KeyGen tool

KeyGen tool

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

Template:ArticleMainWriter Template:ArticleApprovedVersion

STM32 KeyGen is a tool that generates the ECC key pairs needed for signing binary images. The generated keys will be used by Signing tool for signing process.

Contents

1 KeyGen Overview 2
2 Install STM32MP Key Generator 2
2.1 Linux Install 3
2.2 Windows install 3
3 STM32MP Key Generator command line interface 3
3.1 Command line options 3
3.2 Examples 4
3.2.1 Example 1: Key creation using the AES256 algorithm 4
3.2.2 Example 2: Key creation using the AES128 algorithm 4
3.2.3 Example 3: Key creation when one or both the destination folders are missing 5
3.3 Standalone mode 5

1 KeyGen Overview

The STM32MP Key Generator software generates three files:

- Public Key file:

Contains the generated ECC public key in PEM format.

- Private Key file:

Contains the encrypted ECC private key in PEM format. The encryption could be done using the AES128CBC or AES256CBC ciphers. The cipher selection is done using the --prvkey-enc option.

- Hash public key file:

Contains the SHA-256 hash of the public key in binary format.The SHA-256 hash is calculated based on the public key without any encoding format. The first byte of the public key is used to indicate whether the public key is in compressed or uncompressed format. Since only uncompressed format is supported, this byte is removed

2 Install STM32MP Key Generator

This section describes the requirements and procedure to use the STM32MP Key Generator software.

2.1 Linux Install

The STM32MP Key Generator software is tested on Ubuntu 14.04 and 16.04 32-bit and 64-bit and should work on any distribution.

To install the STM32MP Key Generator tool, you need to install the STM32CubeProgrammer. To run it, you will need to launch the ./STM32AP_KeyGen_CLI.sh script.

2.2 Windows install

To install the STM32MP Key Generator tool for windows, you need to install the STM32CubeProgrammer. To run it, launch the STM32AP_KeyGen_CLI.exe executable

3 STM32MP Key Generator command line interface

The following section describes how to use the STM32MP Key Generator from command line

3.1 Command line options

The generation process can be tailored by the requester. The available options are:

- --private-key (-prvk)

Description: Private key file path (.pem extension)

Syntax: -prvk <private_key_file_path>

- --public-key (-pubk)

Description: Public key file path (.pem extension)

Syntax: -pubk <public_key_file_path>

- --public-key-hash (-hash)

Description: Hash image file path (.bin extension)

Syntax: -hash <hash_file_path>

- --absolute-path (-abs)

Description: Absolute path for output files.

Syntax: -abs <absolue_path_folder_path>

- --password (-pwd)

Description: Password of the private key. The password must contain 4 characters at least.

Syntax: -pwd <password>

- --prvkey-enc (-pe)

Description: Encrypting private key algorithm (AES128/AES256) The AES256 algorithm is the default algorithm.

Syntax: -pe aes128

- --ecc-algo (-ecc)

Description: ECC algorithm for keys generation (prime256v1/brainpoolP256t1) The prime256v1 is the default algorithm.

Syntax: -ecc prime256v1

- --help (-h and -?)

Description: Show help

Syntax : --help

- --version (-v)

Description: Display the tool version

Syntax : --version

3.2 Examples

This following section presents some examples of how to use the STM32AP Key Generator software.

3.2.1 Example 1: Key creation using the AES256 algorithm

```
STM32AP_KeyGen_CLI -abs /home/user/KeyFolder/ -pwd azerty
```

Files (publicKey.pem & privateKey.pem & publicKeyhash.bin) will be created in the folder /home/user/KeyFolder/

The private key is encrypted with the default algorithm aes256

3.2.2 Example 2: Key creation using the AES128 algorithm

```
STM32AP_KeyGen_CLI -abs /home/user/keyFolder/ -pwd azerty –pe aes128
```

Files (publicKey.pem & privateKey.pem & publicKeyhash.bin) will be created in /home/user/KeyFolder/ folder.

The private key is encrypted with the algorithm aes128

3.2.3 Example 3: Key creation when one or both the destination folders are missing

```
STM32AP_KeyGen_CLI -pubk /home/user/public.pem –prvk /home/user/Folder1/Folder2
/private.pem –hash /home/user/pubKeyHash.bin –pwd azerty
```

Even if Folder1 and Folder2 does not exist they will be created.

3.3 Standalone mode

When executing the STM32MP Key Generator in standalone mode, you have to enter an absolute path and a password only. In case user press <Enter> the files will be generated in the folder

<C:\Users\User_Name\.STM32AP_KeyGen/>

Then you have to enter the password twice and select one of the two algorithms (prime256v1/brainpoolP256t1) by pressing 1 or 2 key respectively.

And finally, select an encrypting algorithm (AES256/AES128) by pressing 1 or 2 key respectively.

Elliptic curve cryptography

Error Correction Capability

Privacy Enhanced Mail (File format for storing and sending cryptographic keys, certificates, and other data)

Secure Hash Algorithm