AN12251

NHS31xx customer firmware flashing

Rev. 3.1 — 3 May 2022 Application note

Document information

Information	Content
Keywords	NHS3100W8, NHS3100T8, NHS31xxUK, gold bump, CSP, firmware, production, customization
Abstract	This application note explains the procedure to obtain NHS31xx ICs preflashed with your custom firmware application.

Revision history

Rev	Date	Description
v3.1	20220503	Updated revision
v3	20220118	Third, updated version
Modifications:		• The services offered are expanded. Text is adapted accordingly.
v2.1	20200228	Updated revision
v2	20181101	Second version
v1	20180924	Initial version

1 Introduction

The NTAG SmartSensor NHS3100 IC has been released in three packages: HVQFN24, WLCSP25, and as a bumped die with 8 functional bumps, in both a thick (T8) and a thinned version (W8). More information is available in the data sheet. By default, all ICs are delivered without an application image. Customers must flash their own application firmware into each device. The application note "Overview of supported methods for firmware flashing on NHS31xx ICs" (Ref. 1) under `<SDK>/docs` explains how to use the different wired and wireless options to program the NHS31xx ICs.

Customers who develop a high-volume solution face a challenge in their production line, as wired programming takes several seconds to complete. For production efficiency, the application firmware is best preflashed on the device.

- For the HVQFN24 package, accessible external commercial services exist.
- Although commercial services exist for the WLCSP25 package, they are not widespread and accessible in some regions.
- Due to the nature of the T8 and W8 packages, it is not easy to find an external service with fitting equipment.

2 Scope

In this document, NXP Semiconductors explains the procedure to obtain T8 wafers, W8 wafers or UK tape on reels, flashed with the firmware of the customer firmware during production. It requires a prior commercial agreement which is not discussed here.

Using the service, customers can eliminate the programming step during their production cycle by having NXP Semiconductors load their firmware application image in the IC. For practical purposes, a new product type number is derived from the default product type number. The new product type number is coupled with the unique firmware application image the customers provide. When fully set up in the secure environment of NXP Semiconductors, customers can place exclusive orders for this new product type number.

Note: *The procedure touches on both business and technical requirements. The involvement of a product expert is required.*

Note: *The service is only provided for NHS3100T8 ICs, NHS3100W8 ICs and NHS31xxUK ICs. A minimum order quantity (MOQ) is imposed. In addition, the procedure applies for a single firmware application image only. Each new firmware application or updated version of an existing application requires a new NRE purchase order and a new order entry form submission.*

Note: *This service is incompatible with the regular flashing options. The application note "Overview of supported methods for firmware flashing on NHS31xx ICs" (Ref. 1) under `<SDK>/docs` is not applicable to ICs which are preflashed with an application image provided by a customer.*

3 Procedure

3.1 Contact us

The first step for customers is to address their NXP sales contact. As an alternative, customers can initiate the contact via nhs-info@nxp.com. It leads to a commercial agreement for the custom firmware flashing, whereupon a legal contract is negotiated and export control codes are defined.

Moving forward, customers then place an NRE purchase order to nhs-info@nxp.com.

At the end of this step, customers are granted access to the order entry form tool. The operating manual for this secure web-based tool is shared.

3.2 Prepare image

Customers must create their own firmware application image and prepare it in a specific format. This step is best done by a firmware engineer.

Preparation is split in three parts.

3.2.1 Image generation

Using the software development kit (SDK) offering from NXP Semiconductors, customers can develop, test, and deploy their own unique firmware application. It requires setting up an integrated development environment (IDE) and importing the SDK. Both are freely available on nxp.com. See the getting started guide "NTAG SmartSensor getting started: A guide to start developing using an NHS31xx" (Ref. 2) under `<SDK>/docs` for detailed instructions.

The final application firmware image must comply with these prerequisites:

- The image is a single contiguous file, describing the Flash memory contents.
- The image starts at address `0`, that is, the image must be placed on sector `0` and onward.
- The maximum size is 30 kB.
- The image file must be in Intel Hex format. This is the image the MCUXpresso IDE generates with extension `.hex`.

There is no alignment requirement on the end of the application firmware image. The image size does not need to be a multiple of the flash page size (64 bytes), nor of the flash sector size (1024 bytes). When the image is flashed during production, a multiple of the flash page size will be written. The remaining bytes in the last written flash page, from the end of the image up to the next flash page boundary, are written with random data. This means that a variable amount of random bytes, between 0 and 63 bytes in size, is appended to the image.

From the next flash page boundary up to the end of sector 30, all flash bytes are guarantueed to be erased, i.e. to have the value of `FFh`. The firmware application must take this condition into account when it implements flash write operations.

From SDK v9 (released in January 2017) onwards, when making use of the high-level modules available in the SDK, this condition is automatically taken care of. Also, all demo applications in the SDK, making use of flash memory for data storage, take this into account. They only write to the upper pages where no firmware application code resides.

Note: *Before continuing with the next steps, customers must validate the application firmware image file thoroughly. It is impossible for NXP Semiconductors to perform any validation on a customer image file.*

3.2.2 Signature computation

To ensure the validity of the file during upload in the order entry form tool and during handling in the production facilities, a flash signature file must accompany the firmware application image. Starting from SDK 12.0, the SDK offering includes the Python script `<SDK>/tools/flashsignature.py` to compute it. The script provides its own using instructions.

The signature file must be in textual ASCII format. The contents the script generates must be stored in a file with extension `.signature`.

3.2.3 Encryption of files

All uploads must be encrypted and signed. Encryption ensures that only the production facility can decrypt the files and access the contents. Signing ensures that only customers can submit the firmware image.

The two files created above, the binary file `.hex` and the signature file `.signature`, must be encrypted and signed using the OpenPGP standard (RFC 4880). For this, numerous options exist.

- Linux users can use https://gnupg.org
- macOS users can use https://gpgtools.org
- Windows users can use https://www.gpg4win.org

The operating manual for the order entry form tool also details the correct use of the user-friendly Kleopatra GUI program.

Note:

Encryption and signing must be done according to the following guidelines:

- *The binary image `.hex` and the signature file `.signature` must be encrypted and signed separately, resulting in two `.gpg` files.*
- *Encryption must be done using the public key for flash configuration of NXP Semiconductors: `NXP_EE_Flash_and_FK_Configuration.asc`. This certificate can be downloaded before opening or creating an order entry form from the same web interface, available in the Documents section.*
- *Before the encrypted files are accepted, the public key of a customer must be uploaded and verified. This procedure requires manual intervention and may take some time. Follow the steps outlined in the operating manual of the order entry form tool.*

3.3 Submit a new order entry form

Using the account details for the order entry form tool and the prepared encrypted files, customers can now make a new submission. The submission procedure is fully detailed in the operating manual of the order entry form tool. When submitted and validated, the creation of a new and unique customer-specific product type number is initiated.

Each submission of a new form results in the creation of a new product type number. The product type number is named NHS3100W8/A1`bccff`, NHS3100T8/A1`bccff`, or NHS31`ee`UK/A1`bccff`, with:

All information provided in this document is subject to legal disclaimers.

- b referring to the bootloader version, which currently has a fixed value of 2.
- cc a unique customer token, which the NXP Semiconductors business line assigns.
- ee the product identifier. A value of 00, for instance, refers to NHS3100 ICs.
- ff a flash content identifier, allowing to discriminate different submissions from the same customer.

The whole production flow is duplicated and adapted for the unique submission of a customer. When that is in place, one single customer-qualified sample (CQS) wafer is produced. The ICs follow the same production steps and must pass the same quality checks. The difference is that they are not flashed with the default image, but with an application program a customer provides.

Note: *The custom application program the user provides cannot be overwritten. The first sector of the flash is locked after writing the custom application program. The wireless and the wired options as described in the application note "Overview of supported methods for firmware flashing on NHS31xx ICs" (Ref. 1) under* `<SDK>/docs` *are no longer possible.*

At the end of the whole production process, the CQS wafer is sent to customers.

3.4 Validate the CQS wafer

When customers receive the CQS wafer, it is their responsibility to validate it thoroughly. If improvements are to be made, a new binary image file must be prepared. This new image cannot be put to use immediately. Customers must:

- Inform NXP Semiconductors through the local sales contact or via nhs-info@nxp.com.
- Generate a new NRE purchase order.
- Submit a new order entry form. The details of the previous entry can be duplicated and adapted, or a new form can be filled from scratch.

Note: *Customers must validate the application firmware image file thoroughly during the image generation step, as it avoids unnecessary costs and a longer turnaround time.*

Only when the CQS wafer passes all customer checks, the new type can be promoted to ready-for-sale (RFS). Customers must acknowledge the correctness of the CQS wafer in the order entry form tool, in their submitted form.

This acknowledgment allows volume production and logistics in a standard way.

3.5 Order placement

After the new type reaches RFS state, customers can place normal purchase orders, referencing the new type.

Note: *Only customers who created the new type are able to know of its existence and are allowed to purchase this new type.*

This step can be repeated as many times as required.

4 References

[1] **AN12328 application note** — Overview of supported methods for firmware flashing on NHS31xx ICs; 2021, NXP Semiconductors

[2] **UM11153 user manual** — NTAG SmartSensor getting started: A guide to start developing using an NHS31xx; 2021, NXP Semiconductors

5 Legal information

5.1 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.

5.2 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.

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.

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 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 — 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.

5.3 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.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

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

Date of release: 3 May 2022
Document identifier: AN12251