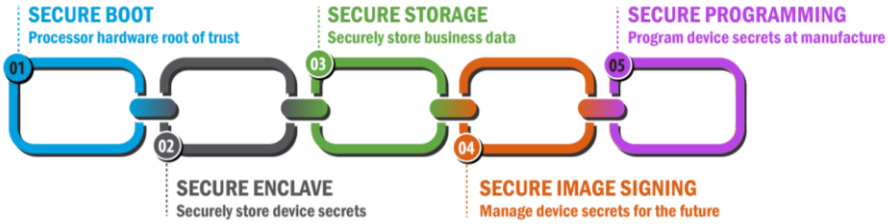
SIMPLIFYING ROOT OF TRUST DEVICE SECURITY TO LOWER COMPLEXITY, COSTS, AND TIME TO MARKET

SUMMIT SUITE
SECURITY SOLUTIONS



Building your own device security architecture, large scale device key programming, and secure key management solution from scratch takes years of development. Leverage our turn-key Summit Suite Chain of Trust Device Security solutions and remove the burden of developing a device security architecture, implementing new secure manufacturing processes, and creating a secure application for device image signing and key management.

It starts with generating cryptographic keys and certificates unique to your company, device family, model number, part number, etc. We've developed a secure system, the Secure Signing Service, to store and manage these secrets for future use. We combine the Secure Signing Service and our expertise in manufacturing custom image programming to allow for high volume secure provisioning and programming of the hardware root-of-trust on each product and securely-signed software images.

We're one partner with every needed capability, providing the device hardware, a device security architecture, large scale manufacturing key programming, and a secure imaging signing service under one roof.

Our device security architectures are custom to each product family's processor-specific hardware capabilities and their respective Yocto or Buildroot Summit Linux board support package (BSP). They're built on our capabilities in maintaining long-term secure Linux BSPs and utilize the hardware root-of-trust inside application processors to balance the trade-offs between security, performance, maintainability, and functionality.

Summit Suite Chain of Trust Device Security also helps you secure future software images for updates in the field or to switching to a new software image to be programmed at manufacture. Upload your software image to our Secure File Service and in conjunction with the Secure Signing Service receive your newly signed image for updates or use it as your new programming image in our factory.

Key Features

Secure and Verified Boot Architecture

A custom secure boot hardware root of trust architecture included in our long-term support BSPs that provide the foundation for ensuring only your software images are loaded onto your devices.

Secure Enclave Architecture

On the Summit SOM 8M Plus family, extends our secure and verified boot architecture to include a run-time isolated trusted environment for using and storing secure keys, certificates, and credentials. Critical cryptographic operations occur in the in secure enclave separate from the bootloaders and Linux memory space. Linux applications can access those operations through an API that never exposes private keys, certificates, or credentials stored in the secure enclave.

Secure File Storage Architecture

Extends our secure and verified boot architectures to include filesystem-level data encryption for secure storage of all your core business data.

Secure Signing service

Maintain the keys and certificates required by the Secure and Verified Boot, Secure File Storage, and Secure Enclave architecture and sign new software images as you require updates to your device.

Signed and Secured at Manufacture

Mass-programmed at manufacture with your custom secured software images and the root of trust to support booting those images, we make it easy to count on device security.

Industry-Leading Support

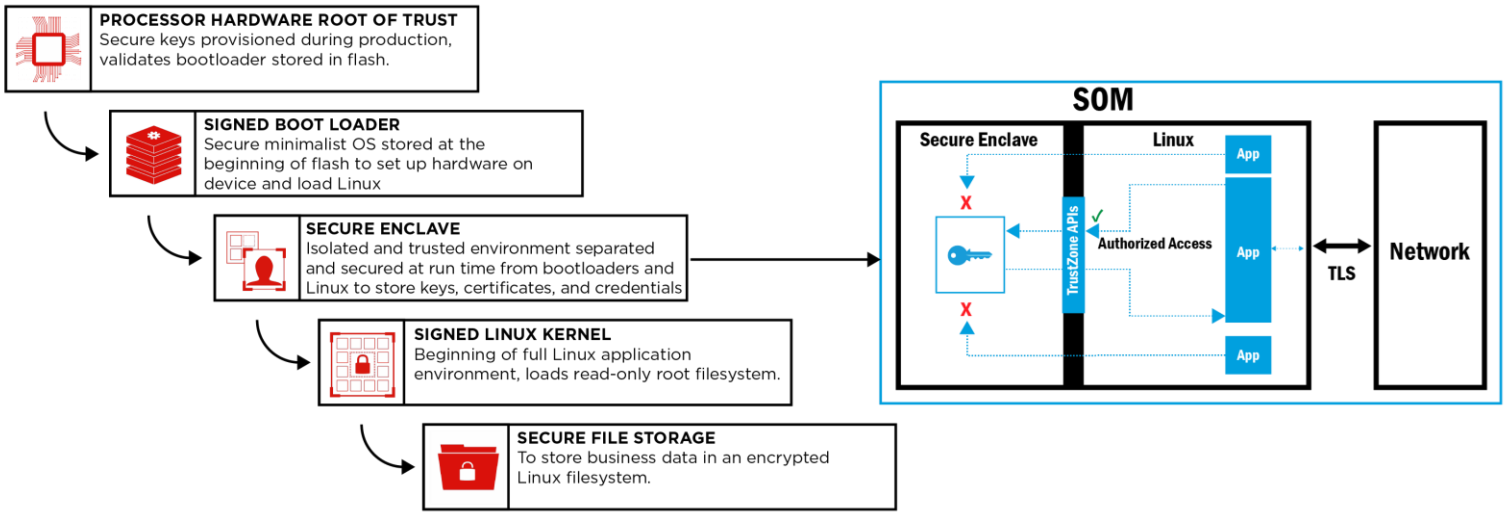
Our Tier 2 and FAE support bring expert assistance, working with you and our engineering to reduce your time to market.

Application Areas

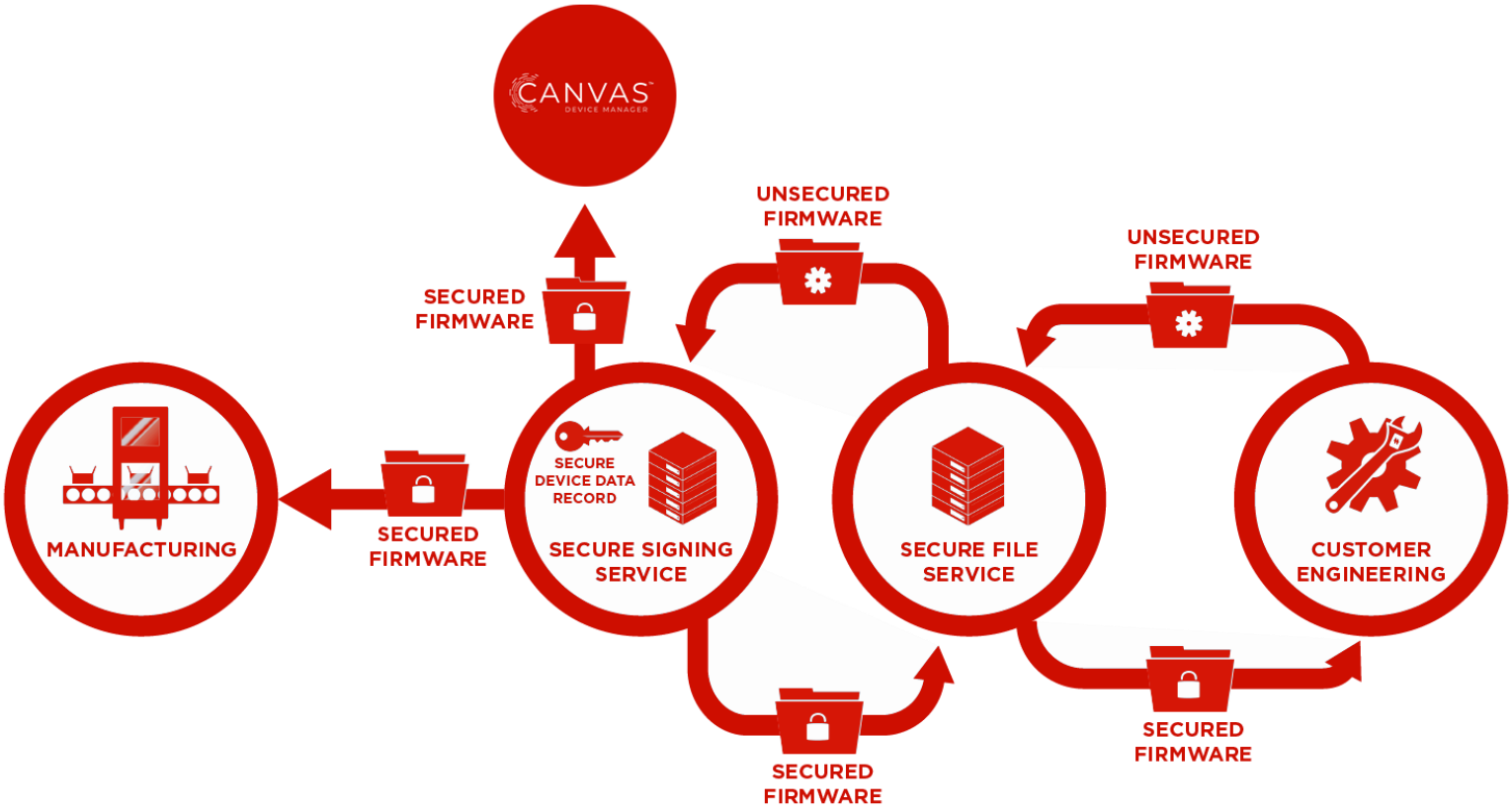
- **Smart Buildings and Appliances**
- **Smart Robots**
- **Industrial IoT, Vision Systems**
- **Printers and Scanners**
- **Medical Devices**

Interested in our Summit Suite?
Visit www.ezurio.com/summit-suite

Example Device Security Architecture



Secure Image Signing and Programming



Ordering Information

Part Number	Description
SAAS-SS-COT-WB50	One Year of Chain of Trust Device Security for the WB50NBT
SAAS-SS-COT-SOM60	One Year of Chain of Trust Device Security for the 60 Series SOM
SAAS-SS-COT-IG60	One Year of Chain of Trust Device Security for the IG60 Summit Linux

Ezurio's products are subject to standard Terms & Conditions.