STM32L5 MCU Series
Excellence in Ultra-low-power with More Security
Main Challenges for Embedded Design

• **Security**
  - Increase the robustness against attacks

• **Low power consumption**
  - Long life time, small battery size

• **Integration, performance, ecosystem**
  - Best fit versus the application requirements
First STM32 Based on Cortex-M33

STM32L5 is the answer

• More security with TrustZone and ST security implementation
  • HW to increase resistance to logical and board level attack

• Lower Power consumption
  • STM32 ultra-low-power technology

• Integration, performance, ecosystem
  • More performance, choice of packages and wide ecosystem
STM32L5
Security
ST implementation provides high granularity of isolation

- Each GPIO or peripheral, DMA channel, clock configuration register, ART or small part of Flash or SRAM can be configured as **Trusted** or **un-Trusted**

- **Full isolation** of trusted and non-trusted world
TrustZone provides full isolation

Example of IoT application implementation

```
STM32L5

- Un-Trusted Application
  - RF

- Trusted Application
  - Sensors
```
Security: TrustZone and Privileged

- More partitioning
- Possibility to separate the trusted and un-trusted area with **privileged and un-privileged** zone
- Strong *granularity* to define each part of memory or each peripheral, DMA channel as privileged or un-privileged
TrustZone: Example

STM32L5

Un-Trusted

Privileged

Un-Trusted & Privileged

RTOS

Trusted

Privileged

Trusted & Privileged

Secured Keys

Secured Boot

Un-Trusted & Un-Privileged

RF Stack

Secured data

Sensor IP

RF

Sensors
A Full Set of Security

**ENCRYPTION**
- AES-128/256 Encryption
- SHA-256 Authentication
- Public Key Acceleration (PKA): for RSA, Diffie-Hellmann or ECC (Elliptic Curve Cryptography)
- Certified Crypto library
- True Random Number Generator
- Unique ID
- OTP Zone

**DECRIPTION**

**AUTHENTICATION**

**MEMORY & IP PROTECTION**
- Active and static Anti-tamper detection
- Memory Protection Unit (MPU)
- Secure Boot
- Read and Write Protection
- HDP (Hide Protect)
- Unique Boot Entry
- OTFDEC (On-the-fly decryption) on Octo SPI to protect external memory
- JTAG fuse
- TrustZone
- SFI (Secure Firmware Installation)
STM32L5
Power Efficiency
Extend the Battery Life Time

• STM32L5 reuses the STM32L4/L4+ technology achieving best-in-class power consumption

• STM32L5 integrates an optional SMPS (DC/DC buck voltage regulator) which can be enabled/disabled on the fly to avoid external noise for external RF or data acquisition.

• Proven by EEMBC test results: 370 ULPMark-CP, 54 ULPMark-PP
# Ultra-low-power Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Current Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_BAT</td>
<td>3 nA / 187 nA*</td>
</tr>
<tr>
<td>Shutdown</td>
<td>17 nA / 122 nA*</td>
</tr>
<tr>
<td>Standby</td>
<td>108 nA / 222 nA*</td>
</tr>
<tr>
<td>Standby + 4-Kbyte RAM</td>
<td>272 nA / 386 nA*</td>
</tr>
<tr>
<td>Stop 2 (full retention: 256-Kbyte RAM)</td>
<td>3.0 µA / 3.1 µA*</td>
</tr>
<tr>
<td>Sleep</td>
<td>26 µA / MHz</td>
</tr>
<tr>
<td>Run up to 110 MHz</td>
<td>Down to 62 µA / MHz</td>
</tr>
</tbody>
</table>

**Note:** * without RTC / with RTC

**Best power consumption numbers with full flexibility**

- **Wake-up time:**
  - 250 µs
  - 14 µs
  - 14 µs
  - 5 µs
  - 6 cycles

- **Wake-up sources:**
  - reset pin, 5 I/Os, RTC
  - + BOR, IWDG
  - + all I/Os, PVD, COMPs, I^2C, LPUART, LPTIM
  - any interrupt or event

- **Tamper detection:** 3 I/Os, RTC
More Performance

Better responsiveness of the application

- **New** Arm® Cortex®-M33 performance: +20% versus Cortex-M4
  - 1.5 DMIPS/MHz
  - 4.02 CoreMark/MHz
  - 165 DMIPS
  - 442 CoreMark

- **New** ST ART Accelerator™: working both on internal and **external** Flash
  - 8 Kbytes of instruction cache
## High Integration and Innovation

Large memory, USB Type-C™ w/ power delivery controller, CAN FD

<table>
<thead>
<tr>
<th>Parallel interface</th>
<th>Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSMC 8-/16-bit (TFT-LCD, SRAM, NOR, NAND)</td>
<td>USB Device Crystal-less, USB Type-C and PD, 1x SD/SDIO/MMC, 3 x SPI, 4 x I²C, 1x CAN FD, 1 x Octo-SPI, 5 x USART + 1 x LPUART</td>
</tr>
<tr>
<td><strong>Digital</strong></td>
<td>Encryption</td>
</tr>
<tr>
<td>2x SAI, DFSDM (4 channels)</td>
<td>AES (256-bit), PKA, SHA-1, SHA-256, TRNG, CRC, OTFDEC</td>
</tr>
<tr>
<td><strong>Timers</strong></td>
<td>Analog</td>
</tr>
<tr>
<td>14 timers including: 2x 16-bit advanced motor control timers, 2x LPUART timers, 3x 16-bit-timers, 2 x 32-bit timers</td>
<td>2 x 12-bit ADC 12/16 bits, 5 MSPS, 2 x DAC, 2x comparators, 2 x op amps, 1 x temperature sensor</td>
</tr>
<tr>
<td><strong>I/Os</strong></td>
<td><strong>256-Kbyte RAM</strong></td>
</tr>
<tr>
<td>Up to 115 I/Os Touch-sensing controller</td>
<td>Up to 512-Kbyte Flash memory Dual Bank</td>
</tr>
</tbody>
</table>

**ARM® Cortex®-M33 CPU**
- 110 MHz
- TrustZone®
- FPU
- MPU
- ETM

**DMA**

**ART Accelerator™**
Large Portfolio

7 packages, several options

Legend:
- without HW crypto
- with HW crypto
## STM32L ULP Portfolio

**STM32L5** completes the ultra-low-power subclass

### Cost-smart ULP champion
- **STM32L0**
  - Cortex-M0+ at 32 MHz
    - 1.65 to 3.6V
  - 8-/16-bit applications
  - Wide range of pin-counts
  - 3 product lines, Cost-effective, Smaller packages, USB, LCD, Analog
  - 8 to 192 Kbytes of Flash, Up to 20 Kbytes of SRAM

### Broad-range foundation
- **STM32L1**
  - Cortex-M3 at 32 MHz
    - 1.65 to 3.6V
  - Wide choice of memory sizes
  - 3 product lines, USB, LCD, AES, Rich Analog
  - True EEPROM, Dual-bank Flash memory (RWW), 32 to 512 Kbytes of Flash, Up to 80 Kbytes of SRAM

### ULP With performance
- **STM32L4**
  - Cortex-M4 w/ FPU at 80 MHz
    - 1.71 to 3.6V
  - High-performance, advanced analog circuits
  - 5 product lines, 5-MSPS ADC, PGA, Compar., DAC, Op Amp, USB OTG, LCD, AES
  - 64 Kbytes to 1 Mbyte
  - Up to 320 Kbytes of SRAM

### ULP with more performance
- **STM32L4+**
  - Cortex-M4 w/ FPU at 120 MHz
    - 1.71 to 3.6V
  - Wide choice of memory sizes
  - 3 product lines, 5-MSPS ADC, PGA, Compar., DAC, Op Amp, USB OTG, LCD, AES
  - 1 to 2 Mbytes of Flash, Up to 640 Kbytes of SRAM

### Advanced security
- **STM32L5**
  - Cortex-M33 w/ FPU at 110 MHz
    - 1.71 to 3.6V
  - Wide choice of memory sizes
  - 1 product line, 5-MSPS ADC, PGA, Compar., DAC, Op Amp, USB Type C, AES
  - 256 to 512 Kbytes of Flash, 256 Kbytes of SRAM
A Complete Ecosystem
STM32CubeL5
One-stop-shop Software Package

STM32Cube MCU Packages

STM32Cube MCU Middleware

- FreeRTOS
- FatFS file system
- mbedTLS and mbedCrypto
- USB Device stacks

STM32Cube HAL & LL drivers

Peripheral drivers

- HAL API
  Hardware Abstraction Layer, highly portable and easy to use
- LL APIs
  Low-Layer APIs, light weight and highly optimized for runtime efficiency

STM32Cube Middleware

Generic Middleware
- FreeRTOS
- FatFS file system
- mbedTLS and mbedCrypto
- USB Device stacks

Dedicated Middleware
- Secure Boot and Secure Firmware Update
- TF-M for trusted execution environment
- USB-PD device driver
- STM32 Touch Sensing library

Project Examples

STM32CubeMX ready
More than 300 project examples for KEIL, IAR and STM32CubeIDE toolchains, with a STM32CubeMX configuration file

www.st.com/stm32cubel5
SBSFU and TF-M in STM32CubeL5

Reference code framework to implement a Trusted Execution Environment

**STM32L5**

- **Un-Trusted, Un-Privileged**
- **Un-Trusted Privileged**
- **TF-M (Application Root of Trust)**
- **TF-M (PSA Root of Trust)**
- **SBSFU TF-M (PSA immutable Root of Trust)**

**TF-M Framework**

- Isolation and Secure execution
- Secure services (crypto, initial attestation, secure storage)
- Easy addition of user secure services
- Leveraging STM32L5 security features

**SBSFU TF-M**

- Secure Boot
- Secure Firmware Update
STM32L5 is One of the First MCU PSA Level 2 Certified
STM32CubeIDE

All-in-1 STM32 development tool

- STM32CubeMX integrated
- TrustZone support
  - TrueSTUDIO / SW4STM32 importer
  - Advanced editor
  - GNU C/C++ for Arm® toolchain
- GDB and OpenOCD debugger
- Support of ST-Link and J-Link debug probes
Partners IDEs Development Flow

Arm V8-M TrustZone architecture support

STM32CubeMX

STM32CubeMX enhanced for TrustZone
- Peripherals/middleware configuration
- Resources allocation to security domains

Optional step

IDEs

Compile and Debug

TrustZone Support
- Partners IDE
- STM32CubeIDE based on Eclipse
- TrustZone debugging

STM32 Programming Tool

STM32CubeProgrammer
- Device and memory configuration
- Program the application
- Secure Firmware Install
Configuration Tool

- Power Consumption Calculator
- MCU or board Selector
- Code Generation
- Load an Example .ioc file
- Pinout Configuration
- Clock Tree Initialization
- Peripherals Configuration
- TrustZone configuration and GPIOs, memories, DMA, peripherals allocation to security domains

- Middleware Parameters
- FreeRTOS
- FatFS
- USB device

- TrustZone support

- macOS®
- Windows
All-in-one Programming Software Tool

- Intuitive GUI
- Command Line Interface for scripting
- API DLL for Custom Integration
- STLink (JTAG, SWD)
- STM32 Bootloader Interface (USB, UART, SPI, I2C, CAN)
- Secure Firmware install (SFI)

- MCU Internal Flash and external Flash services
- MCU configuration (Option bytes)
STM32L5 Hardware Solutions

Speed-up evaluation, prototyping and design

- **Evaluation Boards**
  - Full feature STM32L5 evaluation
    - STM32L552E-EV
  - STM32L562E-DK

- **Discovery Kit**
  - Flexible prototyping & demo
    - STM32L562E-DK

- **Nucleo Boards**
  - Affordable and quick prototyping
    - NUCLEO-L552ZE-Q
Prototype your wearable or sensor application with STM32L562E-DK

**Key Features**

- STM32L562 MCU with AES and PKA
- 240 x 240 pixel-TFT color Display
- state-of-the-art Energy Meter
- 3D accelerometer and 3D gyroscope
- Bluetooth® V4.1 low energy module
- Audio Codec and Headphone amplifier
- Digital microphone
- USB Type-C™ Sink device FS
- 512Mbit Octal Flash memory extension
- ST-Link V3
- STMod+ connector with fan-out expansion board for Wi-Fi®, Grove and mikroBUS™ compatible connectors
STM32CubeMonitor-power

State-of-the art on-board power consumption measurement

STM32L562E-DK

On-board Energy Meter
300 nA to 150 mA measurement range
Secure Your Production Flow
with Secure Firmware Install (SFI)

Protect your code and control the number of products manufactured

Customer premises

- FW
- ST Hardware
- Secure Module (HSM)
- Encrypted FW
- Store encryption key and production counter into HSM

Untrusted environment

- STM32L5
- SFI
- Authenticate target STM32
- Generate installation license
- Encrypted FW transfer
- HSM physical transfer
- Number of products controlled
- HSM
STM32L5 helps designers to answer to IoT challenges

- More security
- Lower power consumption
- Integration, performance, ecosystem
Releasing Your Creativity

www.st.com/STM32L5