Press Release

Ensuring Product Integrity with Intel® Boot Guard

Concurrent Technologies, a leading supplier of processor solutions for demanding environments, now ensures that all their processor boards based on recent Intel® chipsets are running the correct, authorized firmware having implemented Intel Boot Guard. This is important as many of these products are used in defense applications that depend on the firmware acting as the root of trust for subsequent checks on their operating system and application software.

Concurrent Technologies has now implemented all aspects of Boot Guard. The boot firmware in the processor board BIOS is signed using a private key and the board is locked with the public key during the manufacturing process, ensuring that it can only boot Concurrent Technologies signed firmware. Any attempt to use non-authorized firmware will result in the board failing to boot. The firmware can still be updated for maintenance purposes but only with an image signed by the same private key held securely by Concurrent Technologies.

All these processor boards are manufactured by Concurrent Technologies in their own facility in Colchester, UK. Well documented controls are in place to make sure that the correct firmware is loaded according to the product variant ordered. Once these processor boards are delivered, the responsibility for keeping the boards secure passes to the customer. A concern raised by some customers was that the firmware could be interfered during transit to their facility. Boot Guard safeguards against this risk and any subsequent attempts to use non-authorized firmware during the product life-cycle.

Jane Annear, Commercial Director of Concurrent Technologies, commented:

"We are committed to being able to provide our customers with products that meet their needs. Ensuring that our processor boards are running the correct firmware is an example of the way we differentiate our

products and respond to customers' requirements. While security is now a hot topic, it is something we've invested in for many years as we continue to improve our portfolio and capabilities."