PSA Certified Spotlight
Security Platform Inc.

psacertified™

level one

> "Device manufacturers know that our platform is certified on the best global standards which means they can follow those standards, too, and we don't need to open up our product source code for verification or provide stacks of documentation."

Suik Hwang, CEO, Security Platform Inc.

Security Platform Inc AMI 2.0 Secure Smart Meter

Increasingly, utility companies trust PSA Certified to offer a great security foundation on which secure smart meter technology can build.

Utility Smart Meter Growth Relies on Security

As the market for smart meters in the utility industry continues to grow, the need for advanced security features, such as secure boot, key management, firmware updates, and provisioning is growing with it. Security Platform Inc. (SPI) provides an embedded security platform solution for AMI 2.0 that enables device manufacturers to build more secure and robust smart meters efficiently and easily.

Utility companies deploying smart meters throughout communities are often challenged to respond to the many security threats facing a smart meter, including hacking, tampering, and electricity theft. Increasing privacy regulations also mean that utilities must maintain secure communications with smart meters – whether to update software on the devices or to collect customer data.

"Security is a serious issue in the utilities industry," says Suik Hwang, CEO of Security Platforms Inc. (SPI). "Utility companies expect strong security features in smart meters but device manufacturers are not security experts. At SPI, we use the PSA Certified program as the basis of our security architecture for the middleware and security solution we've optimized on Arm-based technology."

Fully Integrated Security Solution

A major benefit of the PSA Certified program for SPI is that all the companies involved in producing smart meters – from chip designers to software providers to device manufacturers – can follow the same security architecture guidelines. The result is a fully integrated device that gives utility service providers the assurance they need that their smart meters comply to fundamental security principles and that their customers' data is protected.

"PSA Certified saves us a lot of time and money because it means everyone involved the design, assembly, and implementation of our solution can work from the same security framework," Hwang says. "Only the PSA Certified program provides detailed guidelines for

the system architecture, not just the application layer. PSA is very organized across all layers and helps us avoid inefficient and lengthy development."

The AMI 2.0 Secure Smart Meter has three core components: the Nuvoton NuMicro M2351 MCU (which is also PSA Certified Level 2), the Arm® Mbed™ OS, and the SPI middleware and security solution. The smart meter goes beyond basic security requirements to include device authentication, data encryption, secure boot, secure key management, and attestation. It also supports secure firmware updates and secure key generation for provisioning.

"We've also integrated Pelion Device Management services for the utility companies," Hwang explains. "This allows us to offer a prepackaged solution that is both more secure and highly efficient, regardless of the number of smart meters on the network."

Platform For Expanding Business Model

The PSA Certified classification is helping SPI expand its business on a security platform that can work with different types of devices and applications while earning customer trust in its solutions. PSA Certified Level 1 checks the foundational level of security, however smart meters need a more robust solution, which SPI factors into its design. This makes the product a prime target for PSA Certified Level 2 which SPI plans to complete. It also intends to put additional SPI products through certification, including a VPN client for the surveillance market.

"Device manufacturers know that our platform is certified on the best global standards which means they can follow those standards, too, and we don't need to open up our product source code for verification or provide stacks of documentation," Hwang says.