EdgeLock® SE050: Plug and Trust Secure Element Family – Enhanced IoT Security with High Flexibility

SE050

Last Updated: Dec 17, 2024

The EdgeLock SE050 secure element (SE) product family offers enhanced Common Criteria EAL 6+ and FIPS 140-2 certified security, for strong protection against the latest attack scenarios, and an extended feature set for a broad range of IoT use cases. This ready-to-use secure element for IoT devices provides a root of trust at the IC level and delivers real end-to-end security – from edge to cloud – without the need to implement security code nor handle critical keys and credentials.

Key Benefits

- Plug & Trust for fast and easy design-in with complete product support package and example codes for a broad range of use cases
- Extended user memory with dynamic file system to store credentials for multiple applications running on one chip
- Easy integration with different MCU/MPU platforms and OSs (Linux®, RTOS, Android®)
- Turnkey solution to reach system-level security with any MCU/MPU without the need to implement security nor handle critical keys and credentials
- Supports compliance to many security standards like IEC 62443, DLMS/COSEM, OPC-UA and ISO15118-2
- Real end-to-end security, from edge to cloud
- Trust anchor for IoT devices with secure credential injection at hardware level

Use Cases

EdgeLock SE050 supports a broad range of IoT security use cases such as TLS connection, cloud onboarding, device-to-device authentication, device integrity protection, attestation, sensor data protection, Wi-Fi credential protection, secure access to IoT services, IoT device commissioning and personalization.

Complete Plug & Trust Product Support Package

Delivered as a ready-to-use solution, the EdgeLock SE050, part of the EdgeVerse™ edge computing platform, comes with multiple pre-implemented cryptographic algorithms and protocols and a complete product support package that simplifies design-in and reduces time to market. In addition to libraries for different MCUs and MPUs, the support package also offers integration with the many common OSs including Linux, RTOS and Android. Time-saving design tools, such as sample code for major use cases, extensive application notes and compatible development kits for i.MX and Kinetis® microcontrollers, accelerate the final system integration.

Certified EdgeLock Assurance
The EdgeLock SE050, part of the Certified EdgeLock Assurance program, is designed to meet industry standards and follows NXP's security-by-design approach. It has been certified by an independent lab.

EdgeLock Plug & Trust Middleware Block Diagram
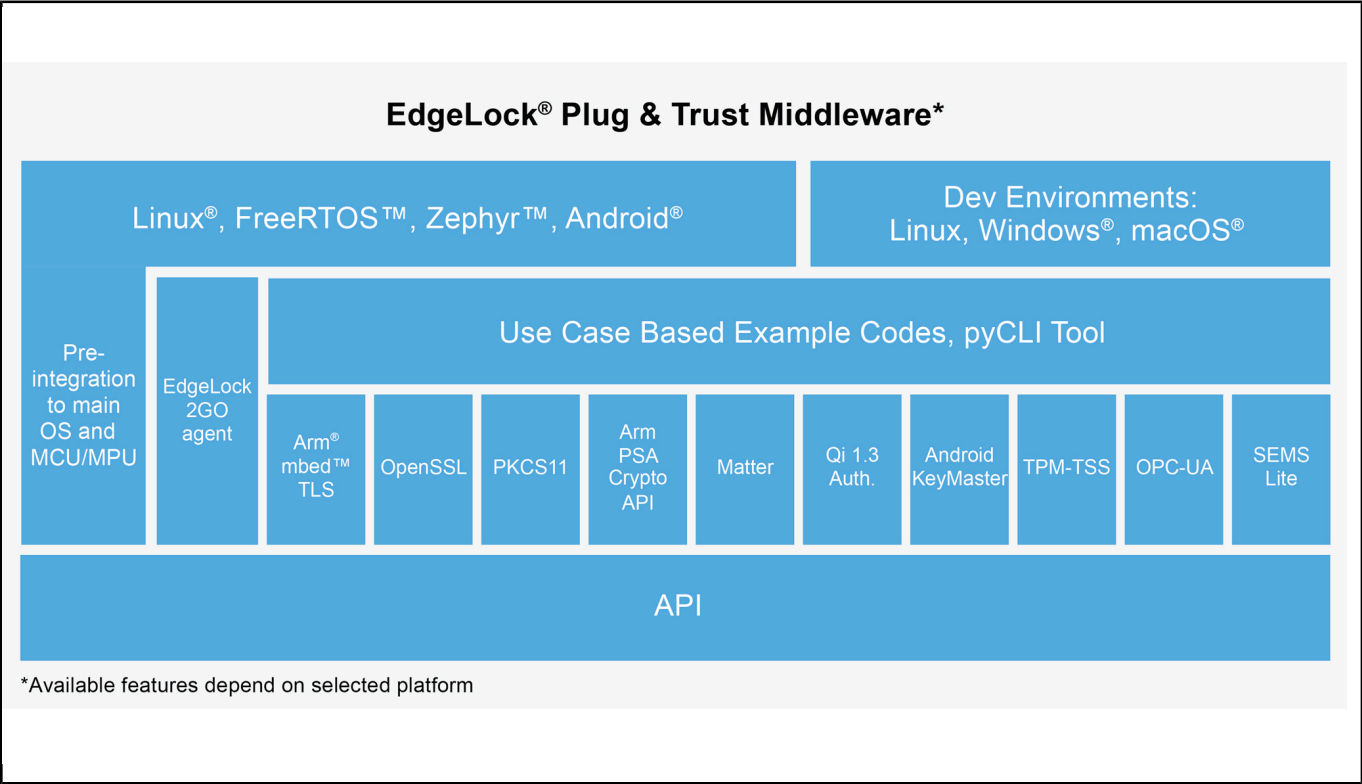
View additional information for EdgeLock® SE050: Plug and Trust Secure Element Family – Enhanced IoT Security with High Flexibility.

Note: The information on this document is subject to change without notice.

www.nxp.com