AN14145

MCX N系列的闪存交换功能

第3版—2024年7月23日 应用笔记

文档信息

信息	内容
关键词	AN14145、MCX N9xx、MCX N2xx、闪存交换
摘要	本应用笔记介绍了如何使用MCX系列的闪存重映射功能。

1 介绍

1.1 简介

本应用笔记介绍了如何使用MCX N系列BootROM中的双镜像启动功能，以实现一个可靠的双固件升级机制。

当嵌入式设备正在进行升级时，断电或强制中断等外部因素都可能会阻碍新固件完整地写入闪存。这会导致系统在启动时出现问题。如果固件文件在设备运行时被损坏，则系统就会崩溃，导致设备无法运行。要解决这些问题，可采用双固件的方法。确保始终至少有一个固件文件能够正常启动和运行。如果出现任何问题，BootROM会检测并使用备份的固件文件。

MCX系列的BootROM支持内部闪存的双固件启动机制。这意味着可以在闪存区域内放置两个固件文件。BootROM会根据固件版本决定启动哪个固件。本应用笔记目前仅涵盖了使用内部闪存作为固件存储介质。通过本文，可以学到：

- MCX N系列MCU的闪存布局和基本用法。
- MCX N系列BootROM及内部闪存双固件启动的介绍。
- 如何使用恩智浦安全预处理工具创建双固件，并将其下载到MCU闪存中进行双镜像启动。

下文使用FRDM-MCXN947作为目标平台，但其他MCX N系列芯片也具有类似的特性和功能。

例如，MCX N23x共有1MB闪存（由2个512KB的块组成），而MCX N947上有2MB闪存（由2个1MB的块组成）。

1.2 内部闪存布局

MCX N947芯片内置了2MB的闪存。该闪存被分为两个块，每个块的大小为1MB。图1直观地展示了该芯片上的闪存架构。

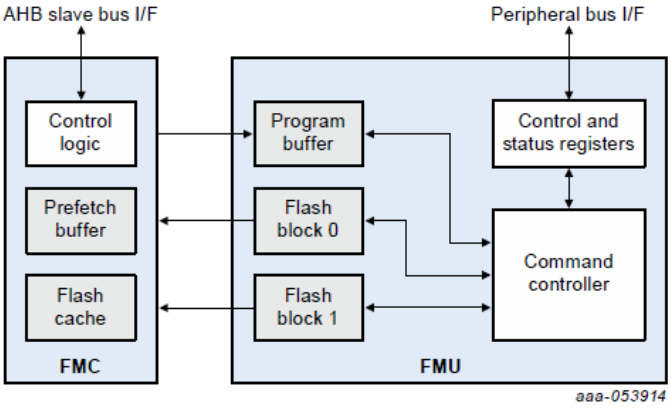

图1. 闪存的架构

该闪存的最小擦除单元被指定为一个大小为8kB的扇区。同时，最小写入单元被称为Phrase，其大小为16B。

2 启动的流程

在上电和启动期间，ROM首先会检测在CMPA中被重定位的镜像文件的位置和大小，然后检查两个镜像的版本号。据此，当使用双镜像时，图2所示为双镜像的内部闪存的启动流程。

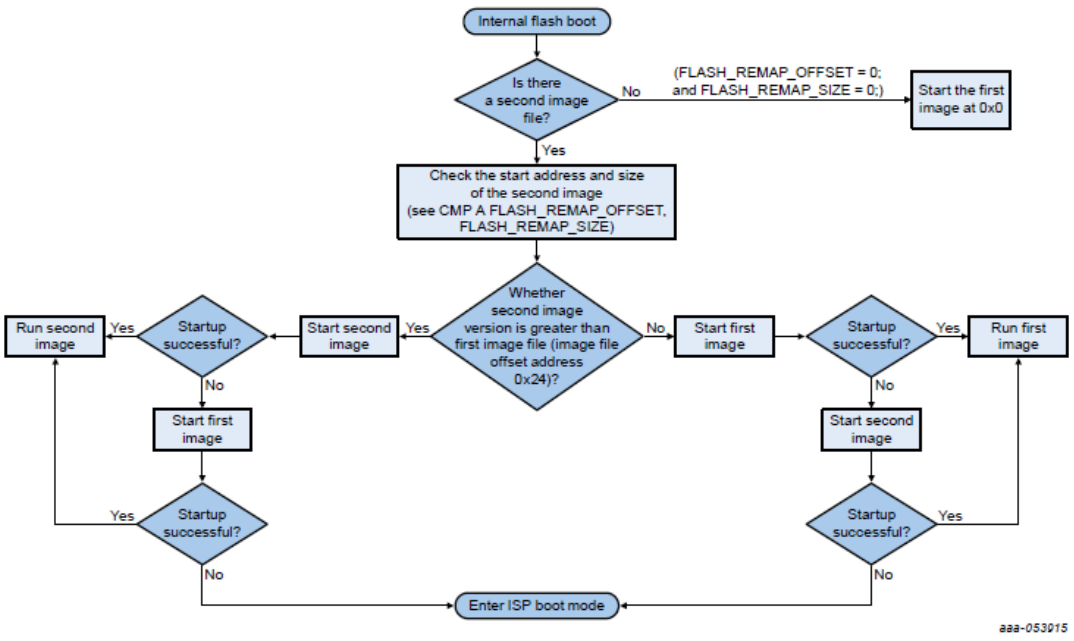

图2. 双镜像内部闪存的启动流程

当BootROM使能双固件启动功能并检测到某个块中有一个更新版本的固件时，它会自动重新映射闪存的AHB访问地址，并启动相应的固件。图3所示为内部闪存控制器的重映射功能：当块1中的固件处于工作状态时，对0h地址的访问会被重映射到闪存块1的起始偏移值。通过这个功能，BootROM实现了两个固件版本的双固件启动。

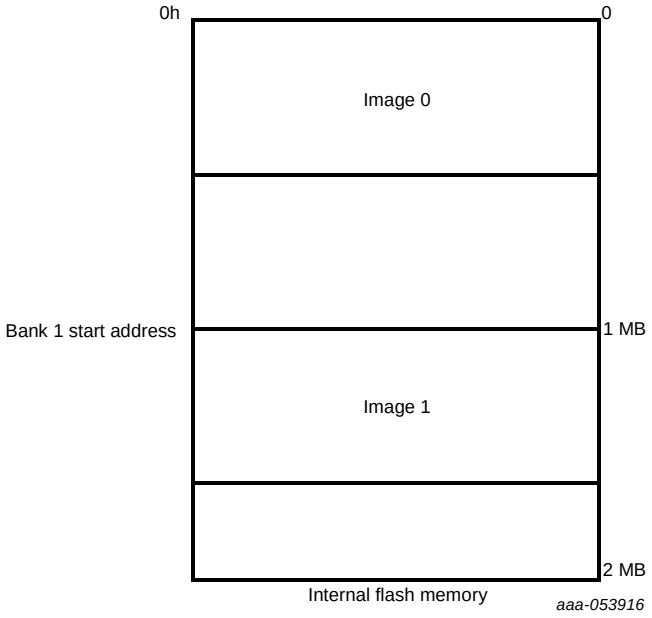

图3. 内部闪存控制器的重映射功能

3 配置固件文件

MCX N947的固件以标准中断向量表开始，其存储位置被定义为固件配置字段。有两个相关字段：

- 镜像长度：表示固件的总长度，包括签名。
- 镜像类型：表示固件的类型。它支持两种类型：纯镜像（无CRC校验或签名）和带CRC的纯镜像（包括固件长度和CRC校验）。镜像类型字段的前16位表示固件版本。在双固件启动期间，BootROM会自动识别该字段，并尝试启动更高版本的固件。

注：*对于从内部闪存启动的双固件，如果*`bit[10]`*设置为0，则BootROM默认认为固件版本为0。*

表1. 固件文件

偏移量（十六进制）	大小（字节）	符号	说明
00	4	初始SP	栈指针
04	4	初始PC	应用程序的第一条执行指令
08	24	向量表	Cortex-M33核的向量表入口
20	4	镜像长度	当前镜像的长度（总长度，包括签名），如果镜像类型为其他值，则设置为实际镜像长度。
24	4	镜像类型	镜像类型，位[7:0]： • 0h：纯镜像 • 2h：带CRC的纯镜像 • 4h：签名镜像 • 5h：带CRC的纯镜像 • 6h：SB3清单 `Load_to_RAM`镜像：镜像在镜像标头中有非零的`image_load_address`和`image_length`。 其他值保留。 位[10]：显示镜像版本是否包含在镜像类型[31:16]中： • 0：镜像版本未包含在镜像类型（**Image Type**）中。 • 1：镜像版本包含在镜像类型（**Image Type**）中，仅适用于内部闪存XIP的使用情况。 位[13]：显示镜像是否包含TZM预设数据： • 0：镜像未包含TZM预设数据。 • 1：镜像包含TZM预设数据。 位[31:16]：当位[10]=1时的镜像版本（用于片上闪存）。

4 CMPA

在CMPA中，只有一项与双固件启动相关的设置：`FLASH_REMAP_SZ`。

表2介绍了CMPA中的内部闪存双固件启动重映射设置。当CMPA中的`FLASH_REMAP_SZ`设置为非零值时，内部闪存的AHB访问会根据当前工作的闪存块号更改其访问地址。例如，如果`FLASH_REMAP_SZ` = 2h，则重映射大小为96kB ((2h+1) × 32kB)。

表2. 启动镜像1的重映射大小

区域	地址	字名称	说明
CMPA	0100_4004h	FLASH_REMAP_SZ	指示从闪存存储区的块1地址，0h，到BootROM的闪存重映射的大小。

有关CMPA的更多详细信息，请参阅《MCX N947用户手册》附带的Excel表格。

5 实操

恩智浦提供了一个安全预处理工具GUI，用于执行各种固件的配置和下载任务。

MCUXpresso安全预处理工具是一款GUI工具，简化了在恩智浦MCU平台上创建和配置可启动的可执行文件的过程。它基于恩智浦提供的经过验证的安全支持工具集，使用了BootROM提供的扩展编程接口。该工具集成了固件创建和烧录功能，大大简化了创建双固件文件的过程！

1. 从以下链接下载恩智浦安全预处理工具：MCUXpresso Secure Provisioning Tool。
2. 配置：在安全可执行镜像（**Secure executable image**）下，选择已编译工程的*bin/hex*文件（如`mcx_dual_swap.hex`）。如图4所示来配置其他选项，然后点击构建镜像（Build Image）生成带CRC镜像的版本。

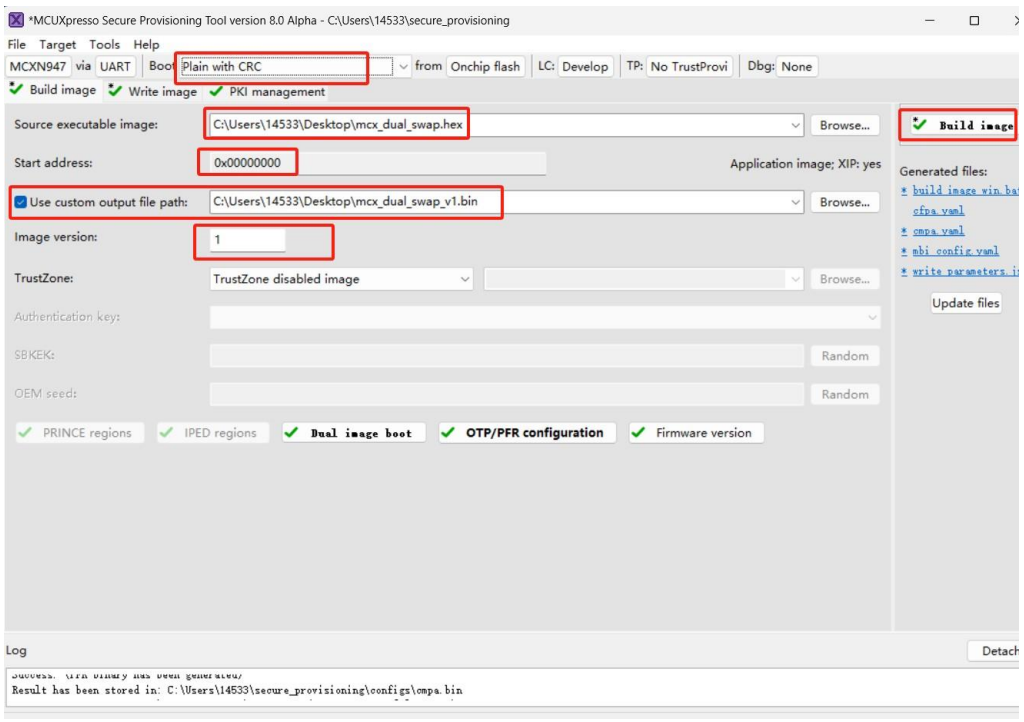

图4. 安全可执行镜像文件选项卡

3. 在“**双镜像启动**”部分，按照以下步骤操作：
   - 将双镜像区域设置为**image0=1MB**、**image1=1MB**。
   - 将第一个版本的固件下载到image 0区域。

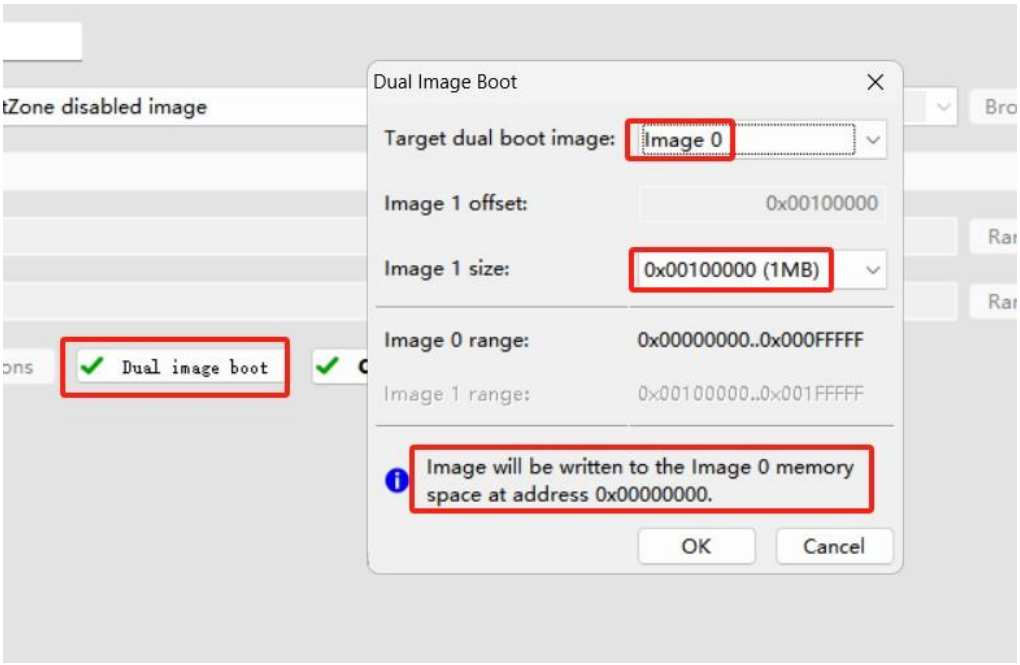

图5. “双镜像启动”部分

4. 点击“构建镜像”（**Build Image**）。此操作会自动生成*mcx_dual_swap_v1.bin*。该文件是嵌入了CRC和长度详细信息的镜像。安全预处理工具还会根据**双镜像启动**的设置构建相应的CMPA和CFPA信息块。

5. 切换到“写入镜像”（**Write Image**）界面。选择UART（或HID）ROM下载方式。默认情况下，GUI会选择最近创建的镜像文件。确保您的电路板已进入到BootROM模式。然后，点击“写入镜像”（**Write Image**）开始下载过程。

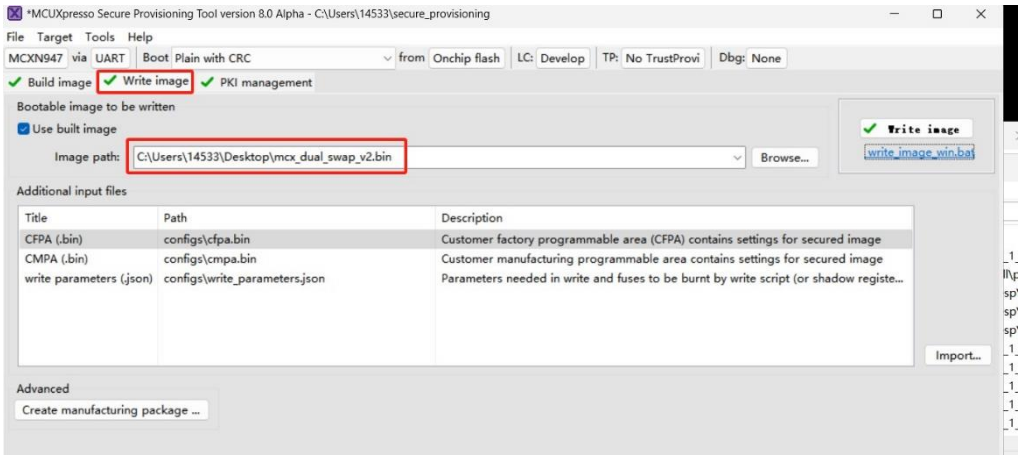

图6. “写入镜像”界面

6. 如果出现“blhost成功”（*blhost succeeded*）消息，则表示下载成功。此固件现在已存储到了*image0*区域。通过复位开发板，相应程序即可运行。
7. 如果有一个更高版本的固件需要更新，请选择将固件下载到*image1*区域。

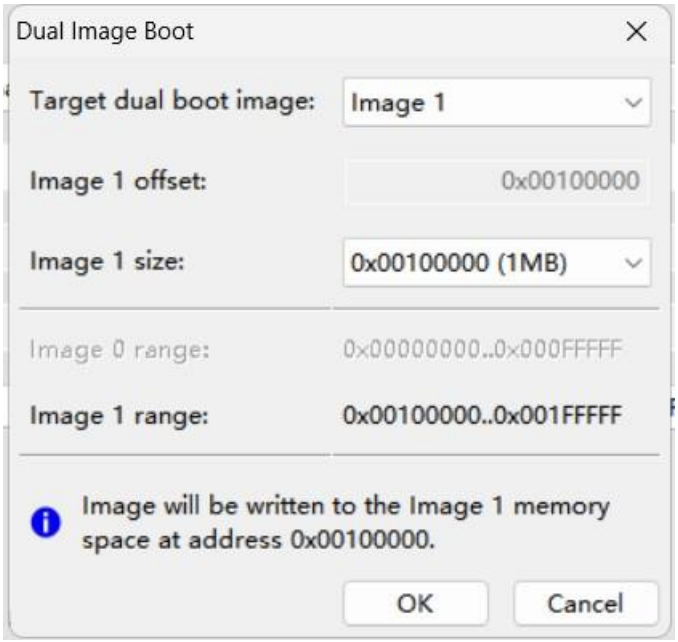

图7. 下载固件

8. 如果新固件的版本高于上一版，则会自动从新版本启动。如果新固件在下载过程中出现通信中断，导致升级失败，则在下一次启动时BootROM会检测到新固件不完整，然后它会回退并从旧版本的固件启动，确保可靠的双固件升级功能。

6 修订历史

表3汇总了对本文档的修订。

表3. 修订历史

文档ID	发布日期	说明
AN14145 v.3	2024年7月23日	更新说明以支持MCX N23x
AN14145 v.2	2024年3月25日	更新说明以支持N11 • 更新了第1.1节
AN14145 v.1	2024年1月20日	首次公开发布

Legal information

Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com.cn/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.

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.

Suitability for use in non-automotive qualified products — Unless this document 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.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

MCX — is a trademark of NXP B.V.

目录