



STM32MP15 secure boot



Contents

1. STM32MP15 secure boot	9
2. Boot chains overview	9
3. STM32MP15 microprocessor	9
4. KeyGen tool	16
5. STM32MP15 ROM code overview	16
6. BSEC internal peripheral	16
7. U-Boot overview	16
8. Signing tool	17
9. STM32CubeProgrammer	17
10. STM32CubeProgrammer release note	17

STM32MP15 secure boot

Stable: 13.05.2020 - 10:33 / Revision: 13.05.2020 - 10:30

Template:ArticleMainWriter Template:ArticleApprovedVersion

Contents

1 Purpose	10
2 Authentication processing	10
2.1 Key generation	11
2.2 Key registration	11
2.2.1 Register hash public key	11
2.3 Image signing	12
2.3.1 STM32 Header	12
2.4 Image programming	14
2.5 PKH check	15
2.6 Authentication	15
2.6.1 Bootrom authentication	15
2.6.2 TF-A authentication	15
2.7 Closing the device	15

1 Purpose

Secure boot is a key feature to guarantee a secure platform.

STM32MP1 boot sequence supports a trusted boot chain that ensures that the loaded images are authenticated and checked in integrity before being used.



The secure boot feature availability is indicated in the *security* field of the chip part number.

2 Authentication processing

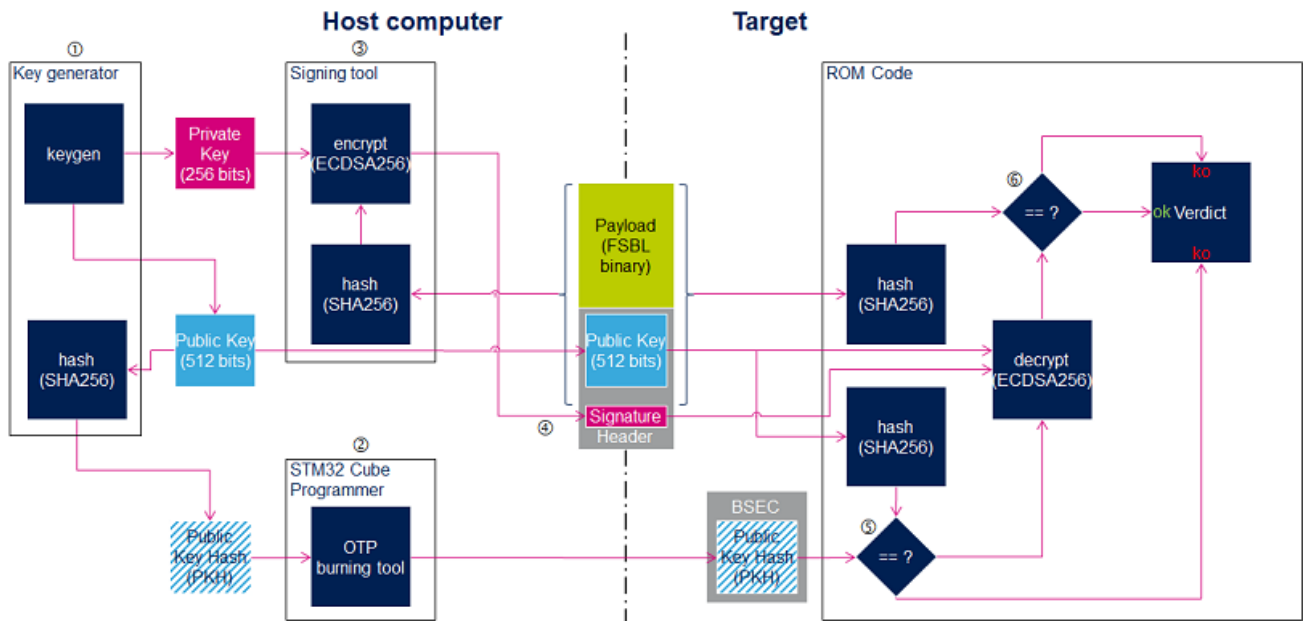
STM32 MPU provides authentication processing with ECDSA ^[1] verification algorithm, based on ECC ^[2]. ECDSA offers better result than RSA with a smaller key. STM32 MPU relies on a 256 bits ECDSA key.

Two algorithms are supported for ECDSA calculation:

- P-256 NIST
- Brainpool 256

The algorithm selection is done via the signed binary header, as shown in [STM32 header](#) (subchapter in this same article).

The EDCSA verification follows the process below:



2.1 Key generation

First step is to generate the ECC pair of keys with STM32 KeyGen tool. This is the key pair that will be used to sign the images.

The tool also generates a third file containing the public key hash (PKH) that will be used to authenticate the public key on the target.

2.2 Key registration



Make sure that a device with Secure boot enabled is used: this is mentioned in the part number, otherwise the device will become permanently unusable.

2.2.1 Register hash public key

First step to enable the authentication is to burn the OTP WORD 24 to 31 in BSEC with the corresponding public key hash (PKH, output file from STM32 KeyGen). OpenSTLinux embeds a **stm32key** tool that can be called from U-Boot command line interface to program the PKH into the OTP.

PKH file (publicKeyhash.bin) must be available in a filesystem partition (like bootfs) on a storage device (like sdcard) before proceeding.

```
Board $> ext4load mmc 0:4 0xc0000000 publicKeyhash.bin
file from mmc 0 partition 4 (ext4) in DDR
32 bytes read in 50 ms (0 Bytes/s)
```

Load hash

```
Board $> stm32key read 0xc0000000
key from DDR to confirm it is valid (without writing it in OTP)
OTP value 24: 12345678
OTP value 25: 12345678
OTP value 26: 12345678
```

Read loaded



```
OTP value 27: 12345678
OTP value 28: 12345678
OTP value 29: 12345678
OTP value 30: 12345678
OTP value 31: 12345678
```



If hash key is ok, the key in OTP can be fused

```
Board $> stm32key fuse -y 0xc0000000
in OTP
```

Write the key

The device now contains the hash to authenticate images.

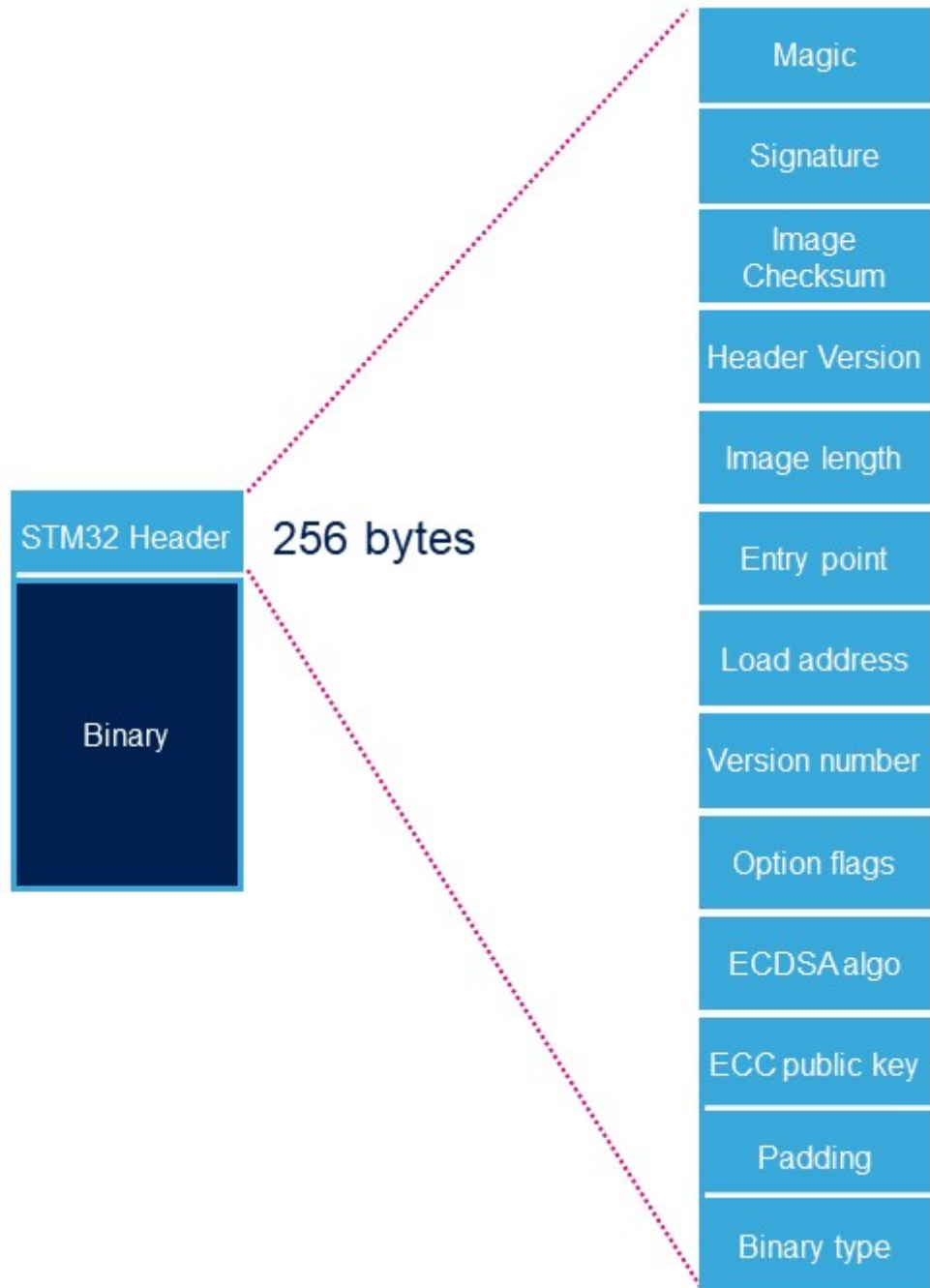
2.3 Image signing

In a second step, FSBL and SSBL binaries must be signed. [STM32 Signing tool](#) allows to fill the STM32 binary header that is parsed by the embedded software to authenticate each binary.

2.3.1 STM32 Header

Each signed binary image includes a specific STM32 header added on top of the binary data.

The header includes the



authentication information.

Name	Length	Byte Offset	Description
Magic number	32 bits	0	'S' ; 'T' ; 'M' ; 0x32
Image Signature	512 bits	4	ECDSA signature for image authentication ¹
Image Checksum	32 bits	68	Checksum of the payload ²



Name	Length	Byte Offset	Description
Header version	32 bits	72	Header version v1.0 = 0x00010000 Byte0: reserved Byte1: major version = 0x01 Byte2: minor version = 0x00 Byte3: reserved
Image Length	32 bits	76	Length of image in bytes ³
Image Entry Point	32 bits	80	Entry point of image
Reserved1	32 bits	84	Reserved
Load address	32 bits	88	Load address of image ⁴
Reserved2	32 bits	92	Reserved
Version Number	32 bits	96	Image Version (monotonic number) ⁵
Option flags	32 bits	100	b0=1: no signature verification ⁶
ECDSA Algorithm	32 bits	104	1: P-256 NIST ; 2: brainpool 256
ECDSA Public key	512 bits	108	ECDSA public key to be used to verify the signature. ⁷
Padding	84 Bytes	172	Reserved padding bytes ⁸ . Must all be set to 0
BinaryType	1 Byte	255	Used to check the binary type 0x00: U-Boot 0x10-0x1F: TF-A 0x20-0x2F: OPTEE 0x30: Copro

¹ Signature is calculated from first byte of header version field to last byte of image given by image length field.

² 32-bit sum of all payload bytes accessed as 8-bit unsigned numbers, discarding any overflow bits. Used to check the downloaded image integrity when signature is not used (if b0=1 in Option flags).

³ Length is the length of the built image, it does not include the length of the STM32 header.

⁴ This field is used by ROM code for specific executable images.

⁵ Image version is an anti rollback monotonic counter. The ROM code checks that it is higher or equal to the [monotonic counter stored in OTP](#).

⁶ Enabling signature verification is mandatory on [secure closed chips](#).

⁷ Hash of (algorithm+pubKey) is stored in [OTP WORD 24 to 31](#).

⁸ This padding forces Header size to 0x100 bytes.

2.4 Image programming

Once the images are signed, they can be programmed into the flash on the target board with [STM32CubeProgrammer](#).

2.5 PKH check

Before really starting the authentication process, the ROM code compares the hash of the public key carried in the STM32 header with the one that was provisionned in OTP.

2.6 Authentication

2.6.1 Bootrom authentication

Using a **signed** binary, the ROM code authenticates and starts the FSBL.

If the authentication fails, the ROM code enters into a serial boot loop indicated by the blinking Error LED (cf [Bootrom common debug and error cases](#))

The ROM code provides secure services to the FSBL for image authentication with the same ECC pair of keys, so there is no need to support ECDSA algorithm in FSBL.

2.6.2 TF-A authentication

TF-A is the FSBL used by the Trusted boot chain. It is in charge of loading and verifying U-boot and (if used) OP-TEE image binaries.

Each time a **signed** binary is used, TF-A will print the following status:

```
INFO:    Check signature on Non-Full-Secured platform
```

If the image authentication fails the boot stage traps the CPU and no more trace is displayed.

2.7 Closing the device

Notice that this last step is not shown in the diagram above.

Without any other modification, the device is able to perform image authentication but non authenticated images can still be used and executed: the device is still opened, let's see this as a kind of test mode to check that the PKH is properly set.

As soon as the authentication process is confirmed, the device can be closed and the user forced to use signed images.

OTP WORD0 bit 6 is the OTP bit that closes the device. Burning this bit will lock authentication processing and force authentication from the Boot ROM. Non signed binaries will not be supported anymore on the target.

To program this bit, the STM32CubeProgrammer or U-Boot command line interface can be used.

Here is how to proceed with U-Boot:

```
Board $> fuse prog 0 0x0 0x40
```



Once this bit is written the platform is locked

- https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm



- https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Microprocessor Unit
 Elliptic Curve Digital Signature Algorithm
 Elliptic curve cryptography
 Error Correction Capability
 One Time Programmed
 Doubledata rate (memory domain)
 First Stage Boot Loader
 Second Stage Boot Loader
 Das U-Boot -- the Universal Boot Loader (see [U-Boot_overview](#))
 Trusted Firmware for Arm Cortex-A
 Read Only Memory
 Light-emitting diode
 Open Portable Trusted Execution Environment
 Central processing unit

Permission error

Stable: 25.06.2020 - 07:35 / Revision: 19.06.2020 - 07:24

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 21.02.2020 - 08:35 / Revision: 12.02.2020 - 11:01

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

STM32MP15 secure boot

Stable: 13.05.2020 - 10:33 / Revision: 13.05.2020 - 10:30

Template:ArticleMainWriter Template:ArticleApprovedVersion

Contents

1 Purpose	10
2 Authentication processing	10
2.1 Key generation	11

2.2 Key registration	11
2.2.1 Register hash public key	11
2.3 Image signing	12
2.3.1 STM32 Header	12
2.4 Image programming	14
2.5 PKH check	15
2.6 Authentication	15
2.6.1 Bootrom authentication	15
2.6.2 TF-A authentication	15
2.7 Closing the device	15

1 Purpose

Secure boot is a key feature to guarantee a secure platform.

STM32MP1 boot sequence supports a trusted boot chain that ensures that the loaded images are authenticated and checked in integrity before being used.



The secure boot feature availability is indicated in the *security* field of the chip part number.

2 Authentication processing

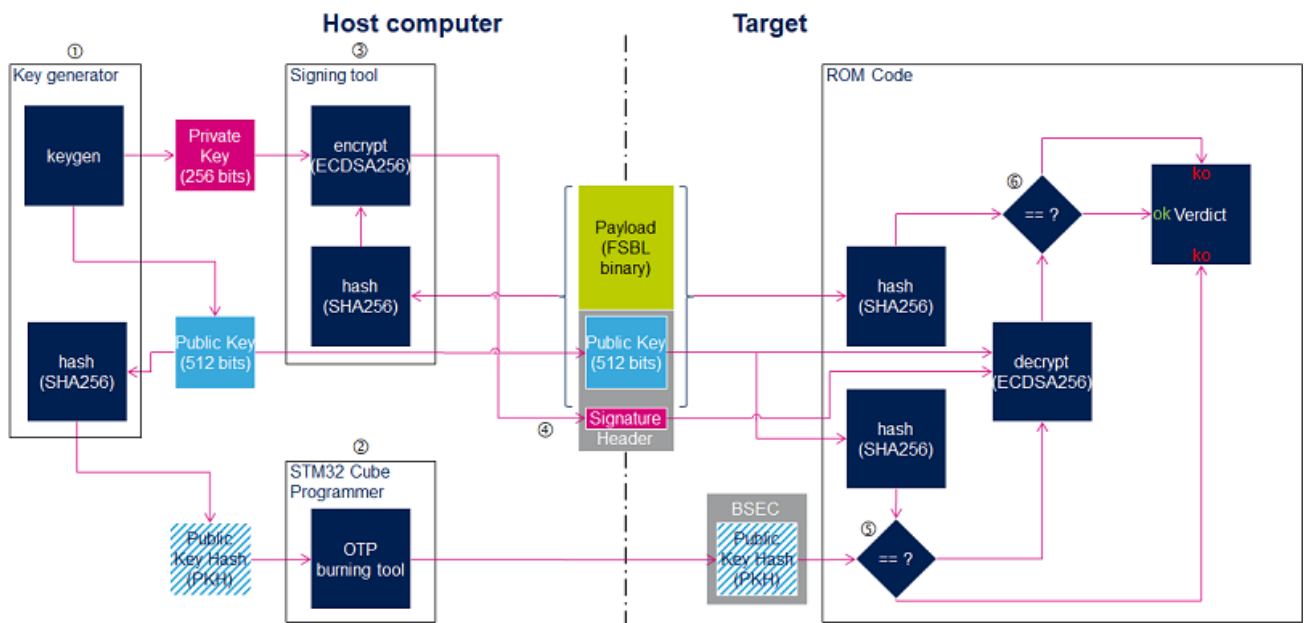
STM32 MPU provides authentication processing with ECDSA ^[1] verification algorithm, based on ECC ^[2]. ECDSA offers better result than RSA with a smaller key. STM32 MPU relies on a 256 bits ECDSA key.

Two algorithms are supported for ECDSA calculation:

- P-256 NIST
- Brainpool 256

The algorithm selection is done via the signed binary header, as shown in [STM32 header](#) (subchapter in this same article).

The ECDSA verification follows the process below:



2.1 Key generation

First step is to generate the ECC pair of keys with STM32 KeyGen tool. This is the key pair that will be used to sign the images.

The tool also generates a third file containing the public key hash (PKH) that will be used to authenticate the public key on the target.

2.2 Key registration



Make sure that a device with Secure boot enabled is used: this is mentioned in the part number, otherwise the device will become permanently unusable.

2.2.1 Register hash public key

First step to enable the authentication is to burn the OTP WORD 24 to 31 in BSEC with the corresponding public key hash (PKH, output file from STM32 KeyGen). OpenSTLinux embeds a **stm32key** tool that can be called from U-Boot command line interface to program the PKH into the OTP.

PKH file (publicKeyhash.bin) must be available in a filesystem partition (like bootfs) on a storage device (like sdcard) before proceeding.

```
Board $> ext4load mmc 0:4 0xc0000000 publicKeyhash.bin
file from mmc 0 partition 4 (ext4) in DDR
32 bytes read in 50 ms (0 Bytes/s)
```

Load hash

```
Board $> stm32key read 0xc0000000
key from DDR to confirm it is valid (without writing it in OTP)
OTP value 24: 12345678
OTP value 25: 12345678
OTP value 26: 12345678
```

Read loaded



```
OTP value 27: 12345678
OTP value 28: 12345678
OTP value 29: 12345678
OTP value 30: 12345678
OTP value 31: 12345678
```



If hash key is ok, the key in OTP can be fused

```
Board $> stm32key fuse -y 0xc0000000
in OTP
```

Write the key

The device now contains the hash to authenticate images.

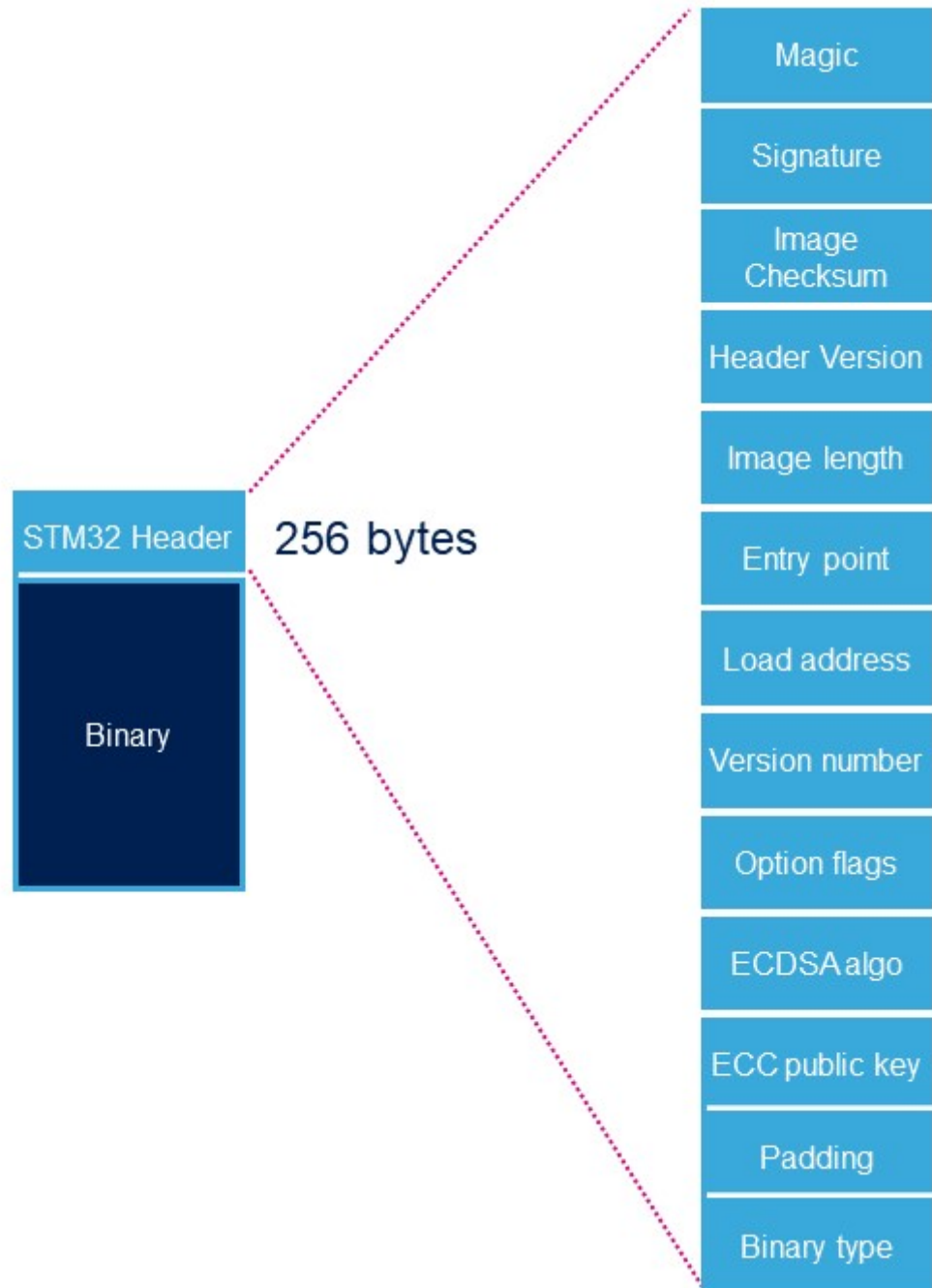
2.3 Image signing

In a second step, FSBL and SSBL binaries must be signed. [STM32 Signing tool](#) allows to fill the STM32 binary header that is parsed by the embedded software to authenticate each binary.

2.3.1 STM32 Header

Each signed binary image includes a specific STM32 header added on top of the binary data.

The header includes the



authentication information.

Name	Length	Byte Offset	Description
Magic number	32 bits	0	'S' ; 'T' ; 'M' ; 0x32
Image Signature	512 bits	4	ECDSA signature for image authentication ¹
Image Checksum	32 bits	68	Checksum of the payload ²



Name	Length	Byte Offset	Description
Header version	32 bits	72	Header version v1.0 = 0x00010000 Byte0: reserved Byte1: major version = 0x01 Byte2: minor version = 0x00 Byte3: reserved
Image Length	32 bits	76	Length of image in bytes ³
Image Entry Point	32 bits	80	Entry point of image
Reserved1	32 bits	84	Reserved
Load address	32 bits	88	Load address of image ⁴
Reserved2	32 bits	92	Reserved
Version Number	32 bits	96	Image Version (monotonic number) ⁵
Option flags	32 bits	100	b0=1: no signature verification ⁶
ECDSA Algorithm	32 bits	104	1: P-256 NIST ; 2: brainpool 256
ECDSA Public key	512 bits	108	ECDSA public key to be used to verify the signature. ⁷
Padding	84 Bytes	172	Reserved padding bytes ⁸ . Must all be set to 0
BinaryType	1 Byte	255	Used to check the binary type 0x00: U-Boot 0x10-0x1F: TF-A 0x20-0x2F: OPTEE 0x30: Copro

¹ Signature is calculated from first byte of header version field to last byte of image given by image length field.

² 32-bit sum of all payload bytes accessed as 8-bit unsigned numbers, discarding any overflow bits. Used to check the downloaded image integrity when signature is not used (if b0=1 in Option flags).

³ Length is the length of the built image, it does not include the length of the STM32 header.

⁴ This field is used by ROM code for specific executable images.

⁵ Image version is an anti rollback monotonic counter. The ROM code checks that it is higher or equal to the [monotonic counter stored in OTP](#).

⁶ Enabling signature verification is mandatory on [secure closed chips](#).

⁷ Hash of (algorithm+pubKey) is stored in [OTP WORD 24 to 31](#).

⁸ This padding forces Header size to 0x100 bytes.

2.4 Image programming

Once the images are signed, they can be programmed into the flash on the target board with [STM32CubeProgrammer](#).

2.5 PKH check

Before really starting the authentication process, the ROM code compares the hash of the public key carried in the STM32 header with the one that was provisionned in OTP.

2.6 Authentication

2.6.1 Bootrom authentication

Using a **signed** binary, the ROM code authenticates and starts the FSBL.

If the authentication fails, the ROM code enters into a serial boot loop indicated by the blinking Error LED (cf [Bootrom common debug and error cases](#))

The ROM code provides secure services to the FSBL for image authentication with the same ECC pair of keys, so there is no need to support ECDSA algorithm in FSBL.

2.6.2 TF-A authentication

TF-A is the FSBL used by the Trusted boot chain. It is in charge of loading and verifying U-boot and (if used) OP-TEE image binaries.

Each time a **signed** binary is used, TF-A will print the following status:

```
INFO:    Check signature on Non-Full-Secured platform
```

If the image authentication fails the boot stage traps the CPU and no more trace is displayed.

2.7 Closing the device

Notice that this last step is not shown in the diagram above.

Without any other modification, the device is able to perform image authentication but non authenticated images can still be used and executed: the device is still opened, let's see this as a kind of test mode to check that the PKH is properly set.

As soon as the authentication process is confirmed, the device can be closed and the user forced to use signed images.

OTP WORD0 bit 6 is the OTP bit that closes the device. Burning this bit will lock authentication processing and force authentication from the Boot ROM. Non signed binaries will not be supported anymore on the target.

To program this bit, the STM32CubeProgrammer or U-Boot command line interface can be used.

Here is how to proceed with U-Boot:

```
Board $> fuse prog 0 0x0 0x40
```



Once this bit is written the platform is locked

- https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm



- https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Microprocessor Unit

Elliptic Curve Digital Signature Algorithm

Elliptic curve cryptography

Error Correction Capability

One Time Programmed

Doubledata rate (memory domain)

First Stage Boot Loader

Second Stage Boot Loader

Das U-Boot -- the Universal Boot Loader (see [U-Boot_overview](#))

Trusted Firmware for Arm Cortex-A

Read Only Memory

Light-emitting diode

Open Portable Trusted Execution Environment

Central processing unit

Permission error

Stable: 19.02.2019 - 16:57 / Revision: 18.02.2019 - 13:40

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 25.06.2020 - 09:47 / Revision: 25.06.2020 - 09:45

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 24.09.2019 - 14:06 / Revision: 24.09.2019 - 07:57

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer



Permission error

Stable: 25.05.2020 - 07:32 / Revision: 25.05.2020 - 07:25

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 19.02.2019 - 18:29 / Revision: 18.02.2019 - 14:35

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 21.02.2020 - 10:10 / Revision: 20.02.2020 - 10:16

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 21.02.2020 - 13:31 / Revision: 12.02.2020 - 08:10

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer