Security and Trusted Execution Environment (TEE)

OVERVIEW

The NXP® trusted execution environment (TEE) implements a safe zone within the application processor. It leverages ARM® TrustZone® security hardware to execute only trusted and authorized software and protect sensitive data. The security of a TEE is especially challenging, as the TEE needs to protect itself and its trusted applications against attacks using only the resources on the device.

The TEE from NXP implements the GlobalPlatform® specification/API. GlobalPlatform is an independent organization that works across industries to identify, develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology.

NXP is a full member of GlobalPlatform and participates in defining the specifications of the TEE. We are therefore in an excellent position to provide you with up-to-date and forward looking implementations of these specifications. Our Professional Services organization can provide you with all the help you need to integrate the TEE stack, certify your products using TEE and if needed tailor TEE to your specific needs and requirements.

SECURITY AND ASSURANCE

Focusing specifically on security, the TEE is a unique environment that is capable of increasing the security and assurance level of services and applications in the following ways:

- **User authentication:** Using the trusted UI, the TEE makes it possible to securely collect a user's password or PIN. This trusted user authentication can be used to verify a cardholder for payment, confirm a user's identification to a corporate server, attest to a user's rights with a content server, and more.
- **Trusted processing and isolation:** Application processing can be isolated from software attacks by running in the TEE. Examples include processing a payment, decrypting premium content, reviewing corporate data, and more.
- **Transaction validation:** Using the trusted UI, the TEE ensures that the information displayed on-screen is accurate. This is useful for a variety of functions, including payment validation or protection of a corporate document.

- Usage of secure resources: By using the TEE APIs, application developers can easily make use of the complex security functions made available by a device's hardware, instead of using less safe software functions.
- Certification: Trusted certification is best achieved through standardization of the TEE, which in turn improves stakeholder confidence that the security-dependent applications are running on a trusted platform.

FEATURES

- Supported on all i.MX6 and i.MX7 application processor families
- Compliant with GlobalPlatform APIs, enabling development of trusted applications
- Leverages the ARM® TrustZone security hardware for SoC system-wide security
- Provides protection of authentication mechanisms, cryptography, key material and DRM

HOW TO GET TEE

NXP offers fully compliant TEE as a licensed software technology for integration into your i.MX based platform. In addition, NXP also offers professional support and engineering services to assist with the development of trusted applications that are customized and optimized to your targeted application.

For more information or obtain your TEE development kit, please visit **www.NXP.com/TEE**.

www.nxp.com and **www.imxcommunity.org**

Date of Release: September 2016
Document Number: TRUSTEXECENVIRFS REV 0