



PSA Certified Spotlight NXP



psacertified™
level one



psacertified™
level two



psacertified™
functional API

PSA Certified Level 1:

LPC5500, i.MX RT600, i.MX RT1060, i.MX RT1050, i.MX 8QuadXPlus, i.MX 8QM, i.MX 8M Nano, i.MX 8M Mini, i.MX 7ULP1

PSA Certified Level 2:

LPC55S16

PSA Certified Functional API:

LPC5500

Security for Mass Market IoT Devices

NXP Delivers the Largest Portfolio of PSA Certified Processors

NXP Semiconductors is a leader in secure connectivity solutions for embedded applications, driving innovation in the automotive, industrial and IoT, mobile, and communication infrastructure markets. As part of its commitment to improving security for the IoT, NXP now has nine PSA Certified Level 1 products and one PSA Certified Level 2 product, including power-efficient MCUs, crossover microcontrollers, and high-performance applications processors.

The PSA Certified program offers a reassurance to the customer that the product's security has been tested. It serves as a general framework to help educate manufacturers—and the consumers who buy their products—about the importance of security.

"Trust is essential to the IoT," says Gowri Chindalore, NXP's head of technology & business strategy for edge processing. "The combination of NXP's reputation for secure processing and the validation from PSA Certified industry-wide security standards provide the confidence that consumers need to embrace IoT."

Connected devices introduce new attack surfaces, prompting an urgent need to address potential vulnerabilities. NXP was one of the first Arm partners to offer a wide breadth of PSA Certified Level 1 product families that are designed with secure foundations in line with PSA Certified principles.

"There's no one-size-fits-all approach to security," Chindalore says, "NXP's broad processing portfolio is designed to address a wide range of IoT applications that require basic to very advanced levels of security."

Independently Verified at Every Level

NXP provides a range of PSA Certified products that offer an independent verified security for a variety of use cases depending on the type and level of security required. For instance, a smart toy that only connects to one or two other devices requires different and less costly security than a smart thermostat that manages many devices and stores important heating and cooling information. “Built-in security is fundamental to our products, so our customers get the security that’s appropriate for their use case at a market-competitive price,” Chindalore explains.

Assured Privacy

“Consumers are putting more and more private information on edge devices, from medical data to financial information,” Chindalore says. “Although consumers say they want security, they don’t necessarily understand what that means. For instance, when fitness trackers download heartrate data to another device, that data must be encrypted, which is best done using strong encryption keys that are generated in the silicon chip itself.”

Growing Mindshare and Expertise

NXP is actively participating in the definition of the Global Platform SESIP certification standard, which is planned to align to PSA Certified Level 3 and intends to achieve PSA Certified Level 3 with its expanding product portfolio.

For PSA Certified Level 2, NXP has taken the PSA requirements and translated them to SESIP language to show that a PSA Certified certificate can be used as an input for software developers who wish to achieve a SESIP certificate.

“When you bring people together, the collective knowledge squares,” Chindalore says. “Our knowledge sharing on security insights with Arm on the PSA Certified program is an example of this.”

