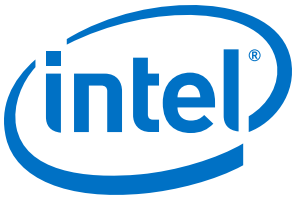
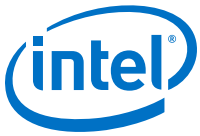


Intel® Arria 10 SoC Secure Boot User Guide

AN-759 | 2017.11.06
Latest document on the web: PDF | HTML

Contents



Intel® Arria® 10 SoC Secure Boot User Guide

The Intel® Arria® 10 SoC device family and supported tools provide features and resources to create a secure boot system. Secure booting is essential to protect the design's intellectual property (through encryption) and prevent malicious software from running on the system (through authentication). A secure boot system establishes a chain of trust. Each piece of firmware or software is validated before running, and also validates the security signature on the next piece of software before loading it for execution.

This document provides methods and design examples for implementing an Arria 10 SoC secure boot system using tools from the Intel SoC FPGA Embedded Design Suite (EDS)SoC Embedded Design Suite (SoC EDS) to secure the second-stage boot loader image. It shows how to generate a secure boot loader, creating and programming secure keys for image authentication and image encryption and decryption.

Note: Securing boot stages after the second-stage boot loader is outside the scope of this document and is dependent on your choice of OS and application. If the boot loader must secure subsequent boot stages (such as the operating system), you must implement a secure boot flow at the second-stage boot loader. The SoC EDS does not provide any specific support for boot security beyond the second-stage boot loader.

Note: This user guide reflects information available at the time of publication. To ensure that you have the most recent information about enhancements to the tools and tool flow, refer to the Intel FPGA website, especially the *Intel FPGA SoC Embedded Design Suite Release Notes*.

Related Links

- Intel SoC FPGA Embedded Design Suite Release Notes
- www.altera.com
  The most recent information about enhancements to Arria 10 secure boot tools and tool flow

Prerequisites

- Supported development platforms:
  - Red Hat Linux version 6 or higher
  - Windows versions as supported by the Quartus Prime software
- Quartus Prime Standard or Pro Design Suite, version 16.0 or later
- SoC EDS version 16.0 or later

Throughout this document, <*SoC EDS installation directory*> denotes the location where SoC EDS is installed. The default installation folder for the SoC EDS v16.0 is:

- `c:\altera\16.0\embedded` on Windows
- `~/altera/16.0/embedded` on Linux

References

To make the best use of this guide, you should be familiar with the *Intel Arria 10 SoC Boot User Guide*, the *Intel Arria 10 Hard Processor System Technical Reference Manual*, and the *Intel FPGA SoC Embedded Design Suite User Guide*.

Related Links

- Intel Arria 10 SoC Boot User Guide
- Intel Arria 10 Hard Processor System Technical Reference Manual
- Intel SoC FPGA Embedded Design Suite User Guide

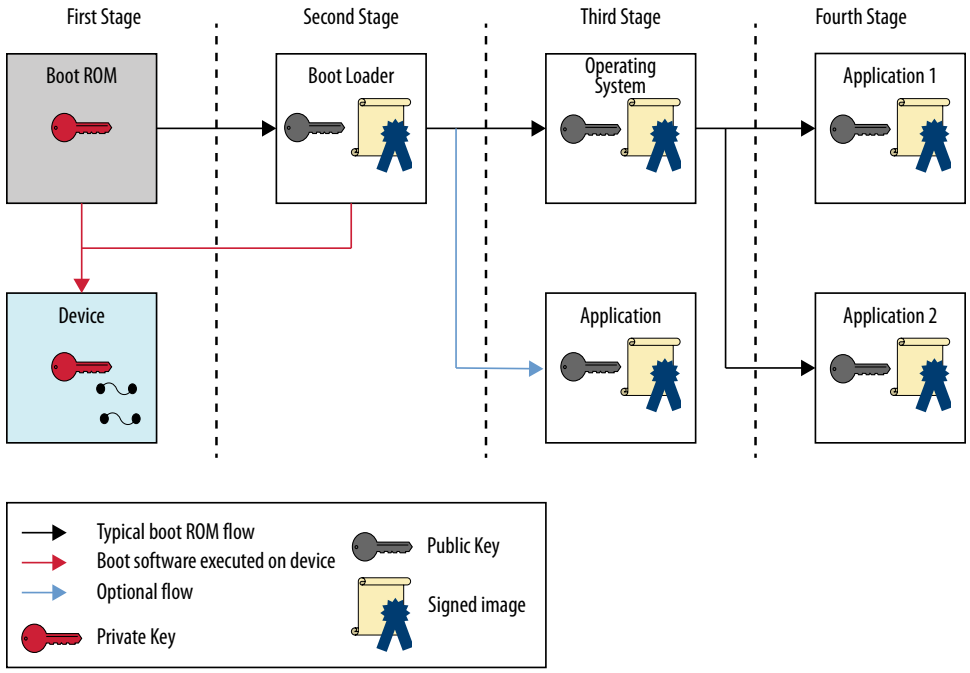
Secure Boot Stages

The main purpose of a secure boot system is to ensure that software running on the Arria 10 SoC hard processor system (HPS) is trusted. To ensure this trust, after power-on reset, the HPS executes the trusted first stage boot ROM firmware stored in the device. Each subsequent stage is only loaded and executed if it is authenticated by the current boot stage.

The Intel Arria 10 secure boot stages are shown in the following figure.

Figure 1. Secure Boot Stages

Note: You can configure the Intel Arria 10 SoC device and the second-stage boot loader so that first and second stages boot securely. If required, you can generate additional signing keys and encryption keys for images in subsequent stages including the OS and application stage. If a subsequent image requires encryption and the encryption key is embedded in the boot loader, then the boot loader image must also be encrypted using the root AES key.



For more information on the Intel Arria 10 boot stages and second-stage boot loader refer to the *Intel Arria 10 SoC Boot User Guide*.

Related Links

Intel Arria 10 SoC Boot User Guide

Root of Trust

The most crucial part of creating a secure boot system is establishing the root of trust. The root of trust ensures that the security levels are configured properly and the security keys are protected.

Related Links

Software Image Authentication on page 8
For more information on root of trust

First-Stage Boot Loader (ROM)

After hardware system initialization is complete, the Intel Arria 10 SoC boot ROM firmware decrypts, authenticates, and executes the next boot stage. The boot ROM firmware is the root of trust: the trusted, inherently secure starting point for booting the Intel Arria 10 SoC.

To decrypt and authenticate the next boot stage, the boot ROM firmware performs these tasks:

1. Determine which boot device contains the next boot stage image, the second-stage boot loader
2. Discover the final code signing key (CSK) through a key chain service
3. Use the CSK to authenticate the boot loader image
4. If the boot loader image is encrypted, the boot ROM sends the image to the CSS for decryption.
5. If boot loader authentication and decryption is successful, load the boot loader into on-chip RAM and execute it

For details about secure system initialization, refer to "Secure Initialization Overview" in the *SoC Security* chapter of the *Intel Arria 10 Hard Processor System Technical Reference Manual*.

Related Links

Secure Initialization Overview

Second-Stage Boot Loader

The second-stage boot loader performs essential tasks to allow an operating system to start.

The boot loader can perform a number of required and optional tasks, such as:

- Configuring I/Os to enable the memory controller prior to FPGA configuration
- Configuring the FPGA portion of the device
- Accessing a file system in flash memory
- Initializing peripherals

In a secure boot implementation, the second-stage boot loader software executes from HPS on-chip RAM.

Third and Fourth Stages

If the stages following the second-stage boot loader need to be trusted, then you must implement features to support authentication in the third and fourth stage.

During the third boot stage, an operating system (OS) or stand alone application, such as Bare Metal, typically loads from flash storage into memory. During the fourth boot stage, the OS commonly launches secure user level applications.

Intel Arria 10 SoC Secure Boot Architecture

You can implement secure boot using the following modules and features provided by the Arria 10 SoC:

- Security Manager
- Boot ROM
- ECDSA Authentication
- Security Fuses
- AES Decryption Engine
- Security Key Storage

A dedicated Security Manager resides in the HPS. It supervises a secure initialization and boot of the system. The Security Manager determines the level of system security in the device by reading the HPS fuse settings after power-on reset (POR).

After the security level is determined, secure boot resources attempt to load software into HPS flash. The boot ROM supervises this bootstrapping process.

Software Image Authentication

Authentication of the second-stage boot loader software by the Intel Arria 10 SoC device provides confidence that it originates from a trusted source. Digital certificates and public key cryptography offer advanced authentication and privacy that less advanced security resources, such as passwords, cannot provide.

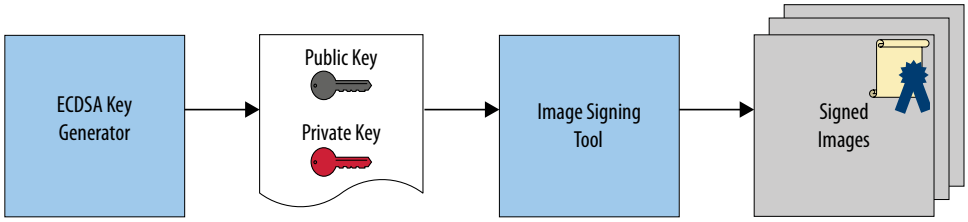
Authentication begins when the boot image is digitally signed. The Intel Arria 10 SoC device requires the image to be signed using an elliptical curve digital signature algorithm (ECDSA) that is based on elliptical curve (EC) cryptography.

Digital Signing

The signing process requires a security key pair and a signing tool to sign the image. The private and public key pair are generated based on a 256-bit ECDSA asymmetric digital signature. The private key has full entropy and is used to derive the public key.

The signing process creates a digital certificate with signatures based on elliptic curve cryptography. The signed image's credentials during authentication are the digital signature and the public key.

Figure 2. Signing with a Secure Key Pair

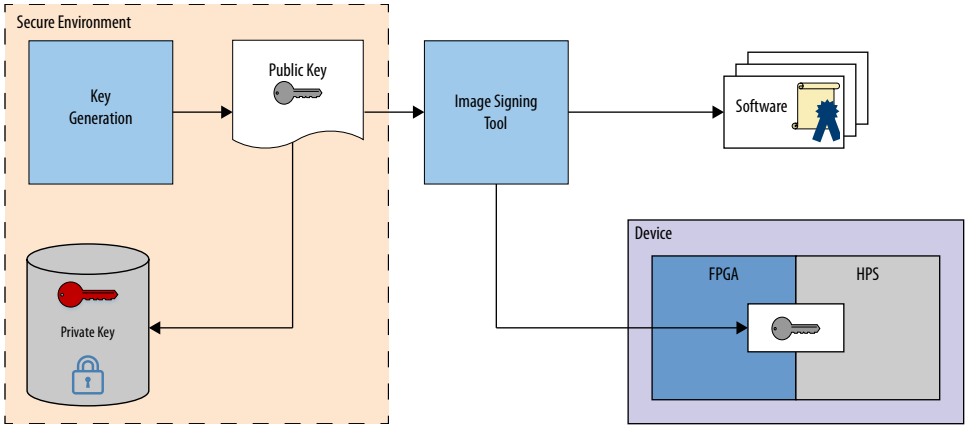


Root of Trust and Root Key

The Root of Trust and the root key pair are the origin where the secure keys are generated. In this secured environment, you can also sign the boot image. A secure environment such as a device manufacturing site, retains the private key to protect it.

The manufacturer generates the root key pair. The root key is programmed into the SoC device and authenticates the software images. The image signing tool is run multiple times for each runtime software on the device. When security is compromised, you must generate a new public key.

Figure 3. Root of Trust



Authentication of the Second-Stage Boot Loader

The security features of the Intel Arria 10 SoC provide you with resources to enforce that only a trusted second-stage boot loader is executed from the HPS. The boot ROM executes the first stage and enforces user security settings. During authentication, the Boot ROM verifies the HPS security fuse settings through the HPS_fusesec shadow registers.

The entire authentication process starts after power-on or cold reset of the device. The process follows a particular order to ensure a secure boot is attempted:

1. On FPGA power-up, the Configuration Subsystem (CSS) powers, initializes and loads the fuse bits. The CSS sends the FPGA its fuse configuration information. If the HPS is powered, the CSS sends the HPS fuse information to the Security Manager. This information is held in the HPS_fusesec shadow register in the Security Manager.
2. When the Security Manager is released from reset, it requests configuration information from the CSS and performs security checks. At this point, the rest of the HPS is still in reset. The security checks validate whether the state of each security option is valid. The Security Manager decodes the fuse bits and brings the rest of the HPS out of reset.
3. When the HPS is released from reset, the Security Manager sends signals to initialize the system blocks, such as the Clock Manager, FPGA Manager, and System Manager. The clock control fuse information is automatically sent to the Clock Manager, the memory control fuse information is automatically sent to the Reset Manager and all other fuse functions (authentication, encryption, and public key source and length) are stored in a memory-mapped location for the boot ROM code to read. After these tasks are successfully completed, CPU0 comes out of reset in a secure state.
4. After CPU0 is released from reset, the boot ROM begins executing. At this time, the HPS is in a trusted state and the boot ROM code is guaranteed to execute as expected. For both secure and non-secure boot, all slave peripherals are brought out of reset in a secure state.
5. The boot ROM determines the boot flash partition and verifies the security header settings of the second-stage boot loader image. The second-stage boot loader requires a signed certificate to be authenticated.
6. The Boot ROM determines the source of the root key by reading the security header.
7. The boot ROM attempts to authenticate the boot image. If authentication is successful, the boot ROM then continues with the process of loading and executing the image.

Security Level Staging

After power-on-reset, the Security Manager determines the initial security level by verifying and reading the fuse data. The Security Manager stores the fuse data in the fuse shadow register, HPS_fusesec. From this point, the boot ROM reads the fuse data from the shadow register and also verifies the security header, if present, in the boot image stored on boot flash partition. The second-stage boot loader is the boot image.

The security header may also contain information to raise the security level for a particular feature implemented in the fuses. The boot ROM merges the fuse values in the shadow registers with the security header values to establish the final security level of the system.

Note: Software may program option registers in the Security Manager to raise the security of the system. The higher level of security takes effect immediately and remains at that level until the next cold reset or for some security features, the next warm or cold reset. After reset occurs, the security level returns to the value programmed by the fuse registers and written in the HPS_fusesec registers.

Signed Image

The signing of an image includes prepending an authentication header, including a security header.

Figure 4. Authentication Header

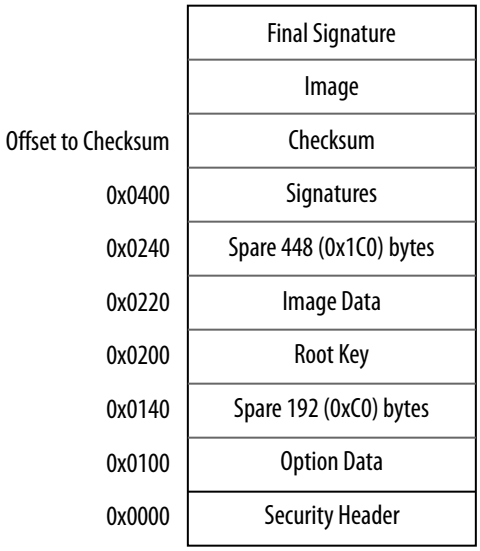
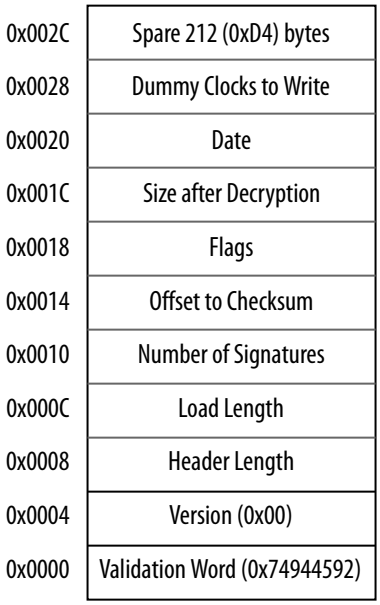


Figure 5. Security Header



Root Key Types

The boot ROM requires the root public key programmed in eFuse and its associated public key to authenticate the second-stage boot loader if the key contained within eFuse, the FPGA or header file (test only) mandates an authenticated flow. Several root key types are available that you can store on the device or second-stage boot loader image.

Note: Using the image itself for storage of the root key is not considered a secure method. It is recommended that this method be used for testing purposes only.

Table 1. Root Key Types

Root Key	Is it stored on the device?	Description
Secure User Key	Yes	User generates secure key pair for boot ROM to attempt authentication. The SHA256 hash of the public key is stored in the User Access Fuses (UAF) of the device. This configuration provides a secure boot.
FPGA Key	Yes	The public key originates from the user bitstream. The key is stored in FPGA on-chip RAM and accessed by the first stage boot ROM for image authentication.
Unsecured User Key	No	User generates a secure key pair but it is not stored on the device. This configuration is considered unsecure. The user includes the root key result in the image header and the boot ROM uses it for authentication.

Root Public Key Authentication

Before boot ROM can use the root public key for authentication, it must authenticate the root public key against the root public key hash stored in eFuse.

Note: Some key types are unsecure. You can use unsecure keys for testing scenarios where permanent key storage on the device is avoided.

The available key type options are detailed in the *Programming the Secure Signing Key* section.

Related Links

Programming the Secure Signing Key on page 13

Test Secure Boot Authentication

You can perform a secure boot test by using an unsecured key for authentication of the signed boot image. Refer to the *Security Level Staging* section for details of how to increase security on the device.

If you choose to implement the unsecure user key type, then the public key in the signed image is accepted and no check is performed against the SHA256 value stored in the device fuses. You can use this method for testing purposes before you burn the fuses.

Related Links

Security Level Staging on page 10

Programming the Secure Signing Key

After the boot image is signed, the private key is retained in secure storage at the original equipment manufacturer (OEM) to protect it. The public key is programmed into the device. For some signing key types, a hash of the public key is programmed.

The signing key type determines the location of the public key. The available signing key types and corresponding locations are described in the following table.

Table 2. Root Key Types

Root Key	Key Type	Description
Secure User Key	Fuse	User generates secure key pair for boot ROM to attempt authentication. The SHA256 hash of the public key is stored in the User Access Fuses (UAF) of the device. This configuration provides a secure boot. For information about secure fuses, refer to the *Secure Fuses* section in the SoC Security chapter of the *Intel Arria 10 Hard Processor System Technical Reference Manual*.
FPGA Key	FPGA	The public key originates from the user bitstream. The key is stored in FPGA on-chip RAM and accessed by the first stage boot ROM for image authentication.
Unsecured User Key	User	User generates a secure key pair but it is not stored on the device. This configuration is unsecure and is for testing only. The user includes the root key result in the image header and the boot ROM uses it for authentication.

Related Links

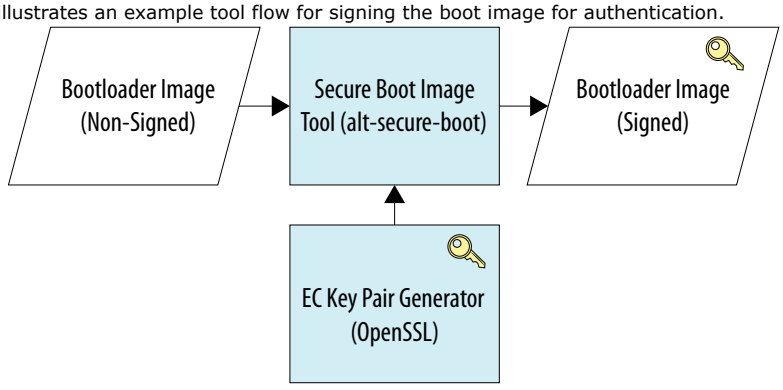
- Secure Boot Stages on page 6
- Generating the Signing Key Pair with OpenSSL on page 14
- Secure Fuses
  For basic information about security fuses, refer to "Secure Fuses" in the *SoC Security* chapter of the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*.

Boot Image Signing Flow

After you have generated the signing key pair, you can build and sign the boot image with the secure boot image tool.

Figure 6. Boot Image Signing Tool Flow

This diagram illustrates an example tool flow for signing the boot image for authentication.

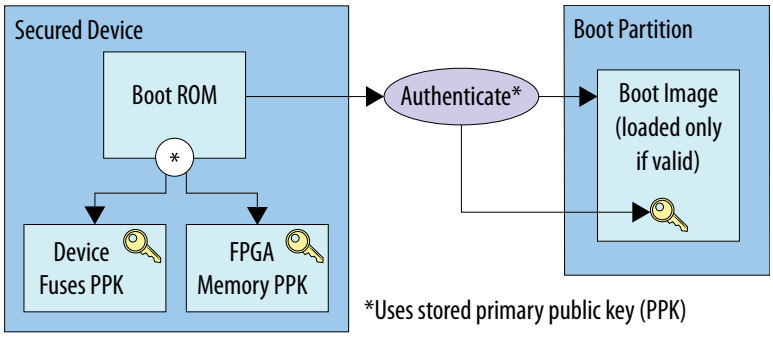


Boot Image Authentication

During a secure boot, the first-stage boot loader (in the boot ROM) uses the root public key and associated key chain to authenticate the second-stage boot loader image as follows:

1. Determine the device's security configuration settings (by reading the fuse values)
2. Attempt to authenticate the boot image, using the root public key type from the configuration settings

Figure 7. Secure Authentication Using Key Types



Related Links

Secure Boot Flow
In the *Booting and Configuration* appendix of the *Intel Arria 10 SoC Hard Processor System Technical Reference Manual*, refer to the following figures: "Verified (Authenticated) Boot Flow", "Second Stage Boot Loader Authentication Process", and "Second Stage Boot Loader Authentication and Decryption Process".

Generating the Signing Key Pair with OpenSSL

You may generate the signing key pair using OpenSSL, an open-source toolkit that supports the Secure Socket Layer (SSL). OpenSSL is available in the SoC EDS embedded command shell, and is provided by common Linux distributions.

You invoke OpenSSL from the boot loader generator. OpenSSL applies the security settings that you select in the boot loader generator, and creates an EC key pair. The boot loader generator invokes OpenSSL as follows to generate the key pair:

```
$ openssl ecparam -genkey -name prime256v1 -out root_key.pem
```

In the example above, the generated key pair is stored in the **root_key.pem** file. You can use this file with the Intel secure boot image tool to sign the image.

Related Links

www.openssl.org
Detailed help and information for the OpenSSL toolkit is available on the OpenSSL website.

Overview of the Secure Boot Flow

To create a secure boot system, you can use one of the following secure boot configurations:

- Encrypted only
- Authenticated only
- Encrypted and authenticated

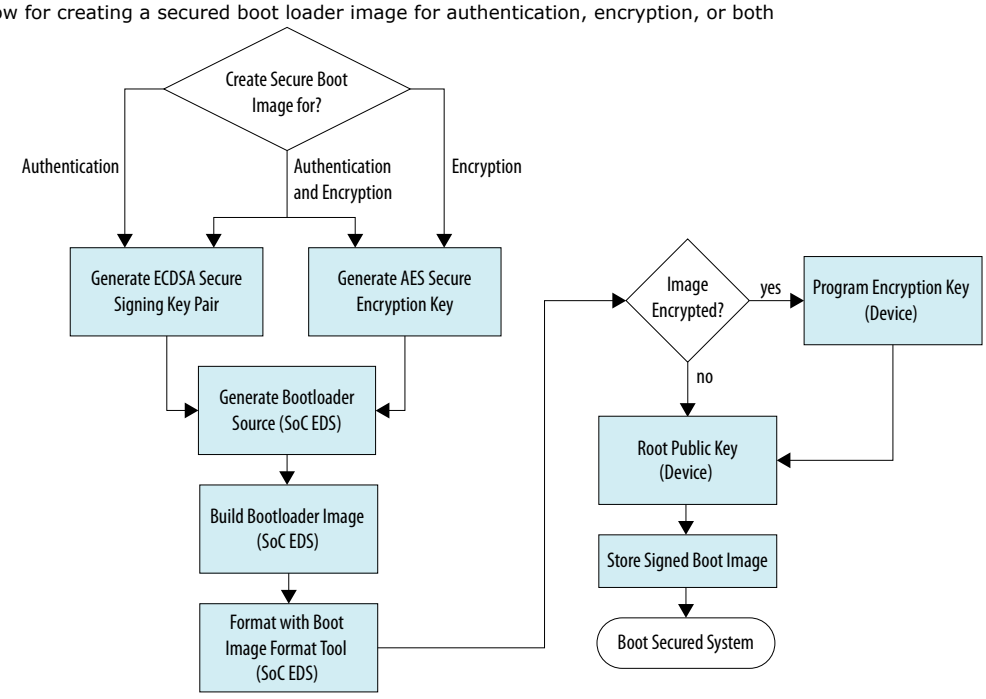
Creating a Secure Boot System

Creating a secure boot loader image entails the following high-level steps:

1. Determine the required security level of the second-stage boot loader: signed for authentication, encrypted, or both.
2. Generate the appropriate secure keys for authentication, encryption, or both.
3. Generate and build the secure boot loader image.
4. Program the secure keys in the Intel Arria 10 SoC device.
5. Configure the security fuses for the desired device security settings.
6. Program the secure boot image to the boot device.

Figure 8. Second-Stage Boot Loader Image Creation Flow

Flow for creating a secured boot loader image for authentication, encryption, or both



Note: The figure above represents SoC EDS secure boot support at the time of publication. Refer to the *Intel FPGA SoC Embedded Design Suite Release Notes* for updates and additions to supported features.

Note: To obtain the steps for programming the secure fuses, please contact Intel Support (NDA required).

Related Links

- Second-Stage Boot Loader Support Package Generator Tool
  In the *Intel Arria 10 SoC Boot User Guide*
- Secure Fuses
  For basic information about security fuses, refer to "Secure Fuses" in the *SoC Security* chapter of the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*.
- Intel SoC FPGA Embedded Design Suite Release Notes

Software Image Encryption

To encrypt a boot image, you generate and apply encryption keys.

Refer to the "Secure Boot Stages" figure for an overview of key usage.

Related Links

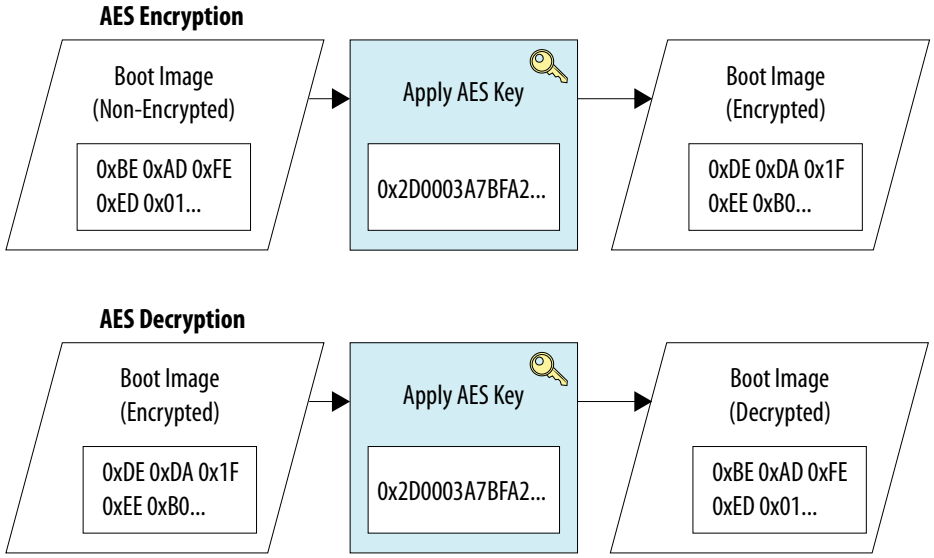
Secure Boot Stages on page 6

AES Encryption and Decryption

The Arria 10 SoC device family supports secure boot with Advanced Encryption Standard (AES) encryption with a 256-bit key length. AES is a symmetric-key algorithm. AES decryption support is provided by the configuration subsystem (CSS) in the FPGA portion of the device. AES decryption is enabled through user fuse settings and software programming.

For information about the CSS, refer to the *SoC Security* chapter in the *Arria 10 Hard Processor System Technical Reference Manual*.

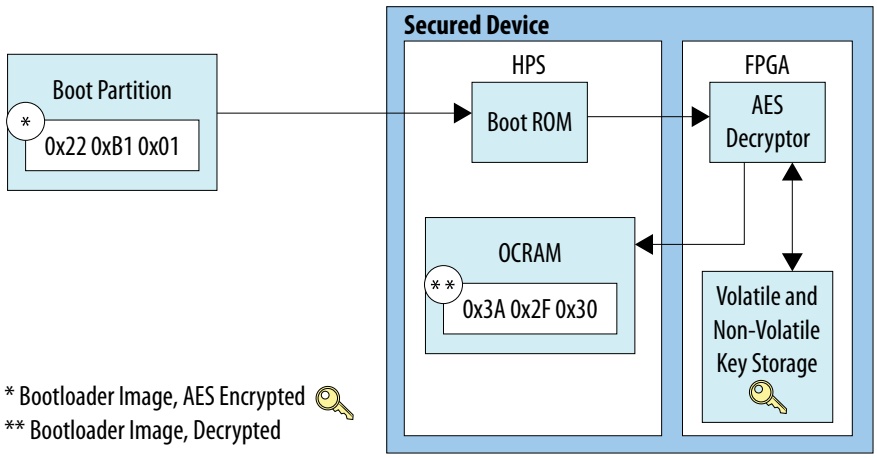
Figure 9. AES Encryption and Decryption



The FPGA portion of the secured device has a dedicated decryption block that uses the AES algorithm to decrypt the boot loader image with a user-defined 256-bit AES key. Before receiving the encrypted data, you must write the user-defined 128-bit key into the device.

The AES algorithm is a symmetrical block cipher that encrypts and decrypts data in blocks of 256 bits. The decryption block uses the AES algorithm to decrypt the boot loader image and configuration data before configuring the FPGA portion of the device. If encryption is not used, the AES decryptor is bypassed.

Figure 10. Encrypted Second-Stage Boot Loader and the AES Decryptor



Related Links

- SoC Security
  Chapter in the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*
- Security Encryption Algorithm
  Refer to "Security Encryption Algorithm" in AN-556: *Using the Design Security Features in Altera FPGAs*

Encrypting the Boot Image and Configuration File

The Quartus Prime Design Suite includes the Quartus Prime Convert Programming File tool, **quartus_cpf**, which you use to generate the AES 256 encryption file.(1) You invoke the Quartus Prime Convert Programming File tool as follows:

```
quartus_cpf -e -k <keyfile>:<key_id>[:<key_id>] <input_sof_file>
<output_ekp_file>
```

If you configure the boot loader generator to encrypt the boot image, **quartus_cpf** requires the encryption key file as specified in the configuration tool's security settings. For an overview of the tool flow, see the figure in "Software Image Authentication and Encryption".

For details of Quartus Prime Convert Programming File tool usage, refer to "How to Generate the Single-Device .ekp File and Encrypt Configuration File Using Quartus Prime Software with the Command-Line Interface" in AN-556: *Using the Design Security Features in the Altera FPGAs*.

Related Links

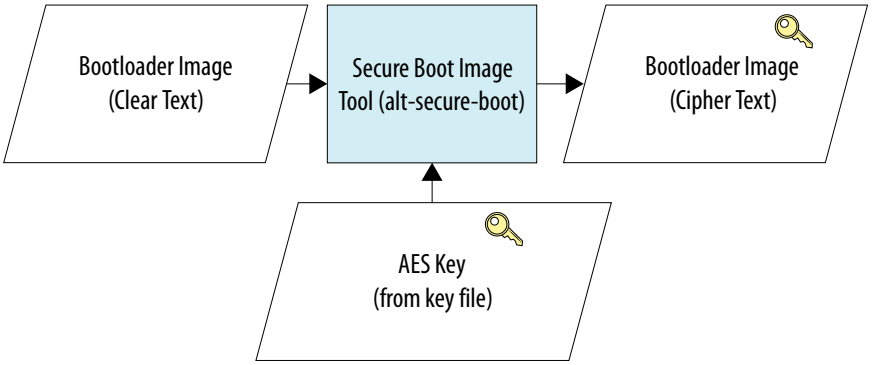
- Software Image Authentication and Encryption on page 20
- How to Generate the Single-Device .ekp File and Encrypt Configuration File Using Quartus Prime Software with the Command-Line Interface
  In AN-556: *Using the Design Security Features in Altera FPGAs*

(1) **quartus_cpf** can also encrypt the configuration bit stream in the SRAM object file (**.sof**).

Boot Image Encryption Flow

Figure 11. Boot Image Encryption Flow

The tool flow for generating an encrypted boot image



Programming the AES Encryption Key

The FPGA device provides both volatile and non-volatile key storage. After the encryption key is generated, you store the key, as described in "Creating an Encrypted Second-State Boot Loader Image". The key is later referenced by the AES-based algorithms that decrypt the boot image. See the "AES Decryption" figure in "AES Encryption and Decryption".

Related Links

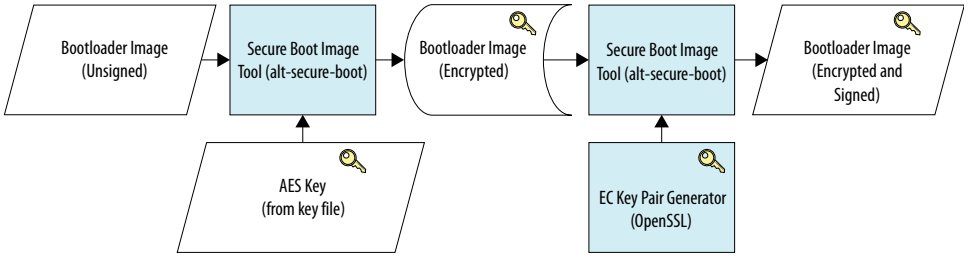
- AES Encryption and Decryption on page 17
- Creating an Encrypted Second-Stage Boot Loader Image on page 27
- Secure Boot Flow
  Refer to the "Second-Stage Boot Loader Decryption Process" figure in "Secure Boot Flow" in the *Booting and Configuration* appendix to the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*.
- Authentication and Decryption
  In the *SoC Security* chapter of the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*

Software Image Authentication and Encryption

To provide the highest level of security during boot, you can apply both signing and encryption to a newly generated second-stage boot loader image. The image must be encrypted first, and then signed, so that the signature is available prior to decryption. During the boot process, the boot ROM firmware first attempts to authenticate the boot loader image. If authentication is successful, the device decrypts and loads the boot loader image.

You can use security settings in the boot loader generator to sign and encrypt a boot loader image.

Figure 12. Boot Image Signing and Encryption Flow



SoC EDS Tools for Secure Boot

The SoC EDS includes tools for creating a secured second-stage boot loader image.

Table 3. Secure Boot Tools

Tool	Name	Description
Boot loader generator	**bsp-editor**	Graphical second-stage boot loader generator
Secure boot image tool	**alt-secure-boot**	Command line tool for image signing or encrypting
Boot image format tool	**alt-image-cat**	Command line tool to format second-stage boot loader image

Related Links

- Intel SoC FPGA Embedded Design Suite User Guide
- Intel SoC FPGA Embedded Design Suite Release Notes

Boot Loader Generator

The boot loader generator, **bsp-editor**, is a graphical tool that performs the following functions:

- Create a new second-stage boot loader board support package (BSP)
- Edit an existing boot loader BSP
- Apply user-specified boot security settings to the boot loader
- Generate source files for the boot loader

For detailed usage of the boot loader generator, refer to "Boot Loader Generator Tool: BSP Editor" in the *Arria 10 SoC Boot User Guide* and to "Building the Arria 10 Bootloader" in the *Intel FPGA SoC Embedded Design Suite User Guide*.

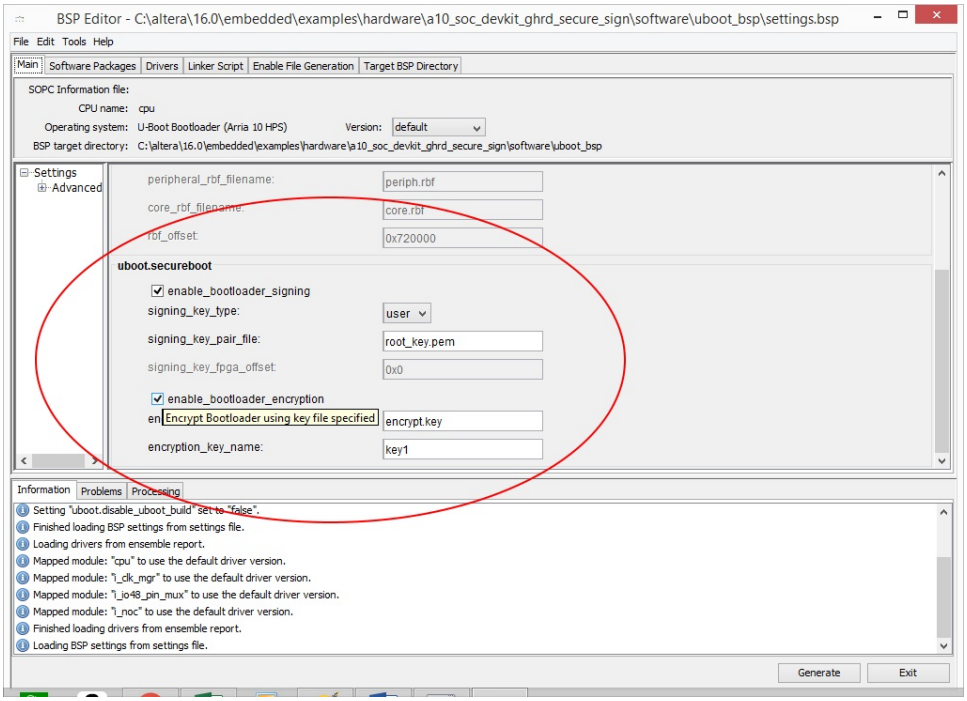
Related Links

- Boot Loader Generator Tool: BSP Editor
  in the Intel Arria 10 SoC Boot User Guide
- Intel SoC FPGA Embedded Design Suite User Guide
- Building the Arria 10 Bootloader
  In the *Intel SoC FPGA Embedded Design Suite User Guide*

Security Settings in the Boot Loader Generator

Figure 13. Security Settings

Boot loader generator security settings in the boot loader generator GUI



Boot loader generator authentication settings:

- **Enable Boot Loader Signing**—When this option is turned on, generate a signed second-stage boot loader
- **Signing Key Type**—Specifies where the boot ROM firmware should retrieve the signing keys from. Signing keys can be stored in one of the following locations:
  - User—Public key is stored boot loader image header

    Note: This is a non-secure configuration for testing only.
  - Fuse—Hash of public key is stored in user fuses
  - FPGA—Public key stored in FPGA memory.

  For more information about signing keys, refer to the "Signing Key Types" table in "Programming the Secure Signing Key".

- **Signing Key Pair File**—File name of signing key pair (generated by OpenSSL)
- **Signing Key FPGA Offset**—Location of public signing key, if stored in FPGA memory.

Boot loader generator encryption settings:

- **Enable Boot Loader Encryption**—When this option is turned on, generate an encrypted second-stage boot loader.
- **Encryption Key File**—Name of AES encryption key file.
- **Encryption Key Name**—AES encryption key name (specified in the key file)

Related Links

Programming the Secure Signing Key on page 13

Secure Boot Image Tool

The secure boot image tool, **alt-secure-boot**, applies the security settings to the second-stage boot loader image.

If the boot loader is to be authenticated, the secure boot image tool signs the boot loader image with the private key from the previously-generated key pair file. The boot loader generator invokes the tool with the `sign` option and associated parameters from the security settings, as follows:

```
$ alt-secure-boot sign [<param1> <param2> ...]
```

If the boot loader is to be encrypted, the secure boot image tool encrypts the boot loader image with the key from the previously-generated AES key file. The boot loader generator invokes the tool with the `encrypt` option and associated parameters from the security settings, as follows:

```
$ alt-secure-boot encrypt [<param1> <param2> ...]
```

Related Links

- Generating the Signing Key Pair with OpenSSL on page 14
- Encrypting the Boot Image and Configuration File on page 18
- Appendix A: SoC EDS Secure Boot Image Tool: alt-secure-boot on page 30
  Descriptions of all tools used in the secure boot system examples
- Intel SoC FPGA Embedded Design Suite User Guide

Boot Image Format Tool

When you are developing a secure boot loader, you use the boot image format tool to combine up to four boot images to be stored in flash or FPGA memory.

The Arria 10 SoC boot ROM firmware supports up to four boot loader images in flash or FPGA memory, as described in the *Arria 10 SoC Boot User Guide*. When you create a secure boot loader, you must perform an extra step to combine multiple boot loader image files into a single image file.

The SoC EDS includes the boot image format tool, **alt-image-cat**, to combine up to four boot loader images and concatenate them into a single image file. Because the resulting image might span multiple flash memory partitions, the boot image format tool ensures that the images are aligned properly to partition boundaries.

The boot image format tool formats the boot loader image after it is built. You invoke this tool from the SoC EDS embedded command shell as follows:

```
$ alt-image-cat <input_image> <input_image2> –o <output_image> –A <alignment size>
```

The input files are `.bin` or `.abin` files that are typically generated by the boot loader generator. The output file is also a `.bin` or `.abin` file.

Related Links

- Creating a Secure Boot System on page 15
- Intel SoC FPGA Embedded Design Suite User Guide

Secure Boot Examples

You can create a secure boot loader image for authentication, encryption, or both. "Creating a Signed Second-Stage Boot Loader Image" and "Creating an Encrypted Second-Stage Boot Loader Image" show examples of these processes.

Creating a Signed Second-Stage Boot Loader Image

The following example shows how to perform the following tasks:

1. Create a secure signing key for boot loader image authentication, with the user signing key type.
2. Generate and build a signed boot loader image with the secure signing key, using the SoC EDS.
3. Demonstrate secure boot using the signed boot loader image.

User signing key types are described in "Programming the Secure Signing Key".

1. Launch the boot loader generator from the embedded command shell with the following command

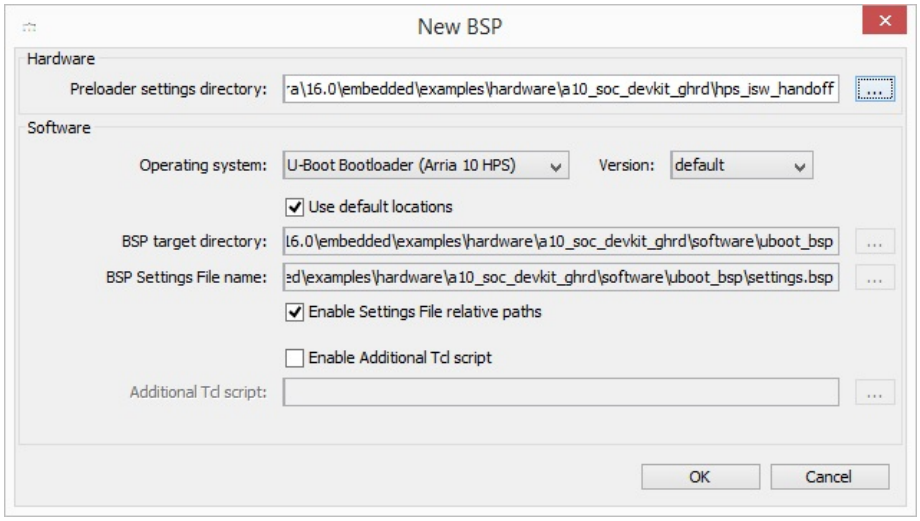
   ```
   $ bsp-editor &
   ```

   For general information about the boot loader generator, refer to "Second Stage Bootloader Support Package Generator" in the *Intel FPGA SoC Embedded Design Suite User Guide*.
2. Create a new boot loader BSP for the Intel Arria 10 HPS.

   For instructions to create a boot loader, refer to "BSP Generator Graphical User Interface" in the *Intel FPGA SoC Embedded Design Suite User Guide*.

Figure 14. Creating a New Second-Stage Boot Loader in the Boot Loader Generator

The boot loader generator dialog box



3. In the embedded command shell, change directories to the newly created boot loader folder (BSP target directory), for example:

```
$ cd <SoC EDS installation directory>/examples/hardware/ \
    a10_soc_devkit_ghrd_sb_auth/software/uboot_bsp
```

4. Type the following **make** command to generate a signing key pair stored in a key pair file.

```
$ make generate-signing-key-pair-file
```

5. Type the following OpenSSL command to show the contents of the key pair file and verify that it has been correctly created:

```
$ openssl ec –in root_key.pem –noout –text
```

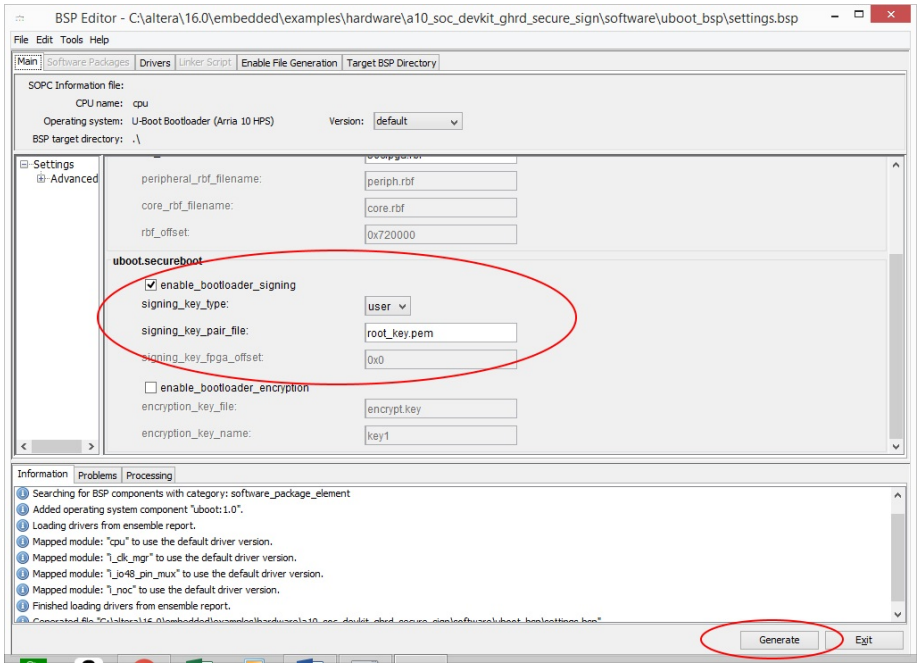
Note: The Generating the Signing Key Pair with OpenSSL on page 14 section describes this step in detail.

The key file contents should be similar to the following:

```
read EC key
Private-Key: (256 bit)
priv:
00:85:fa:a0:18:e8:97:72:fd:d4:19:07:c0:d8:09:
ae:e1:73:e8:80:fa:cf:35:bb:12:24:19:ec:7f:51:
56:34:f4
pub:
04:c1:a7:ba:ed:40:d6:0e:cc:08:97:c4:10:16:ac:
81:8b:33:73:ce:e2:d7:af:d6:78:ac:ea:48:f7:10:
b2:80:c4:c4:ef:de:d5:c5:03:76:c5:1c:62:04:72:
e7:1f:f7:32:aa:4c:a6:83:70:ae:b5:39:25:b1:e6:
51:0a:3a:74:ba
ASN1 OID: prime256v1
$
```

6. Apply security settings for authentication as shown in the following figure.

Figure 15. Security Settings in the Boot Loader Generator



- Turn on **enable_bootloader_signing** in the main boot loader generation settings.
- Set **signing_key_type** to **user**.
- Set **signing_key_pair_file** to the name of the file you created in the previous steps.

7. Click **Generate** to generate the secure boot loader source.
8. Exit the boot loader generator.
9. On the command line, navigate to the boot loader source folder.
10. Build the boot loader image with the **make** command:

```
$ make
```

11. Verify that the signed boot loader image was built by verifying that the following file exists:

    u-boot_w_dtb-mkpimage-encrypted-x4.abin

12. Store the signed boot loader image from 11 on page 26 in the appropriate flash boot device partition and reset the device.

Related Links

- Programming the Secure Signing Key on page 13
- Creating an Encrypted Second-Stage Boot Loader Image on page 27
- Second Stage Bootloader Support Package Generator
  Information about the boot loader generator in the *Intel SoC FPGA Embedded Design Suite User Guide*

- BSP Generator Graphical User Interface
  In the *Intel SoC FPGA Embedded Design Suite User Guide*: detailed information about creating a boot loader

Creating an Encrypted Second-Stage Boot Loader Image

The following example demonstrates how to perform the following tasks:

- Create an encryption key
- Generate and build an encrypted boot loader image using the SoC EDS
- Store the encryption key in the device's volatile key storage
- Demonstrate the secure boot using the encrypted boot image and encryption key

1. Launch the boot loader generator from the embedded command shell with the following command.

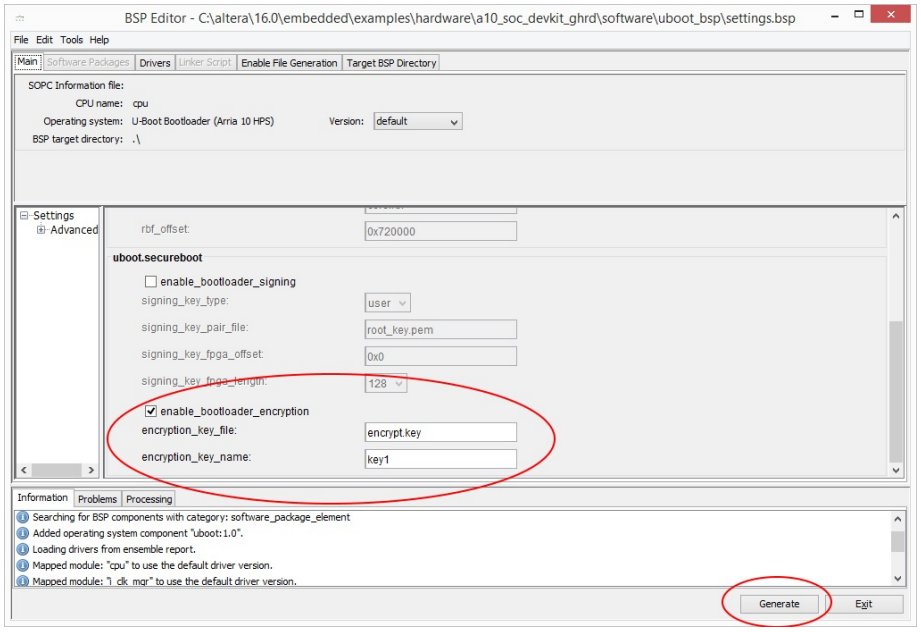
   ```
   $ bsp-editor &
   ```

   For general information about the boot loader generator, refer to "Second Stage Bootloader Support Package Generator" in the *Intel SoC FPGA Embedded Design Suite User Guide*.
2. Create a new boot loader BSP for the Arria 10 HPS.

   For instructions on how to create a boot loader, refer to "BSP Generator Graphical User Interface" in the *Intel SoC FPGA Embedded Design Suite User Guide*. Also refer to the "Creating a New Second-Stage Boot Loader in the Boot Loader Generator" figure in "Creating a Signed Second-Stage Boot Loader Image".
3. Create an AES encryption key file using the Quartus Prime Convert Programming File tool.

   For details, refer to "How to Generate the Single-Device .ekp File and Encrypt Configuration File Using Software with the Command-Line Interface" in AN-556: *Using the Design Security Features in Altera FPGAs*.
4. Apply security settings for encryption as shown in the following figure.

Figure 16. Creating an Encrypted Second-Stage Boot Loader Image in the Boot Loader Generator



- Turn on **enable_bootloader_encryption** in the main boot loader generation settings.
- Specify the name of the **encryption key file**.
- Specify the **encryption key name** (as found in the encryption key file).

5. Click **Generate** to generate the secure boot loader source.
6. Exit the boot loader generator.
7. On the command line, navigate to the boot loader source folder.
8. Build the boot loader image with the **make** command:

   ```
   $ make
   ```

9. Verify that the encrypted boot loader image was built by verifying that the following file exists:

   u-boot_w_dtb-mkpimage-encrypted-x4.abin

10. Store the AES encryption key in the device.

    For details, refer to "Steps for Implementing a Secure Configuration Flow" in AN-556: *Using the Design Security Features in Altera FPGAs*.

11. Save the encrypted boot loader image from 9 on page 28 in the appropriate flash boot device partition using the SD card boot utility.

    Note: Refer to the *SD Card Boot Utility* chapter of the *Intel SoC Embedded FPGA Design Suite User Guide*.

12. Generate the encrypted key programming file using the encrypted key file generated in 3 on page 27.

Usage:

```
quartus_cpf --key <encryption key file: key name> <design.sof> \
    <encryption key programming file>
```

Example:

```
$ quartus_cpf --key encrypt_key.key:key1 ghrd_10as066n2.sof encrypt_key.ekp
```

This example generates `encrypt_key.ekp`.

13. Make sure the updated SD card (11 on page 28) is inserted into the kit.

    Note: Do not power on the system in this step.

14. Connect the device to your development platform using the Intel FPGA Download Cable cable on the USB JTAG port, and power on the system.

    Note: The boot loader code will not execute at this time, because the encryption key has not been stored.

15. From the SoC EDS embedded command shell, verify that the device is connected, and obtain the JTAG interface IDs, by running one of the following commands:

    - `$ quartus_pgm -c USB-BlasterII –a`
    - `$ jtagconfig -N`

    If the device is successfully connected, either of the commands above displays the Intel FPGA Download Cable II device JTAG interface IDs and other information.

    Note: Important! For the remaining steps **DO NOT** power off the system.

16. Program the encryption key using the encryption programming key file from 12 on page 28.

    ```
    quartus_pgm -c USB-BlasterII -m jtag -o "p;encrypt_key.ekp;10AS066H2ES" \
        -o "s;SOCVHPS"
    ```

    Note: Refer to the device Intel FPGA Download Cable II interface IDs displayed in 15 on page 29.

    Note: **Do not** power off system until the key has been programmed.

17. After the key has been successfully programmed, the system will automatically reset and execute the encrypted boot image.

    Note: You must repeat 14 on page 29 each time the system has been power cycled.

Related Links

- Creating a Signed Second-Stage Boot Loader Image on page 24
  Boot loader generator dialog box
- BSP Generator Graphical User Interface
  In the *Intel SoC FPGA Embedded Design Suite User Guide*: detailed information about creating a boot loader
- How to Generate the Single-Device .ekp File and Encrypt Configuration File Using Quartus Prime Software with the Command-Line Interface
  In AN-556: *Using the Design Security Features in Altera FPGAs*
- Steps for Implementing a Secure Configuration Flow
  In AN-556: *Using the Design Security Features in Altera FPGAs*
- The *SD Card Boot Utility* chapter of the *Intel SoC FPGA Embedded Design Suite User Guide*

Appendix A: SoC EDS Secure Boot Image Tool: alt-secure-boot

Example 1. Secure Boot Image Tool Usage for Boot Image Authentication (Signing)

```
alt-secure-boot sign --help
usage:
  alt-secure-boot sign [-h] \
    --inputfile INPUTFILE --outputfile OUTPUTFILE \
    [--fuseout FUSEOUT] [--pubkeyout PUBKEYOUT] \
    [--rootkey-type {fuse,fpga,user}] \
    [--keypair KEYPAIR] \
    [--fpga-key-offset FPGA_KEY_OFFSET]

Sign a bootloader image to allow BootROM verification

optional arguments:
  -h, --help            show this help message and exit
  --inputfile INPUTFILE, -i INPUTFILE
                        Bootloader image to sign
  --outputfile OUTPUTFILE, -o OUTPUTFILE
                        Signed output image
  --fuseout FUSEOUT, -fo FUSEOUT
                        Hash of root public key, to be burned into device
                        fuses
  --pubkeyout PUBKEYOUT, -pko PUBKEYOUT
                        Root public key in raw data form. This data may then
                        be built into the FPGA image for usage with
                        --rootkey-type=fpga
  --rootkey-type {fuse,fpga,user}, -t {fuse,fpga,user}
                        The trusted root key's type. (default: fuse) 'fuse':
                        embed root pubkey in image. BootROM verifies its hash
                        against device fuses. 'fpga': fetch trusted root
                        pubkey from location in FPGA memory. 'user': embed
                        root pubkey in image. BootROM does not verify.
  --keypair KEYPAIR, -k KEYPAIR
                        Signature keypairs specified in order from the
                        trusted root key to final user key
  --fpga-key-offset FPGA_KEY_OFFSET
                        Offset from H2F bridge base address (0xC0000000) to
                        location of logic-embedded root public key. Used for
                        '--rootkey-type fpga' authentication.
```

Example 2. Secure Boot Image Tool Usage for Boot Image Encryption

```
alt-secure-boot encrypt --help
usage:
  alt-secure-boot encrypt [-h] \
    --inputfile INPUTFILE --outputfile OUTPUTFILE \
    --key KEY [--non-volatile]

Convert a pimage into an encrypted boot image

optional arguments:
  -h, --help            show this help message and exit
  --inputfile INPUTFILE, -i INPUTFILE
                        Bootloader image to encrypt
  --outputfile OUTPUTFILE, -o OUTPUTFILE
                        Encrypted output image
  --key KEY, -k KEY     File containing symmetric key to use for encryption
  --non-volatile        Decryption key stored in non-volatile fuses, instead
                        of battery-backed storage
```

Appendix B: Frequently Asked Questions

Table 4. Frequently Asked Questions (FAQs) Summary Table

Topic
What are the secure configurations for HPS JTAG debug and access? How are these affected during warm or cold reset? on page 32
Can the HPS perform decryption of the boot image instead of the FPGA CSS? on page 32
What happens if the first stage boot ROM is unsuccessful in authenticating the second-stage boot loader? on page 32
Can you use the first-stage root key as the subsequent stage root key? on page 32
When the second-stage image is authenticated, is the image header only copied to on-chip RAM for authentication? on page 33
Can the AES encryption key be updated by the HPS using JTAG hosting? on page 33
How does U-Boot (SSBL) authenticate next stage boot images? on page 33
Which elliptical cryptography is used for boot image signing and authentication? on page 33
How do I generate a signing key pair? on page 33
Where can I store the signing keys for second-stage boot loader authentication? on page 33
What type of cryptography is used for boot image encryption and decryption? on page 34
What FPGA locations are available for AES key storage? on page 34
How do I generate an AES key to encrypt a boot image? on page 34
How is secure boot defined within the Intel Arria 10 SoC product family? on page 35
What security choices are available for the second-stage boot image or user software? on page 35
Where is the authentication of the boot image performed? on page 35
How can I configure the Arria 10 SoC device so that it always performs authentication or authentication and decryption? on page 35
How can I program the key authentication key (KAK) into the Arria 10 SoC device? on page 36
How can I configure the second stage boot loader image for the correct authentication signing key type? on page 36
How do I configure the second-stage boot loader image for encryption using the pre-generated AES key? on page 36
Is the ECDSA private and public key pair that is used for signing the boot image also used for authentication of the FPGA image? on page 36

What are the secure configurations for HPS JTAG debug and access? How are these affected during warm or cold reset?

Two efuse bits, dbg_disable_access and dbg_lock_JTAG, control the secure JTAG debug configurations. You can read the programmed efuse values for your device through the HPS_fusesec register. A bit value of 1 in the HPS_fusesec register represents a "blown" fuse state and a 0 represents an "unblown" fuse state.

The table below describes the possible HPS configurations with JTAG. The dbg_access_f and dbg_lock_JTAG columns reflect the efuse value of these bits in the HPS_fusesec register. If both efuse are unblown then after the device exits reset, full JTAG access is possible. This configuration is the default configuration.

Table 5. JTAG Security Configuration Options

JTAG Configuration	dbg_disable_access	dbg_lock_JTAG	Description
HPS JTAG include	0	1	• This configuration includes the HPS in the JTAG chain by default. • Your software application cannot remove the HPS from the JTAG chain. • This configuration allows HPS debug from power-on reset.
HPS JTAG exclude	1	1	Permanently exclude the HPS from the JTAG chain.
Default	0	0	Enable JTAG with software debug programmability.

Can the HPS perform decryption of the boot image instead of the FPGA CSS?

The HPS portion of the SoC does not support AES operations. It can only perform public key-based authentication. The HPS can, however, push the boot image into the FPGA CSS and perform the same decryption used in the FPGA configuration flow.

When decryption is complete, the CSS returns the image to the HPS and the HPS uses that image as the boot image. The HPS and FPGA share the same AES root key which is stored in efuse. The CSS uses a simple key derivation function, AES (efuse or BBRAM key, #constant) for the HPS and FPGA configuration images.

What happens if the first stage boot ROM is unsuccessful in authenticating the second-stage boot loader?

The first stage boot ROM attempts to authenticate all four second stage images that are stored in the boot partitions of your flash device. If the device cannot authenticate the images or identifies the images as corrupt, then the boot ROM attempts to execute a fall back image located in the on-chip RAM of the FPGA.

Can you use the first-stage root key as the subsequent stage root key?

Intel recommends using a separate final signing key between different boot stages. Intel does not recommend using a root key for the first-stage or subsequent stage boot loader direct signing. Sharing the same root key between the first-stage and subsequent stage boot loader is only successful if you use the same ECC algorithm for each.

When the second-stage image is authenticated, is the image header only copied to on-chip RAM for authentication?

The entire boot loader image is always copied into the on-chip RAM and authenticated.

Can the AES encryption key be updated by the HPS using JTAG hosting?

You can only update the AES key in volatile memory through a connected JTAG interface. The HPS does not support JTAG hosting.

How does U-Boot (SSBL) authenticate next stage boot images?

The current GSRD U-Boot does not feature image authentication beyond the second stage bootloader (U-Boot). You can enable U-Boot to authenticate subsequent boot images (Linux*) by configuring or adding authentication capability to U-Boot. Reference the latest U-Boot releases for support on authentication. The user may also want to add specific third-party or open source solutions.

Which elliptical cryptography is used for boot image signing and authentication?

The Intel Arria 10 SoC device family uses the elliptical curve digital signing algorithm with NIST-approved ECDSA on NIST P-256 curve for signing and authentication of second-stage boot images.

How do I generate a signing key pair?

You may use the open source OpenSSL toolkit or your own tool to generate a key pair file that contains a private and public key pair. The SoC EDS boot tool requires a key pair file for signing an image. If you decide to use OpenSSL, you may refer to the OpenSSL website for more information about how to use the tool.

Related Links

www.openssl.org
Detailed help and information for the OpenSSL toolkit is available on the OpenSSL website.

Where can I store the signing keys for second-stage boot loader authentication?

You can store the signing keys for second-stage boot loader authentication by the Intel Arria 10 SoC device in:

Table 6. Root Key Types

Root Key	Key Type	Description
Secure User Key	Fuse	User generates secure key pair for boot ROM to attempt authentication. The SHA256 hash of the public key is stored in the User Access Fuses (UAF) of the device. This configuration provides a secure boot.

continued...

Root Key	Key Type	Description
		For information about secure fuses, refer to the *Secure Fuses* section in the SoC Security chapter of the *Intel Arria 10 Hard Processor System Technical Reference Manual*.
FPGA Key	FPGA	The public key originates from the user bitstream. The key is stored in FPGA on-chip RAM and accessed by the first stage boot ROM for image authentication.
Unsecured User Key	User	User generates a secure key pair but it is not stored on the device. This configuration is unsecure and is for testing only. The user includes the root key result in the image header and the boot ROM uses it for authentication.

Related Links

Secure Fuses
For basic information about security fuses, refer to "Secure Fuses" in the *SoC Security* chapter of the *Intel Arria 10 SoC FPGA Hard Processor System Technical Reference Manual*.

What type of cryptography is used for boot image encryption and decryption?

The Intel Arria 10 SoC device family supports secure boot using the Advanced Encryption Standard (AES) encryption with a 256-bit key length. You can encrypt your boot image using quartus_cpf tools. The Arria 10 SoC AES engine only supports decryption.

What FPGA locations are available for AES key storage?

Within the FPGA, you can store the public (root) key in key registers located in:

- User fuses (non-volatile memory)
- Battery-backed RAM (volatile memory) within the FPGA

The contents of the volatile key registers are retained between power-cycles with battery power. Non-volatile key registers are fuse-based and are one-time programmable.

How do I generate an AES key to encrypt a boot image?

The AES key file (.key) is a text file that you generate using a true random number generator (TRNG) or some other trusted tool. Refer to *AN-556: Using the Design Security Features in Altera FPGAs* for the content format of this file.

Related Links

- Encrypting the Boot Image and Configuration File on page 18
  For more information about using quartus_cpf to store keys
- AN-556: Using the Design Security Features in Altera FPGAs
  For content format of the AES key file

How is secure boot defined within the Intel Arria 10 SoC product family?

Within the Intel Arria 10 SoC device family, a secure boot implies that before the system loads any user (non-device modifiable) software, such as a second-stage boot loader image, it:

- Checks the image for authenticity
- Decrypts any encrypted image before signing it as certified

What security choices are available for the second-stage boot image or user software?

Authentication is provided for the second-stage boot loader code and both the HPS and FPGA can utilize the AES algorithms in the Configuration Subsystem (CSS) to decrypt boot images and POF files, respectively.

Three levels of boot are available to the device:

- Authentication only: The second-stage boot loader code is not encrypted, but there are public key signatures attached to the image and the code only executes if all of the signatures pass. ECDSA256 (SHA 256) is used for authenticated boot.
- Decryption only: The user boot code is encrypted and must be decrypted before execution. AES-based algorithms in the FPGA are used for decryption.
- Authentication and Decryption: The user boot code is encrypted and signed.

If authentication and decryption are enabled, the data is first authenticated and then decrypted using the AES algorithms. Authentication is performed using the public key authorization key (KAK) held in the user fuses. The KAK can be 256 bits. The KAK public key authentication fuses are lockable by the user in groups of 64 bits or less.

Where is the authentication of the boot image performed?

The HPS boot ROM authenticates the boot image in the SoC. The FPGA does not perform this authentication.

Where is decryption of the boot image performed?

If the boot ROM detects that the boot image is encrypted, it sends the image to the CSS for the AES to perform decryption.

How can I configure the Arria 10 SoC device so that it always performs authentication or authentication and decryption?

You can ensure that the Intel Arria 10 SoC device always performs a signed authentication check or an authentication check with runtime decryption by programming the device fuses for these features and by using the required security keys. Specifically, you must:

- Program the aes_en_f fuse so that an AES decryption of a flash image is always performed.
- Program the kak_src_f fuse to indicate where the key authorization key (KAK) resides
- Program the kak_len_f fuse to configure the length of the KAK
- Program the authen_en_f fuse so that HPS authentication is required for all flash images prior to execution
- Program the security authorization key in the location you have selected

How can I program the key authentication key (KAK) into the Arria 10 SoC device?

You can program the KAK into the device fuses permanently using the Intel FPGA Download Cable and the programmer tool installed with the Design Tool Suite.

How can I configure the second stage boot loader image for the correct authentication signing key type?

You must select the appropriate security settings for authentication before generating the second-stage boot loader in the SoC EDS bsp-editor. After the settings are applied, you build the boot loader and the configurations are incorporated in the image. After these steps, you must build and sign the boot loader.

If you use the SoC EDS bsp-editor tool to generate the boot loader source, then you must build the image and then use **alt-secure-boot tool** to sign the final image.

How do I configure the second-stage boot loader image for encryption using the pre-generated AES key?

If you require a signed and encrypted second-stage boot loader image for authentication and decryption, then the image is encrypted prior to signing. Otherwise the image is encrypted after the source is generated and the image is built. You encrypt the final image using the SoC EDS secure boot tool, **alt-secure-boot tool**. You must select the appropriate security settings for encryption before generating the second-stage boot loader in the **alt-secure-boot tool**. After the settings are applied, you must build the boot loader image to include the configuration.

Is the ECDSA private and public key pair that is used for signing the boot image also used for authentication of the FPGA image?

The ECDSA signing key pair is only used for signing of the second-stage boot image. The FPGA does not support public key-based authentication.

Revision History

Date	Version	Changes
November 2017	2017.11.06	• Updated "Secure Boot Stages" figure in Secure Boot Stages on page 6 to include more stage details • Added Third and Fourth Stages on page 7 subsection to the Secure Boot Stages topic. • Clarified authentication process in *Software Image Authentication* section and added the subsections: — Digital Signing on page 8 — Root of Trust and Root Key on page 9 — Authentication of the Second-Stage Boot Loader on page 9 — Security Level Staging on page 10 — Signed Image on page 11 — Root Key Types on page 12 — Root Public Key Authentication on page 12 • Added Appendix B: Frequently Asked Questions on page 31
March 2016	2016.03.29	Initial release