

DnX (Download and Execute)

User Guide

November 2019

Revision 1.0

Intel Confidential



By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>.

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2019, Intel Corporation. All rights reserved.



Contents

1	Introduction.....	5
	1.1 Terminology.....	5
	1.2 Reference Documents.....	5
2	Download and Execute (DnX)	6
	2.1 Introduction	6
	2.2 Use Cases	7
	2.3 Triggers	7
	2.4 DnX flow.....	8
	2.5 Tools	8
3	High-Level Setup Detail for DnX	9
	3.1 Setup Requirements.....	9
4	Intel® Platform Flash Tool (PFT) Overview	10
	4.1 Installation Details	10
	4.2 Usage.....	10
	4.2.1 PFT Command Line Tools for DnX	11
	4.2.2 Using GUI interface	14



Revision History

Revision Number	Description	Revision Date
0.7	<ul style="list-style-type: none">• Initial release	July 2019
0.71	<ul style="list-style-type: none">• Updates for SPI based platform	Aug 2019
1.0	<ul style="list-style-type: none">• Removed capabilities no supported for SPI	Nov 2019

§ §



1 Introduction

The purpose of the document is to provide guidance on the Download and Execute (DnX) feature, usage of this feature and how it gets enabled using Intel® CSE components as well as Intel® Platform Flash Tool (PFT).

1.1 Terminology

Table 1: Terminology

Acronym or Term	Definition
Intel® CSE	Intel® Converged Security Engine
DnX	Download and Execute
Intel® FIT	Intel® Flash Image Tool
FW	Firmware
Intel® PFT	Intel® Platform Flash Tool

1.2 Reference Documents

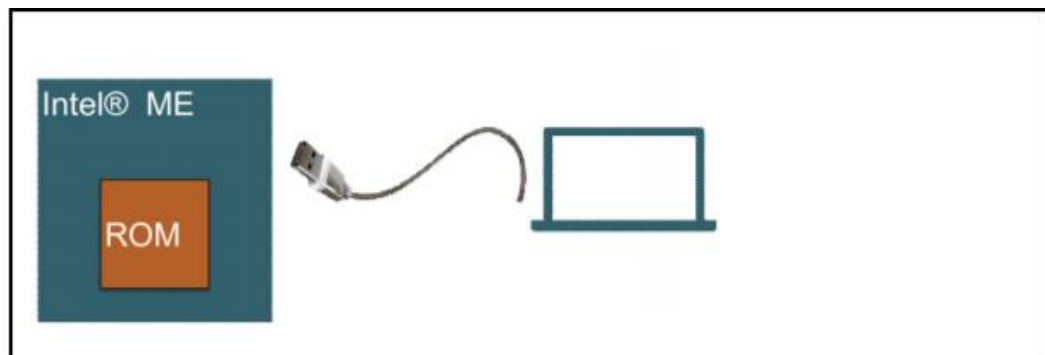
Table 2: Reference Documents

Document	Document No. / Location
Tiger Lake Intel® CSE FW 15.0 POR	Contact your Intel field representative.

2 Download and Execute (DnX)

2.1 Introduction

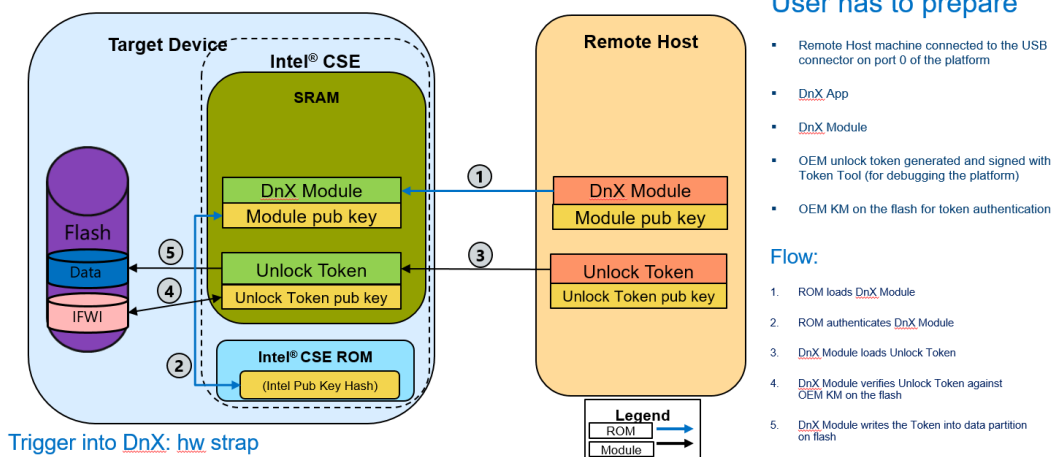
DnX is Intel's proprietary solution to download FW module to a target machine from a host machine by means of USB cable and execute it. DnX flows are executed over fixed USB 2 port. On SPI platforms, this capability allows signed Token injection for debug unlock after the platform have completed manufacturing.



DnX is a capability in Intel® CSE ROM, where during the boot ROM can configure the USB port #0 on the PCH to connect to a remote computer to download DnX module which is signed by Intel. This module initiates rest of the Intel® CSE and sets up an environment to accept unlock token from a remote computer. The flow is explained below:



Injecting Unlock token for Debug



2.2

Use Cases

Below use-cases are supported on TGL platform.

Scenario	Use Case
Debug	<ul style="list-style-type: none"> Write/Read/Erased signed debug tokens into the platform

2.3

Triggers

Following methods can be used to trigger DnX on the platform

Method	Detail
Pin Strap	For details refer to TGL External Design Specification (EDS)
Intel® CSE or BIOS Error Handling Flow	If Intel® CSE or BIOS reach a critical error which prevent platform from booting, it can be programmed to enter DnX flow. (e.g Failure to authenticate BIOS signature, CSE detect FW corruption, etc.)
Empty Flash Device	When CSE ROM detects an empty flash device on the platform, it will enter DnX mode



Method	Detail
BIOS HECI Call	BIOS can make a HECI call to Intel® CSE during boot to enter DnX after the reset

2.4 DnX flow

1. DNX Trigger:
 - a. ROM Detect empty Flash
 - b. Corrupted Flash
 - c. User Trigger via BIOS or Strap
2. ROM enumerates USB and establish USB Comm. with the Host
3. ROM DNX Logic establish connection with the recovery app via USB
4. ROM DNX logic download DNX module from recovery app to SRAM and authenticates it
5. DNX Module performs DnX operation requested by user

2.5 Tools

Following tools are applicable for DnX:

- **Intel® PFT** (Platform Flash Tool) – Intel implementation of DnX tool running on remote host computer. DnX module, config.xml and IFWI.bin are inserted to the target machine via this tool. Will be included in the Intel® CSE Kit for TGL platform.
- **DnX Module** - binary file signed by Intel. This file has the DnX logic Intel® CSE ROM will run. Will be included in the Intel® CSE kit for TGL Platform.
- **Intel® FIT** – can be used to create DnX based IFWI image. For more detail on how to create IFWI image for DnX, please refer to Intel® Bring up Guide in the Intel® CSE kit for TGL Platform.
- **Intel® FPT** - can be used to configure DnX fuse and close manufacturing on the platform. Will be included in the Intel® CSE kit for TGL Platform.



3 High-Level Setup Detail for DnX

3.1 Setup Requirements

In order to complete DnX flow, the following setup is required

DnX Test Setup

Target Device

- Enters DnX mode based on trigger

Management Console

- Platform Flash Tool (PFT)
- DnX module
- IFWI image



Requirements:

Requirement	Usage
Management Console / Remote Host	A host that can be used to execute the DnX flows
H/W Connection	USB cable connection between the Remote Host to the system under test
Intel® Platform Flash Tool (PFT)	Tool supporting DnX flows running on the Remote Host
DnX module binary	Provided in the Intel® CSE FW kit. This binary is provided as an input to the Intel® PFT.
OEM signed unlock token	Token binary to be flashed on the target system (Can be created by Intel® PFT tool provided in the Intel® CSE)



4 Intel® Platform Flash Tool (PFT) Overview

Intel® Platform Flash Tool supports GUI (Graphic User Interface) as well as CLI (Command Line Interface) and runs on the Remote Host.

This tool supports DnX flows and consumes DnX related input files like: DnX module, unlock token file to be flashed on the target system.

Please install this tool on Host system before executing DnX flows.

4.1 Installation Details

PFT tool is available within Intel® CSE FW Kit->Tools->DnX Tools. Run the installation package. Setup wizard will start. Click “Next” to complete the installation.

This installation process installs Tools as well as necessary USB drivers along with it as well.



4.2 Usage

Once PFT tool is installed on the Remote Host:

- Make sure the target system is connected to the Remote Host using USB cable.
- Make sure all input files required for DnX operation (e.g. DnX module, token) are available on the Remote Host.



4.2.1 PFT Command Line Tools for DnX

- **DnX Firmware Downloader**

This command line tool provides means to interact with Intel® CSE firmware and perform different DnX operations.

This tool supports serial number argument, however does not provide USB port hence less convenient for setups with multiple targets connected to one remote host.

Note: target machine has to be already in DnX mode (e.g jumper, virgin storage)

4.2.1.1 DnX Firmware Downloader

Usage:

```
dnxFwDownloader --command <command> <command-options>
```

Help Menu

dnxFwDownloader.exe --help command lists available options/commands supported with this embedded tool.

4.2.1.1.1 Get storage device general info

In order to get storage related information such as OEM PLAT ID (from IFPs), Platform Unique ID, DnX Trigger, Image Error Values, '**iddevice**' command shall be used.

Sample:

```
dnxFwDownloader.exe --command iddevice
```

4.2.1.1.2 Reset Target Platform

In order to reset the platform, '**startover**' command shall be used.

Sample:

```
dnxFwdownloader.exe --command startover --flags 9
```

Where:

Option	Description



--flags	<p>Firmware reset command flags. In the command line appear in decimal display.</p> <p>Comprises of following info (in binary):</p> <p>Bit [1:0]: RESET_TYPE*</p> <ul style="list-style-type: none">• 00: Reset DnX protocol (no Intel® CSE /device reset) by cancelling currently active command (if any) and wait for the next command• 01: Global reset• 10: Not supported• 11: Not supported <p>Bit [3:2]: POST_RESET_STEPS</p> <ul style="list-style-type: none">• 00: After reset, take normal boot path (including honoring the DnX triggers etc.)• 01: After reset, enter OS DNX flow• 10: After reset, ignore optional DnX triggers such as HW strap etc. and perform a full host boot• 11: Reserved
---------	---

4.2.1.1.3 Read Token

In order to read token, '**readtoken**' command shall be used.

Sample:

```
dnxFwDownloader.exe --command readtoken --fw_dnx DNXP_0x1.bin --path  
read_token.bin --slot 0
```

Where:



Option	Description
--fw_dnx	path to the DnX module binary
--path	path to output file to dump the content of the token
--slot	Slot Index of the token

4.2.1.1.4 Write Token

In order to write token, '**writetoken**' command shall be used.

Sample:

```
dnxFwDownloader.exe --command writetoken --fw_dnx DNXP_0x1.bin --token  
token_to_write.bin --slot 0
```

Where:

Option	Description
--fw_dnx	path to the DnX module binary
--token	path to the token
--slot	Slot Index of the token

4.2.1.1.5 Erase Token

In order to erase token, '**erasetoken**' command shall be used.

Sample:

```
dnxFwDownloader.exe --command erasetoken --fw_dnx DNXP_0x1.bin --slot 0
```

Where:

Option	Description
--fw_dnx	path to the DnX module binary
--slot	Slot Index of the token



4.2.1.1.6 Get Token Part ID

In order to get part ID specific to this token, '**gettokenpid**' command shall be used.


Sample:

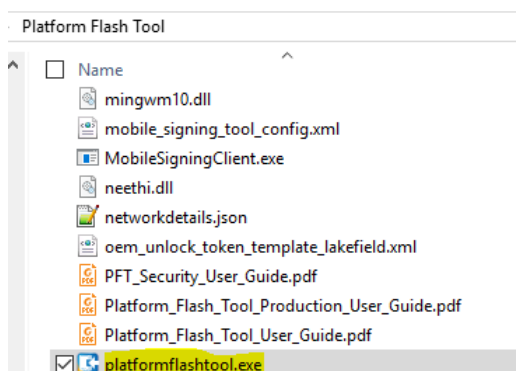
```
dnxFwDownloader.exe --command gettokenpid --fw_dnx DNXP_0x1.bin --flags 0
```

Where:

Option	Description
--fw_dnx	path to the DnX module binary
--flags	Slot number for anti-replay protection of corresponding token: <ul style="list-style-type: none">• 0: No AR protection needed. Nonce is stored in the temp storage in SRAM• 1: Nonce generated is stored in first Nonce slot

4.2.2 Using GUI interface

- To launch GUI interface, click on the Desktop icon  which launches GUI interface or open it from Intel® PFT installation folder.



- Go to the Security tab on the left.
- To inject a token



- Generate+ Sign a new token or brows for an existing token to write into the device. For guidance on how to generate and sign unlock token, see “Secure Token Guide”
- Select a device
- press button “Write” in “Write / Read / Erase” section of the GUI
- To Read or Erase a token
 - Select a device
 - press button “Read” / “Erase” in “Write / Read / Erase” section of the GUI

