PN5180 Product Versions (C1-C4)

Comparison and Firmware Upgrade to FW 4.1

English version | December 17, 2025

Executive Summary

In the PN5180 ordering code, the suffix C1 to C4 typically indicates the product version (silicon and factory-programmed firmware baseline). In practice, the most material differences are driven by the factory firmware generation (3.x vs 4.x) and the related RF control and certification-oriented behavior. Electrical pinout and package are not changed by C1-C4 alone; however, certain behaviors and features depend on the firmware that is currently installed.

Related products: https://www.elechouse.com/product/pn5180-nfc-module/

1. Key Differences at a Glance

The table below summarizes the most practical engineering differences.

Product Version	Typical Ordering Example	Factory Firmware (Baseline)	Practical Notes / Recommendation
C1	PN5180A0HN/C1E (example)	FW 3.4	Legacy baseline. Often seen in older designs. If you target payment or robust field behavior, plan a firmware upgrade.
C2	PN5180A0HN/C2E (example)	FW 3.5	Newer than C1. Introduced improvements such as EMVCo-oriented EMD handling updates and AWC (Adaptive Waveform Control).
C3	PN5180A0HN/C3E (example)	FW 4.0	4.x generation. Once upgraded to 4.x, major-version downgrade to 3.x is not supported. Suitable for new designs if C4 is unavailable.
C4	PN5180A0HN/C4E (example)	FW 4.1	Recommended baseline for new designs. Includes incremental fixes and interoperability improvements vs 4.0, including FeliCa-related behavior in release notes.

Current our version is C3. For other version, we offer customization service.

2. What Actually Changes Between Versions

C1-C4 are best understood as different factory baselines. Because PN5180 supports secure firmware updates, the behavior you get in your product is primarily determined by the firmware currently installed, not only the ordering suffix. Do not rely on package marking to determine firmware; read the version from EEPROM.

2.1 C1 (FW 3.4) vs C2 (FW 3.5)

Typical field-observed differences are driven by the 3.4 to 3.5 firmware increment, including:

- Updates related to EMVCo-oriented EMD error handling.
- Introduction of AWC (Adaptive Waveform Control) behavior in the 3.5 firmware line.

2.2 3.x Feature Notes (Example: LDO_OUT changes introduced later in 3.x)

Some features were introduced within the 3.x line (for example, LDO_OUT behavior changes described in later firmware notes). If your design depends on LDO_OUT as a functional power rail, validate the exact firmware behavior on your target hardware and treat C3/C4 as the more conservative choice for new designs.

2.3 4.0 vs 4.1 (C3 vs C4)

The 4.1 release is an incremental update over 4.0. Typical release-note items include:

- Improved FeliCa-related EMD handling and interoperability corner cases.
- Fixes for certain dynamic power control (DPC) corner-case behaviors observed during receive conditions.
- General robustness notes for host-side register access and protocol handling.

3. Before You Upgrade: Constraints and Preconditions

3.1 Key Constraints (Read Before Proceeding)

- Firmware updates are secured and signed. Only NXP-signed firmware images can be accepted.
- Major-version downgrade is not supported (for example, once on 4.x, you cannot go back to 3.x).
- A firmware update typically resets or overwrites EEPROM and RF configuration to default values. Backup and restore are required if you tuned parameters.
- Power loss or interruption during update can leave the device in download mode until a full successful update is completed.

3.2 Hardware Preconditions

- You must be able to control RST (reset) and REQ (download request) to force the device into secure download mode.
- A stable SPI connection is required during the update procedure.
- BUSY/handshake behavior in download mode can differ from normal RF operation; follow the update protocol timing requirements.

4. Upgrade to FW 4.1 (From C1/C2)

Below are two practical upgrade paths. If you are upgrading only a small number of units for development or verification, Path A (NXP evaluation board and NFC Cockpit) is usually the fastest. For production or field upgrade capability, Path B is the common approach (host-controlled secure update).

4.1 Path A: PNEV5180B (or compatible) with NFC Cockpit

1. Obtain the official PN5180 firmware package that contains the FW 4.1 secure update file (typically distributed as a .sfwu image).
2. Before upgrading, dump and archive your current EEPROM/RF configuration (if you tuned antenna matching, power, DPC/AWC parameters, etc.).
3. Open NFC Cockpit and use the Secure Upgrade function.
4. Select the FW 4.1 .sfwu file and start the upgrade procedure.
5. After completion, reset the PN5180 and verify the reported firmware version.
6. Restore your EEPROM/RF configuration (if applicable) and re-run functional and RF regression tests.

4.2 Path B: Secure Firmware Update from Your Host MCU (ESP32/STM32/etc.)

For custom hardware, the host MCU performs a secure update by placing PN5180 into download mode and streaming the signed update frames over SPI. The most reliable approach is to port or reuse the NXP reference update application/library rather than implementing the full protocol from scratch.

High-level SOP:

- Read and record the current firmware version (recommended via EEPROM addresses 0x12 and 0x13).
- Backup EEPROM and any application-specific RF configuration you rely on.
- Enter download mode: assert REQ, then toggle reset (RST) so PN5180 boots into secure download mode.
- Stream the signed firmware image (.sfwu) using the secure update command set and frame format (including CRC).
- Complete integrity verification, then reset back into normal mode.
- Restore your EEPROM/RF configuration, then execute a full regression test plan (Type A/B/F, LPCD if used, and any payment/EMVCo-specific test cases).

5. Post-Upgrade Validation Checklist

- Confirm firmware version after upgrade by reading EEPROM (0x12/0x13) and recording results in your build log.
- Verify your RF configuration is correct (especially if the update reset EEPROM to defaults).
- Run protocol smoke tests: ISO14443-A, ISO14443-B, FeliCa (if applicable), and any proprietary modes used by your stack.
- If you use dynamic power control or waveform control features, validate power steps and field strength across your antenna load range.
- If your product is payment-adjacent, re-run EMVCo-related waveform/interoperability checks on the final antenna design.

Appendix: Key Terms

REQ: Download request pin used to force PN5180 into secure firmware download mode at boot.

RST: Reset pin; used together with REQ to enter download mode.

BUSY: Handshake signal indicating PN5180 availability for the next SPI transaction.

.sfwu: Secure firmware update image format used by the PN5180 secure update mechanism.

EEPROM 0x12/0x13: Addresses commonly used to read firmware version (minor/major), depending on the release note mapping.

References (Document Names)

- NXP PN5180 Product Data Sheet (C1/C2 and C3/C4 document sets).
- NXP PN5180 Firmware Release Notes (3.x and 4.x).
- NXP Application Note: PN5180 Secure Firmware Update / Secure Firmware Upload (NFC Cockpit and host-controlled update flow).