CLAIMS

1. A digital key device adapted to be in communication with a host, the digital key device comprising:

a casing;

an input device, disposed near the casing or mounted on the casing, receiving a first user operation input;

a data storage unit, disposed in the casing, storing digital data and a digital key; and

a controlling unit, disposed in the casing and in communication with the host, the input device and the data storage unit, using the digital key stored in the data storage unit to perform a digital key service or outputting the digital data stored in the data storage unit to the host when authentication is complete, wherein the authentication comprises a first operation verification procedure for verifying the first user operation input, and the authentication is complete when the controlling unit determines that the first user operation input conforms to a first preset timing-based input set.

2. The digital key device according to claim 1, wherein the first user operation input is a gesture operation input and the input device is

a touch button, a physical button or a touch pad exposed from the casing, the input device receiving one or more user touch or pressing actions applied to the input device to generate one or more timing-based input events in response to the one or more user touch or pressing actions, or

a vibration sensor disposed in the casing, the vibration sensor sensing vibration or touch made on the casing held by the user to generate the one

or more timing-based input events in response to the vibration or touch made on the casing.

3. The digital key device according to claim 1, wherein the first user operation input is an audio operation input and the input device is a microphone disposed on the casing, the microphone sensing a sound made by the user to generate one or more timing-based input events in response to a rhythm of the sound.

4. The digital key device according to claim 2 or 3, wherein the one or more timing-based input events are generated according to a specific rhythm of the first user operation input and conform to an encoding format.

5. The digital key device according to claim 2 or 3, further comprising a prompting device issuing a light signal or a sound signal to prompt the user for input timing of the first user operation input.

6. The digital key device according to claim 1, wherein the authentication further comprises a personal identification number verification procedure prior to the first operation verification procedure after the digital key device is electrically coupled to the host, wherein the digital key device receives a personal identification number from the host and verifies the received personal identification number.

7. The digital key device according to claim 6, wherein the authentication further comprises a second operation verification procedure posterior to the first operation verification procedure; the digital key device activates the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a data

read command from the host; and the controlling unit outputs the digital data to the host in response to the data read command after the authentication is passed.

8. The digital key device according to claim 1, wherein the digital key service is using the digital key to encrypt first data received from the host to generate encrypted data with a digital signature, wherein the authentication further comprises a second operation verification procedure posterior to the first operation verification procedure; the digital key device activates the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a digital signing command from the host; and the controlling unit outputs the encrypted data with the digital signature to the host in response to the digital signing command after the authentication is passed.

9. The digital key device according to claim 1, wherein the digital key service is using the digital key to encrypt first data or decrypt second data received from the host to generate first encrypted data or second decrypted data; the authentication further comprises a second operation verification procedure posterior to the first operation verification procedure; the digital key device activates the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a data encrypt command or a data decrypt command from the host; and the controlling unit outputs the first encrypted data or the second decrypted data to the host or stores the first encrypted data or the second decrypted data in the data storage unit in response to the

data encrypt command or the data decrypt command after the authentication is passed.

10. The digital key device according to claim 1, wherein the data storage unit includes a first data storage unit and a second data storage unit, wherein the digital key is stored in the first data storage unit disposed in a secure element, and the digital data are stored in the second data storage unit separate from the secure element.

11. A method for activating a digital key service used with a host and a digital key device, the digital key device storing therein digital data and a digital key, the method comprising steps of:

providing a first user operation input to the digital key device; and

the digital key device activating the digital key service using the digital key stored in the digital key device or outputting the digital data to the host automatically when authentication is complete, wherein the authentication comprises a first operation verification procedure for verifying the first user operation input, and the authentication is complete when the first user operation input conforms to a first preset timing-based input set.

12. The method according to claim 11, wherein the first user operation input is a gesture operation input including one or more touch actions, one or more sliding actions, one or more pressing actions, or one or more shaking actions applied to the digital key device and being corresponding to one or more timing-based input events.

13. The method according to claim 11, wherein the first user operation input is an audio operation input including one or more sound-making

actions of the user, the one or more sound-making actions following a rhythm and being corresponding to one or more timing-based input events.

14. The method according to claim 12 or 13, wherein the one or more timing-based input events are generated according to a specific rhythm of the first user operation input and conform to an encoding format.

15. The method according to claim 12 or 13, further comprising a step of issuing a light signal or a sound signal through a prompting device of the digital key device to prompt the user for input timing of the first user operation input.

16. The method according to claim 11, wherein the authentication comprises a step of performing a personal identification number verification procedure prior to the first operation verification procedure after the digital key device is electrically coupled to the host.

17. The method according to claim 11, wherein the authentication comprises a second operation verification procedure posterior to the first operation verification procedure, the method comprising steps of:

activating the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a data read command from the host; and

outputting the digital data stored in the digital key device to the host in response to the data read command after the authentication is passed.

18. The method according to claim 11, wherein the digital key service is using the digital key to encrypt first data received from the host to generate encrypted data with a digital signature, and the authentication further

comprises a second operation verification procedure posterior to the first operation verification procedure, the method comprising steps of:

activating the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a digital signing command from the host; and

outputting the encrypted data with the digital signature to the host in response to the digital signing command after the authentication is passed.

19. The method according to claim 11, wherein the digital key service is using the digital key to encrypt first data or decrypt second data received from the host to generate first encrypted data or second decrypted data, and the authentication further comprises a second operation verification procedure posterior to the first operation verification procedure, the method comprising steps of:

activating the second operation verification procedure to verify whether a second user operation input conforms to a second preset timing-based input set after completing the first operation verification procedure and receiving a data encrypt command or a data decrypt command from the host; and

outputting the first encrypted data or the second decrypted data to the host or storing the first encrypted data or the second decrypted data in the data storage unit in response to the data encrypt command or the data decrypt command after the authentication is passed.