AN14361

启用RTF时使用ELS ECSIGN命令生成数字签名

第1.0版—2024年7月29日 应用笔记

文档信息

信息	内容
关键词	AN14361、MCX、MCX Nx4x、数字签名、ECSIGN、RTF、ELS
摘要	本应用笔记主要介绍了ECSIGN命令，并在启用RTF的情况下使用该命令创建了一个演示工程。

1 介绍

MCX Nx4x是一系列面向嵌入式应用的基于ARM Cortex-M33的微控制器。它配备了先进的串行外设、CoolFlux BSP32、PowerQuad DSP协处理器以及增强型安全功能，可支持各种各样的应用。

该系列微控制器支持不同的安全功能，包括ELS和PKC模块。这些模块支持安全启动、AES、ECDSA、UUID、动态加密和解密、调试认证以及DICE。

1.1 EdgeLock安全子系统（ELS）

随着物联网设备的使用量不断激增，这些设备易受各种漏洞攻击的风险也随之增加。因此，对用户来说，所拥有的设备中的数据是安全、隐蔽且不可篡改的，就变得至关重要。这就是ELS作为解决方案发挥作用的地方。

ELS也称为EdgeLock安全飞地（ELE），为设备凭证和平台完整性密钥提供了一个安全的存储空间。它为执行敏感的安全功能（包括加密操作或SoC完整性保护功能）提供了最高级别的隔离。

MCX Nx4x配备了EdgeLock安全子系统S50模块。该安全子系统在SoC上提供强大的密钥隔离，并支持多种加密算法。这些算法包括AES、HMAC、基于HMAC的HKDF、CMAC等。ELS是SoC不可变信任根的主要构件。在安全启动、安全调试访问、生命周期管理和信任配置过程中，它被用作信任锚的一部分。ELS的AES运算被配置为对旁路攻击提供抵御。ECC P-256运算对旁路攻击和低成本故障攻击提供保护，如非局部电磁故障注入（EMFI）、电源和时钟毛刺攻击。有关ELS的更多详细信息，请参阅《MCX Nx4x安全参考手册》（文档MCXNx4xSRM）[1]。

1.1.1 ELS命令

ELS的主要用户接口是通过ELS命令。表1列出了这些命令。此表中仅提供了简要说明。有关命令及其用法的详细信息，请参阅MCX Nx4x SRM。

表1. ELS命令列表

命令	命令ID（十进制）	说明
CIPHER	0	这条命令在ECB、CBC、CTR等密码模式中的一种模式下运行分组密码，如NIST SP 800-38a“BLOCK CIPHER MODES”中所述。
AUTH_CIPHER	1	这条命令运行经过身份认证的分组密码，如NIST SP 800-38d_topic_is_GCM_BLOCK_CIPHER_MODE_中所述。
ECSIGN	4	这条命令运行ECDSA P-256签名操作。
ECVFY	5	这条命令运行ECDSA P-256签名验证操作。
KEYGEN	8	这条命令运行ECDSA P-256 diffie-hellman密钥交换计算，以创建共享密钥。
KEYIN	9	这条命令创建非对称密钥对。
KEYOUT	10	这条命令使用RFC3394算法“封装”（加密）ELS内部密钥，并将已加密的密钥存储在系统内存中。

1 要获取本文，请联系当地的恩智浦现场应用工程师（FAE）或销售代表。

表1. ELS命令列表（续）

命令	命令ID（十进制）	说明
KDELETE	11	这条命令从ELS内部密钥库中删除密钥。
CKDF	16	这条命令从ELS主密钥派生（创建）新密钥，并使用NIST SP 800-108算法将新密钥存储在ELS内部密钥库中。
HKDF	17	这条命令从ELS主密钥派生（创建）新密钥，并将新密钥存储在ELS内部密钥库中。HKDF使用RFC5869算法或NIST SP 800-56C算法中的基于哈希的选项。
TLS_INIT	18	这条命令创建由TLS 1.2标准定义的会话密钥。
HASH	20	这条命令使用NIST FIPS 180-4 (SHA2)标准对消息进行哈希运算。
HMAC	21	这条命令根据NIST FIPS 198-1定义创建经过身份验证的消息哈希。
CMAC	22	这条命令根据NIST SP 800-38b定义创建经过身份验证的消息哈希。
RND_REQ	24	这条命令根据NIST SP 800-90Ar1定义创建伪随机数据块或由ELS TRNG输出的原始随机数据块。
DRBG_TEST	25	这条命令支持FIPS CAVP测试。它支持3种模式。
DTRNG_CFG_LOAD	28	这条命令加载已准备好的TRNG配置，以正确配置ELS内部TRNG。

本应用笔记主要介绍了ECSIGN命令，并在启用RTF后使用该命令创建一个演示工程。MCX Nx4x SDK包含了各种ELS命令示例工程，其中包括ECSIGN的使用，但不包括启用RTF的情况。有关此特定用例的更多信息，请参阅以下章节。

1.2 运行时指纹（RTF）

RTF是一个256位的内部寄存器，可用于支持系统硬件和固件的认证流程。它位于内部ELS寄存器中，但无法通过寄存器映射访问。这种访问限制可防止试图制作RTF的伪造副本，即未通过对系统内存进行哈希运算而创建的副本。每当ELS复位时，它就会被初始化为256'h0的常量值。这种支持步骤的示例如下：

- ELS可以配置为将HASH命令的结果输出到RTF。以这种方式配置时，RTF的当前值包含在HASH输入数据中。因此，使用RTF进行的每个连续哈希的输出都取决于先前所有使用RTF进行的哈希的结果。这样，使用RTF的HASH可用于从系统内存的多个部分构建累积摘要。这可用作系统固件的代表性摘要。固件创建者必须能够独立地重新创建相同的摘要值。有关如何通过ELS HASH命令更新RTF的详细信息，如下所示：
  1. 对HASH的输入消息进行正常哈希运算。
  2. 然后，将生成的摘要附加到RTF的当前值并再次进行哈希运算。有关将RTF与哈希消息结合的算法详情，请参阅HASH参数（位于MCX Nx4x SRM）中的RTFUPD参数。
  3. 最终RTF值存储在RTF中。
  4. 生成的哈希值（含RTF）存储到HASH命令提供的输出缓冲区中。输出结果如下：*Output = HASH || RTF*

- 从系统内存的哈希值更新RTF后，可将其“添加”到要签名的消息（质询）中。然后，可以使用ECSIGN命令对结果进行签名。有关将RTF添加到要用ECSIGN命令签名的消息中的算法详情，请参阅ECSIGN参数（位于MCX Nx4x SRM）中的SIGNRTF参数。由于生成的签名取决于RTF值，而RTF值又取决于系统内存的内容，因此正确的签名可证明系统内存的内容符合预期，且未被篡改。
  由于该步骤可帮助用户验证设备的系统固件和内存，因此本应用笔记演示了上述部分。
- 为了进一步证明经过认证的固件是在可信硬件上运行的，ELS还支持从系统中收集“硬件签名”，即硬件认证数据（HAD）。实际认证包括“质询-响应”步骤。示例如下：
  验证者创建一个质询，并将其发送给ELS。ELS将质询、RTF和HAD拼接起来。然后，它使用可信的签名密钥对结果进行签名，并将签名和HAD一起返回给验证者。验证者拥有质询和HAD，可以重新创建RTF。因此，验证者可以独立地重新创建拼接的消息，并使用它来验证ELS返回的签名。

1.3 ECSIGN命令

ECSIGN命令生成ECC P-256数字签名。它通过ELS密钥库，使用ECC签名密钥计算调用者提供的质询（数据）的签名。根据需求，用户或预生成的ELS密钥之一可用于生成ECC签名密钥。此命令还有特定的字节和位顺序要求。

ECSIGN包括以下子操作：

1. 从系统内存中读取质询，并在需要时对质询进行哈希运算（质询可以预先进行哈希运算。在这种情况下，不需要进行哈希运算）。
2. 使用ECC签名密钥计算质询哈希值上的签名。
3. 将签名写入系统内存。

1.3.1 数字签名在身份认证场景中的使用

ECSIGN命令生成数字签名。通常情况下，数字签名是“加密身份认证”场景要求的一部分，其中ELS嵌入到必须向“主机”验证自身身份的“外设”中。为此，外设必须持有非对称密钥对的私钥，以及包含此密钥对的公钥的证书。

其步骤如下：

1. 外设将其证书发送给主机。
2. 主机随后验证并解包该证书，以获取外设的公钥。这样，主机确认该公钥是可信的。
3. 主机生成一个随机数，即“质询”，并将其作为明文发送给外设。
4. （可选）外设创建一个随机数“nonce”，并将其与“质询”拼接起来。
5. 外设使用标准的数字签名算法对质询进行签名。这一步需要私钥。结果就是外设返回给主机的“质询”。
   如果此质询包括nonce，外设必须同时将nonce和质询返回给主机。
6. 主机使用标准的验证算法验证响应。如果结果正常，则证明外设是可信的。

ELS在上述步骤中的作用如下：

- 生成nonce：ELS通过RND_REQ命令完成此操作。这是可选的。
- 对质询进行签名：ELS通过ECSIGN命令完成此操作。ECSIGN执行*{r, s} = signature(hash(c))*操作，其中：
  – *{r, s}*是ECSIGN输出的签名。
  – *c*是质询；是从主机接收到的随机数，位于外设的内存中。
  – hash是标准SHA256哈希值。
  – signature是使用NIST P-256曲线的ECDSA签名。

表2. ECSIGN参数

参数	寄存器	说明
SRC0_ADDR	DMA_SRC0	摘要/质询的起始地址。 如果ECHASHCHL = 0，则为摘要在系统内存中的起始地址。质询已被预先进行哈希运算，摘要就是质询的哈希值。如果ECHASHCHL = 1，则是未进行哈希运算的质询在系统内存中的起始地址。在这种情况下，命令会对质询进行哈希运算，并在ECSIGN操作中使用生成的摘要。
SRC0_LEN	DMA_SRC0_LEN	如果ECHASHCHL = 0，则忽略该参数。摘要具有固定长度。无需指定长度。 如果ECHASHCHL = 1，则长度为未进行哈希运算的质询的字节长度。
RES0_ADDR	DMA_RES0	系统内存中存储签名的起始地址。
KIDX0	KIDX0	用于对消息进行签名的密钥在ELS密钥库中的索引。
SIGNRTF	CMDCFG0[1]	0 = RTF未包含在要签名的消息（质询）中。1 = RTF已包含在要签名的消息（质询）中。以下表达式是用于合并RTF的算法： *signature = ECDSA P-256 (signing key, SHA256(RTF || HAD || message_to_be_signed_with_padding_adjusted_for_sizeof_RT F_plus_HAD))* ***注：** 如果SIGNRTF=1，则必须在签名密钥上设置URTF或UECSG中的一个。*
ECHASHCHL	CMDCFG0[0]	指示质询是否已进行预哈希运算。如果质询尚未经过哈希运算，则该命令将对质询进行哈希运算以创建摘要，并在ECSIGN操作中使用该摘要。 0 = 质询已预先经过哈希运算（即摘要）。该命令直接在ECSIGN操作中使用该摘要。 1 = 质询未预先经过哈希运算。该命令将对质询进行哈希运算，并在ECSIGN操作中使用生成的摘要。
REVF	CMDCFG0[4]	0 = 假定摘要和签名（但不包括质询，见下文）采用32位字小端格式进行访问（读取/写入）。 1 = 假定摘要和签名（但不包括质询，见下文）采用32位字大端格式进行访问（读取/写入）。 ***注：** 读取质询时将忽略 REVF。读取质询时始终假定它采用32位字大端格式。*

表3. ECSIGN数据结构

对象	说明
密钥	必须使用256位密钥库密钥。

表3. ECSIGN数据结构（续）

对象	说明
输入消息： “质询”	如果ECSIGN配置为从系统内存中获取质询，用户必须将质询放置在那里。否则，无需采取任何操作，因为ELS已经内部持有质询。 如果质询需要哈希运算，其大小必须是SHA-256块的整数倍。SHA2-256块为512位。 如果质询已经进行哈希运算，其大小必须为512位。
运行时指纹（RTF）	这是一个256位的ELS内部寄存器，包含一个或多个系统内存哈希的结果。当命令开关SIGNRTF = 1时，RTF与输入消息拼接在一起。对HAD和结果进行签名。 *Concatenation = RTF || HAD || input message.*
硬件认证数据（HAD）	这是一个系统内存块，包含表示系统硬件“状态”的数据。当命令开关SIGNRTF = 1时，HAD与输入信息和RTF拼接在一起，并对结果进行签名。 *Concatenation = RTF || HAD || input message.*
签名	签名由ECSIGN写入系统内存。其大小为512位。它由两个256位组件拼接而成：R和S。 *Concatenation = R || S.* 如果R || S位于系统内存中，R必须位于较低地址，S必须位于较高地址。

1.3.2 未启用RTF的ECSIGN命令

以下是在不启用RTF的情况下使用ECSIGN命令的步骤：

1. 用户准备输入消息。此输入消息可以是纯消息，也可以是消息的哈希值。如果输入消息是输入消息的预先计算的哈希值，则“ECHASHCHL”位必须设置为0。否则，如果输入消息是纯消息，则“ECHASHCHL”位必须设置为1。这样，ECSIGN命令就会对质询进行哈希运算，并使用生成的摘要进行签名操作。此外，在这种情况下，用户必须注意填充。标准的SHA2-256填充必须与纯消息添加在一起（基于FIPS-180-4第5.1节）。
2. 用户设置命令参数并启动ECSIGN。仅提及RTF相关参数（SIGNRTF = 0）。其他参数也必须按要求准备。更多信息请参见表2或MCX Nx4x SRM。
3. ECSIGN完成。签名输出到系统内存中。

SDK示例工程（在MCX Nx4x SDK软件包中）已可用于此用例。有关ECSIGN参数的更多信息，请参阅MCX Nx4x SRM。

1.3.3 启用RTF的ECSIGN命令

以下是启用RTF时使用ECSIGN命令的步骤：

1. 用户准备输入消息。当必须使用RTF时，输入消息必须未经哈希运算并进行了填充。
   填充（标准SHA256填充，基于FIPS-180-4第5.1节）必须按以下方式进行：签名的消息是RTF、HAD和输入消息的拼接。ELS内部会拼接RTF和HAD，但用户必须为它们提供填充。
   Concatenation = RTF || HAD || Input Message

因此，用户提供的输入数据必须包含输入消息。标准的SHA-256填充考虑了RTF和HAD。为了演示一个例子，采用如下输入消息：

```
Input_message[] = {0x11111111, 0x22222222, 0x33333333};
```

这里，*Input_message*为12字节。此外，RTF和HAD分别为32字节和48字节（对于MCX Nx4x芯片）。因此，缓冲区ECSIGN命令的实际大小为：

总大小 = 32 (RTF) + 48 (HAD) + 12 (输入消息) + 36（添加填充字节，使整个缓冲区是64的倍数）字节

由于ELS内部添加了RTF和HAD，实际缓冲区（由用户传递）仅包括输入消息和填充字节。我们传递给ECSIGN命令的最终消息如下所示：

```
Final_message_padding_for_rtf_plus_HAD_and_whole_msg [] =
{0x11111111, 0x22222222, 0x33333333, 0x00000080, 0x00000000, 0x00000000,
0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0xE0020000};
```

第四个字包括0x80字节，表示数据在此之前一直存在。最后一个字包括整个数据的大小，采用大端无符号整数格式。这两种变化都是标准SHA256填充的一部分：

32字节RTF + 48字节HAD + 12字节输入消息 = 92字节 = 736位 (0x2E0)

2. 用户设置命令参数并启动ECSIGN。仅提及RTF相关参数（SIGNRTF = 1）。其他参数也必须按要求准备。如需了解更多信息，请参见表2或MCX Nx4x SRM。
3. ECSIGN完成。签名会输出到系统内存中。
   要验证生成的签名（在所附示例工程中也进行了验证），用户必须准备好RTF和HAD，然后将它们添加到缓冲区，如下所示：
   Message_for_verification = RTF || HAD || Input Message || Padding
   将其传递给ECVFY命令。ECVFY命令还需要其他参数。有关详细信息，请参阅MCX Nx4x SRM。
   这里同样使用标准SHA-256填充。

2 设置和SDK示例

本节介绍了运行附带SDK示例工程的硬件和软件设置。

2.1 硬件设置

硬件设置使用FRDM-MCXN947开发板，通过J17 USB Type-C接口连接到主机。该开发板上的SWD调试器使用MCU-LINK VCOM输出。它作为串行到USB的桥接器连接到主机，并提供SWD调试接口。MCU调试器被编程和配置为CMSIS DAP调试器。

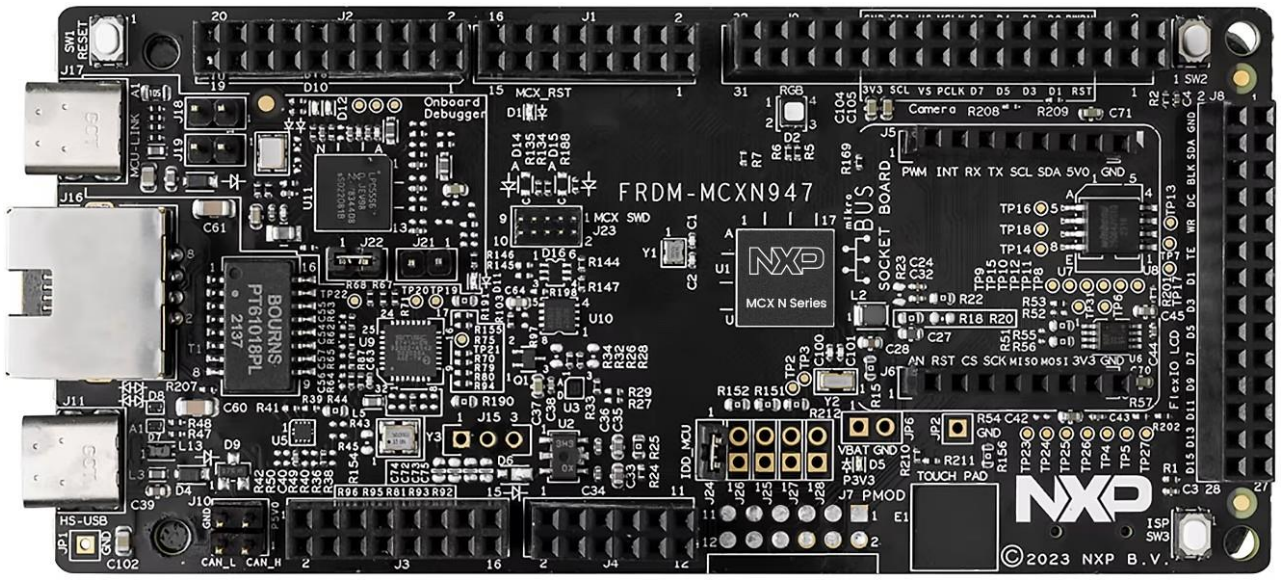

图1. FRDM-MCXN947开发板

2.2 软件设置

在软件设置方面，使用MCUXpresso IDE v11.9.0来构建和写入映像，此应用笔记稍后将对此进行介绍。该软件可在以下链接中下载：https://www.nxp.com.cn/design/software/development-software/mcuxpresso-software-and-tools-/mcuxpresso-integrated-development-environment-ide:MCUXpresso-IDE。

构建和调试代码需要MCXN947的SDK。此应用笔记附带有示例工程。下面的示例工程使用了SDK_2.14.0（可从https://mcuxpresso.nxp.com/en/welcome下载）。输出结果可在任何终端应用程序（如Tera Term）上显示。使用终端应用程序时，必须使用以下设置：

- 115200波特率
- 无奇偶校验
- 8个数据位
- 1个停止位

2.3 SDK示例工程

本文附有一个示例工程以显示此功能。要导入示例工程（归档文件夹），请执行以下步骤：

1. 打开MCUXpresso工具。
2. 从Quickstart Panel中，选择“Import Project(s) from file system”>“Browse”。
3. 然后，浏览压缩文件夹并选择“Finish”。

该工程此时在Project Explorer窗口中可用。要构建工程，请点击顶部面板上的锤子图标，如图2所示。

要将工程刷写到MCU并同时启动调试会话，请从“MCUXpresso IDE - Quickstart Panel”中选择“Debug”选项。或者点击顶部面板上的蓝色虫子按钮，如图2所示。

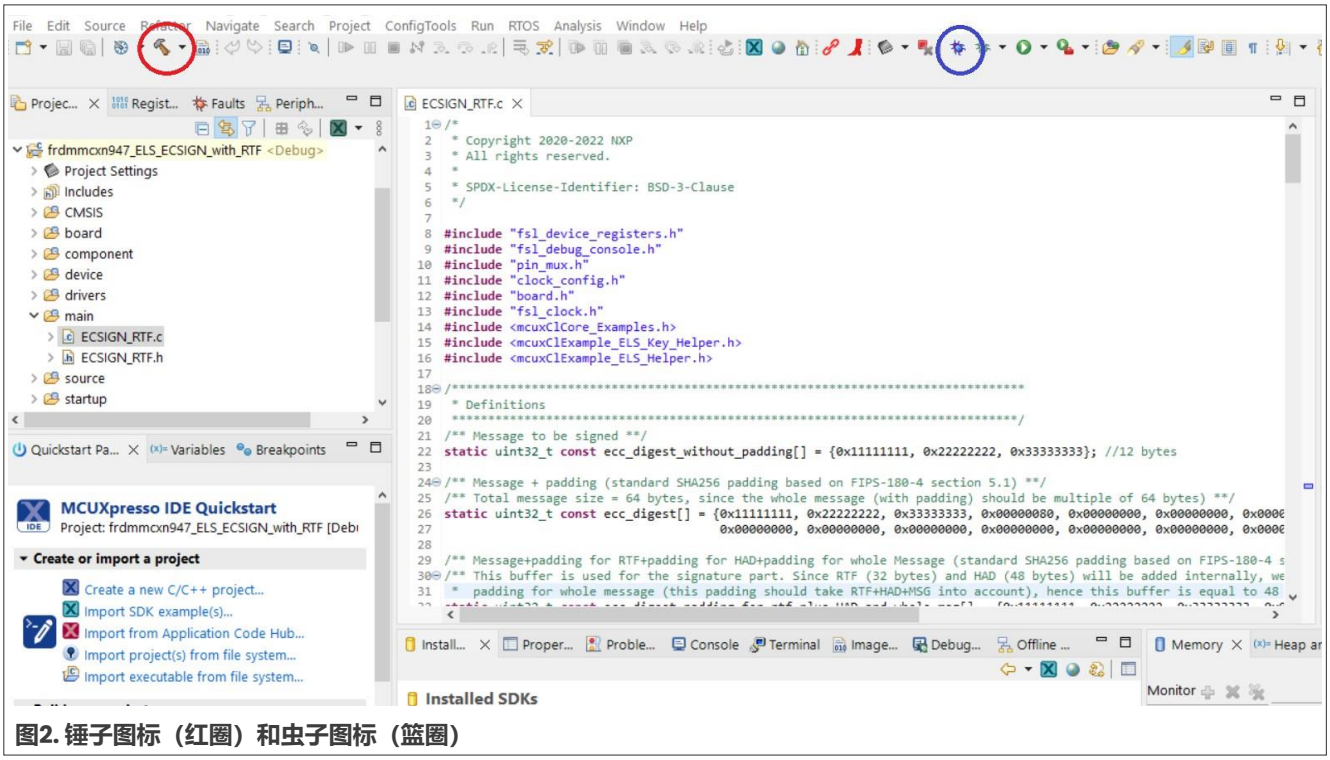

图2. 锤子图标（红圈）和虫子图标（篮圈）

2.4 输出

输出结果使用UART COM41端口显示在Tera Term应用程序中。成功构建并将代码刷写到MCU后，用户可以看到如图3所示的输出。图3显示了已生成RTF和签名密钥，然后在RTF启用时成功对数据进行了签名和验证。

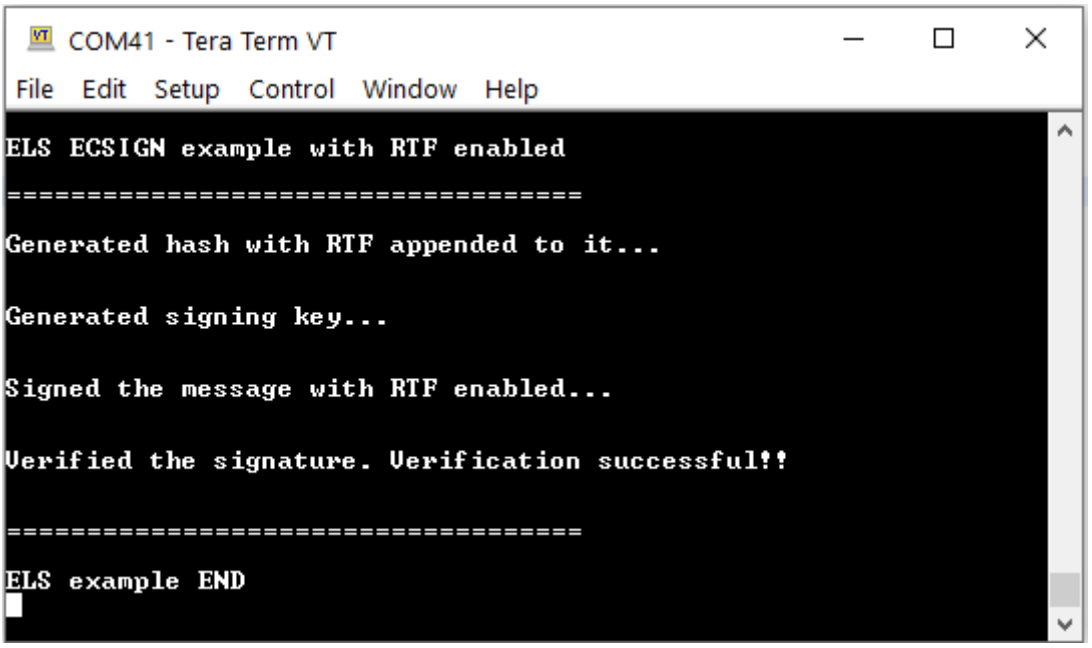

图3. 演示的输出

3 缩略语

表4介绍了本文所用的缩略语。

表4. 缩略语与定义

缩略语	定义
PKC	公钥密码学
DICE	设备标识符组合引擎
AES	高级加密标准
EMFI	电磁故障注入
ECDSA	椭圆曲线数字签名算法
UUID	通用唯一标识符
ELS	EdgeLock安全子系统
ELE	EdgeLock安全飞地
HMAC	密钥哈希消息认证码
HKDF	提取和扩展密钥派生函数
CMAC	基于密码的消息认证码

4 关于本文中源代码的说明

本文中所示的示例代码具有以下版权和BSD-3-Clause许可：

2024年恩智浦版权所有；在满足以下条件的情况下，可以源代码和二进制文件的形式重新分发和使用本源代码（无论是否经过修改）：

1. 重新分发源代码必须保留上述版权声明、这些条件和以下免责声明。
2. 以二进制文件形式重新分发时，必须在文档和/或随分发提供的其他材料中复制上述版权声明、这些条件和以下免责声明。
3. 未经事先书面许可，不得使用版权所有者的姓名或参与者的姓名为本软件的衍生产品进行背书或推广。

本软件由版权所有者和参与者“按原样”提供，不承担任何明示或暗示的担保责任，包括但不限于对适销性和特定用途适用性的暗示保证。在任何情况下，无论因何种原因或根据何种法律条例，版权所有者或参与者均不对因使用本软件而导致的任何直接、间接、偶然、特殊、惩戒性或后果性损害（包括但不限于采购替代商品或服务；使用损失、数据损失或利润损失或业务中断）承担责任，无论是因合同、严格责任还是侵权行为（包括疏忽或其他原因）造成的，即使事先被告知有此类损害的可能性也不例外。

5 修订历史

表5汇总了本文的修订情况。

表5. 修订历史

文档ID	发布日期	说明
AN14361 v.1.0	2024年7月29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.

目录