QVLx

Secure Boot Services

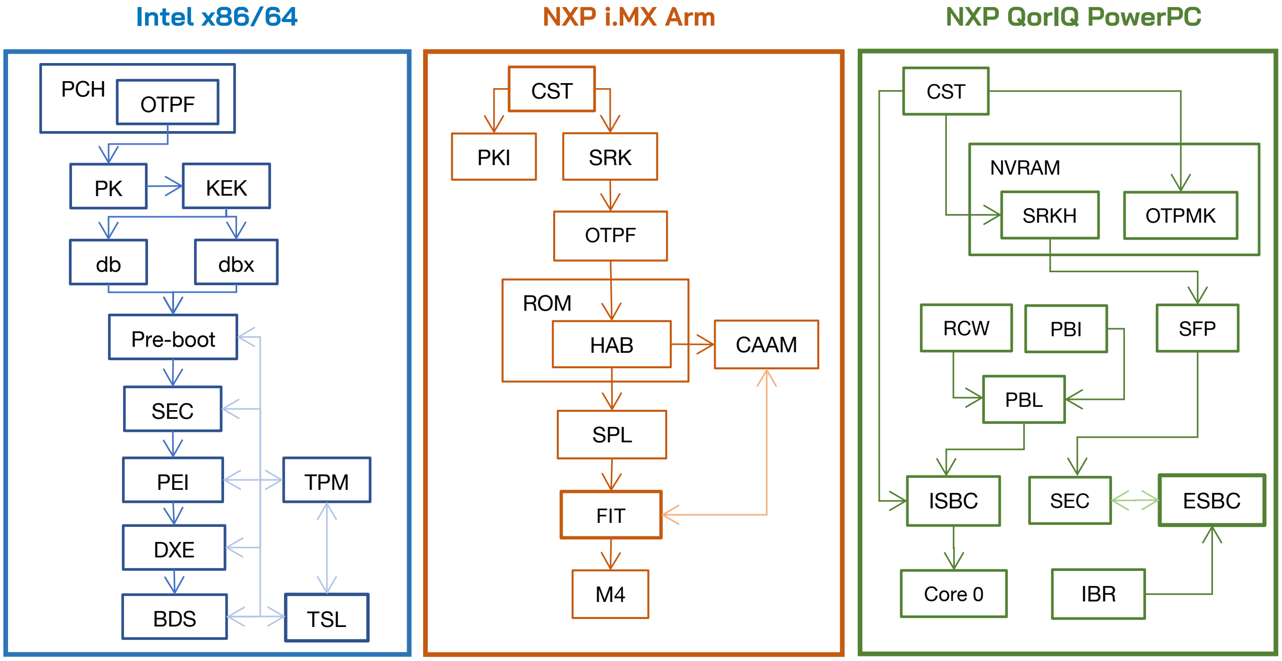
Delivering tailored Chain of Trust solutions so that our customer's vision is actualized using customer-authenticated software foundations

Secure boot is a crucial component to securing embedded systems, preventing malicious software from loading when the board boots up. Tampering in firmware, bootloaders, data, operating system files and other executables is detected by the validation of digital signatures.

Code, files, and data that have bad credentials are rejected by a precautionary fabric that requires distinct hardware features. These features not only accelerate the cryptography, detection, storage, and locking functionality needed for system protection, but more importantly establish ground truth of the system's rightful ownership through mechanisms collectively known as Root of Trust.

QVLx provides secure boot engineering and hardware selection services to meet growing demands for embedded system protection. Delivered solutions can be customized to meet customer requirements and span across various a variety of computer architectures and SoC paradigms.

Some example solutions delivered in the past are diagrammed below:



For more information on QVLx Secure Boot Services, please feel free to contact us:

Email: security@qvlx.com **Phone:** (256)-607-4044