

Sectigo Secure Key Storage SDK

IoT device manufacturers must authenticate device identity to protect against increasingly sophisticated attacks that target embedded devices and expose customers to theft of confidential information, disruption of services, and spread of the attack to other systems. Cryptographically strong identity starts at the device, and it is critical private keys are protected and securely stored for each device. But the reality is that many IoT devices from industrial controls to medical instruments do not have a hardware secure element required for secure key storage.

Device manufacturers deploying software-based secure key storage for devices with limited resources need a comprehensive, yet compact and portable software development kit (SDK) that allows them to programmatically:

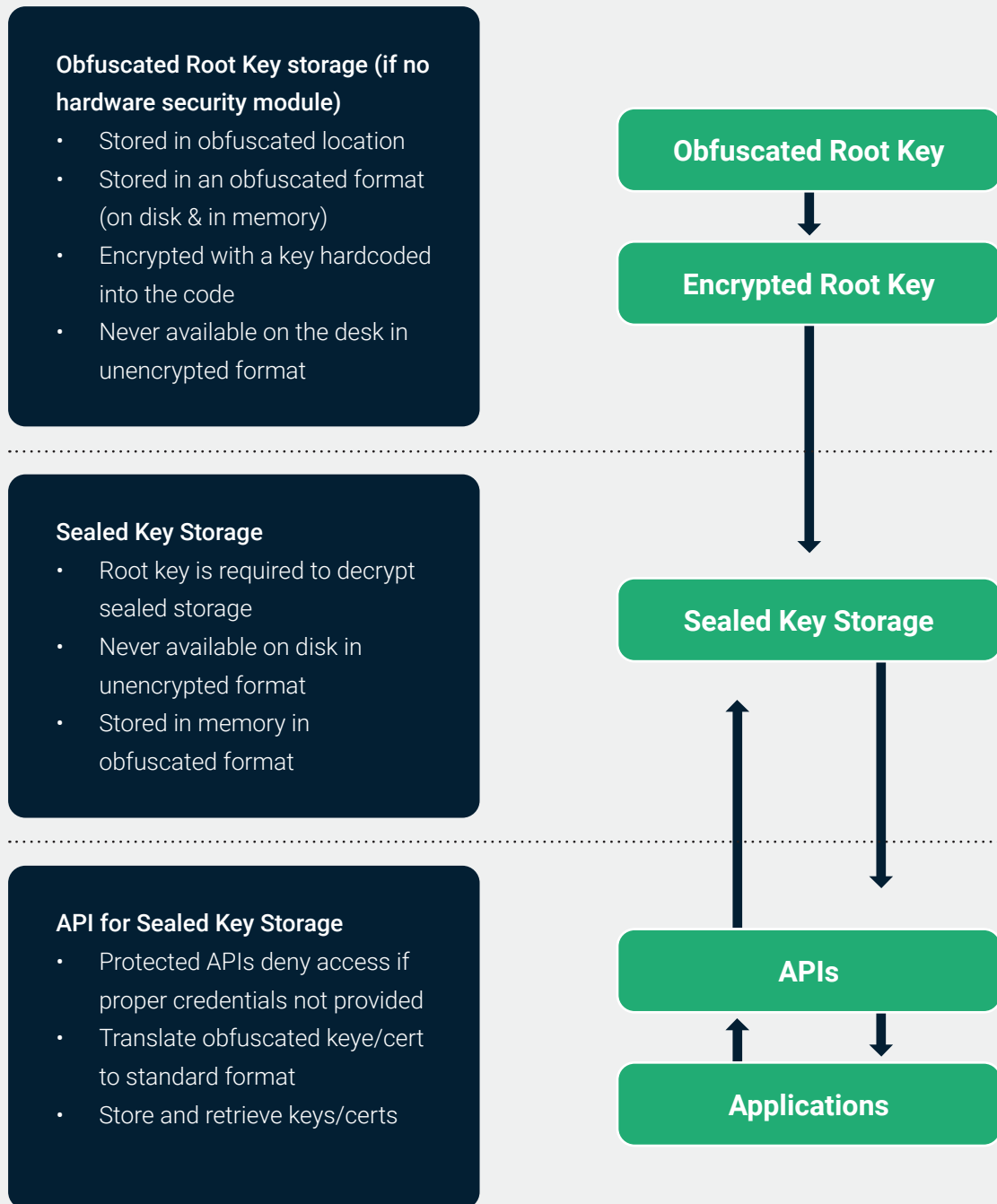
- Authenticate device identities using transport layer security (TLS) protocols
- Encrypt data on embedded devices
- Store and access passwords and other secret data



Sectigo can help.

Sectigo Secure Key Storage SDK is a configurable library that cost-effectively manages, seals, and stores encryption keys, passwords, and other confidential artifacts and removes the risk of exposing credentials of devices lacking a Trusted Platform Module (TPM) or another hardware-based secure storage mechanism.

Figure: Sectigo Secure Key Storage SDK uses patent-pending obfuscation algorithms to securely manage, seal, and store all embedded device keys.



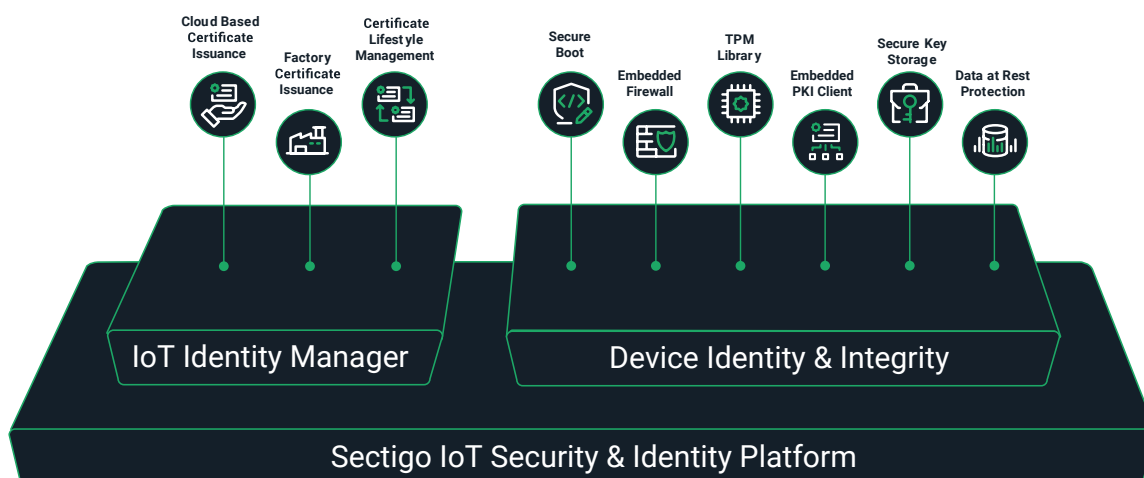
PROGRAMMATIC SECURE KEY STORAGE FOR EMBEDDED DEVICES

The Sectigo Secure Key Storage SDK enhances security of device identities for products without a trusted platform module (TPM) or hardware secure element and enables you to benefit from:

- **Sealed key storage:** Using patent-pending obfuscation algorithms, Sectigo Secure Key Storage SDK seals and stores all device keys, passwords, and confidential data in an obfuscated format on the embedded device disk or in memory.
- **Protected API:** Sectigo Secure Key Storage SDK includes a hardened API that provides programmatic creation, retrieval, and deletion of device keys when needed.
- **Storage root key (SRK):** Sectigo Secure Key Storage SDK generates and obfuscates the format and location of an encrypted storage root key required to protect and manage access to all device keys.
- **Customization:** Each original equipment manufacturer (OEM) can customize the obfuscated format and location ensuring it is unique to your device and that hackers do not have the details required to discover the SRK.
- **Interoperable and portable:** Sectigo Secure Key Storage SDK has been ported to support FreeRTOS, Linux, and Windows platforms, and can be easily ported to new platforms.
- **Regulation and certification compliance:** Sectigo Secure Key Storage SDK is a component of the Sectigo Security and IoT Identity Platform that provides an important building block for achieving compliance with local and international IoT security regulations and standards, including NIST, ETSI, BITAG, CTIA and IETF, certification via ISO and Eurosmart, as well as compliance with emerging security regulations including the IoT Cybersecurity Act of 2020.

Sectigo is the first trusted third-party Certificate Authority to offer security for every connected device from the point of manufacture throughout the entire device lifecycle so that you don't have to build your own security provisioning and management process from the ground up.

Sectigo Secure Key Storage SDK is a component of the Sectigo Security and IoT Identity Platform that provides comprehensive device identity, integrity security, data protection, and high-scalable certificate lifecycle management. By reducing security and authentication as barriers, you can maximize the value of your IoT solutions and enjoy the peace of mind that comes from knowing your connected devices are protected in a shifting threat environment, not just today but for years to come.



About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As a large global Certificate Authority (CA) with more than 700,000 customers and over 20 years of online trust experience, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions to secure web servers and user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow.