NXP EdgeLock SE050 "Plug & Trust" Secure Element Family Provides Deeper Security for the IoT

June 12, 2019

NUREMBERG, GERMANY – June 12, 2019 – NXP Semiconductors N.V. today announced availability for its EdgeLock SE050 Plug & Trust Secure Element (SE) family to secure Industrial 4.0 and Internet-of-Things (IoT) applications – from edge to cloud. The Common Criteria (CC) EAL 6+ certified EdgeLock SE050 makes it easy to implement high- performance security for sensing and control. Additionally, it streamlines deployment of IoT services and onboarding of edge devices to public and private clouds, edge computing platforms and infrastructure.

"NXP's EdgeLock SE050 is converging secure sensing, secure connections to multiple cloud services, and integrity protection of a trusted IoT platform," said Philippe Dubois, vice president and general manager of IoT security and smart mobility and retail at NXP Semiconductors. "As part of our "Plug & Trust" approach, EdgeLock SE050 simplifies the implementation of strong security mechanisms to meet the ever-increasing demand for easy-to-design and scalable IoT security."

High-Performance Security and Integration Features

- CC EAL 6+ certification up to OS level provides unprecedented hardware and operating system security to protect against the latest attack scenarios and evolving IoT threat landscape.
- Supports up to 4096 bits RSA cryptography and integration of Elliptic Curve (ECC) cryptography with an expanded set of curves such as Brainpool, Edwards and Montgomery.
- Pre-integrated, flexible applet that eliminates the need to write security code, and scalable software with built-in protections.

Streamlines Deployment of IoT Services and Onboarding of Edge Devices to the Cloud

- I2C master functionality for direct control of critical functions as well as integrity and confidentiality of sensor data.
- Contactless interface for late-stage parameter configuration of unpowered devices.
- Integrates functionality typical to Trusted Platform Modules (TPM), combining into a unique solution security of IoT connections, as well as IoT platform integrity and attestation.
- Simplifies integration with different microcontrollers, microprocessors, operating systems (Linux, RTOS, Windows, Android) and major cloud platforms.

Meets Global Compliance and Standards Requirements

NXP EdgeLock SE050 Secure Element supports compliance to some of world's most rigorous standards and protocols, including the National Institute of Standards and Technology (NIST), EU General Data Protection Regulation (GDPR), International Society of Automation Industrial Network and System Security IEC62443, OPC Industrial Interoperability Standard for Unified Architecture (OPC UA), and the Open Connectivity Foundation (OFC) specification. EdgeLock SE050's compliance and certifications also illustrate NXP's commitment to the Charter of Trust initiative and its binding rules and standards to build trust in cybersecurity and further advance the future of digitalization.

Pricing and Availability

Delivered as a ready-to-use solution, EdgeLock SE050 includes a complete product support package that simplifies design-in and reduces time-to-market. NXP's timesaving design tools, such as sample code for major use cases, extensive application notes, and compatible development kits for i.MX applications processors, LPC and Kinetis microcontrollers, further accelerate the final system integration. EdgeLock SE050 will be mass market available by July 31st.