



# 设备HSM可信配置

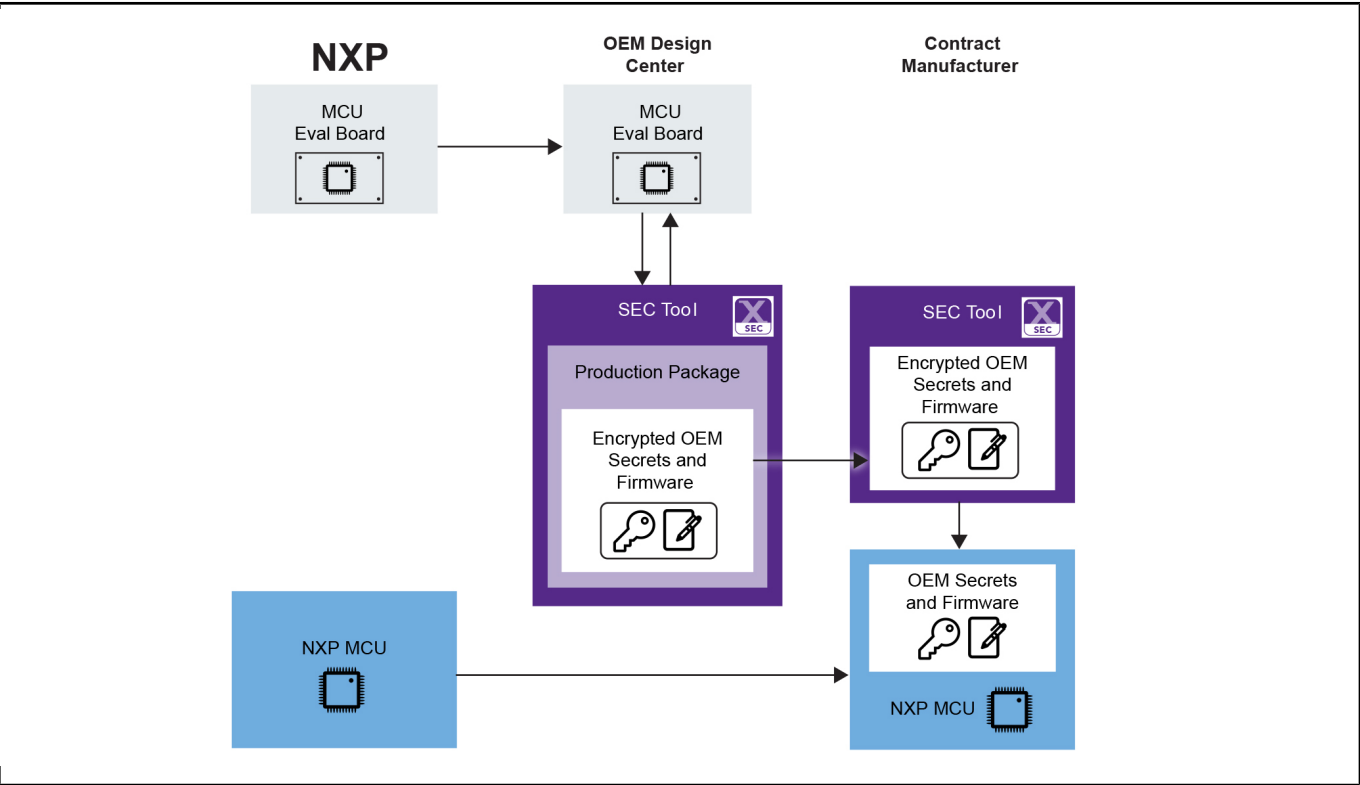
## DEVICEHSM-TRUST-PROVISIONING

Last Updated: Jul 12, 2023

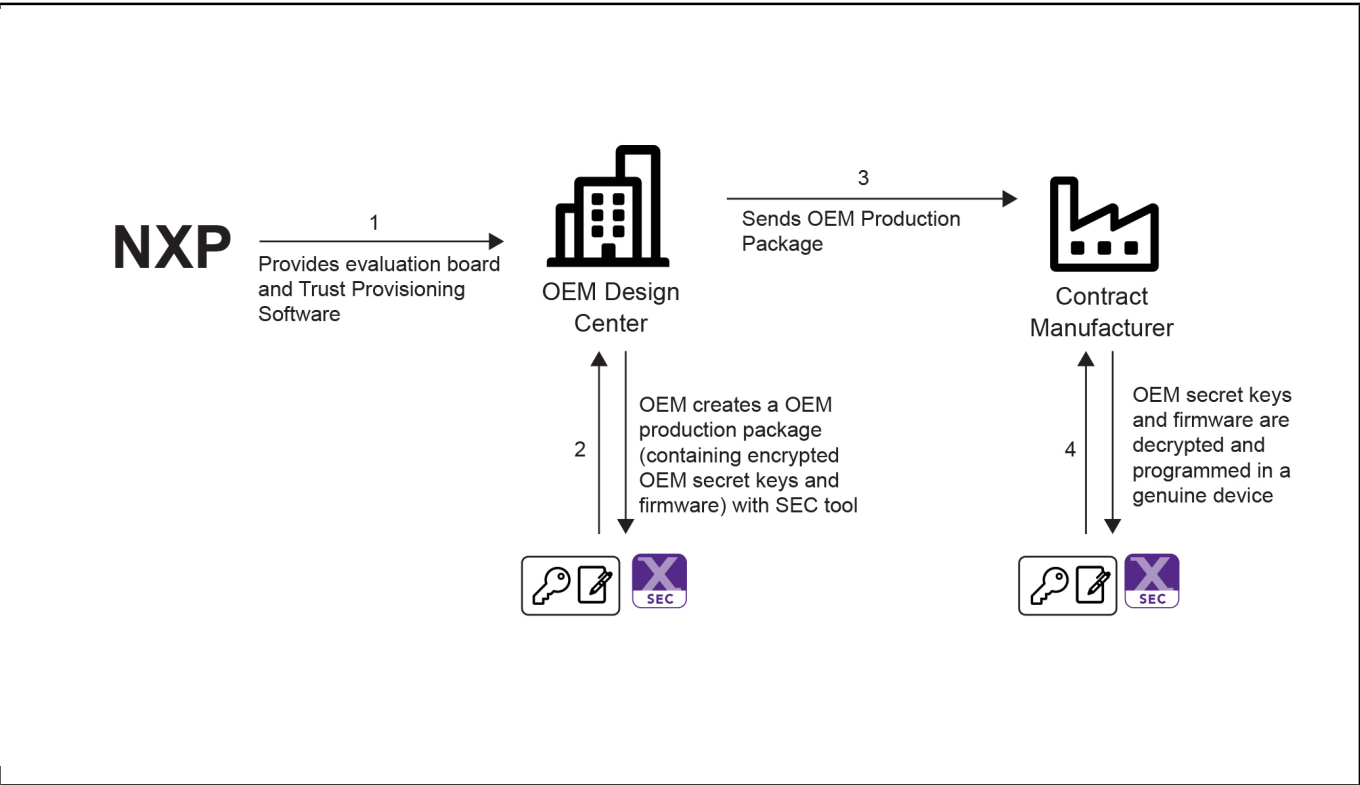
恩智浦微控制器配有设备HSM可信配置功能，能够将OEM的资产及软件IP安全地交付给生产工厂。即使在不安全的制造环境下，也能实现安全编程和配置。硬件安全模块(HSM)是一种专用设备，用于在坚固、防篡改的硬件中安全地管理、处理和存储加密密钥。恩智浦将这一概念应用到设备层面，让我们的微控制器具有HSM的功能，为OEM管理机密信息。我们把这种可信配置解决方案称为“设备HSM”。

使用设备HSM可信配置来保护您的软件IP和其他资产，只需要微控制器评估板和MCUXpresso安全配置(SEC)工具。请联系您当地的恩智浦销售代表，获取更多详情。

设备HSM可信配置 Block Diagram



设备HSM可信配置流程 Block Diagram



View additional information for [设备HSM可信配置](#).

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

---

**www.nxp.com**

NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved. © 2025 NXP B.V.