# Device Commissioning and Characterization

## nRF70 Series

**Application Note**

4486_179 / 2023-03-02

NORDIC® SEMICONDUCTOR

# Contents

# Revision history

| Date | Description |
|---|---|
| 2023-03-02 | Updated QSPI encryption key on page 9 |
| 2023-01-31 | First release |

# 1 Introduction

This document provides information about steps needed for nRF70 Series device commissioning (production line) and characterization (product development) purposes.

On the production line, some steps are optional and depend on your product or use case. Most steps involve updating a small region of the *One Time Programmable (OTP) memory* in nRF70 Series devices. Use the Wi-Fi® Radio test sample included in the nRF Connect SDK for all steps including programming the OTP memory.

# 2 Production line operations

This section provides a summary of recommended and optional steps.

| Step | Description | Requirement |
|---|---|---|
| 1 | Crystal/crystal oscillator frequency trimming | Recommended |
| 2 | MAC address programming | Recommended |
| 3 | QSPI encryption key programming | Optional |
| 4 | Assembly test | Optional |

*Table 1: Production line steps*

Before programming any values in the *OTP memory*, set the register REGION.PROTECT to allow full read/write access. See OTP memory programming on page 13 for more information.

## 2.1 Crystal/crystal oscillator frequency trimming

The *IEEE 802.11 specification* defines the worst-case frequency offset that can be tolerated, measured in ppm.

The limit is ± 20 ppm in the 5 GHz band, and ± 25 ppm in the 2.4 GHz band. This limit ensures that demodulation is successful for all modulation schemes even when both sender and receiver exhibit worst-case and opposite offsets. This limit needs to hold across the full operating temperature range.

The offset is a combination of the selected crystal and the on-chip crystal oscillator circuit. The nRF70 Series device includes a programmable capacitor bank that can be configured to correct this frequency offset. The configuration of this capacitor bank needs to be determined using calibrated test equipment, with the resulting parameter (trim value) programmed into the *OTP memory* on the nRF70 Series device.

The following table shows the ppm offsets that need to be managed.

| Offset source | Ppm offset | Mitigation |
|---|---|---|
| Crystal oscillator variation over process | ± 24 ppm | Production line trim |
| Crystal oscillator stability over temperature | ± 3 ppm | None |
| Crystal tolerance | Crystal dependent<br>Typically ± 20 ppm | Production line trim |
| Crystal stability over temperature | Crystal dependent<br>Typically ± 10 ppm | None |
| Crystal aging | Crystal dependent<br>Typically ± 3.5 ppm | None |
| Production line trim accuracy | ± 3.5 ppm | None |

*Table 2: Ppm offsets*

The table shows that there are several sources that cannot be trimmed and therefore must be included in the IEEE 802.11 limit of ± 20 ppm (or ± 25 ppm if only operating in the 2.4 GHz band). These are the crystal oscillator and crystal stability over temperature, the crystal aging, and the resolution or accuracy on the trim function itself. To operate over an extended temperature range, it is necessary to trim the crystal/crystal oscillator combination. The trim function has sufficient range to trim a crystal with ± 20 ppm tolerance in addition to the ± 24 ppm crystal oscillator variation.

### 2.1.1 Determine the trim value

To determine the trim value, it is recommended to transmit at a known frequency a modulated packet or carrier wave. Then measure the frequency offset using a *Vector Signal Analyzer (VSA)* for a modulated packet or a *Spectrum Analyzer (SA)* for a carrier wave. This is repeated with different trim values until the minimum *Carrier Frequency Offset (CFO)* is found. This value is then programmed into the *OTP memory*.

The crystal oscillator trim range is 0 to 127, where 0 represents the highest frequency the crystal oscillator generates, while 127 represents the lowest frequency.

The following diagram shows the CALIB_XO process.

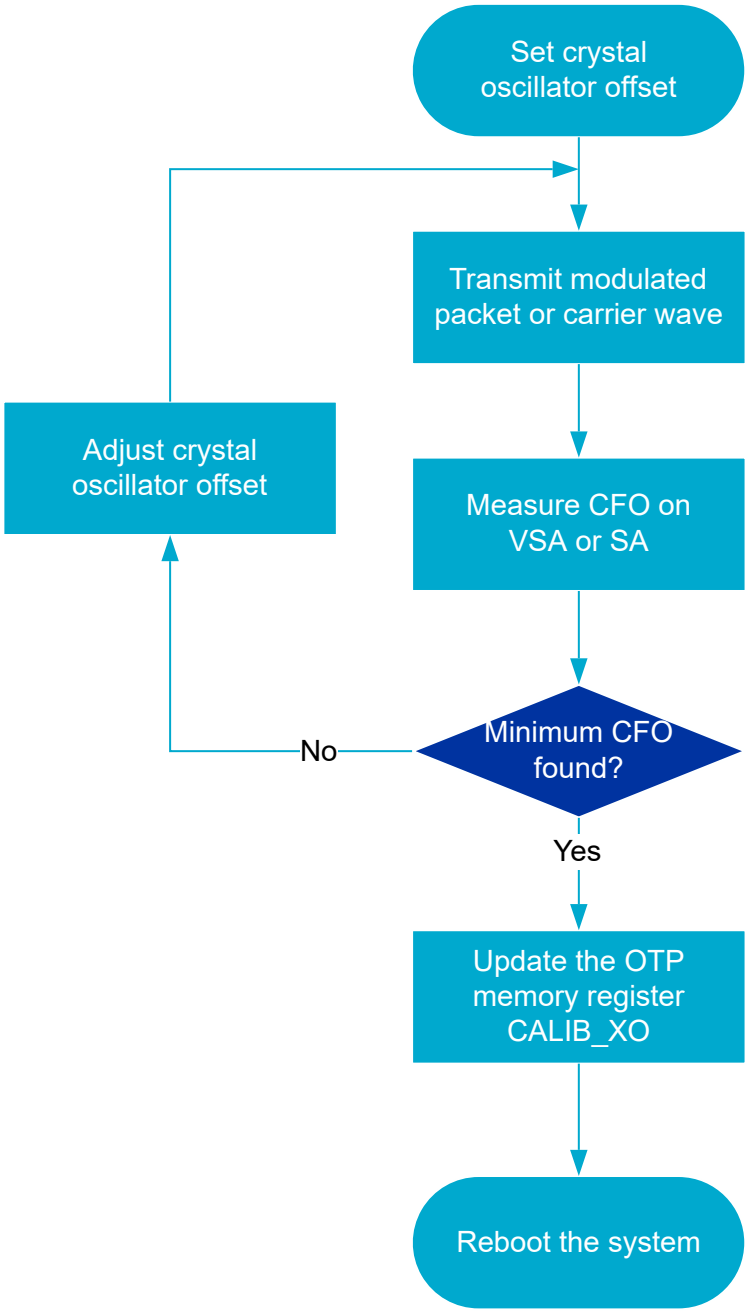


*Figure 1: CALIB_XO process*

The process shown in the diagram is based on searching for the minimum CFO. Multiple approaches can be used. The following example is based on the bisection/binary search method.

```
L=0, H=127
minCFO=1e6
For i in range(7)
    trimVal = (INT) (L+H)/2
    Set crystal oscillator offset to trimVal
    Transmit modulated packet or carrier wave
    Measure CFO on VSA or SA
    if abs(CFO) < minCFO:
         minCFO = abs(CFO)
         minTrimVal = trimVal
    L= trimVal if CFO > 0 else H= trimVal
```

The following table provides example Wi-Fi Radio test commands for performing the steps described in the algorithm.

| Step | Commands |
|---|---|
| Set crystal oscillator offset to trimVal | `wifi_radio_test set_xo_val <trimVal>` |
| Transmit a modulated packet (for example, legacy 6 Mbps in 2.437 GHz) | `wifi_radio_test init 6`<br>`wifi_radio_test tx_pkt_tput_mode 0`<br>`wifi_radio_test tx_pkt_rate 6`<br>`wifi_radio_test tx_power 10`<br>`wifi_radio_test tx 1` |
| Alternative - transmit a carrier wave (for example, at 2.439 GHz) | `wifi_radio_test init 6`<br>`wifi_radio_test tx_tone_freq 2`<br>`wifi_radio_test tx_power 10`<br>`wifi_radio_test tx_tone 1` |
| Update the OTP memory register CALIB_XO with the required trim value | `wifi_radio_ficr_prog otp_write_params 0x130 <minTrimVal>` |

*Table 3: Wi-Fi Radio test commands*

Reboot the system to activate the trim values for TX/RX operations.

### 2.1.2 Alternative method

An external temperature-controlled crystal oscillator can be used to avoid trimming. These devices are typically more expensive, but this method avoids the need for executing the trimming algorithm on the production line.

## 2.2 MAC address configuration

A Wi-Fi device requires a MAC address to communicate with another device. This address must be unique on the network.

Typically, blocks of addresses are purchased by a product vendor and a unique address is assigned to each unit. nRF70 Series devices support up to two *Virtual Network Interface (VIF)*s, each requiring a MAC address. These are usually allocated next to each other, but it is not a requirement. The mechanisms available for configuring MAC addresses are:

- Program into *OTP memory* on the production line
- Configure at interface initialization through the **`NET_REQUEST_ETHERNET_SET_MAC_ADDRESS`** net_mgmt nRF Connect SDK *Application Programming Interface (API)* at runtime

The runtime mechanism can be used if the MAC address is stored elsewhere in the product or if a random MAC address is used. For the random MAC address scenario, no support is currently included in the Wi-Fi driver beyond exposing an API to configure at interface initialization.

### 2.2.1 Program the MAC address

It is recommended to assign two addresses on the production line and program them into the *OTP memory*.

The 6-byte MAC address for VIF0 is held in registers MAC[0].ADDRESS0 and MAC[0].ADDRESS1, while the VIF1 address is held in registers MAC[1].ADDRESS0 and MAC[1].ADDRESS1. The ordering of the bytes in the two registers is documented in the nRF70 Series Product Specifications.

For example, the MAC address F0:CE:36:00:00:4A can be programmed to MAC[0] by using the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_write_params 0x120 0x0036CEF0 0x4A00`.

### 2.2.2 Alternative method

If the MAC address is not programmed in the *OTP memory*, a MAC address needs to be provided through the **`NET_REQUEST_ETHERNET_SET_MAC_ADDRESS`** net_mgmt command before the Wi-Fi interface is activated.

> **Note:** Even if the MAC address is programmed in the OTP memory, it is still possible to override it with the **`NET_REQUEST_ETHERNET_SET_MAC_ADDRESS`** net_mgmt command.

## 2.3 QSPI encryption key

Since the nRF70 Series device is a companion to a host *Microcontroller Unit (MCU)* (or *Microprocessor Unit (MPU)*) with the MAC functionality fully contained in the nRF70 Series device, the traffic over the *Quad Serial Peripheral Interface (QSPI)/Serial Peripheral Interface (SPI)* is not protected by any of the Wi-Fi security measures.

As such, this interface (that is, pins and *Printed Circuit Board (PCB)* tracks) is potentially vulnerable to a physical attack, where the unencrypted payload data could be observed. If application-level security is employed, this risk is mitigated.

The nRF70 Series device includes hardware AES128 encryption/decryption as part of QSPI/SPI which is described in the Product Specification. By using equivalent AES128 encryption/decryption on the host, all traffic over the physical QSPI/SPI can be protected. This is invisible to all layers of the Wi-Fi stack and can be enabled at any time. Once enabled, it cannot be disabled without a reboot.

To use this protection, matching keys need to be programmed into both the nRF70 Series device and the host MCU. The key for the nRF70 Series device is configured through the *OTP memory*. If hardware support exists on the host side, QSPI encryption can be enabled using the qspi_enable_encryption API with a key passed to it. See the Wi-Fi Station sample in the nRF Connect SDK. For host devices without hardware encryption/decryption support, it is feasible to implement this encryption/decryption in software if needed.

### 2.3.1 Program the QSPI encryption key

The encryption key is 128 bits and is held in registers QSPI.KEY[0] to QSPI.KEY[3]. The ordering of the bits in the four registers is documented in the nRF70 Series Product Specifications.

For example, the key 0xFFEEDDCCBBAA99887766554433221100 can be programmed using the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_write_params 0x110 0x33221100 0x77665544 0xBBAA9988 0xFFEEDDCC`.

### 2.3.2 Alternative method

Using QSPI/SPI link encryption is optional.

# 2.4 Assembly test

It is recommended to test the assembled product at the RF level, ensuring all discrete components are correctly fitted and the RF paths (independent 2.4 GHz and 5 GHz) from the chip pins to the antenna are verified.

## 2.4.1 Test method

Since the TX and RX paths are common from the chip pin to the antenna, it is sufficient to only test in the TX direction.

Use the Wi-Fi Radio test sample to transmit a carrier wave or a modulated packet in each band with control over the channel, modulation type, and transmit power. The following Wi-Fi Radio test commands transmit MCS0 IEEE 802.11n packets at 16 dBm on channel 7:

```
wifi_radio_test init 7
wifi_radio_test tx_pkt_tput_mode 1
wifi_radio_test tx_pkt_mcs 0
wifi_radio_test tx_power 16
wifi_radio_test tx 1
```

Measure the received signal power on a *VSA* to confirm it is within an acceptable limit, taking into account test setup losses. The carrier frequency offset can also be measured to confirm the crystal oscillator trim *OTP memory* programming was successful.

This TX test should be repeated in the 5 GHz band by selecting an appropriate 5 GHz `channel` (for example, 48) with the `wifi_radio_test init 48` command.

## 2.4.2 Alternative method

The received signal power can be checked while performing crystal/crystal oscillator trimming. However, this is typically only conducted on a single band, so an additional check of the other band is recommended.

# 3 Characterization lab operations

During product development, it may be required to fully characterize TX and RX performance of the final product. This is a time-consuming process and should not be performed on each unit on the production line.

## 3.1 TX performance

TX performance typically involves a sweep of TX power versus *Spectral Emission Mask (SEM)* and *Error Vector Magnitude (EVM)* identifying the maximum transmit power at each EVM limit.

The SEM limit is a function of operating band and bandwidth, while the EVM limit is a function of modulation. Measurement of these requires transmitting modulated packets from the *Device Under Test (DUT)* and using a *VSA* to measure EVM and SEM. The transmit power of the DUT should be swept until either SEM or EVM compliance fails.

The following table summarizes the EVM requirement as a function of modulation for *Orthogonal Frequency Division Multiplexing (OFDM)* modulation types.

| MCS index | Modulation | Code rate | EVM (dB) |
|---|---|---|---|
| 0 | BPSK | 1/2 | -5 |
| 1 | QPSK | 1/2 | -10 |
| 2 | QPSK | 3/4 | -13 |
| 3 | 16-QAM | 1/2 | -16 |
| 4 | 16-QAM | 3/4 | -19 |
| 5 | 64-QAM | 2/3 | -22 |
| 6 | 64-QAM | 3/4 | -25 |
| 7 | 64-QAM | 5/6 | -27 |

*Table 4: EVM requirements*

For *Direct-sequence Spread Spectrum (DSSS)/Complementary Code Keying (CCK)* modulation types, the EVM limit is -9 dB.

Use the Wi-Fi Radio test sample to control the TX parameters of the DUT. For example, the following sequence transmits an MCS0 IEEE 802.11n packet at 15 dBm on channel 7 in the 2.4 GHz band:

```
wifi_radio_test init 7
wifi_radio_test tx_pkt_tput_mode 1
wifi_radio_test tx_pkt_mcs 0
wifi_radio_test tx_power 15
wifi_radio_test tx 1
```

To set the next value in sweep (for example, to 16 dBm), use the following sequence:

```
wifi_radio_test tx 0
wifi_radio_test tx_power 16
wifi_radio_test tx 1
```

## 3.2 RX performance

RX performance is usually characterized by quoting sensitivity, which is determined through a *Packet Error Rate (PER)* measurement.

The *IEEE 802.11 specification* defines the parameters for sensitivity measurements for the different PHY modes. A sensitivity measurement involves a *Vector Signal Generator (VSG)* transmitting a fixed number of packets (typically 10,000) of a specific modulation type and length at a known signal strength. The *DUT* records the number of packets successfully received (that is, *Cyclic Redundancy Check (CRC)* check passes). The ratio of failed packets to total transmitted packets is the PER. The sensitivity is defined as the receive signal strength (in dBm) where a 10% or lower PER is achieved.

To find this limit, a sweep of signal strength at the VSG must be performed (that is, the PER measurement repeated multiple times at different signal strengths). Various approaches to sweeping the transmit power can be adopted in order to minimize test time, or a linear sweep of the entire receive signal strength range can be performed in order to produce a bathtub curve of receive signal strength (x-axis) vs PER (y-axis), from which the sensitivity can be identified.

Use the Wi-Fi Radio test sample to enable RX mode and record the packet statistics on the DUT. For example, the following sequence sets the device into receive mode on channel 7 in the 2.4 GHz band.

```
wifi_radio_test init 7
wifi_radio_test rx 1
```

Once RX mode is enabled, the VSG should be enabled to transmit 10,000 packets at the required modulation, code rate, and transmit power. Once complete, request the DUT to record the number of successfully received packets with the `wifi_radio_test get_stats` command. The PER can be calculated from the number of successfully received packets.

Then disable the DUT to make it ready for another measurement at an alternate receive signal strength (controlled through the transmit power at the VSG) with the command `wifi_radio_test rx 0`.

# 4 OTP memory programming

Although the *OTP memory* is one time programmable, any bit still in a `1` state can be reprogrammed into a `0` state. To avoid deliberate or accidental modification of the OTP memory data, a protection mechanism is provided.

The following table shows how the protection mechanism controls access to the OTP memory through the register REGION.PROTECT.

| OTP memory access state (REGION.PROTECT) | Disabled (0xFFFFFFFF) | Enabled (0x50FA50FA) | Protected (0x00000000) |
|---|---|---|---|
| CALIB.x | No access | Read/write access | Read-only access |
| MAC.x | No access | Read/write access | Read-only access |
| QSPI.x | No access | Read/write access | No access |

*Table 5: Protection mechanism*

Devices are shipped with the OTP memory access in the disabled state. The Wi-Fi Radio test sample includes commands for programming the OTP memory. The following steps are required:

1. Set the protection registers (REGION.PROTECT[0..3]) to `0x50FA50FA` to enable read/write access of the remaining OTP memory locations with the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_write_params 0x100 0x50FA50FA`.
2. Reboot the device to finish enabling read/write access to the OTP memory.
3. Update the OTP memory registers described in various steps in Production line operations on page 5.
4. Set the OTP memory to protected state with the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_write_params 0x100 0x00000000`.

Updates to the OTP memory are no longer possible. If needed, enabling protection can be deferred. Programmed values will take effect even without protection enabled.

> **Note:** Whenever an OTP memory register is updated, the corresponding bit in the register REGION_DEFAULTS must be updated to instruct the firmware to utilize the value programmed into the OTP memory, and not the firmware-based default value. When using the Wi-Fi Radio test sample to program the individual OTP memory locations, setting the appropriate bit in the register REGION_DEFAULTS is done automatically.

Use the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_read_params` to confirm the state of OTP memory. This reports the value of all OTP memory registers, including the register REGION_DEFAULTS, except for the QSPI encryption keys which cannot be read. Alternatively, use the Wi-Fi Radio test command `wifi_radio_ficr_prog otp_get_status` to indicate which registers have been programmed without reporting the actual values.

# Glossary

**Application Programming Interface (API)**

A language and message format used by an application program to communicate with an operating system, application, or other service.

**Carrier Frequency Offset (CFO)**

The frequency offset from the expected carrier wave frequency or channel center frequency.

**Complementary Code Keying (CCK)**

A modulation scheme used with wireless networks that follow the IEEE 802.11b specification amendment.

**Cyclic Redundancy Check (CRC)**

An error-detecting code commonly used in digital networks and storage devices to detect accidental changes to digital media.

**Device Under Test (DUT)**

A manufactured product undergoing testing.

**Direct-sequence Spread Spectrum (DSSS)**

A spread-spectrum modulation technique primarily used to reduce overall signal interference.

**Error Vector Magnitude (EVM)**

A measure used to quantify the performance of a digital radio transmitter or receiver.

**Microcontroller Unit (MCU)**

A small computer on a single metal-oxide-semiconductor integrated circuit chip.

**Microprocessor Unit (MPU)**

A computer processor where the data processing logic and control is included on a single integrated circuit or a small number of integrated circuits.

**Orthogonal Frequency Division Multiplexing (OFDM)**

A type of digital transmission and a method of encoding digital data on multiple carrier frequencies.

**One Time Programmable (OTP) memory**

A type of non-volatile memory that permits data to be written to memory only once.

**Packet Error Rate (PER)**

The number of incorrectly received data packets divided by the total number of received packets.

**Printed Circuit Board (PCB)**

A board that connects electronic components.

**Quad Serial Peripheral Interface (QSPI)**

A Serial Peripheral Interface (SPI) controller that allows the use of multiple data lines.

**Spectrum Analyzer (SA)**

An instrument that measures the magnitude of an input signal versus frequency within the full frequency range of the instrument.

**Spectral Emission Mask (SEM)**

A spectrum mask where the spectrum emissions should not be higher at any frequency offset than the values specified in the mask.

**Serial Peripheral Interface (SPI)**

Synchronous serial communication interface specification used for short-distance communication.

**System on Chip (SoC)**

A microchip that integrates all the necessary electronic circuits and components of a computer or other electronic systems on a single integrated circuit.

**Vector Signal Analyzer (VSA)**

A signal analyzer capable of analyzing digitally-modulated radio signals that may use any of a large number of digital modulation formats.

**Vector Signal Generator (VSG)**

A signal generator capable of generating digitally-modulated radio signals that may use any of a large number of digital modulation formats.

**Virtual Network Interface (VIF)**

An abstract virtualized representation of a computer network interface that may or may not correspond directly to a network interface controller.

# Recommended reading

In addition to the information in this document, you may need to consult other documents.

## Nordic documentation

- nRF7002 Product Specification
- nRF Connect SDK Wi-Fi: Radio test sample
- nRF Connect SDK Wi-Fi: Station sample

# Legal notices

By using this documentation you agree to our terms and conditions of use. Nordic Semiconductor may change these terms and conditions at any time without notice.

## Liability disclaimer

Nordic Semiconductor ASA reserves the right to make changes without further notice to the product to improve reliability, function, or design. Nordic Semiconductor ASA does not assume any liability arising out of the application or use of any product or circuits described herein.

Nordic Semiconductor ASA 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. If there are any discrepancies, ambiguities or conflicts in Nordic Semiconductor's documentation, the Product Specification prevails.

Nordic Semiconductor ASA reserves the right to make corrections, enhancements, and other changes to this document without notice.

## Life support applications

Nordic Semiconductor products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury.

Nordic Semiconductor ASA customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nordic Semiconductor ASA for any damages resulting from such improper use or sale.

## RoHS and REACH statement

Complete hazardous substance reports, material composition reports and latest version of Nordic's REACH statement can be found on our website www.nordicsemi.com.

## Trademarks

All trademarks, service marks, trade names, product names, and logos appearing in this documentation are the property of their respective owners.

## Copyright notice

© 2023 Nordic Semiconductor ASA. All rights are reserved. Reproduction in whole or in part is prohibited without the prior written permission of the copyright holder.