AN13041

NFC program downloader interface

Rev. 1.03 — 2 June 2021 Application note

Document information

Information	Content
Keywords	SWD, NFC, firmware
Abstract	How to interface the on-chip one-time NFC program downloader of the NHS31xx.

Revision history

Rev	Date	Description
v.1.0	20210602	Major format update and refresh of contents
v.0.3	20170324	Updated “Response (Target to Host)”
v.0.2	20170209	Rework after review
v.0.1	20161213	Initial version

1 NFC program downloader

The NHS31xx NFC program loader is a firmware application which NXP Semiconductors provides. It comes preloaded in every NHS31xx IC and allows programming of the IC via the NFC interface.

This application note expands on the information supplied in the "Overview of supported methods for firmware flashing on NHS31xx ICs" application note (AN12328; Ref. 1). It provides more detailed information on how to interact with the NFC program loader firmware application via NFC from the host side.

1.1 Benefits

See the "Overview of supported methods for firmware flashing on NHS31xx ICs" application note (AN12328; Ref. 1), section Wireless, "Benefits and drawbacks".

1.2 Example implementations

See the "Overview of supported methods for firmware flashing on NHS31xx ICs" application note (AN12328; Ref. 1), section Wireless.

1.3 State machine

See the "Overview of supported methods for firmware flashing on NHS31xx ICs" application note (AN12328; Ref. 1), section Wireless, "Target: NHS31xx".

1.3.1 Message sequence

The firmware application is started right after power-on, when the target enters the NFC field of the host. The target (NHS31xx) initiates communication by writing a response containing version information in its tag memory. The host (card reader) is given approximately 5 seconds to read and verify this automatic response.

After verification, the host can start the transfer by sending the first command with the first data chunk.

From this moment on, the complete transfer is done by repeating successive commands (carrying subsequent data chunks) and waiting for the respective responses of the target (acknowledging the previous command).

During the download, the target calculates a CRC over all the received data chunks. When the host transfers the last chunk, a special command is issued, which also carries the CRC of the file. This CRC is used at the target side to compare with the calculated one and verify the integrity of the transferred data.

Figure 1 describes the communication between the host (card reader/writer) and the target (NHS31xx).

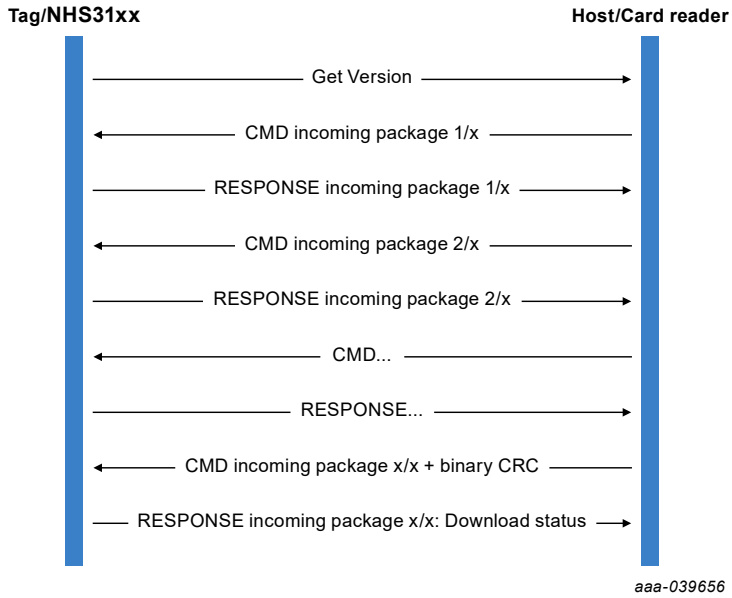

Figure 1. Communication between the host (card reader/writer) and the target (NHS31xx)

1.4 Protocol

All commands and responses are formatted as single-record NDEF messages carrying one MIME record with MIME type `N/P`.

Within the MIME record payload, the first byte indicates the message ID. The second byte contains the tag field and is used to distinguish commands from responses. To give the host the possibility to check the direction of the message at a certain moment present in the tag, the target always flips the LS bit in the tag field. Using this bit, the host can find out when a message in the tag is a response (toggled bit).

The following sections give the format (content of the payload of the MIME type NDEF record) of the MIME type messages interchanged between the card reader/writer and the target.

1.4.1 Command (host to target)

Table 1. Format of the NDEF MIME record payoad data of the command with an incremental data package (host to target)

CMD name	1 byte per field		2 bytes	(Chunk size) bytes		
Incremental package	Msg ID	Tag	Chunk size (cs)	Data		
	0x48	0x00	[1 - 486][1]	D_0	...	D_{cs}

[1] 489 minus mime type length, for example 3 for `N/P`.

Table 2. Format of the NDEF MIME record payoad data of the command with the final data package (host to target)

CMD name	1 byte per field		2 bytes	(Chunk size) bytes			2 bytes	
Last package	Msg ID	Tag	Chunk size (cs)	Data			CRC	
	0x49	0x00	[1 - 484][1]	D_0	...	D_{cs}	C0	C1

[1] 487 minus mime type length, for example, 3 for `N/P`.

1.4.2 Response (target to host)

Table 3. Format of the NDEF MIME record payoad data available in NFC memory after power-on (target to host)

Response name	1 byte per field		2 bytes per field					4 bytes
Version (initial tag content)	Msg ID	Tag	Reserved	SW major version	SW minor version	API major version	API minor version	Reserved
	0x02	0x01	0xXXXX	1	2	4	0	0xXXXXXXXX

Table 4. Format of the NDEF MIME record payoad data of the response to an incremental data package (target to host)

Response name	1 byte per field		4 bytes
Incremental package	Msg ID	Tag	Download status
	0x48	0x01	[STATUS]

Table 5. Format of the NDEF MIME record payoad data of the response to the final data package (target to host)

Response name	1 byte per field		4 bytes
Final package	Msg ID	Tag	Download status
	0x49	0x01	[STATUS]

Table 6. [STATUS] possible values

1	DOWNLOAD_COMPLETE_OK	Expected if the command given was `0x48`.
2	DOWNLOAD_ONGOING	Expected if the command given was `0x49`.
3	DOWNLOAD_FAILED_IMAGE_TOO_BIG	The provided binary file did not fit in user flash. The maximum size supported by the NFC loader is 25 kB. Either the size must be reduced by optimizing for size or another method of programming (wired), like SWD, must be used.
4	DOWNLOAD_FAILED_FILE_INVALID_CHUNKSIZE	The message ID was recognized, but the payload size was wrong. Check the implementation of the communication protocol.
5	DOWNLOAD_FAILED_FILE_CRC_MISMATCH	The calculated CRC does not match with the received CRC. Most likely data was corrupted during the NFC transfer or the file was changed during the transfer. Ensure that the tag is properly placed in the NFC field and retry.
6	DOWNLOAD_COMMUNICATION_FAILED	Indicates a non-specific error, that is, a glitch in the NFC transfer. If the tag-reader is connected via a USB hub, try using a direct USB port to avoid accidental power glitches and retry.
0x10007	MSG_ERR_UNKNOWN_COMMAND	The message ID was not recognized. Check the implementation of the communication protocol.
0x1000D	MSG_ERR_INVALID_COMMAND_SIZE	The message ID was recognized, but the payload size was wrong. Check the implementation of the communication protocol.
0x1000E	MSG_ERR_INVALID_PARAMETER	The message ID was recognized and the payload size check passed. A parameter did not have a valid value. Check the implementation of the communication protocol.

1.5 Critical point

When the last packet, including the right CRC value, is transferred to the target, the IC is considered to be in a critical state. The critical state lasts until a status is reported, either `DOWNLOAD_COMPLETE_OK` or any other error message. It is at this point that flash sector 0, including the interrupt vector table, is overwritten. If during this timeslot a power drop or a reset pulse is observed, the target may end up with an invalid firmware image. In that case, no retry is possible.

The only way to overcome this issue, is to program the IC wired via the HW pins (SWD pins).

Also, the data integrity check is only performed at the moment the data has been received. Only the wireless transfer is secured, there is no validation test to check proper flashing. Extensive testing from our part of the on-chip flash driver did not raise any concern.

1.6 End state

- After reception of `DOWNLOAD_COMPLETE_OK` (value: `1`) response, the provided firmware is fully programmed and the target is brought to power-off state. It will wake up again after a resetN trigger or by the presence of an NFC field.
- To ensure that the host is able to read the response, the target stays awake for 5 seconds after reception of any error response. Then, the IC enters power-off mode. The host can then check the error, make adjustments, and retry.
  The extra delay before going to power-off means that if an error response is received, the host should wait for at least 5 seconds before restarting the download.

2 Abbreviations

Table 7. Abbreviations

Acronym	Description
SWD	serial wire debug
NFC	near-field communication
CRC	cyclic redundancy check
MIME	multipurpose internet mail extension

3 References

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

4 Legal information

4.1 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.

4.2 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 — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. 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.

4.3 Trademarks

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

I²C-bus — logo is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

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

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: 2 June 2021
Document identifier: AN13041