Press RELEASES

PR-Nr. 12 – 10. December 2020

Introducing ESP32-C3

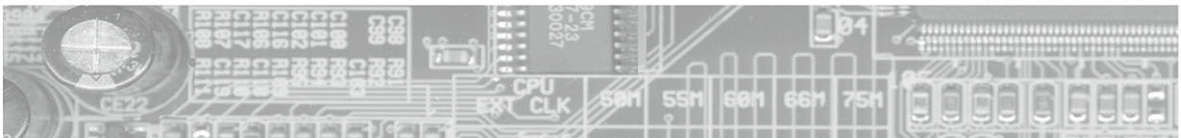
ESP32-C3 is a cost-effective, RISC-V-based MCU with Wi-Fi and Bluetooth LE 5.0 connectivity for secure IoT applications.

Shanghai, China Nov 27, 2020

Espressif launched ESP8266 in 2014 and ESP32 in 2016. ESP8266, with its Wi-Fi-only MCU, facilitated simple connectivity use-cases, whereas ESP32 addressed use-cases that required dual connectivity (Wi-Fi + Bluetooth/Bluetooth LE), considerably more computing power, or strong security features. These two chips became undisputed segment leaders on the IoT market, powering up a huge number of connected devices. In the meantime, the IoT market itself has not only become mainstream, but it has also matured in terms of features and cost expectations. So, from now on, whenever defining a new product, we at Espressif understand that we have to strike a fine balance between features and cost. In fact, we understand that the one-size-fits-all model is not viable, as there should be multiple products for various needs. Hence, for simple and secure connectivity applications, Espressif is introducing ESP32-C3.

ESP32-C3 attempts to address the most common needs for connected devices. Here are the key criteria that have been considered for the design of ESP32-C3:

- Security is of prime importance. Even the lowest-cost connectivity solution needs to provide an appropriate level of security for common security threats.
- Bluetooth Low Energy availability is useful for improving user experience and field diagnostics.
- While cost is a very important parameter, the availability of sufficient memory for common use-cases is equally important. Optimizing applications for memory utili-



zation, while maintaining such memory-constrained devices in the field, is challenging.

ESP32-C3 is a single-core, 32-bit, RISC-V-based MCU with 400KB of SRAM, which is capable of running at 160MHz. It has integrated 2.4 GHz Wi-Fi and Bluetooth LE 5.0 with a long-range support. It has 22 programmable GPIOs with support for ADC, SPI, UART, I2C, I2S, RMT, TWAI, and PWM. A detailed ESP32-C3 datasheet is already available.

In the following parts of this article, we will discuss some of the key benefits of ESP32-C3 for our customers.

Security

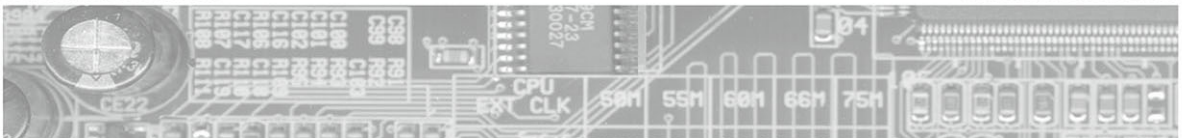
The attacks on connected devices are generally meant to:

1. gain access to sensitive data
2. get unauthorized control of the device
3. steal the device's identity and, subsequently, gain unauthorized access to the device's cloud.

There are various ways to carry out these attacks, either remotely by exploiting software and protocol vulnerabilities, or physically by accessing the device for direct flash access and fault injection. Subsequently, the attacks can be made permanent by installing the malicious firmware as the default one on the device.

It is important that the connectivity platform provides sufficient protection against these types of attacks. ESP32-C3 is designed to address this threat model.

- **Secure Boot**: ESP32-C3 implements the standard RSA-3072-based authentication scheme to ensure that only trusted applications can be used on the platform. This feature protects from executing a malicious application programmed in the flash. We understand that secure boot needs to be efficient, so that instant-on devices

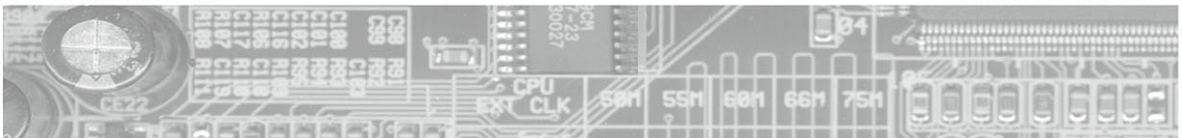


(such as light bulbs) can take advantage of this feature. ESP32-C3's secure boot implementation adds less than 100ms overhead in the boot process.

- **Flash Encryption**: ESP32-C3 uses the AES-128-XTS-based flash encryption scheme, whereby the application as well as the configuration data can remain encrypted in the flash. The flash controller supports the execution of encrypted application firmware. Not only does this provide the necessary protection for sensitive data stored in the flash, but it also protects from runtime firmware changes that constitute time-of-check-time-of-use attacks.
- **Digital Signature and HMAC Peripheral**: ESP32-C3 has a digital signature peripheral that can generate digital signatures, using a private-key that is protected from firmware access. Similarly, the HMAC peripheral can generate a cryptographic digest with a secret that is protected from firmware access. Most of the IoT cloud services use the X.509-certificate-based authentication, and the digital signature peripheral protects the device's private key that defines the device's identity. This provides a strong protection for the device's identity even in case of software vulnerability exploits.
- **World Controller**: ESP32-C3 has a new peripheral called world controller. This provides two execution environments fully isolated from each other. Depending on the configuration, this can be used to implement a Trusted Execution Environment (TEE) or a privilege separation scheme. If the application firmware has a task that deals with sensitive security data (such as the DRM service), it can take advantage of the world controller and isolate the execution.

Bluetooth LE 5.0 with Long-Range Support

Typically, connected devices use Wi-Fi connectivity to connect to cloud services. However, Wi-Fi-only devices pose some difficulty to the network configuration of the devices, as these devices fail to provide reliable configuration feedback to the provisioner, while at the same time iOS and Android provisioners have additional complexity when connecting to the network. The availability of Bluetooth LE radio in the device makes



the provisioning easy. Also, Bluetooth LE provides easy discovery and control in the local environment.

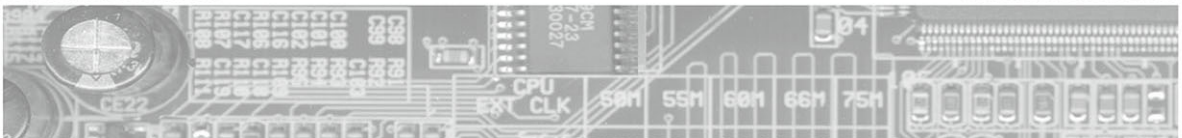
Previous versions of the Bluetooth LE protocol had a smaller range, and that made it not very suitable a protocol for local control in large spaces, e.g. big homes. ESP32-C3 adds support for the Bluetooth LE 5.0 protocol, with coded PHY and extended advertisement features, while it also provides data redundancy to the packets, thus improving the range (typically 100 meters). Furthermore, it supports the Bluetooth LE Mesh protocol. This makes it a strong candidate for controlling devices in a local network, and for communicating with other Bluetooth LE 5.0 sensor devices directly.

Sufficient Memory

With a large variety in the use-cases and their memory requirements, it is tricky to determine the most suitable memory size for the SoC. However, in our experience, it is important to support use-cases with one or, sometimes, two TLS connections to the cloud, which are Bluetooth-LE-active all the time, while also supporting a reasonable application headroom on top of that. ESP32-C3's 400 KB of SRAM can meet these requirements, while still keeping the chip's cost within the budget target. Also, ESP32-C3 has dynamic partitioning for the instruction (IRAM) and data (DRAM) memory. So, the usable memory is effectively maximized. It is also important to note here that we have optimized the Bluetooth subsystem's memory requirements, in comparison with ESP32. We will provide more details when we are closer to the SDK release.

Mature Software Support

ESP32-C3 will be supported through Espressif's popular ESP-IDF platform. If we take a look at the total software that enables the connected devices, a large portion of that comprises hardware-independent software components. ESP-IDF already supports millions of connected devices, and undergoes rigorous testing and release cycles. The maturity of ESP-IDF, as well as familiarity with APIs and tooling will make it easy for developers to build applications for ESP32-C3. With the availability of ESP-IDF,



other software components like cloud agents can be used on ESP32-C3 without any change.

ESP32-C3 will also support the hosted mode of operation, in order to provide Wi-Fi and Bluetooth LE connectivity for external microcontrollers or microprocessors through ESP-AT and ESP-Hosted SDKs.

ESP32-C3 provides so much at a cost that is close to that of ESP8266. There is a variant, ESP32-C3F, which comes with integrated flash for simplified designs. We continue providing certified and cost-effective modules for building connected devices easily. The ESP32-C3-MINI-1 module comes with a small form-factor (13×19mm) and support for a maximum operating temperature of 105°C. For ease of migration, we have ensured that the ESP32-C3-WROOM-1 module is pin-to-pin compatible with the ESP-WROOM-02D and ESP-WROOM-02 modules. ESP32-C3-WROOM-1 also supports a maximum temperature of 105°C.

As mentioned earlier in this article, ESP32-C3 targets the most common use-cases for connected devices. However, we continue building solutions that will address additional use-cases. In doing so, we always take community feedback into serious consideration and we are grateful for all the support from our maker friends, partners and customers.

Pricing and Availability

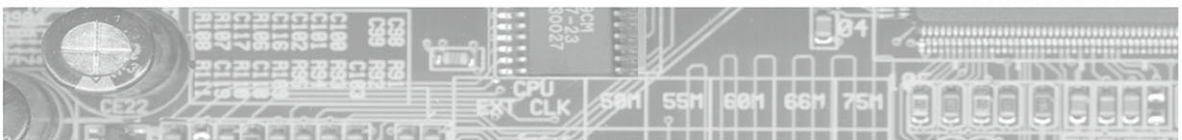
For more information please visit email: sales.europe@macnica.com.

Contact:

Press
Macnica GmbH
Josef Sigl
Tel. +49-89-899143-11
Email: sales.europe@macnica.com

Sales
Macnica GmbH

Tel. +49-841-88198-102
Email: sales.europe@macnica.com



Press

RELEASES

About Espressif Systems

Espressif Systems (Shanghai) Pte. Ltd. is a fabless semiconductor company, with headquarters in Shanghai Zhangjiang High-Tech Park, providing low power Wi-Fi and Bluetooth SoCs and wireless solutions for the Internet of Things (IoT). The company build the widely popular ESP8266 and ESP32 chips with an innovative team of chip-design specialists, software and firmware developers and marketers. Espressif is committed to providing the best IoT devices and software platforms in industry.

The company also helps their customers build their own solutions and connect with other partners in the IoT ecosystem. Their passion lies in creating state-of-the-art chipsets and enabling partners to deliver great products. Espressif's products are widely deployed in the tablet, OTT boxes, cameras, and Internet of Things markets.

For more information, please visit http://www.espressif.com.

About Macnica Europe GmbH

Macnica's European headquarter was originally established in the UK in 2006, and moved to Germany in July 2008, to increase efficacy of its service for European customers.

By it's acquisition of the Munich based company Scantec Mikroelektronik in 2014 Macnica Europe formed a powerful semiconductor distribution with headquarters in Munich and Ingolstadt and numerous sales offices in Europe offering an attractive and competitive portfolio of highly sophisticated devices.

Macnica provides end to end support from design-in to production through its global service network to its customers, regardless of the final destination of the product shipment to customers' manufacturing locations.

About Macnica, Inc.

Macnica was established in 1972 as a semiconductor distribution company headquartered in Yokohama, Japan, and has over 84 sales offices worldwide in eastern Asia, Europe and the USA. Total number of employees is over 3,000 and its consolidated revenue for fiscal 2019 was approximately US$ 5 B.

Macnica is famous for having an excellent engineering team of more than 900 application support engineers, IC designers and software developers with strong focus on providing technical support for its customers including custom design services. Macnica is continuing to extend its presence globally by having successful partners in strategic areas in the electronics market.