life.augmented

Press release

P4231S

Ultra-Low Power and Security for IoT Come First on New STM32L5 Microcontrollers from STMicroelectronics

- *Proprietary security builds on Arm TrustZone technology to achieve PSA Certified Level 2 certification*
- *Secure boot, full HW isolation, crypto accelerators*
- *Best-in-class power management for energy-conscious applications*

Geneva, February 13, 2020 – STMicroelectronics (NYSE: STM), a global semiconductor leader serving customers across the spectrum of electronics applications, announces ultra-low-power STM32L5x2 microcontrollers (MCUs) that emphasize security to assure better protected IoT-connected applications.

Operating at clock frequencies to 110MHz, the STM32L5-series MCUs start from the Arm® Cortex®-M33 32-bit RISC core with Arm TrustZone® hardware-based security. First conceived for equipment such as desktops, mobile devices, and communication infrastructure, trusted computing authenticates devices connected to a network by creating a protected execution environment for cyber-protection and sensitive code (cryptography and key storage) that blocks attempts to corrupt devices or software. A second, independent, execution environment allows for the running of untrusted code.

To this foundation, ST adds the freedom to include or exclude each I/O, peripheral, or area of Flash or SRAM from TrustZone protection, allowing sensitive workloads to be fully isolated for maximum security. In addition, ST has engineered TrustZone to ensure support for secure boot, special read-out and write protection for integrated SRAM and Flash, and cryptographic acceleration, including AES 128/256-bit key hardware acceleration, public key acceleration (PKA), and AES-128 On-The-Fly Decryption (OTFDEC), to protect external code or data. The STM32L5 also supports active tamper detection and secure firmware installation. With this attention to security, the STM32L5 has been certified to PSA Certified Level 2.

"As IoT and embedded devices increase in intelligence and functionality, security must be built in from the ground up," said Thomas Ensergueix, senior director, Automotive

and IoT Line of Business at Arm. *"The STM32L5 series makes it easier for developers to build trusted PSA Certified devices based on the Arm Cortex-M33 processor, providing a robust and secure foundation for devices ranging from consumer products to industrial equipment."*

On top of this protection and design flexibility, ST mixes in its proprietary ultra-low-power expertise through techniques like adaptive voltage scaling, real-time acceleration, power gating, and multiple reduced-power operating modes, to enable the MCUs to deliver high performance and long run-times, whether powered by coin cells or even through energy harvesting. In addition, a highly efficient switched-mode step-down regulator can be powered up or down on-the-fly to improve low-power performance when the VDD voltage is high enough. The resulting ULPMark scores, which are key measures of ultra-low-power efficiency based on real-world benchmarks developed by EEMBC, are excellent: 370 ULPMark-CoreProfile and 54 ULPMark-PeripheralProfile at 1.8V.

"As a market leader in MCUs with a strategic focus in areas like Smart Cities, Smart Buildings, and Smart Industry, ST recognized the importance of a series of MCUs that combined world-class ultra-low-power consumption with industry-leading security and data protection, for mission-critical applications and at-the-edge node processing," said Ricardo De Sa Earp, Microcontroller Division General Manager, STMicroelectronics. *"Applying ST's expertise in ultra-low-power design and processing technologies and adding our security and data protection on top of the solid foundation of Arm TrustZone and the outstanding STM32 ecosystem, the STM32L5x2 MCUs are ideal for Industrial IoT applications – metering, health (human or machine) monitoring, mobile point-of-sale – that require reliability and security."*

The STM32L5x2 MCUs offer 512 Kbyte dual-bank Flash that allows read-while-write operation to aid device management and the Flash ensures a high level of safety by supporting Error Correction Code (ECC) with diagnostics. There is also a 256Kbyte-SRAM and features to support high-speed external memory including single, dual, quad, or octal SPI and Hyperbus Flash or SRAM, and an interface for SRAM, PSRAM, NOR, NAND or FRAM.

Digital peripherals for the STM32L5x2 include USB Full Speed with dedicated supply, allowing customers to keep USB communication even when the system is powered at 1.8V, and a UCPD controller compliant with USB Type-C Rev. 1.2 and USB Power Delivery Rev. 3.0 specifications. Smart analog features include a state-of-the-art analog-to-digital converter (ADC), two power-gated digital-to-analog converters (DAC),

two ultra-low-power comparators, and two operational amplifiers with external or internal follower routing and programmable-gain amplifier (PGA) capability.

As part of the industry-leading STM32 family of MCUs, the STM32L5 series is fully supported by the STM32 ecosystem and features its own STM32CubeL5 one-stop-shop software package, which includes Hardware Abstraction Layer and Low-Level drivers, FreeRTOS, Trusted Firmware-M (TF-M), Secure Boot and Secure Firmware Update (SBSFU), USB-PD device driver, MbedTLS and MbedCrypto, FatFS file system, and Touch Sensing drivers. In addition, the STM32CubeL5 features more than 300 project examples that can run on the STM32L552E-EV evaluation board, STM32L562E-DK discovery kit, and NUCLEO-L552ZE-Q. These projects can be compiled with the Arm Keil® development tool, IAR or STM32CubeIDE toolchains, and are delivered with a STM32CubeMX configuration file, enabling easy customization and code update.

Starting at $2.60 in 1k quantities, the STM32L5x2 MCUs are in full production and available now in standard temperature grade (-40°C to +85°C) for consumer and commercial applications, or high-temperature grade specified from -40°C to +125°C for challenging environments.

You can also read our blogpost at https://blog.st.com/stm32l5-trustzone-security/

About STMicroelectronics

ST is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST's products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and homes, along with the next generation of mobile and Internet of Things devices.

By getting more from technology to get more from life, ST stands for life.augmented. In 2019, the Company's net revenues were $9.56 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.

For Press Information Contact:

Michael Markowitz
Director Technical Media Relations

STMicroelectronics
Tel: +1 781 591 0354
Email: michael.markowitz@st.com