Smart Card Trust Provisioning for MCUs

SMARTCARD-TRUST-PROVISIONING

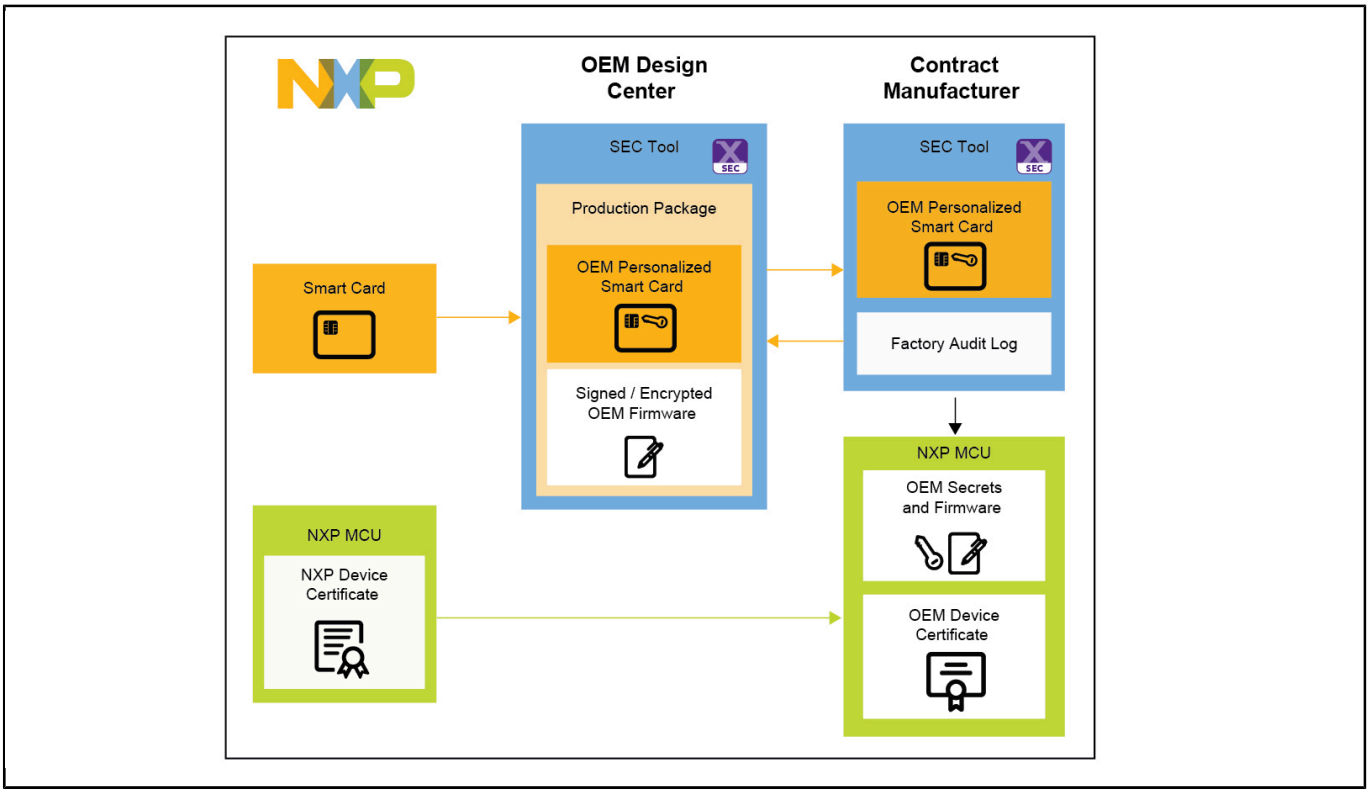
Last Updated: Feb 15, 2024

NXP Smart Card Trust Provisioning is a security enablement for original equipment manufacturers (OEMs) to manage their production process with contract manufacturers (CMs). With MCUXpresso SEC tools and a smart card provided by NXP, OEM’s secrets and intellectual property are sealed and securely transferred to NXP genuine devices during their manufacturing process.

OEMs have the control of the manufacturing process: a production limit is configured and locked in the smart card, and a factory audit log generated by the SEC tool at the CM premise enables the OEM to review the number of provisioned devices. Device-specific certificates are generated and passed to the OEM, which can then be used for cloud onboarding. Smart Card Trust Provisioning is provided as a part of the MCUXpresso SEC tool, supporting NXP general purpose MCUs.

The Smart Card Trust Provisioning solution is available for qualified customers. Contact your local NXP sales representative to learn more.

Smart Card Trust Provisioning Block Diagram Block Diagram



View additional information for Smart Card Trust Provisioning for MCUs.

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