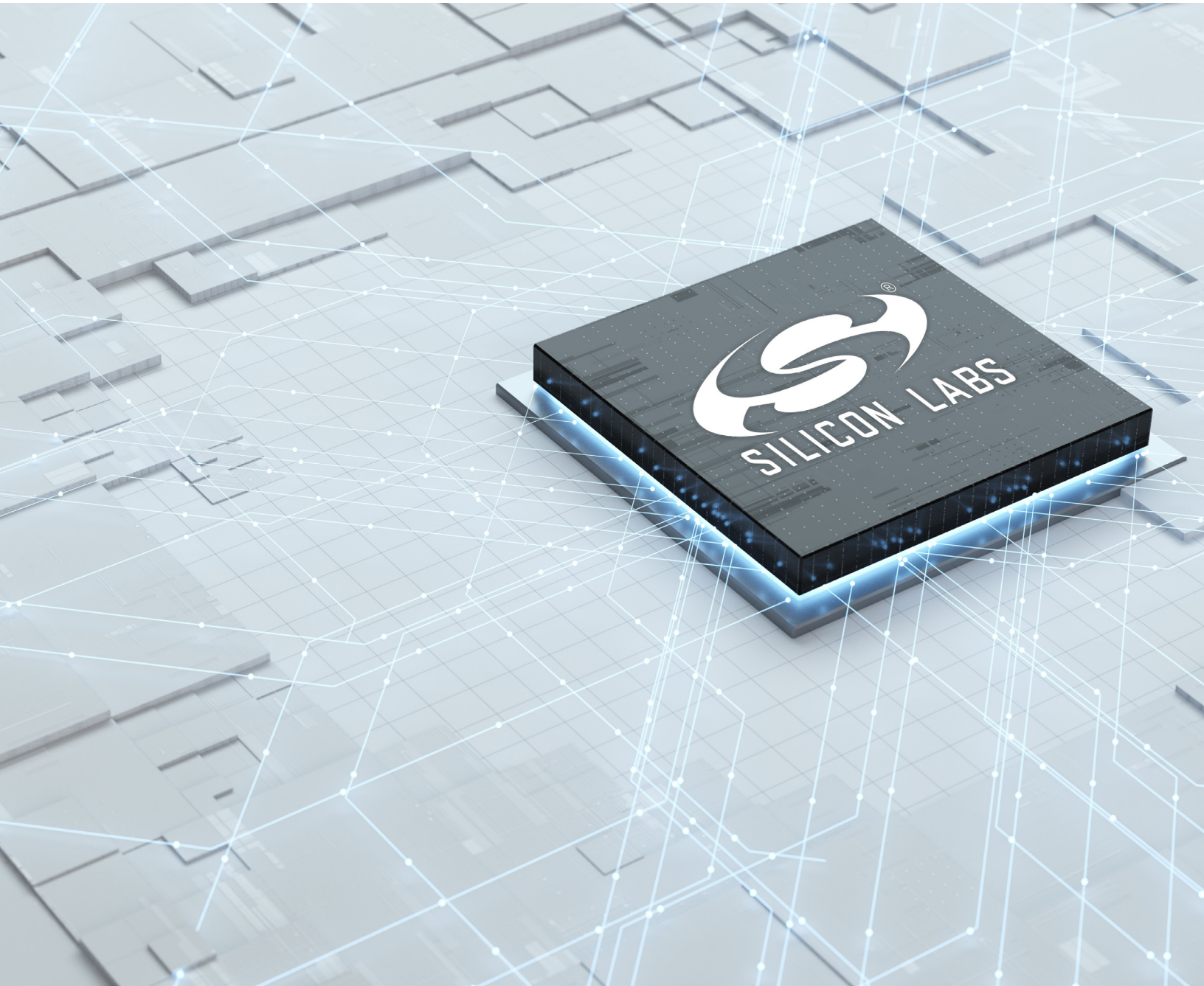
SILICON LABS

Nine things IoT device makers can do with Custom Part Manufacturing Service (CPMS)



Silicon Labs is the only IoT embedded solution provider offering a Custom Part Manufacturing Service (CPMS) to device makers.

This new secure provisioning service allows IoT device makers to order customized hardware straight from the factory via a web portal.

Why do you need custom part manufacturing? What are the benefits?

Read this article for a full explanation and learn about nine things you can do with CPMS today.

Introduction

Historically, building an IoT device was straightforward: developing code, flashing it on a chip, and manufacturing. Today, security is the ultimate challenge for IoT device makers. IoT devices now face severe security threats throughout the entire supply chain, starting with the manufacturing process. Unfortunately, many companies do not have the required capabilities and resources to ensure their products can withstand the ever more sophisticated, rapidly evolving security attacks that can occur during the product lifecycle.

Supply Chain Security Risks

Your software intellectual property (IP) is jeopardized any time you send an unencrypted image to a contract manufacturer. To avoid counterfeiting and grey market sales, you must prevent product cloning and unauthorized production during outsourced manufacturing.

"Zero Trust" Security Paradigm

"Zero trust" is the new security paradigm in IoT. Your products must be authenticated with a unique certificate to pair with other devices and connect to IoT networks and cloud platforms such as AWS, Matter and Wi-SUN. In the future, unauthenticated IoT devices will not be able to generate revenue.

IoT Security Regulation and Legislation

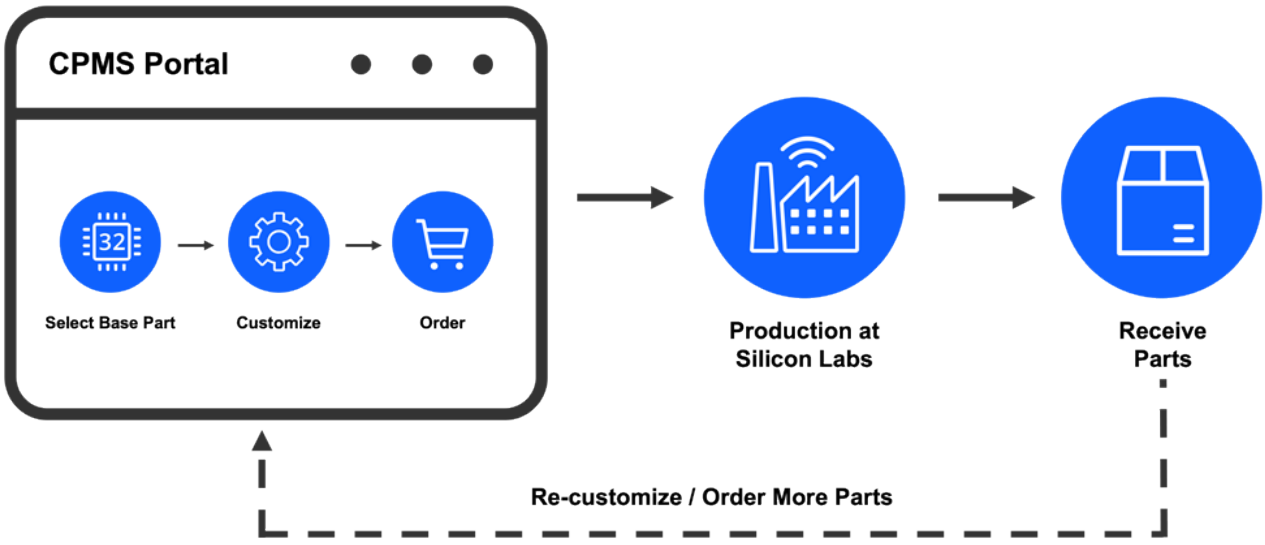
US and European authorities are responding to the rapidly increasing security and privacy threats with laws mandating IoT device makers to implement more robust security measures.

Some examples include:

- IoT devices must run only authenticated code
- Only secure interfaces are allowed for debugging and communication
- Secure, remote software update capability is mandatory
- All devices must have a unique identifier

The Old Way vs. The Secure Way

With the onset of these new, extremely demanding security challenges, the old product development processes are no longer sufficient for the IoT market. Device makers and application developers must increase the level of security in product development radically.



What is CPMS?

CPMS allows you to order customized Silicon Labs hardware online. The CPMS web portal guides you through the customization process and its various customizable features and settings. You can place orders for customized test and production parts easily and securely.

CPMS is a secure provisioning service, not traditional flash programming. It enables you to customize wireless Systems on Chip (SoCs), modules and MCUs with several highly advanced features – these can include secure boot, secure debug, encrypted OTA, public, private and secret keys, secure custom identity certificates, and more.

The custom features, identities and certificates are injected into the hardware securely, quickly and cost-efficiently, directly at the factory.

Why Custom Part Manufacturing (CPMS)?

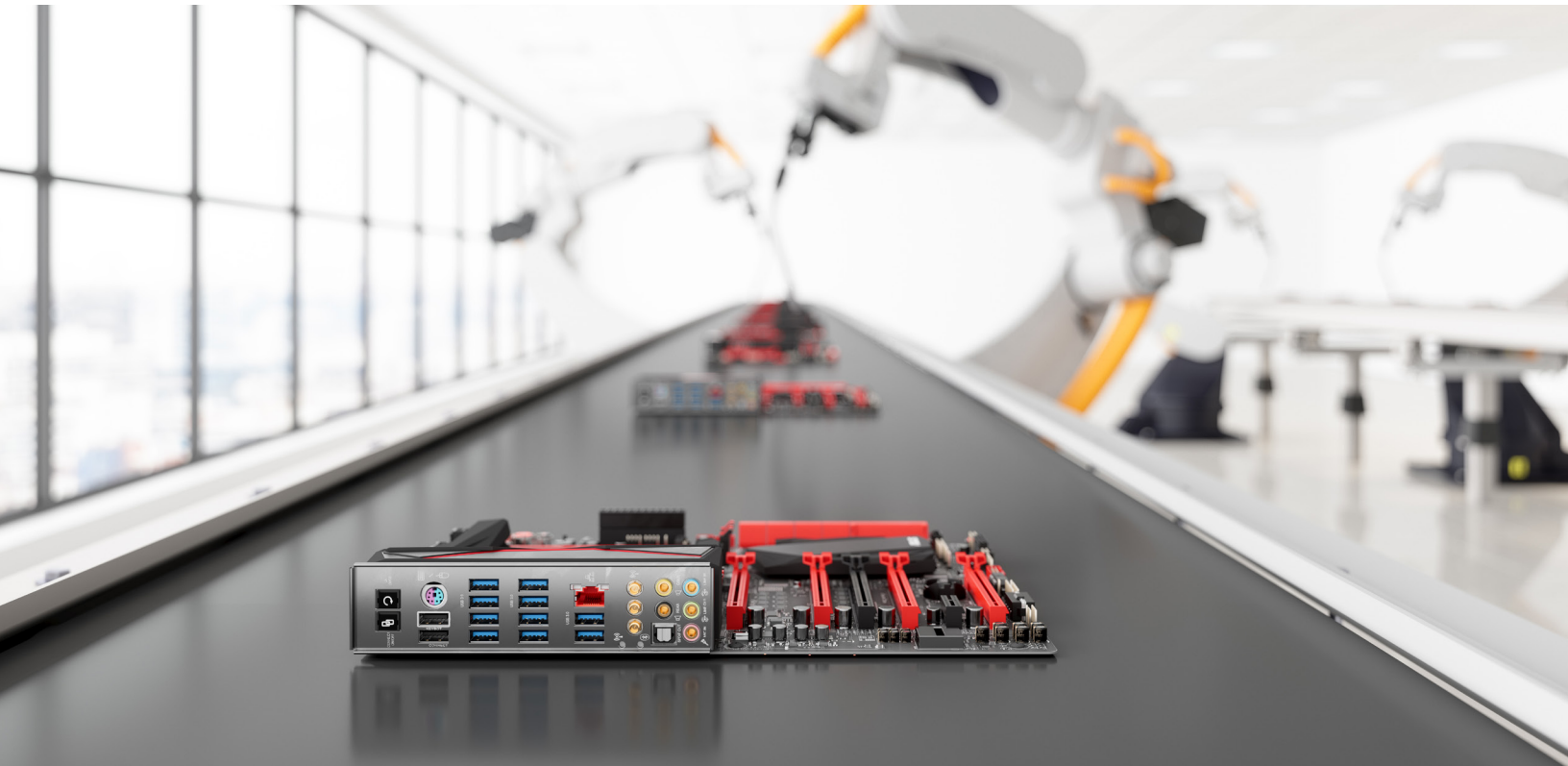
Because securing an IoT device is a highly complicated and costly process – you must generate public and private key pairs for secure boot and secure debug, sign code with a private key, store all the private keys in an HSM, place the public keys for secure boot and secure debug in one-time-programmable (OTP) memory, flip OTP bits for secure boot and secure debug and flash the encrypted code and identity certificates within the hardware.

Silicon Labs' CPMS streamlines the programming part of this process for you. Even the most advanced security features, certificates and identities are programmed on your hardware securely, in total confidentiality, at the Silicon Labs factories. CPMS enables secure IoT cost-efficiently and quickly, without third parties and massive investments.

Where Can CPMS be Used?

CPMS can be used in many IoT sectors and applications:

- All IoT applications using Public Keys
- Medical devices for professionals and consumers
- Products that require a secure identity
- Device anti-counterfeiting
- Securing contract manufacturing and tracking supply chain
- Industrial IEC 62443 compliant devices
- Injecting certificates for ecosystem products



Benefits of Custom Part Manufacturing

Protect Revenue and Brand

CPMS allows IoT device makers to protect their revenue and brand by safeguarding products against cloning and counterfeiting during contract manufacturing and tracking shipped quantities to prevent overproduction and over-pricing. With CPMS, you can inject a unique, customized secure identity on your chips at the Silicon Labs factories. This unique product-level identity provides a hardware-based root-of-trust anchor guaranteeing devices entering your ecosystem are authentic.

Safeguard Competitive Advantage

Protect software IP by pre-flashing a secure bootloader on your Silicon Labs hardware and locking them at our factory. Now you can send encrypted images to any contract manufacturer, trusted or not, while keeping your software IP safe. With the broader contract manufacturer selection, you gain more flexibility, reduce sourcing costs, and increase capacity.

Protect IP and Investment

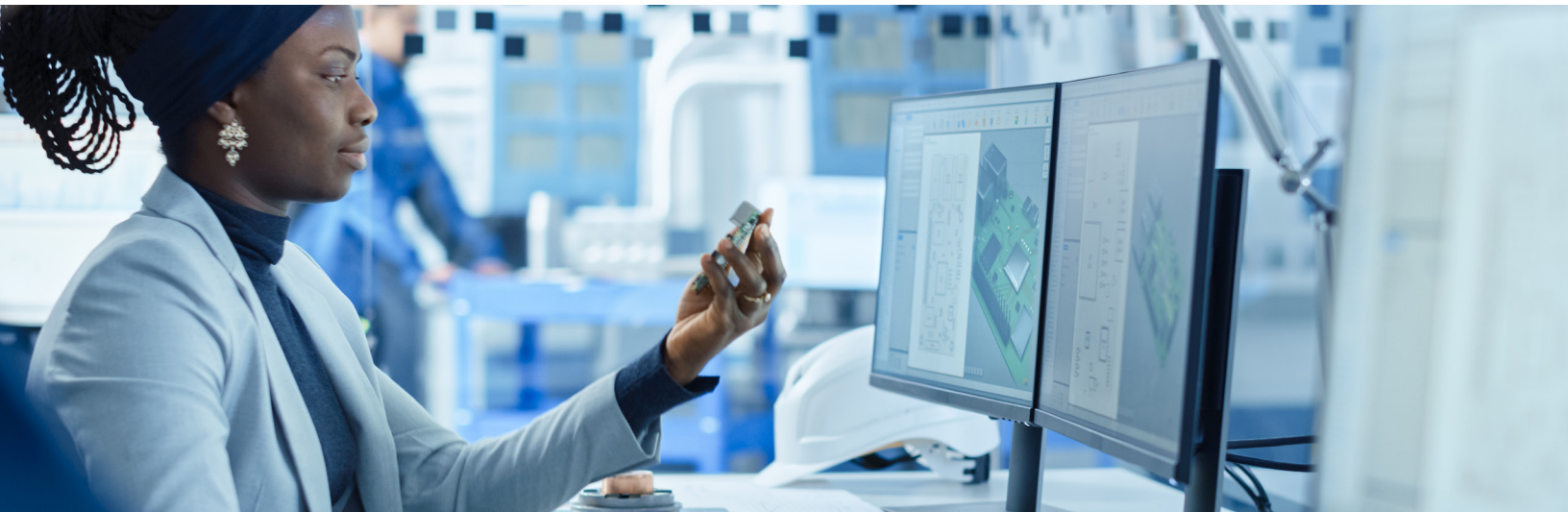
Prevent tampering by configuring the most effective tamper detection features at Silicon Labs factory, allowing your products to withstand even the most sophisticated physical tampering attacks throughout the supply chain - from production to shipment and further.

Accelerate Revenue Generation

Enable your devices with unique custom certificates, allowing them to successfully authenticate to join the most popular IoT cloud platforms in the market, such as AWS, Matter, and Wi-SUN. CPMS injects appropriate certifications (custom certificate chains) on-chip securely, during manufacturing.

Maximize Security, Minimize Costs and Time

Enabling IoT products with robust security requires specialist resources and costly in-house investments. On the other hand, outsourcing programming to a third party adds cost and could cause delays. Silicon Labs CPMS can provision the most advanced security features during part manufacturing, cutting your costs and time-to-market significantly.



Nine Things You Can Do with CPMS

Silicon Labs CPMS allows you to customize hardware in several ways. Here is a list of nine things you can provision securely on your hardware using CPMS:

1. Unique Part Number

Programming your wireless and microcontroller SoCs and modules with a unique part number allows for tracking shipments and prevents over-production, counterfeiting and use of fake components. With unique part numbers, you know exactly how many parts your contract manufacturers order from Silicon Labs. If the shipments do not match the agreed amounts, there is a risk of counterfeiting or illegitimate components being used in your products. By programming unique part numbers on your Silicon Labs hardware at our factory, you can track shipments and reduce your outsourced manufacturing and supply chain risks.

2. Secret Keys Programming

Inject custom public and private keys and other custom secret keys on the chips during the manufacturing process – safeguard your products right from the beginning of their lifecycle.

3. Secure Bootloader Setup

The software running on your IoT devices and applications is vulnerable to copying and cloning throughout the entire product lifecycle. Provisioning a secure bootloader on the wireless and MCU hardware to encrypt software can safeguard your IP efficiently. Our CPMS streamlines this complicated procedure for you at our factories without third parties and massive investments. You can securely provision a secure bootloader on the hardware, inject the secure boot public key into OTP memory and set the Secure Boot OTP flag.

4. Tamper Detection Configuration

IoT devices must withstand various tampering attempts during the lifecycle, starting from the contract manufacturing and supply chain level. Silicon Labs wireless and MCU hardware can be protected with several intelligent anti-tamper solutions. The CPMS web portal helps you navigate the anti-tamper settings to protect your products against the most sophisticated tampering attacks during outsourced manufacturing and beyond.

5. Debug Port Configuration

The debug port is a classic source of security vulnerability if left unlocked. The security best practice is to lock or disable debug access before production releases a product. Silicon Labs microcontroller hardware includes a secure debug port mechanism, which you can now configure with CPMS to ensure your products are safe right from the beginning of their lifecycle.

6. Software Flashing

Suppose you are planning to pre-flash your application software on SoC or module hardware. In that case, the quickest and most cost-efficient way is to use Silicon Labs CPMS – the software will be available on the Silicon Labs chips when manufactured, without additional investments and increased time to market.

7. Custom Markings

CPMS allows you to customize markings on the hardware to hide the actual wireless and microprocessor SoC and module used in the products, thus preserving your competitive advantage.

8. Custom Device Certificates

Custom certificates can be used to authenticate (attestation) devices with various IoT cloud services, smartphone applications and ecosystems such as Wi-SUN, Matter, AWS IoT Core, Google IoT Cloud, Microsoft Azure, IBM Watson and more. CPMS makes programming these custom certificates easy.

9. Unique Product Identity

A unique identity is the ultimate method for verifying the authenticity of your products at any time during their lifecycle – production, onboarding, ecosystem sign-up and more. Silicon Labs Secure Vault solution provides a hardware root-of-trust anchor to form a unique product-level identity. The unique product identity is placed securely into the Silicon Labs wireless and MCU SoC and module. With CPMS, you can provision a unique, secure identity on your wireless MCUs at the Silicon Labs factories quickly and cost-efficiently.

Why Choose Silicon Labs and CPMS?

Silicon Labs' CPMS provides several advantages over using a third-party programming provider or investing in an in-house solution and resources.

- Silicon Labs is already programing the default security settings during production – custom programming can be added with minimum effect on cost and time to market.
- Our testers are optimized for our hardware, providing you an economy-of-scale advantage compared to other services and making CPMS the most cost-competitive solution amongst similar secure provisioning service providers.
- Silicon Labs is the world's most trusted and skilled entity for customizing our hardware.
- Securing semiconductor solutions requires tuning countless parameters. With Silicon Labs' security experts on board, you don't have to learn and teach contractors secure provisioning.
- We are the only entity that can customize our silicon identity certificate with ease of mind and turn it into your own unique and secure device identity certificate.
- Silicon Labs leads the IoT security space with several cutting-edge solutions, such as the world's first SoCs and modules with PSA Certification Level 3.

More about Custom Part Manufacturing

Visit our CPMS page to learn more about CPMS. Contact Silicon Labs sales directly for detailed product information, or go directly to the CPMS portal and start customizing your parts today.

Ready to Get Started?

Click below to get started with Custom Part Manufacting Services.

Get Started with CPMS