AN12251

NHS3100W8 customer firmware flashing

Rev. 2.1 — 28 February 2020 Application note

Document information

Information	Content
Keywords	NHS3100W8, gold bump, firmware, production, customization
Abstract	This application note explains the procedure to obtain NHS3100W8 gold bump wafers flashed with a custom firmware application.

Revision history

Rev	Date	Description
v.2.1	20200228	updated revision
Modifications:		• Text has changed throughout the document
v.2	20181101	new main revision
v.1	20180924	Initial version

1 Introduction

The NTAG SmartSensor NHS3100 IC has been released in three packages: HVQFN24, WLCSP25, and W8 (bumped die with 8 functional bumps). 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 AN12328 (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 based on the NHS3100 face a challenge in their production line, as wired programming takes several seconds to complete. For production efficiency, the application firmware should be preflashed on the device. For the HVQFN24 and WLCSP25 packages, external commercial services exist. Due to the nature of the W8 package, it is not easy to find an external service with fitting equipment.

2 Scope

In this document, NXP Semiconductors explains the procedure to obtain flashed W8 wafers, given a prior commercial agreement.

Using the service, customers can eliminate the programming step during their production cycle by having their firmware application image loaded in the IC by NXP Semiconductors. For practical purposes, a new product type number is derived from the default NHS3100W8/A1, which is then coupled with the unique firmware application image as provided by customers. 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 provided for NHS3100W8 ICs only and 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 AN12328 (Ref. 1) under `<SDK>/docs` is not applicable to W8 wafers which are flashed 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 should lead 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 toward nhs-info@nxp.com.

At the end of this step, customers are granted access to the order entry form tool OEF2 and the operating manual for this web-based secure 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 user manual UM11153 (Ref. 2) under `<SDK>/docs` for detailed instructions.

The final firmware application 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` onwards.
- The maximum size is 30 kB.

The image file must be in Intel Hex format: the image generated by the LPCXpresso IDE with extension `.hex`.

Note: *Customers must validate the application firmware image file profoundly before continuing with the next steps. 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 OEF2 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 "flashsignature.py" to compute it, under `<SDK>/tools`. The script provides its own usage instructions.

The signature file must be in textual ASCII format. The contents generated by the script are to be stored in a file with extension `.signature`.

3.2.3 Encryption of files

All uploads in OEF2 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 OEF2 details the correct usage 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 fetched from the Documents section in OEF2 and can be downloaded before opening or creating an order entry form.*
- *The public key of a customer must be uploaded and verified before OEF2 accepts the files. Follow the steps outlined in the operating manual of OEF2.*

3.3 Submit a new order entry form

Using the account details for OEF2 and the prepared encrypted files, customers can now make a new submission. The submission procedure is fully detailed in the operating manual of OEF2. When submitted and validated, the creation of a new and unique customer-specific product type number, which is derived from NHS3100W8/A1, 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`bbccff`, with:

- `bb` referring to the boot loader version, which has currently the fixed value of `12`.
- `cc` a unique customer token, which the NXP Semiconductors business line assigns.
- `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 as all other NHS3100W8/A1 ICs. The difference is that they are not flashed with the default image, but with an application program provided by a customer.

Note: *The custom application program provided by the user cannot be overwritten. The first sector of the flash is locked after writing the custom application program. Both the wireless and the wired options as described in the application note AN12328 (Ref. 1) under `<SDK>/docs` are then 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 profoundly 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 OEF2, 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; 2020, NXP Semiconductors

[2] **UM11153 user manual** — NTAG SmartSensor getting started: A guide to start developing using an NHS31xx; 2019, NXP Semiconductors

5 Legal information

5.1 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.

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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

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.

5.3 Trademarks

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

Contents

1 Introduction 3
2 Scope 3
3 Procedure 4
3.1 Contact us 4
3.2 Prepare image 4
3.2.1 Image generation 4
3.2.2 Signature computation 4
3.2.3 Encryption of files 5
3.3 Submit a new order entry form 5
3.4 Validate the CQS wafer 6
3.5 Order placement 6
4 References 7
5 Legal information 8

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

Date of release: 28 February 2020
Document identifier: AN12251