WHAT IS CLAIMED IS:

1. An integrated circuit module for information security, comprising:

a secure circuit unit, qualified as a cryptographic module after passing a security evaluation and storing therein at least one digital key for providing a digital key service; and

a controller unit set in communication with the secure circuit unit, including a fast service unit and a trusted zone unit, wherein the trusted zone unit and the secure circuit unit respectively use a first channel establishment key and a second channel establishment key, which are dependent on each other, to establish a secure signal channel, and the secure circuit unit transmits a specific data to the fast service unit via the security signal channel to perform a fast service,

wherein the first channel establishment key and the second channel establishment key are derived from the digital key, and

wherein the trusted zone unit includes a volatile memory; after the trusted zone unit uses a main key to perform an initialization process with the digital key provided by the secure circuit unit, and after a set of derived data is obtained from the digital key and the main key and stored back to the secure circuit unit, the secure circuit unit sends the set of derived data to the trusted zone unit in a subsequent process of establishing the secure signal channel, and the trusted zone unit uses the main key and the set of derived data to restore the digital key and stores it in a volatile memory; after the trusted zone unit completes mutual verification with the secure circuit unit by way of the digital key, the trusted zone unit and the secure circuit unit use the digital key to derive the first channel establishment key and the second channel establishment key respectively; the secure signal channel, by way of the first channel establishment key and the second channel establishment

key, has the specific data transmitted therevia under encryption; and the specific data obtained by the trusted zone unit is stored into the volatile memory, wherein after the controller unit set is powered off, the digital key stored in the volatile memory will disappear, and the process of establishing the secure signal channel will be restarted once the controller unit is powered on.

2. The integrated circuit module for information security according to claim 1, wherein the first channel establishment key and the second channel establishment key are session keys of the same contents; the secure signal channel, by way of the session keys, has the specific data transmitted therevia under encryption; and the specific data contains a key for fast service for the fast service unit to perform the fast service.

3. The integrated circuit module for information security according to claim 1, wherein the mutual verification includes steps of: the trusted zone unit issuing a first challenge to the security circuit unit, which is a generated random number, and sending it to the security circuit unit; in response to the first challenge, the security circuit unit sending back a first response to the trusted zone unit, which is the random number encrypted with the digital key; the trusted zone unit decrypting the first response based on the digital key to get back the decrypted random number, thereby determining whether the decrypted random number is the same as the generated random number; the security circuit unit issuing a second challenge to the trusted zone unit, which is another generated random number, and sending it to the trusted zone unit; in response to the second challenge, the trusted zone unit sending back a second response to the security circuit unit, which is the another random

number encrypted with the digital key; and the security circuit unit decrypting the second response according to the digital key to get back the decrypted another random number, thereby determining whether the decrypted another random number is the same as the generated another random number, thereby completing the mutual verification.

4. The integrated circuit module for information security according to claim 1, wherein the trusted zone unit uses a secure technology of Physically Unclonable Function (PUF) to generate the main key.

5. The integrated circuit module for information security according to claim 1, wherein the secure circuit unit is a secure integrated circuit chip, and the controller unit set is a controller integrated circuit chipset.

6. The integrated circuit module for information security according to claim 1, wherein the fast service unit is implemented with an AI chip, a field programmable gate array unit, or an application specific integrated circuit (ASIC) for conducting the fast service, which is a fast service via a changeable interface.

7. A memory module exhibiting an information security function, which includes the integrated circuit module for information security as recited in claim 1 and the following devices:

a non-volatile memory for storing digital information; and

an interface controller in communication with the non-volatile memory, the integrated circuit module for information security, and a host for conducting digital data transmission between the non-volatile memory and

the host, and using the fast service provided by the integrated circuit module for information security.

8. A memory module exhibiting an information security function, comprising: the integrated circuit module for information security as recited in claim 1, and a non-volatile memory for storing digital information, wherein the integrated circuit module for information security is in communication with the non-volatile memory and a host for conducting digital data transmission between the non-volatile memory and the host, and providing the fast service.

9. A hardware module exhibiting an information security function, comprising: the integrated circuit module for information security as recited in claim 1, and a communication controller, wherein the communication controller is in communication with a host for conducting digital data transmission between the non-volatile memory and the host, and providing the fast service.

10. The hardware module exhibiting an information security function according to claim 9, wherein the communication controller is a network interface controller; the integrated circuit module for information security is further coupled to a network module; the network module is used for communicating with the external internet or mobile network; and data information transmitted between the host and a user device at the other end of the internet or mobile network are encrypted/decrypted by way of the fast service unit in the integrated circuit module for information security.

11. The hardware module exhibiting an information security function according to claim 9, wherein the integrated circuit module for information security and the communication controller are integrated in a housing to form the hardware module exhibiting information security and encryption/decryption functions; the integrated circuit module for information security conducts digital data transmission with a non-volatile memory in the host via the communication controller; the host transmits unencrypted information in the non-volatile memory to the fast service unit in the integrated circuit module for information security to be fast encrypted; the encrypted information is transmitted back to the non-volatile memory in the host via the communication controller to be stored; the host transmits the encrypted information to the fast service unit in the integrated circuit module for information security to be fast decrypted; and the decrypted information is transmitted back to the non-volatile memory in the host via the communication controller to be stored.

12. An integrated circuit module for information security, comprising:

a secure circuit unit, having passed a security evaluation as a cryptographic module and storing therein at least one digital key for providing a digital key service; and

a controller unit set in communication with the secure circuit unit, including a fast service unit and a trusted zone unit, wherein the trusted zone unit and the secure circuit unit respectively use a first channel establishment key and a second channel establishment key, which are dependent on each other, to establish a secure signal channel, and the secure circuit unit transmits a specific data to the fast service unit via the security signal channel to perform a fast service,

wherein the trusted zone unit obtains a first public key pairing the digital key in an initialization process; a second public key of a second public-private key pair in the trusted zone unit is sent to the secure circuit unit, and stored in the secure circuit unit; the trusted zone unit uses a PUF secure technology to generate the main key, and uses the main key to conduct encryption protection of the second public-private key pair; the trusted zone unit uses a key establishment process to derive a share key from the first public key and a second private key of the second public-private key pair; the secure circuit unit uses the key establishment process to derive the share key from the second public key and the digital key; and the secure circuit unit and the trusted zone unit use a session key derived from the shared key to serve as the first channel establishment key and the second channel establishment key.