Device HSM Trust Provisioning

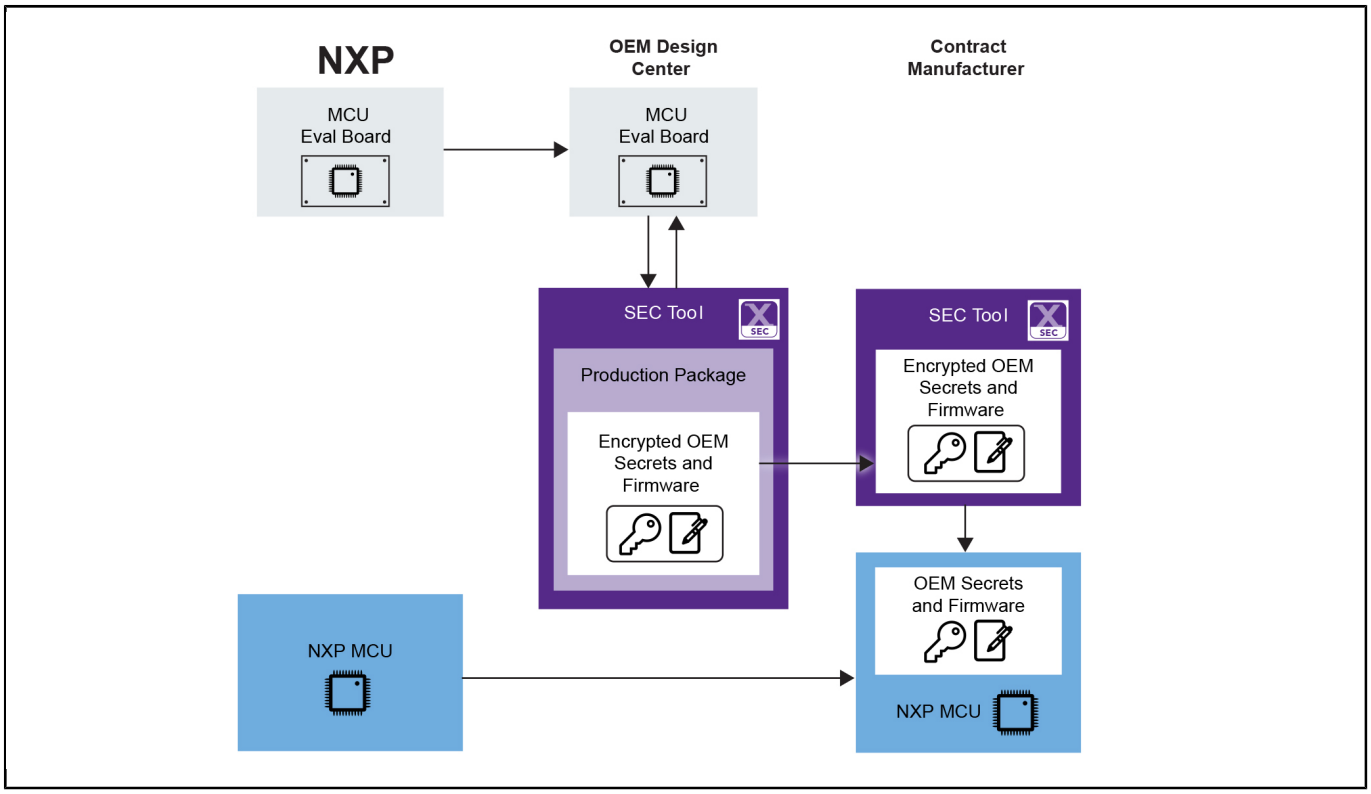
DEVICEHSM-TRUST-PROVISIONING

Last Updated: Apr 24, 2024

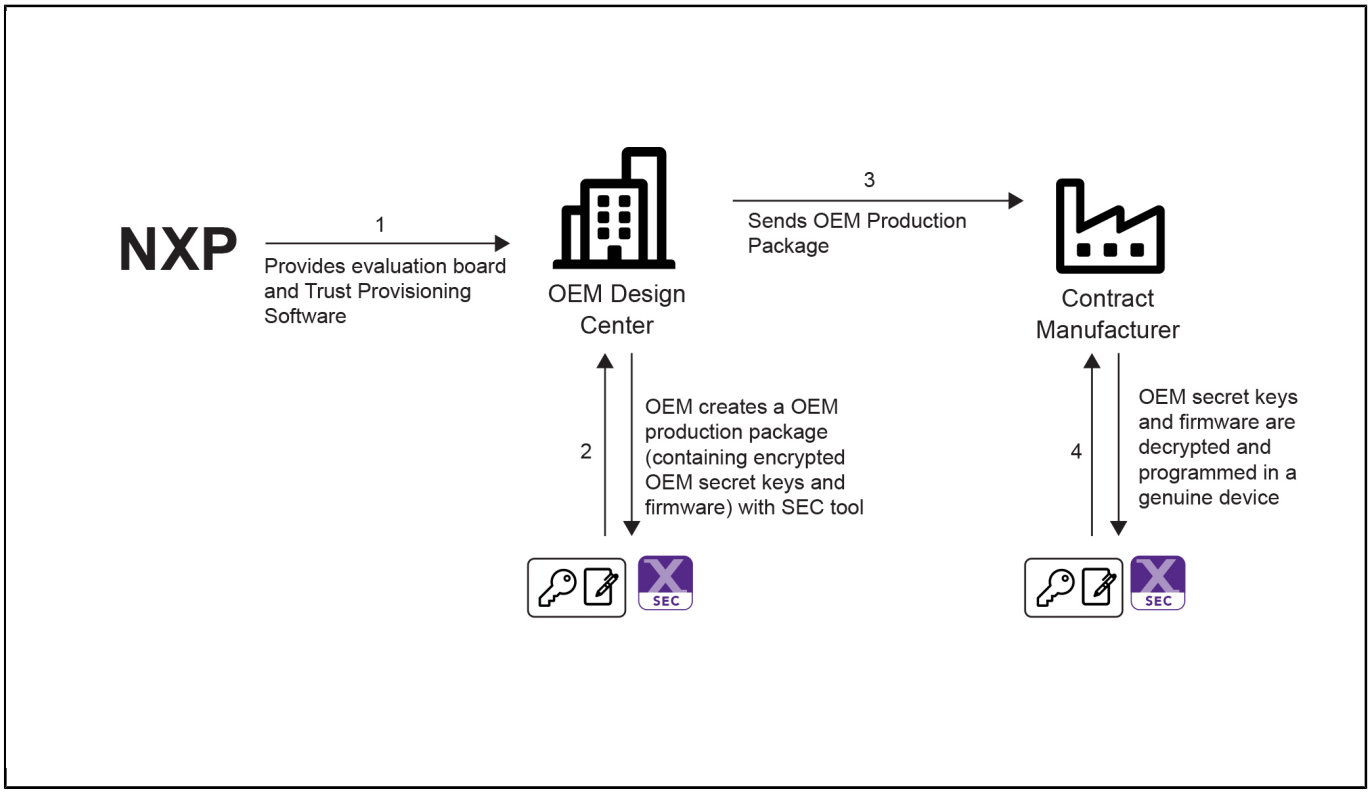
With NXP microcontrollers equipped with the Device HSM trust provisioning feature, OEMs' assets and their software IP can be transferred securely to production factories. Secure programming and provisioning can be achieved even under an unsecure manufacturing environment. A hardware security module (HSM) is typically a device used for securely managing, processing and storing cryptographic keys inside a hardened, tamper-proof hardware. NXP implements this concept at device level so that the HSM capabilities are found in our microcontrollers with the purpose of managing secrets for OEMs. We call this trust provisioning solution "Device HSM".

A microcontroller evaluation board and MCUXpresso Secure Provisioning (SEC) tool are the only required tools to implement Device HSM trust provisioning to protect your software IP and other assets. Contact your local NXP sales representative to learn more.

Device HSM Trust Provisioning Block Diagram



Device HSM Trust Provisioning Flow Block Diagram



View additional information for Device HSM Trust Provisioning.

Note: The information on this document is subject to change without notice.