

TITLE: SECURE COMMUNICATION DEVICE

BACKGROUND OF THE INVENTION

(a) Technical Field of the Invention

The present invention is generally related to Internet of Things techniques,
5 and more particular to a secure communication device.

(b) Description of the Prior Art

Communication devices are widely applied in various areas such as
vehicle monitor and remote control, wireless tags, wireless networks, smart
appliances, etc. Currently, Internet of Things (IoT) is mostly implemented on
10 public Internet, and communication data are transmitted in plain text without
encryption through communication devices. Data security is easily
compromised. Especially for some devices responsible for security and safety,
they may be easily cracked, causing significant damages.

SUMMARY OF THE INVENTION

According to an embodiment of the present invention, the secure communication device includes a master control chip, an encryption chip, a SIM card slot, and a communication chip.

5 The SIM card slot is for storing a SIM card.

 The master control chip's MOSI (Master Output, Slave Input) pin is connected to the encryption chip's MOSI pin through the SPI bus and, the master control chip's MISO (Master Input, Slave Output) pin is connected to the encryption chip's MISO pin through the SPI bus, the master control chip's
10 CLK pin is connected to the encryption chip's CLK pin through the SPI bus, and the master control chip's CS pin is connected to the encryption chip's CS pin through the SPI bus.

 The master control chip's DATA pin is connected to the SIM card slot's DATA pin through the 7816 interface bus, the master control chip's CLK pin
15 is connected to the SIM card slot's CLK pin through the 7816 interface bus, and the master control chip's RST pin is connected to the SIM card slot's RST pin through the 7816 interface bus.

 The master control chip's AUX_ANT pin and MAIN_ANT pin are connected to the communication chip.

20 The foregoing objectives and summary provide only a brief introduction to the present invention. To fully appreciate these and other objects of the present invention as well as the invention itself, all of which will become apparent to those skilled in the art, the following detailed description of the

invention and the claims should be read in conjunction with the accompanying drawings. Throughout the specification and drawings identical reference numerals refer to identical or similar parts.

Many other advantages and features of the present invention will become
5 manifest to those versed in the art upon making reference to the detailed description and the accompanying sheets of drawings in which a preferred structural embodiment incorporating the principles of the present invention is shown by way of illustrative example.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a hardware block diagram showing a secure communication device according to an embodiment of the present invention.

FIG. 2 is a functional block diagram showing the secure communication device of FIG. 1 connected with a first electronic device.

FIG. 2A is a functional block diagram showing the secure communication device of FIG. 1 connected with a first electronic device and a second electronic device.

FIG. 3 is a hardware block diagram showing a secure communication device according to another embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following descriptions are exemplary embodiments only, and are not intended to limit the scope, applicability or configuration of the invention in any way. Rather, the following description provides a convenient illustration
5 for implementing exemplary embodiments of the invention. Various changes to the described embodiments may be made in the function and arrangement of the elements described without departing from the scope of the invention as set forth in the appended claims.

As shown in FIGS. 1 and 2, a secure communication device 10 according
10 to an embodiment of the present invention includes a master control chip 110, an encryption chip 120, a communication chip 130, and a SIM (Subscriber Identity Module) card slot 140.

The encryption chip 120, communication chip 130, and SIM card slot 140 are all connected to the master control chip 110.

15 The master control chip 110 is connected to the encryption chip 120 through SPI (Serial Peripheral Interface) , I²C(Inter-Integrated Circuit) bus, or GPIO (General-purpose input/output). The master control chip 110 is connected to the SIM card slot 140 through 7816 interface bus, and the SIM card slot 140 is connected to a SIM card stored in the SIM card slot 140
20 through contacts, thereby achieving the connection between the master control chip 110 and the SIM card. In addition, the master control chip 110 is also connected to the communication chip 130.

Using the SPI bus as an example, the SPI bus is for hardware

communication, and each SPI line corresponds to a pin of the master control chip 110. Through the SPI bus, the master control chip 110's MOSI (Master Output, Slave Input) pin is connected to the encryption chip 120's MOSI pin, the master control chip 110's MISO (Master Input, Slave Output) pin is
 5 connected to the encryption chip 120's MISO pin, the master control chip 110's CLK (Clock) pin is connected to the encryption chip 120's CLK pin, and the master control chip 110's CS (Chip Select) pin is connected to the encryption chip 120's CS pin.

Specifically, SPI_MOSI, and SPI_MISO are data exchange channels
 10 between the master control chip 110 and the encryption chip 120. The exchanged data are often represented by high and low levels. The master control chip 110 provides clock signal and chip select signal to the encryption chip 120 through SPI_CLK and SPI_CS channels.

The 7816 interface bus is for the master control chip 110's accessing the
 15 SIM card data. Each line of the 7816 interface bus corresponds a pin of the master control chip 110. Through the 7816 interface bus, the master control chip 110's DATA pin is connected to the SIM card slot's DATA pin. the master control chip 110's CLK (Clock) pin is connected to the SIM card slot 140's CLK pin, and the master control chip 110's RST (Reset) pin is connected to
 20 the SIM card slot 140's RST pin.

Specifically, the master control chip 110 provides reset signal, clock signal, and data signal to the SIM card through 7816_RST channel, 7816_CLK channel, and 7816_DATA channel, respectively. The data are

often represented by high and low levels

The master control chip 110's AUX_ANT pin and MAIN_ANT pin are connected to the communication chip 130.

The secure communication device 10 may link with a CAS
5 (Cryptographic Authentication Server) in a wireless manner. When a first secure communication device and a second secure communication device exchange data, one of the secure communication devices may transmit communication data to the CAS, where CAS relays the communication data to the other secure communication device. Alternatively, the first and second
10 secure communication devices may directly communicate with each other. A first key is produced at the first secure communication device and a second key is produced at the second communication device. During their exchange of data, the transmitted communication data is encrypted using the respective key of the sending secure communication device, and the received
15 communication data is decrypted using the respective key of the receiving communication device.

The SIM card slot 140 is for storing a SIM card. The SIM card is connected to the master control chip 110 through contacts. After the communication device 10 is powered on, the master control chip 110 engages
20 the SIM card through the communication chip 130 to achieve connection with a network.

After the SIM card's establishing network connection, the secure communication device 10 and the CAS may conduct data exchange.

The encryption chip 120 is for storing certificates used for the authentication of the secure communication device 10 to the CAS, so as to ensure the uniqueness and non-repudiation of the secure communication device 10.

- 5 The CAS is responsible for the mutual authentication of the secure communication device 10 and the CAS, and the generation of session keys.

The encryption chip 120 is also for producing single-use session keys.

- Furthermore, the encryption chip 120 produces asymmetric keys using a random number from a real random number generator. The asymmetric keys
10 includes a public key and a private key. Please note that the random number generator may also be a random number generator.

- The master control chip 110 transmits a random number produced by the encryption chip 120 's random number generator to the CAS through the communication chip 130. The CAS encrypts the received random number
15 using the public key of the encryption chip 120 and sends the encrypted random number to the communication device 10, where the encrypted random number is decrypted by the private key of the encryption chip 120. If the decryption result is the same as the random number sent to the CAS, the secure communication device and the CAS are mutually authenticated.

- 20 The communication chip 130 is for the data transmission and reception between the master control chip 110 and the CAS.

In the present embodiment, the communication chip 130 may be a wireless communication chip. In some alternative embodiments, the secure

communication device 10 may also include UART interface so as to communicated an external device through the UART interface. The external device may be an Internet of Things (IoT) device requiring a high security such as a Smart lock.

5 Furthermore, the communication chip 130 achieves connectivity with a mobile network, a WIFI network, a NB-IOT network, or a LPWAN (Low-Power Wide-Area Network) through LoRa technique.

As the communication chip 130 achieves connectivity through a mobile network, the communication chip 130 may specifically be an antenna
10 communication chip .

In the present embodiment, the mobile network may be a TD-LTE, FDD-LTE, TD-SCDMA, WCDMA, CDMA, CDMA2000, and GSM network. As technology advances, the mobile network may also be an emerging mobile network, such as a 5G network.

15 The master control chip 110 accesses the certificate and asymmetric keys stored in the encryption chip 120 and, based on the public key of the asymmetric keys, encrypts and the certificate. The encrypted certificate is then transmitted to the CAS, which decrypts the certificate using CAS's private key. The CAS then authenticates the decrypted certificate and determines whether
20 the certificate is legal. If the certificate is determined to be legal, the secure communication device 10 is considered as a legal device. If the certificate is determined to be illegal, the secure communication device 10 is considered as an illegal device and no communication would be conducted.

If the certificate from the master control chip 110 is legal, the CAS encrypts its CAS certificate using its public key and transmits the encrypted CAS certificate to the master control chip 110. The master control chip 110 receives the encrypted CAS certificate through the communication chip 130, and uses the private key from the asymmetric keys to decrypt the encrypted CAS certificate and to obtain the decrypted CAS certificate. The public key from the encryption chip 120's asymmetric keys is different from the public key from the CAS's asymmetric keys. The private key from the encryption chip 120's asymmetric keys is different from the private key from the CAS's asymmetric keys.

The master control chip 110 authenticates the decrypted CAS certificate. If the CAS certificate is determined to be not legal, the CAS is considered to be not legal and no communication would be conducted. If the CAS certificate is determined to be legal, the CAS is considered to be legal and communication would be conducted.

After authentication, the CAS produces a new session key and encrypts the session key using asymmetric encryption through public key. The encrypted session key is then transmitted to a third party's legal electronic device so that the third party's legal electronic device and the secure communication device 10 may communicate through asymmetric encryption for enhanced data security.

Alternatively, after authentication, the secure communication device 10 and the CAS may negotiate and produce the session key through a key

exchange algorithm. It should be noted that, in the process of producing the session key, data exchanged between the secure communication device 10 and the CAS are all asymmetrically encrypted before transmission for enhanced data security.

5 Furthermore, the asymmetrically encrypted session key received by the master control chip 110 from the CAS is different each time. Each session key is random and unique so that it will not be cracked by hackers

 Furthermore, the CAS produces the session key through the random number generated by the random number generator.

10 Specifically, the CAS conducts a series of arithmetic and logic computations to obtain a series of session key using the random numbers generated by the random number generator. The random number generator guarantees that a different random number is generated each time. Therefore, a different session key would be produced after the arithmetic and logic
15 computations using the different random number.

 Furthermore, to guarantee data security during each communication, the secure communication device 10 and the CAS may negotiate to produce session keys through key exchange algorithm. A different session key is produced each time. Through a different session key for each communication,
20 communication security and key validity is ensured, and key breaking by hackers through monitoring or probability combinations of massive data is prevented.

 During each communication, the encryption chip 120 and the CAS use a

common base number for random number generation and a common key exchange algorithm to produce session keys. The encryption chip 120 produces a session key as described above, and the CAS produces a corresponding session key following the same above process. The encryption
5 chip 120's session key and the CAS's session key are different. The master control chip 110 conducts encryption or decryption using the session key accessed from the encryption chip 120.

For example, during a communication when the master control chip 110 transmits data to the CAS, the master control chip 110 encrypts the data to be
10 transmitted using the session key produced by the encryption chip 120 and transmits the encrypted data to the CAS. The CAS decrypts the encrypted data using its produced session key, and carries out subsequent process to the decrypted data. When the CAS transmits encrypted data to the master control
15 chip 110, the master control chip 110 decrypts the encrypted data using the session key produced by the encryption chip 120, and carries out subsequent process to the decrypted data. As such, the work flow of the secure communication device 10 is optimized, making authentication and key exchange more precise and effective.

In a next communication, the secure communication device 10 and the
20 CAS encrypt and decrypt communication data through a different session key. Therefore, even a hacker captures encrypted data packets, the secure communication device 10 and the CAS would have finished data communication for this session before the hacker cracks the session key. Even

though the session key is cracked, it is no longer valid as the secure communication device 10 and the CAS would engage in a new session using a session key different from the previous one.

In the present embodiment, the master control chip 110 may support
5 protocols such as TCP/UDP, HTTP, COAP, LWM2M, MQTT, etc. In alternative embodiments, the master control chip 110 may support some new protocols as technology advances.

Furthermore, the master control chip 110 may specifically be a SIM7600C chip, a ME3630 chip, or a SIM7500-series chip. SIM7600C chip
10 is a SMT packaging module, supporting bands such as LTE-TDD, LTE-FDD, HSPA+, TD-SCDMA, GSM, GPRS, EDGE, etc., and supporting LTE CAT4 having a downstream speed 150Mbps. SIM7600C chip has advantages such as stability, compact form factor, high price-performance ratio, and capability to achieve SMS and data communication with low power consumption.
15 SIM7600C chip has a dimension of 30x30x2.9 mm, capable of meeting various compact product designs and customer requirements.

The SIM7500-series chip may be a SIM7500CE, SIM7500X, etc. The SIM7600C chip, ME3630 chip, or SIM7500-series chip are all applicable to IoT applications.

20 In the present embodiment, the encryption chip 120 may support encryption algorithms such as ECC, RSA, SM1, SM2, SM3, SM4, DES, AES, SHA, etc. In alternative embodiments, the encryption chip 120 may also support other asymmetric or symmetric encryption algorithms, such as elliptic

curve cryptography.

Specifically, the encryption chip 120 supports the SM2 algorithm, which is a high-intensity and irreversible algorithm, and cannot be cracked using existing technical means, thereby ensuring the security and non-repudiation
5 for the authentication and data communication between the secure communication device 10 and the CAS. In the meantime, the one-time, single-use session key between the secure communication device 10 and the CAS guarantees communication security and high performance.

Furthermore, the encryption chip 120 may be a CIU98320 chip or an
10 Infineon 97 series chip. CIU98320 chip has a power consumption lower than 160 μ A/MHz. The CIU98320 chip and the Infineon 97 series chip both support SM1/SM2/SM3/SM4, RSA, ECC (elliptic curve cryptography), SHA (Secure Hash Algorithm), DES (Data Encryption Standard), AES(Advanced Encryption Standard) algorithms. The Infineon 97 series chip may be a SLE97
15 chip, a SLM97 chip, or a SLI97 chip.

The SIM card slot 140 is for storing a SIM card. The SIM card is connected to the master control chip 110. After the communication device 10 is powered up, the master control chip 110 controls the SIM card through the communication chip 130 to achieve networking between the secure
20 communication device 10 and the CAS.

Furthermore, in the present embodiment as shown in FIGS. 2 and 2A, the master control chip 110 is data-linked with a first electronic device 2. The first electronic device 2 is a smart portable or wearable electronic device with

networking capability (e.g., 4G or above, WiFi, Bluetooth) such as a smart band, a smart watch, an electronic card. The first electronic device 2 may provide authentication or authorization with the secure communication device 10. In addition, there may be a second electronic device 3, such as a smart
5 phone, a tablet computer, a PC (Personal Computer). The first electronic device 2 may be data-linked with the second electronic device 3 through, for example, USB or Bluetooth. Through an APP application on the second electronic device 3, the second electronic device 3 is data-linked with the master control chip 110. The first electronic device 2 therefore may still
10 provide authentication or authorization with the secure communication device 10.

Furthermore, in the present embodiment, if the certificate incorporates a third-party encryption algorithm so that the third party's public key is delivered to the CAS, and the CAS uses its private key to sign the third party's
15 public key. The certificate becomes a third party certificate.

FIG. 3 provides a functional block diagram of a secure communication device 10 according to another embodiment of the present invention.

The secure communication device 10 includes the master control chip 110, the encryption chip 120, the communication chip 130, the SIM card slot
20 140, and a power 150.

The encryption chip 120, communication chip 130 are both connected to the master control chip 110.

The encryption chip 120 is for storing certificates and producing

asymmetric keys.

The master control chip 110 conducts asymmetric encryption on the certificates using the asymmetric keys and uses the asymmetrically encrypted certificate to conduct authentication between the secure communication
 5 device 10 and the CAS.

The master control chip 110 is also for receiving an asymmetrically encrypted session key from the CAS for each communication session after authentication and conducting encryption or decryption on the communication data according to the session key.

10 The communication chip 130 is for carrying out data communication between the master control chip 110 and the CAS.

The power 150 provides electricity to the master control chip 110, the encryption chip 120, the communication chip 130, and the SIM card slot 140 of the secure communication device 10.

15 Specifically, the power 150 includes a power connector 151 and an AC/DC conversion circuit 152. The power connector 151 is for receiving external electrical power, and the AC/DC conversion circuit 152 converts the external electrical power through the power connector 151 into DC electricity required by the secure communication device 10 so that all chips of the secure
 20 communication device 10 are stably powered.

Specifically, in addition to the above wireless connection, the secure communication device 10 may further include an UART interface so as to achieve a wired connection between the secure communication device 10 and

an external device such as a smart lock for enhanced communication speed and safety.

Furthermore, the secure communication device 10 may further include a debugging port for testing the secure communication device 10 so as to ensure
5 the normal operation of the secure communication device 10's various modules.

Therefore, the secure communication device 10 of the present invention achieves the mutual authentication and communication data encryption/decryption between IoT external devices such as mobile terminals
10 and smart locks and the CAS. The use of asymmetric keys guarantees ensures the uniqueness and non-repudiation of authentication. Through asymmetric session keys, the validity of the keys is time-dependent, and plain-text transmission of the keys and the communication data is avoided, thereby enhancing communication data security.

15 While certain novel features of this invention have been shown and described and are pointed out in the annexed claim, it is not intended to be limited to the details above, since it will be understood that various omissions, modifications, substitutions and changes in the forms and details of the device illustrated and in its operation can be made by those skilled in the art without
20 departing in any way from the claims of the present invention.

I CLAIM:

1. A secure communication device, comprising a master control chip,
an encryption chip, and a communication chip, wherein the master
control chip's Master Output, Slave Input (MOSI) pin is connected
5 to the encryption chip's MOSI pin; the master control chip's Master
Input, Slave Output (MISO) pin is connected to the encryption chip's
MISO pin; the master control chip's Clock (CLK) pin is connected to
the encryption chip's CLK pin; the master control chip's Chip Select
(CS) pin is connected to the encryption chip's CS pin; and the master
10 control chip's AUX_ANT pin and MAIN_ANT pin are connected to
the communication chip.
2. The secure communication device according to claim 1, further
comprising a power providing electricity to the master control chip,
the encryption chip, and the communication chip of the secure
15 communication device.
3. The secure communication device according to claim 2, wherein the
power comprises a power connector and a AC/DC conversion circuit;
the power connector receives external electrical power; and the
AC/DC conversion circuit converts the external electrical power into
20 DC electricity required by the secure communication device.
4. The secure communication device according to claim 1, wherein the
master control chip is data-linked with a first electronic device.
5. The secure communication device according to claim 4, further

comprising a second electronic device, wherein the second electronic device is connected to the master control chip through the first electronic device.

- 5 6. The secure communication device according to claim 1, further comprising a Subscriber Identity Module (SIM) card slot for storing a SIM card, wherein the master control chip's DATA pin is connected to the SIM card slot's DATA pin through a 7816 interface bus; the master control chip's CLK pin is connected to the SIM card slot's CLK pin through the 7816 interface bus; and the master control
- 10 chip's Reset (RST) pin is connected to the SIM card slot's RST pin through the 7816 interface bus.