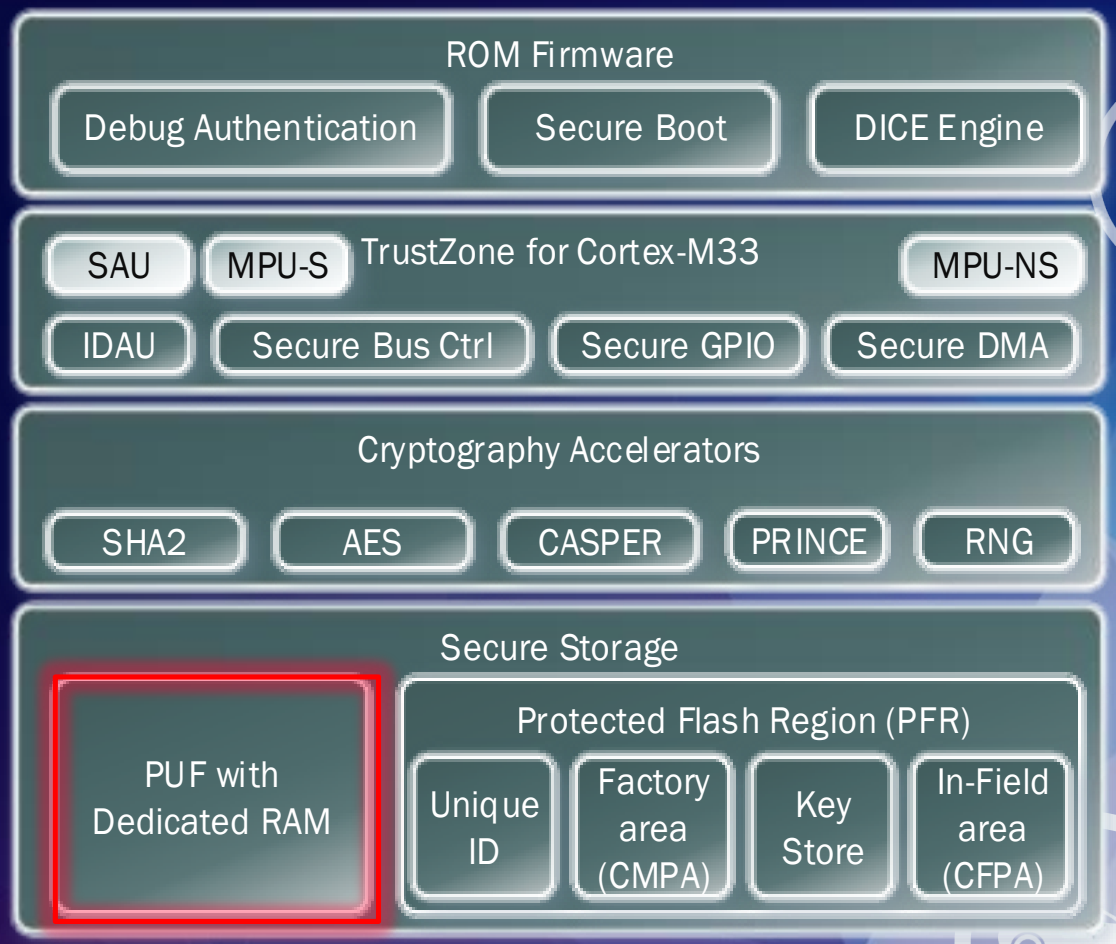
CASPER


ROM Firmware
Debug Authentication
Secure Boot
DICE Engine
SAU
MPU-S
TrustZone for Cortex-M33
MPU-NS
IDAU
Secure Bus Ctrl
Secure GPIO
Secure DMA
Cryptography Accelerators
SHA2
AES
CASPER
PRINCE
RNG
Secure Storage
PUF with Dedicated RAM
Protected Flash Region (PFR)
Unique ID
Factory area (CMPA)
Key Store
In-Field area (CFPA)

Asymmetric Cryptography Accelerator (CASPER)

- **Challenges of Asymmetric cryptography**
  - Require (very-)large number mathematical operations
  - SW-only approach is painfully slow & Power-hungry
  - Algorithms continue to evolve
    - new ECC curves
      - OpenSSL baseline NIST curves: Curves with 256b, 384b and 521b (National Inst. Of Standards & Technology)
        - Services like Google and Amazon claim ECC curves, after Snowden
- **Cryptographic Accelerator and Signaling Processing Engine with RAM-sharing (CASPER)**
  - Hardware accelerator engine
  - Safe time, effort and power consumption

PUF


ROM Firmware
Debug Authentication
Secure Boot
DICE Engine
SAU
MPU-S
TrustZone for Cortex-M33
MPU-NS
IDAU
Secure Bus Ctrl
Secure GPIO
Secure DMA
Cryptography Accelerators
SHA2
AES
CASPER
PRINCE
RNG
Secure Storage
PUF with Dedicated RAM
Protected Flash Region (PFR)
Unique ID
Factory area (CMPA)
Key Store
In-Field area (CFPA)

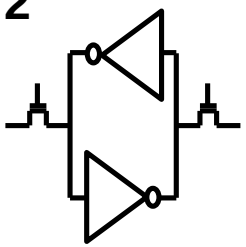
SRAM PUF Technology

1

Process Variation

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

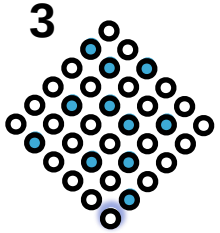
2



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

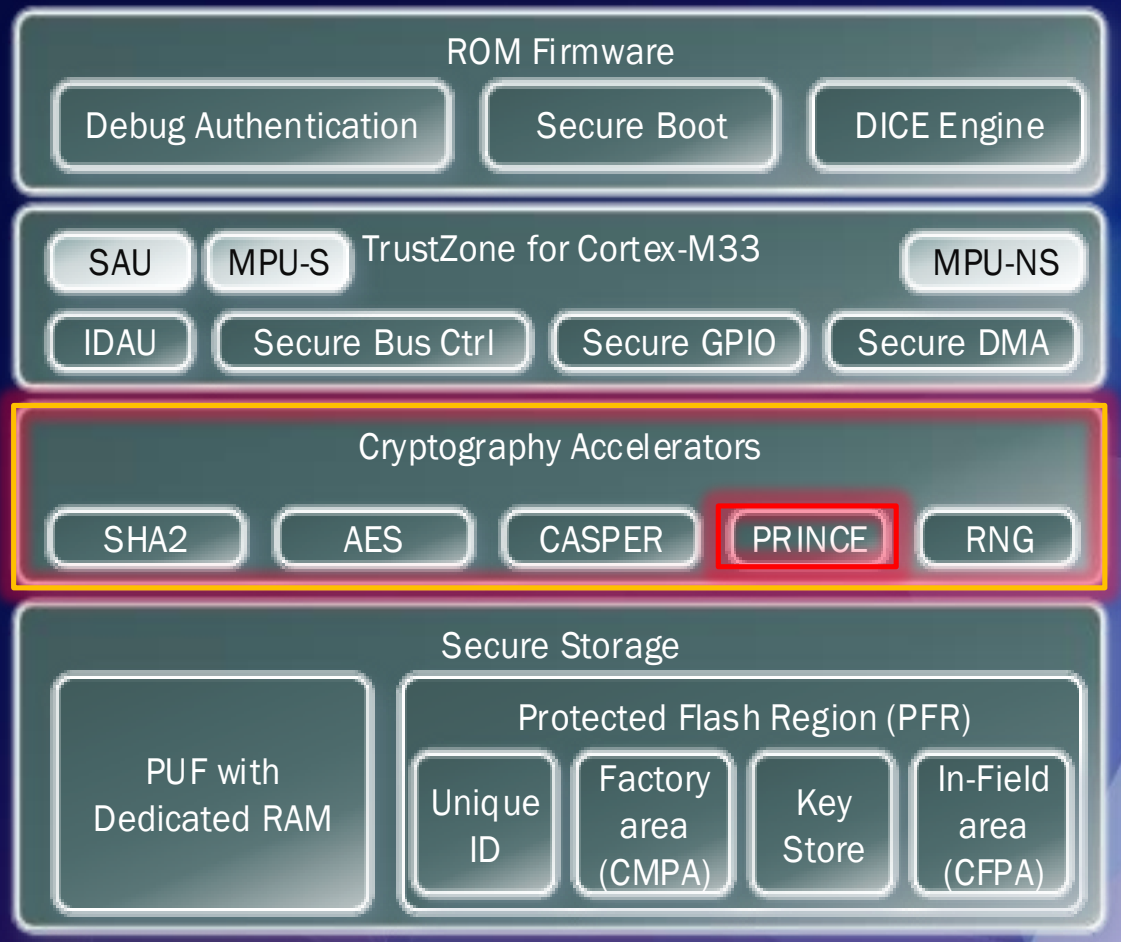
SRAM PUF Key

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

SRAM PUF Benefits

- Device-unique, unclonable fingerprint
- No key material programmed

PRINCE


ROM Firmware
Debug Authentication
Secure Boot
DICE Engine
SAU
MPU-S
TrustZone for Cortex-M33
MPU-NS
IDAU
Secure Bus Ctrl
Secure GPIO
Secure DMA
Cryptography Accelerators
SHA2
AES
CASPER
PRINCE
RNG
Secure Storage
PUF with Dedicated RAM
Protected Flash Region (PFR)
Unique ID
Factory area (CMPA)
Key Store
In-Field area (CFPA)

PRINCE

- Is a cryptographic algorithm **developed by NXP** + 2 Universities
  - https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2012/529&version=20140612:115014&file=529.pdf
- On the fly encryption / decryption
  - 64b block cipher, with 128b crypto key
  - Same HW block supports encrypt and decrypt
- Real-time
  - Low latency decryption, no additional cycles added to read path (compared to 10-14 cycles in AES)
  - No initialization time
  - Combinatorial logic
- Efficient
  - Low cost (Si area)
  - Power efficient
  - No RAM buffers needed

SECURE CONNECTIONS
FOR A SMARTER WORLD