

WHAT IS CLAIMED IS:

1. A storage device comprising:
a non-volatile memory (NVM);
at least one memory configured to store unique device secret (UDS) data comprising a UDS, and pre-installed device secret (PDS) data comprising a PDS, the UDS and the PDS being different and independent; and
a processor configured to
receive a first firmware image and a first endorsement generated based on the PDS and the first firmware image,
store the first firmware image in the NVM,
perform a first integrity check for the first firmware image based on the PDS of the PDS data, the first firmware image stored in the NVM, and the first endorsement, and
generate a second endorsement based on the UDS and the first firmware image stored in the NVM in response to a pass result of the first integrity check.
2. The storage device of claim 1, wherein the NVM is configured to store a second firmware image, and
wherein the processor is configured to output a UDS-based endorsement, a write command instructing to store the first endorsement and the first firmware image, and an address to the NVM, before the first integrity check is performed.
3. The storage device of claim 2, wherein, based on the storage device being rebooted, the processor is configured to
load the first endorsement and the first firmware image stored in the NVM, and
perform a second integrity check for the first firmware image based on the UDS, the first firmware image, and the UDS-based endorsement.
4. The storage device of claim 3, wherein the processor is configured to
generate a measurement from the UDS and the first firmware image based on a message authentication code (MAC)-based crypto algorithm, and
perform the second integrity check based on determining whether the measurement and the UDS-based endorsement are identical to each other.

5. The storage device of claim 3 or claim 4, wherein the UDS-based endorsement comprises an invalid value, and

the processor is configured to perform the first integrity check in response to a failure result of the second integrity check.

6. The storage device of any one of claims 1 to 3, wherein the processor is configured to

generate a measurement from the PDS and the first firmware image of the PDS data based on a message authentication code (MAC)-based crypto algorithm, and

perform the first integrity check based on determining whether the measurement and the first endorsement are identical to each other.

7. The storage device of claim 1, wherein

the processor is configured to generate the second endorsement from the UDS and the first firmware image based on a message authentication code (MAC)-based crypto algorithm, and

the second endorsement corresponds to a UDS-based endorsement comprising a valid value.

8. The storage device of claim 1, wherein the at least one memory comprises at least one non-volatile memory configured to store the UDS data and the PDS data.

9. A method of operating a storage controller connected to a non-volatile memory (NVM), the method comprising:

receiving a first firmware image and a first endorsement generated based on a pre-installed device secret (PDS) and the first firmware image;

storing the first firmware image in the NVM;

performing a first integrity check for the first firmware image based on the PDS of pre-stored PDS data, the first firmware image stored in the NVM, and the first endorsement; and,

in response to a pass result of the first integrity check, generating a second endorsement based on a unique device secret (UDS) of pre-stored UDS data and the first firmware image stored in the NVM, the UDS and the PDS being different and independent.

10. The method of claim 9, further comprising, before the performing of the first integrity check, controlling the NVM to store a UDS-based endorsement, the first endorsement, and the first firmware image in the NVM.

11. The method of claim 10, further comprising:
in response to a re-booting performed after the controlling of the NVM, loading the UDS-based endorsement, the first endorsement, and the first firmware image stored in the NVM; and
performing a second integrity check for the first firmware image based on the UDS, the first firmware image, and the UDS-based endorsement.

12. The method of claim 11, wherein the performing of the second integrity check comprises:
generating a measurement from the UDS and the first firmware image based on a message authentication code (MAC)-based crypto algorithm; and
determining whether the measurement and the UDS-based endorsement are identical to each other.

13. The method of claim 12, wherein, in the performing of the first integrity check, the first integrity check is performed in response to a failure result indicating that the measurement and the UDS-based endorsement are different from each other.

14. The method of any one of claims 9 to 11, wherein the performing of the first integrity check comprises:
generating a measurement from the PDS and the first firmware image of the PDS data based on a message authentication code (MAC)-based crypto algorithm; and
determining whether the measurement and the first endorsement are identical to each other.

15. The method of claim 9, further comprising controlling the NVM to store the second endorsement and the first firmware image in the NVM.

16. A universal flash storage (UFS) system comprising:

a UFS host configured to generate a first endorsement based on a pre-installed device secret (PDS) and a first firmware image and transmit the first endorsement and the first firmware image; and

a UFS device configured to update firmware based on the first endorsement and the first firmware image,

the UFS device comprising

a non-volatile memory (NVM);

at least one memory configured to store unique device secret (UDS) data comprising a UDS and PDS data including the PDS, the UDS and the PDS being different and independent;

a processor configured to store the first firmware image in the NVM, perform a first integrity check for the first firmware image stored in the NVM based on the PDS of the PDS data, the first firmware image stored in the NVM, and the first endorsement and, in response to a pass result of the first integrity check, generate a second endorsement based on the UDS, and store the second endorsement in the NVM.

17. The UFS system of claim 16, wherein the processor is configured to generate a measurement from the PDS of the PDS data and the first firmware image based on a message authentication code (MAC)-based crypto algorithm, and perform the first integrity check based on determining whether the measurement and the first endorsement are identical to each other.

18. The UFS system of claim 16, wherein the processor is configured to generate the second endorsement from the UDS and the first firmware image based on a message authentication code (MAC)-based crypto algorithm.

19. The UFS system of any one of claims 16 to 18, wherein the at least one memory comprises:

one-time programmable (OTP) memory configured to store the UDS data; and read-only memory (ROM) configured to store the PDS data.

20. The UFS system of any one of claims 16 to 18, wherein the at least one memory comprises one-time programmable (OTP) memory configured to store the UDS data and the PDS data.