

Test/Validation

"On-Device Cryptographic Key Provisioning for PSA Level 3 MCU: Secure Firmware Synthesis and Attestation"

PSA Level 3 embedded security manufacturing depends on external key infrastructure—secure servers, encrypted transmission, and OTA provisioning—creating critical bottlenecks in production. This creates three problems: infrastructure bottlenecks, inability to verify key uniqueness, and lack of in-situ failure detection.

This paper demonstrates an on-device key generation approach executing within the ATE window, enabling secure, verifiable key synthesis without external server dependency. The architecture has been validated for wireless MCU products requiring PSA Level 3 certification.

- Lalitha Abraham / *Principal Test Development Engineer* / **Synaptics**