LPC55S00

SESIP Security Target

Rev. 1.1 — 25 February 2019 **Evaluation document**

PUBLIC

Document information

Information	Content
Keywords	SESIP, Security Target, LPC55S00
Abstract	Evaluation of the LPC55S00 developed and provided by NXP Semiconductors, BL MICR, according to SESIP Assurance Level 1 (SESIP1)

Revision History

Rev.	Date	Description
1.0	2018-02-21	First version
1.1	2018-02-25	Update after evaluator comments

1 Introduction

This Security Target describes the LPC55S00 platform that is evaluated according to the Security Evaluation Scheme for IoT Platforms (SESIP) [1]. The security properties are described in Section 3 of this document, and will be uphold by the platform when the objectives for the environment (described in Section 2) are fullfilled by the platform consumer.

1.1 ST Reference

LPC55S00, SESIP Security Target, Revision 1.1, NXP Semiconductors, 25 February 2019.

1.2 TOE Reference

Table 1. TOE Reference

Reference	Value
TOE Name	LPC55S00
TOE Version	Rev. A0
TOE Identification	LPC55S00
TOE Type	Microcontroller platform for connected applications

1.3 Guidance Documents

The following documents are included with the platform:

Table 2. Guidance Documents

Document	Reference
User Manual	UM11126, LPC55S6x User Manual, NXP Semiconductors [2]

1.4 TOE Overview and Description

The LPC55S00 MCU family builds on the world's first general-purpose Cortex-M33 based microcontroller introduced with the LPC55S00 series. This high-efficiency family leverages the new Armv8-M architecture to introduce new levels of performance and advanced security capabilities including TrustZone-M and co-processor extensions. The LPC55S00 family enables these co-processors extensions and leverages them to bring significant signal processing efficiency gains from a proprietary DSP accelerator offering a 10x clock cycle reduction. Processors in this family include a second Cortex-M33 core for additional flexibility, balancing high performance and power efficiency, and enabling a higher level of security based on hardware spearation.

In addition, the LPC55S00 MCU family provides benefits from 40nm NVM based process technology cost advantages, broad scalable packages, and memory options, as well as a robust enablement including MCUXpresso Software and Tools ecosystem and low-cost development boards.

The LPC55S00 family offers the following security features:

- Dual core M33 based on Arm v8/M architecture, and Arm TrustZone enabled

- PRINCE module for real-time encryption of data being written to on-chip flash and decryption of encrypted flash data during reading to allow asset protection
- AES-256 encryption/decryption engine
- Secure Hash Algorithm (SHA2) module supporting secure boot with dedicated DMA controller
- Physical Unclonable Function(PUF) using dedicated SRAM for silicon fingerprint. PUF can generate, store, and reconstruct key sizes from 64 to 4096 bits. Includes hardware for key extraction
- RSA and ECC support
- Random Number Generator (RNG)
- 128-bit unique device serial number for identification (UUID)
- Secure GPIO

The functional block diagram is shown in the figure below. This diagram provides a view of the chip's major functional components and core complexes.

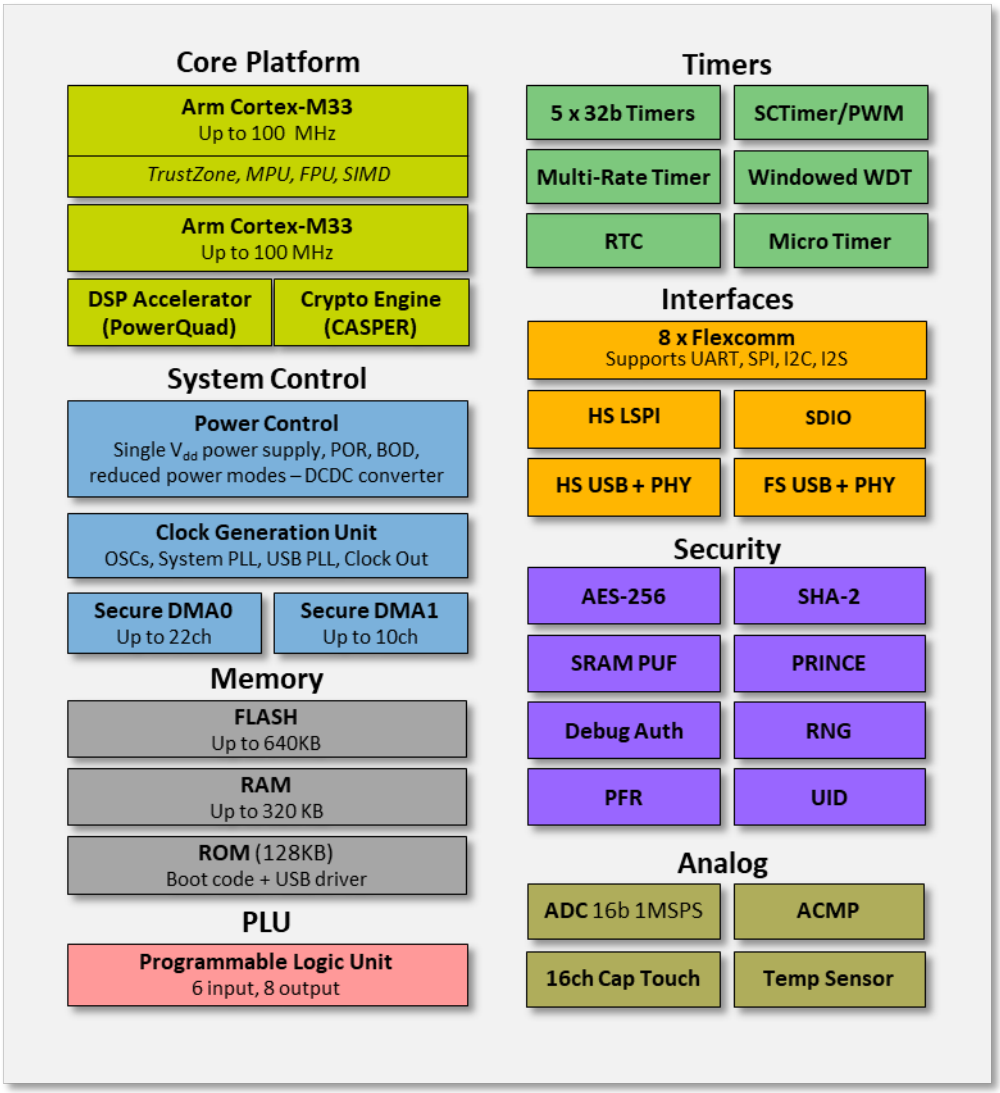

Figure 1. Functional Block Diagram

Figure 2 shows the Firmware functionality supported by the LPC55S00.

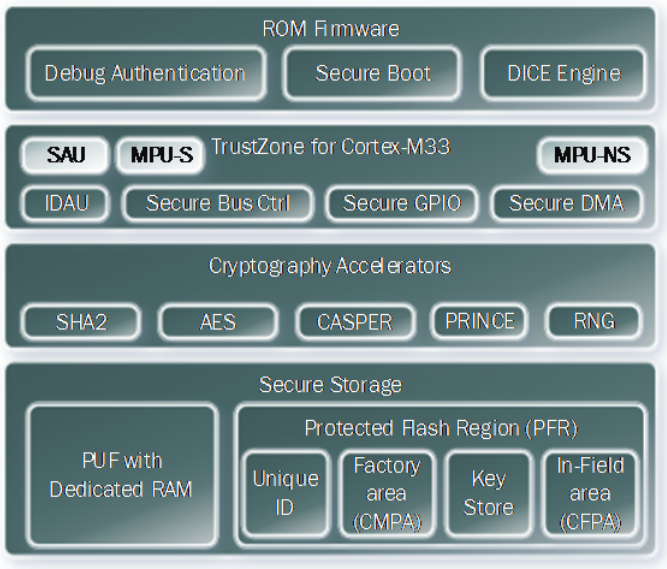

Figure 2. Firmware Overview

The platform consists of a microcontroller implementing Secure Boot, support for cryptographic primitives AES-128/256, SHA-1, SHA-224, SHA-256, random number generation, support of tamper detection and more.

Figure 1 further shows that the LPC55S00 include a dual Cortex-M33 (ARMv8-M architecture), which supports TrustZone. The Secure Processing Environment controls all the security mechanisms and peripherals, and it runs in the Secure mode of one of the M33 core, with other parts of the system running on that core's Normal mode. Untrusted services run on the other core, with the interface with the first code running in Secure Mode.

The platform is intended to be used by an integrator that deploys it into a connected solution together with its own operating systems and user applications.

The main security features of the platform are listed in Section 3 of this document.

1.4.1 Physical Scope of the TOE

The physical scope is the LPC55S00 microcontroller as identified in Table 1 and whose functional blocks are identified in Figure 1. It includes the dedicated firmware located in the on-chip boot ROM.

1.4.2 Logical Scope of the TOE

The logical scope includes the hardware interfaces that operating systems or applications would make use of. The logical scope of the firmware is limited to the Secure Boot functionality stored in the on-chip boot ROM.

Any OS or application software stored on the platform is not in scope of this evaluation.

1.4.3 Required non-TOE Hardware/Software/Firmware

No additional non-TOE hardware, software or firmware is required for the correct functioning of the security claims described in this document.

2 Security Objectives for the Operational Environment

In order for the platform to fulfill its security requirements, the operational environment (technical or procedural) must fulfil the following objectives:

- The OS or application developer shall verify the correct version of all platform components it depends on as described in the User Manual
- The OS or application developer shall enable the Secure Boot feature as described in the User Manual.
- To allow execution of unknown code while maintaining the protection of platform security features as declared in Section 3, the OS or application developer shall configure restrictive memory boundaries via the MPU as described in the User Manual.

Please refer to Section 1.3 for references to the guidance documentation mentioned above.

3 Security Requirements

3.1 Security Functional Requirements

The Security Functional Requirements (SFRs) are listed below, together with a short rationale explaining why the platform meets the requirement (*in italics*).

3.1.1 Identification and Attestation of Platforms and Applications

3.1.1.1 Identification of Platform Type

The platform provides a unique identification of the platform type, including all its parts and their versions.

The chip includes values in a protected FLASH memory region that uniquely identify the platform type, including a part of the Lot identifier and a Silicon Revision Number as described in the User Manual.

The protected FLASH memory region is written as part of the production and test process, and the production testing procedures verify the value has been written correctly.

3.1.1.2 Identification of Individual Platform

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

The chip includes in the protected FLASH memory region a 128-bit unique identifier.

The content of the protected FLASH memory region is written as part of the production test process, and this procedure verify that the value has been written correctly.

3.1.1.3 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to a secure state.

When the device boots, the execution starts in the device's physical ROM by the secure boot mechanism that verifies the authenticity of the firmware before executing it. The signature uses RSASSA-PKCS1-v1_5 signature [6] of a SHA256 digest with 2048-bit or 4096-bit key size. An option is available to force the use of 4096-bit keys.

The public key used for signing the firmware is itself authenticated by a chain of signatures in a certificate, using one of four root keys. A fingerprint of these root keys is stored in the device's fuses, and used to validate the root key.

The secure boot feature is tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.2 Product Lifecycle: Factory Reset / Install / Update / Decomission

3.1.2.1 ~~Secure Update of Platform~~

~~The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.~~

The platform does not support the update or patching of firmware located in the on-chip ROM. It does offer a feature for customers to implement secure update mechanisms of their own code. According to [1] the absence of this functionality for the platform must be explained as part of ALC_FLR.2. Please see Section 3.2.1 for this explanation.

3.1.2.2 Decommission of Platform

The platform can be decommissioned.

The chip includes a Field Return mode, in which sensitive data is destroyed on the chip. In that mode, debugging is possible, as well as execution of any firmware.

The switch to Field Return mode can only be obtained by loading a chip-specific boot image that includes the chip's unique ID, verifying its authenticity, and by running it. Such a boot image can only be authenticated by using one of the keys allowed to sign firmware images.

The Field Return mode is tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.3 Extra Attacker Resistance

3.1.3.1 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

The Processors in the TOE include a dual Cortex-M33 (ARMv8-M architecture), which supports TrustZone. The Secure Processing Environment controls all the security mechanisms and peripherals, and it runs in the Secure mode of one of the M33 core, with other parts of the system running on that core's Normal mode. Untrusted services run on the other core, with the interface with the first code running in Secure Mode.

The separation mechanisms are tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.4 Cryptographic Functionality

3.1.4.1 Cryptographic Operation

The platform provides the application with *encryption and decryption* functionality as specified in *FIPS 197 (AES)* [5] for key length *128 or 256 bit* and modes *ECB and CBC and CTR*.

The platform provides the application with *hashing* functionality as specified in *FIPS 180-4* [4] for digests of *160 bits (SHA-1) and 256 bit (SHA-256)*.

The support for cryptographic operations is described in the User Manual.

The cryptographic functionalities are tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.4.2 Cryptographic Keystore

The platform provides the application with a way to store *cryptographic keys* such that not even the application can disclose this data. This data can be used for the cryptographic operations: *encryption, decryption, signature generation*.

The TOE supports a hardware unique key, managed by the PUF Keystore, which is a 256-bit AES key derived from a PUF output; this key is never accessible in main memory, as it is directly fed to the AES accelerator when needed.

For the authentication checks during boot, several keys can be used to sign the files. A hash of the hashes of the corresponding public keys is stored on the chip's Protected Flash Region (PFR) and is used to verify the validity of the public key in the boot image.

Other secret keys used by the secure processing environment can be derived from the hardware unique key and can be managed directly by the PUF keystore.

The PUF is tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.4.3 Cryptographic Random Number Generation

The platform provides the application with a way based on *physical noise* to generate random numbers to as specified in AIS31 (P1/PTG.1) [3].

The platform includes a Standalone True Random Number Generator (SA-TRNG) module that generates a 256-bit entropy as needed by an entropy-consuming module or by other post-processing functions.

The RNG functionality is tested against a defined stochastic model by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.1.5 Compliance Functionality

3.1.5.1 Secure Encrypted Storage

The platform ensures that all data stored by the application, with the exception of *data that the user doesn't explicitly encrypt*, is encrypted as specified in *FIPS 197 (AES)* [5] with a platform instance unique key of keylength *128* in *ECB or CTR* modes.

The TOE firmware offers a secure storage service to be used by the application. The secure storage service implements an AES-GCM based AEAD encryption policy to protect data integrity and authenticity. It uses a key derived from the device's HUK (Hardware Unique Key).

The secure storage functionality is tested thoroughly by means of simulation tests during the design phase and by validation campaigns before chip release. Each die undergoes production tests to ensure its correct functioning on each final product.

3.2 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP1** as defined in [1]. The assurance requirements are as follows:

Table 3. Security Assurance Requirements for SESIP1

Assurance Class	Assurance Families
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction ASE_OBJ.1 Security requirements for the operational environment ASE_REQ.3 Listed security requirements ASE_TSS.1 TOE summary specification
ALC: Life-cycle Support	ALC_FLR.2 Flaw reporting procedures

3.2.1 Flaw Reporting Procedures (ALC_FLR.2)

In accordance with the requirement for flaw reporting procedures (ALC_FLR.2), the developer has defined the following procedure:

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes 4 steps:

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The firmware located in the on-chip ROM of the platform cannot be updated or patched. However, the platform's Secure Boot feature is able to verify the authenticity of customer code during the initial boot and outside of the boot sequence, providing an appropriate mechanism for supporting the update of this code. The update mechanism itself has to be provided by the customer, most likely at the operating system level and is not in scope of this evaluation.

4 Mapping and Sufficiency Rationales

4.1 ITP1 Sufficiency

Assurance Class	Assurance Familiy	Covered By	Rationale
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.2, the TOE overview and description in TOE Overview and Description.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in the SFR.
ALC: Life-cycle Support	ALC_FLR.2 Flaw reporting procedures	Section 3.2.1	The flaw reporting and remediation procedure is described.

5 Bibliography

5.1 Evaluation Documents

[1] Security Evaluation Scheme for IoT Platforms, Version 1.1.

5.2 Developer Documents

[2] UM11126, LPC55S6x User Manual, NXP Semiconductors.

5.3 Standards

[3] A proposal for: Functionality classes for random number generators, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 18 September 2011.

[4] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, Information Technology Laboratory, National Institute of Standards and Technology, August 2015.

[5] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

[6] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

6 Legal information

6.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

6.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 25 February 2019