

US009270466B2

(12) **United States Patent**  
**Hsien**

(10) **Patent No.:** **US 9,270,466 B2**  
(45) **Date of Patent:** **Feb. 23, 2016**

(54) **SYSTEM AND METHOD FOR TEMPORARY SECURE BOOT OF AN ELECTRONIC DEVICE**

H04L 9/00; H04L 9/0813; H04L 9/3226;  
H04L 9/32

See application file for complete search history.

(71) Applicant: **HTC Corporation**, Taoyuan County (TW)

(56) **References Cited**

(72) Inventor: **Chao-Chung Hsien**, Taoyuan County (TW)

U.S. PATENT DOCUMENTS

(73) Assignee: **HTC Corporation**, Taoyuan District, Taoyuan (TW)

6,799,197 B1 9/2004 Shetty  
6,975,727 B1 12/2005 Vandergeest  
7,051,206 B1 5/2006 Giest  
7,428,750 B1 9/2008 Dunn  
7,552,333 B2 6/2009 Wheeler

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 450 days.

(Continued)

FOREIGN PATENT DOCUMENTS

(21) Appl. No.: **13/682,752**

CN 1731726 A 2/2006  
CN 101379506 A 3/2009

(22) Filed: **Nov. 21, 2012**

(Continued)

(65) **Prior Publication Data**

OTHER PUBLICATIONS

US 2013/0145140 A1 Jun. 6, 2013

Office action mailed on Sep. 24, 2014 for the U.S. Appl. No. 13/674,068, filed Nov. 11, 2012, p. 1-17.

**Related U.S. Application Data**

(Continued)

(60) Provisional application No. 61/565,955, filed on Dec. 1, 2011.

*Primary Examiner* — Dennis M Butler

(51) **Int. Cl.**

(74) *Attorney, Agent, or Firm* — Winston Hsu; Scott Margo

**G06F 21/00** (2013.01)  
**H04L 9/32** (2006.01)  
**G06F 21/57** (2013.01)  
**G06F 21/60** (2013.01)  
**H04L 9/08** (2006.01)  
**H04L 9/00** (2006.01)

(57) **ABSTRACT**

(52) **U.S. Cl.**

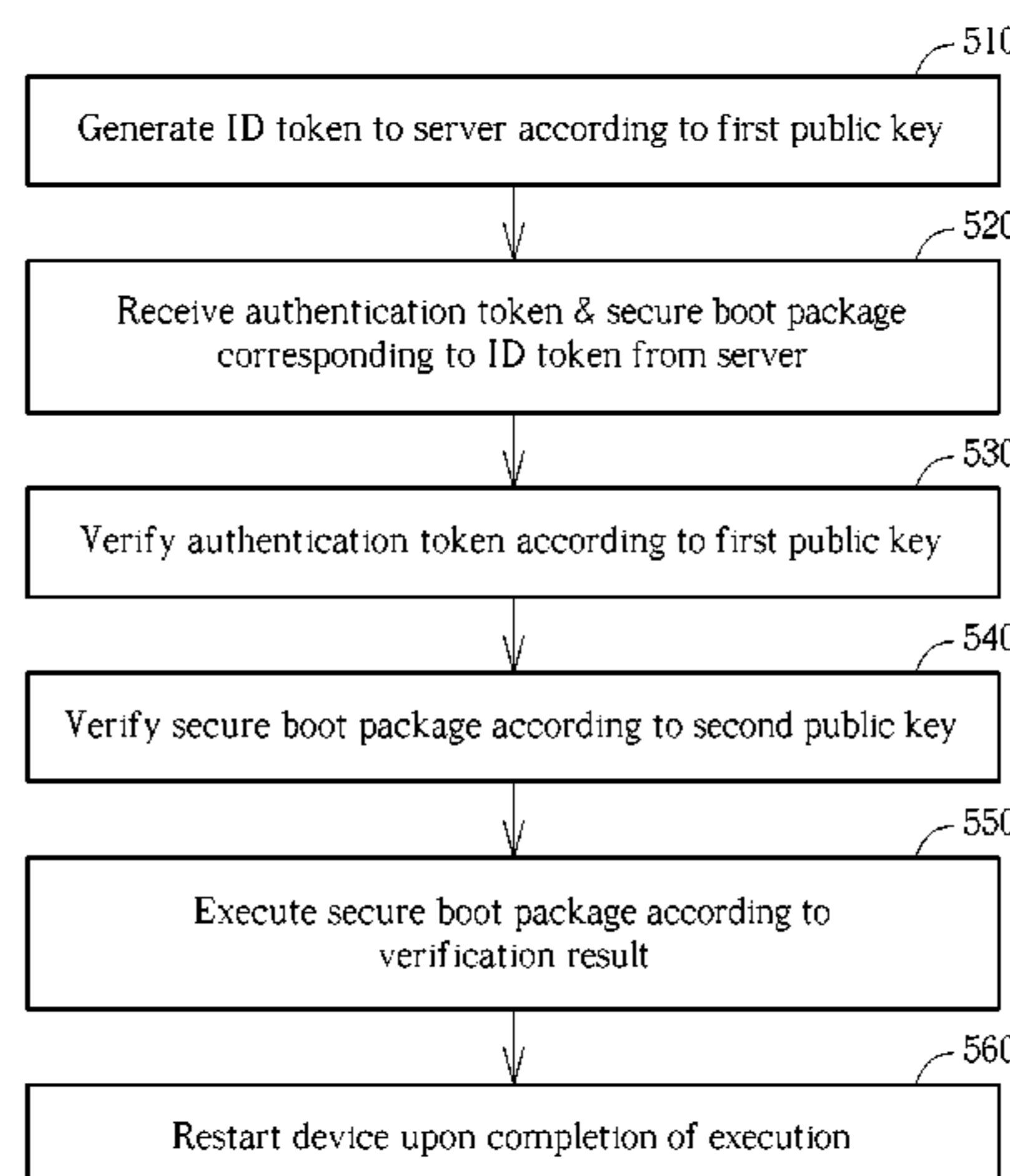
CPC ..... **H04L 9/3247** (2013.01); **G06F 21/575** (2013.01); **G06F 21/606** (2013.01); **H04L 9/0866** (2013.01); **H04L 9/3226** (2013.01); **H04L 9/00** (2013.01); **H04L 9/0813** (2013.01)

The invention discloses system and method of temporary secure boot process of an electronic device. The method comprises: generating a first token according to an identification data of the electronic device; sending a request along with the first token to a service provider, the request corresponding to a boot package; receiving a second token and a boot package from the service provider; verifying the second token and the boot package; and executing the boot package according to verification result.

(58) **Field of Classification Search**

CPC ... G06F 21/575; G06F 9/4401; G06F 9/4416;

**17 Claims, 8 Drawing Sheets**



(56)

References Cited

U.S. PATENT DOCUMENTS

7,681,048	B2	3/2010	Starr	
8,165,303	B1	4/2012	Steele	
8,301,884	B2	10/2012	Choi	
8,393,001	B1	3/2013	Libenzi	
8,452,969	B2	5/2013	Iyer	
8,527,618	B1*	9/2013	Wiese	709/223
2002/0073306	A1*	6/2002	Aluzzo et al.	713/1
2002/0112161	A1	8/2002	Thomas	
2004/0111331	A1	6/2004	Yano	
2004/0123109	A1	6/2004	Choi	
2005/0097316	A1	5/2005	Kim	
2007/0214370	A1	9/2007	Sato	
2007/0269042	A1	11/2007	Tanaka	
2008/0028209	A1	1/2008	Dare	
2008/0082813	A1	4/2008	Chow	
2008/0184218	A1*	7/2008	Largman et al.	717/168
2008/0189550	A1	8/2008	Roundtree	
2008/0244271	A1	10/2008	Yu	
2010/0005304	A1	1/2010	Maruyama	
2010/0031034	A1	2/2010	Kim	
2010/0050241	A1	2/2010	Yan	
2010/0250925	A1	9/2010	Hiraide	
2010/0290076	A1	11/2010	Itoh	
2010/0332820	A1	12/2010	Matsushima	
2011/0002462	A1	1/2011	Stewart	
2011/0021181	A1	1/2011	Weiner	
2011/0066859	A1	3/2011	Iyer	
2011/0093714	A1	4/2011	Schaecher	
2011/0274273	A1	11/2011	Fiske	
2011/0296174	A1	12/2011	Nakayama	
2012/0087493	A1*	4/2012	Chidambaram et al.	380/44
2012/0240211	A1*	9/2012	Counterman	726/9
2012/0294445	A1	11/2012	Radutskiy	
2013/0117564	A1*	5/2013	Chang et al.	713/168

FOREIGN PATENT DOCUMENTS

CN	101398764	A	4/2009
CN	102007505	A	4/2011

EP	0 725 512	A2	8/1996
TW	200539706		12/2005
TW	200629085		8/2006
TW	200841187		10/2008
TW	200915183		4/2009
TW	200951848		12/2009
TW	201021500		6/2010
TW	201108699		3/2011
TW	201110653		3/2011
TW	201137659		11/2011
TW	201141125		11/2011

OTHER PUBLICATIONS

Office action mailed on Dec. 29, 2014 for the Taiwan application No. 101144444, filed Nov. 28, 2012, p. 1-9.

Office action mailed on Jul. 17, 2014 for the U.S. Appl. No. 13/682,739, filed Nov. 21, 2012, p. 1-27.

Office action mailed on Feb. 11, 2014 for the U.S. Appl. No. 13/682,739, filed Nov. 21, 2012, p. 1-23.

Notice of Allowance mailed on Jan. 28, 2015 for the Taiwan application No. 101144442, filing date: Nov. 28, 2012, p. 1-5.

Office action mailed on Jun. 16, 2014 for the Taiwan application No. 101144442, filing date Nov. 28, 2012, p. 1-9.

Office action mailed on Feb. 2, 2015 for the China application No. 201210510215.9, filing date Dec. 3, 2012, p. 1-13.

Office action mailed on Apr. 30, 2015 for the U.S. Appl. No. 13/682,739, filed Nov. 21, 2012, p. 1-41.

Office action mailed on May. 29, 2015 for the China application No. 201210511241.3, filing date Dec. 3, 2012, p. 1-6.

Yandji et al., "Research on a Normal File Encryption and Decryption," Computer and Management (Caman), 2011 IEEE International Conference on Year: 2011, pp. 1-4.

Zugenmaier et al., "Transparent Encryption for External Storage Media with Key Management Adapted to Mobile Use," Annual Computer Security Applications Conference, 2009 IEEE computer society, ACSAC.2009.38 Year: 2009 pp. 333-339.

Notice of Allowance mailed on Sep. 14, 2015 for the U.S. Appl. No. 13/682,739, filed Nov. 21, 2012, p. 1-18.

Notice of Allowance mailed on Nov. 16, 2015 for the U.S. Appl. No. 14/686,752, filed Apr. 14, 2015, p. 1-20.

\* cited by examiner

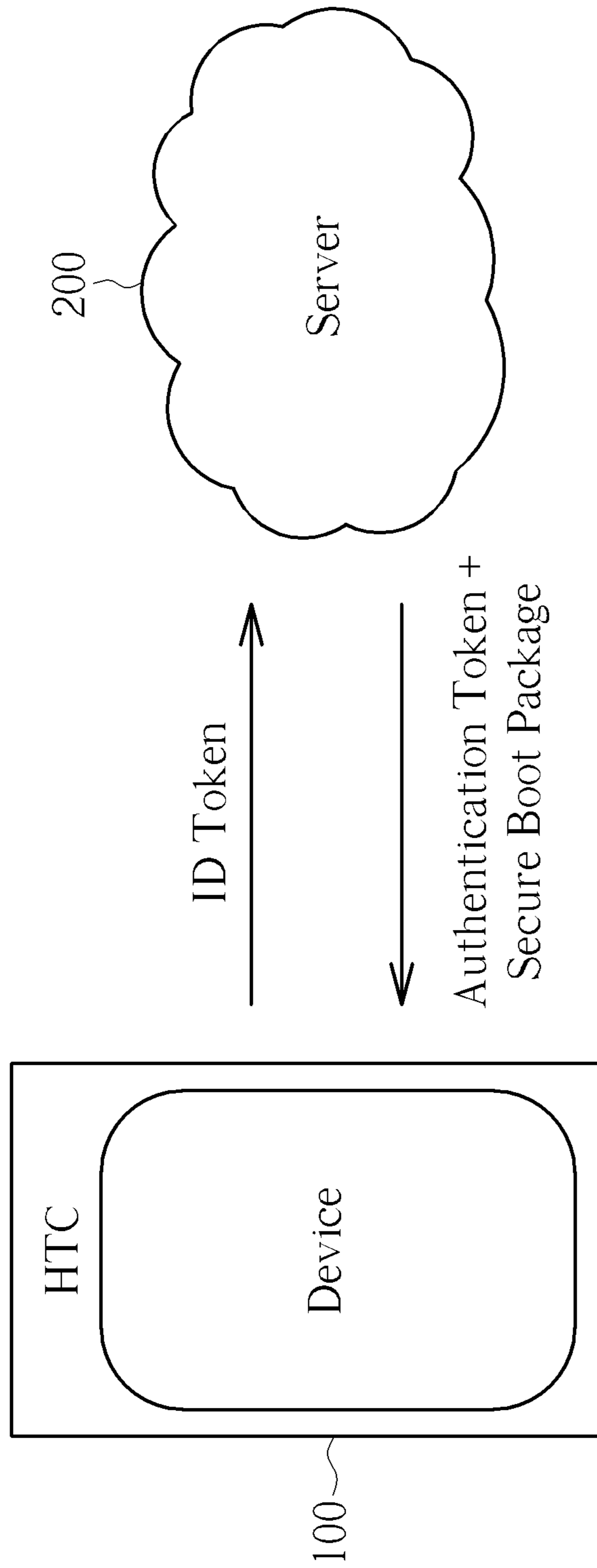


FIG. 1

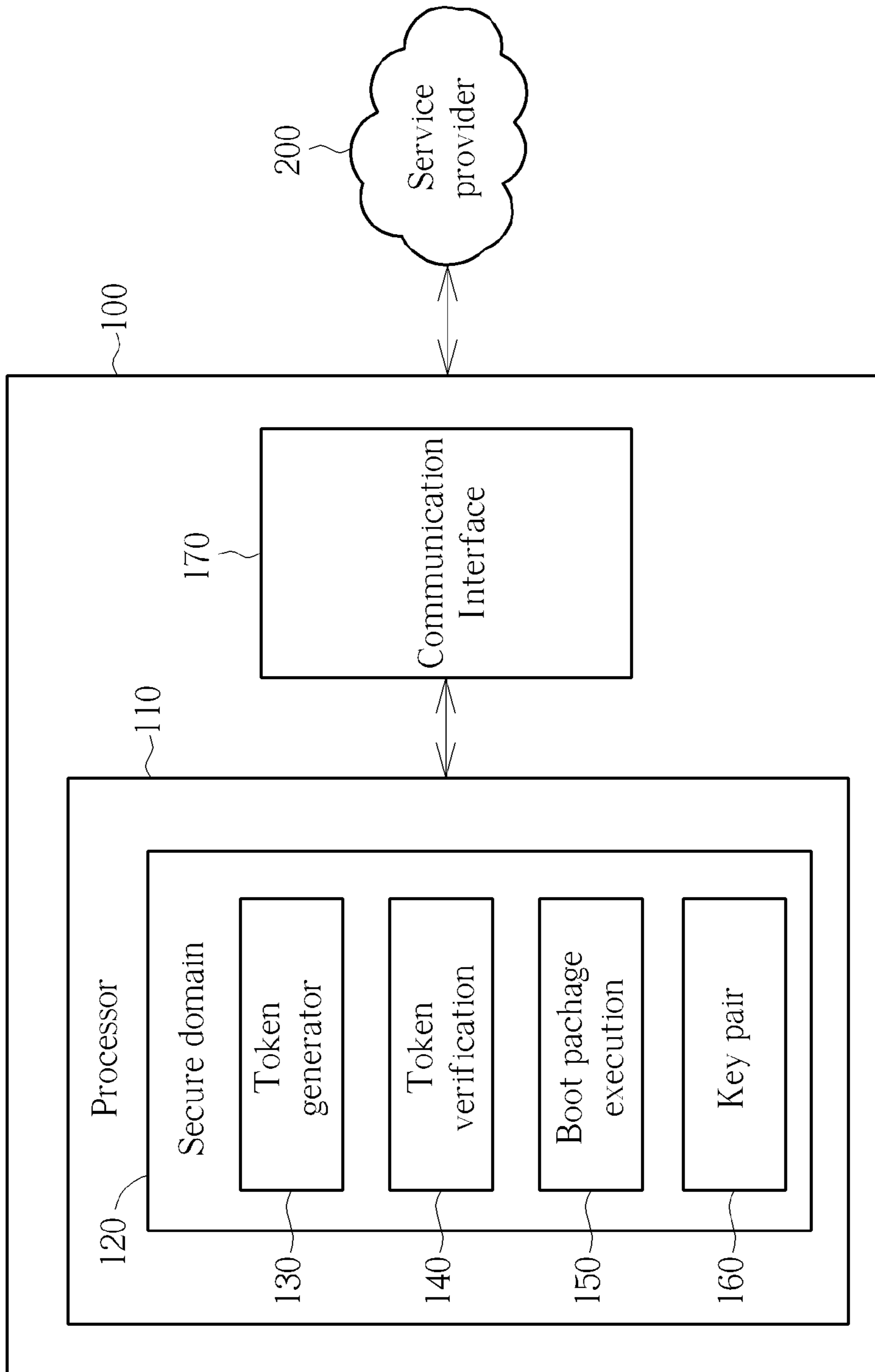


FIG. 2

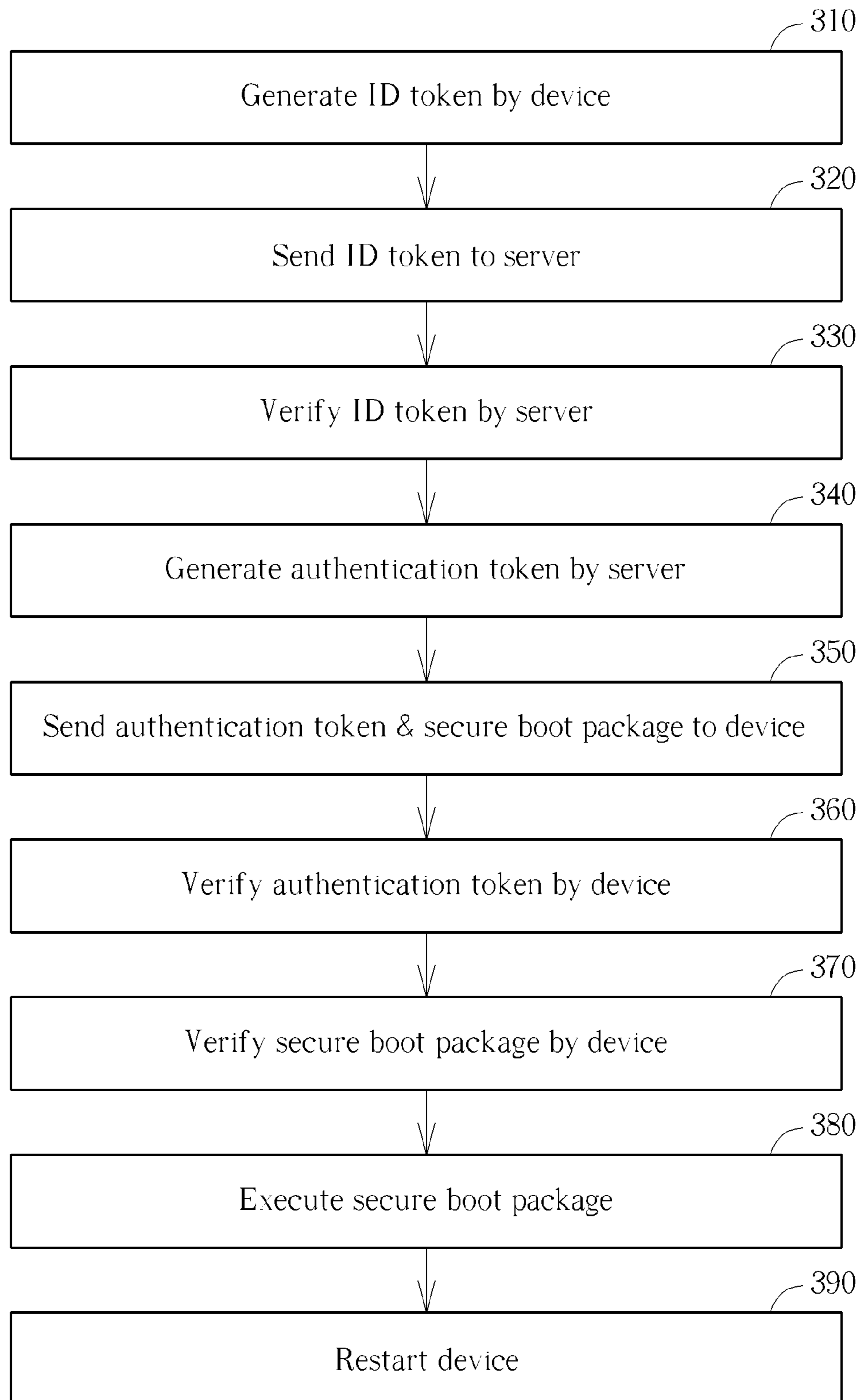


FIG. 3

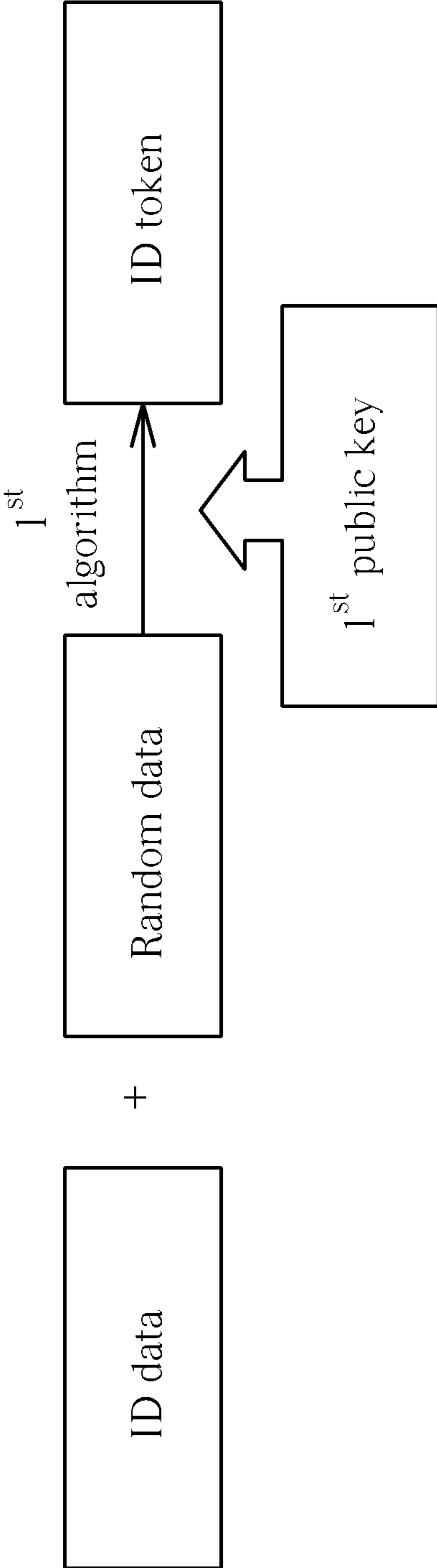


FIG. 4

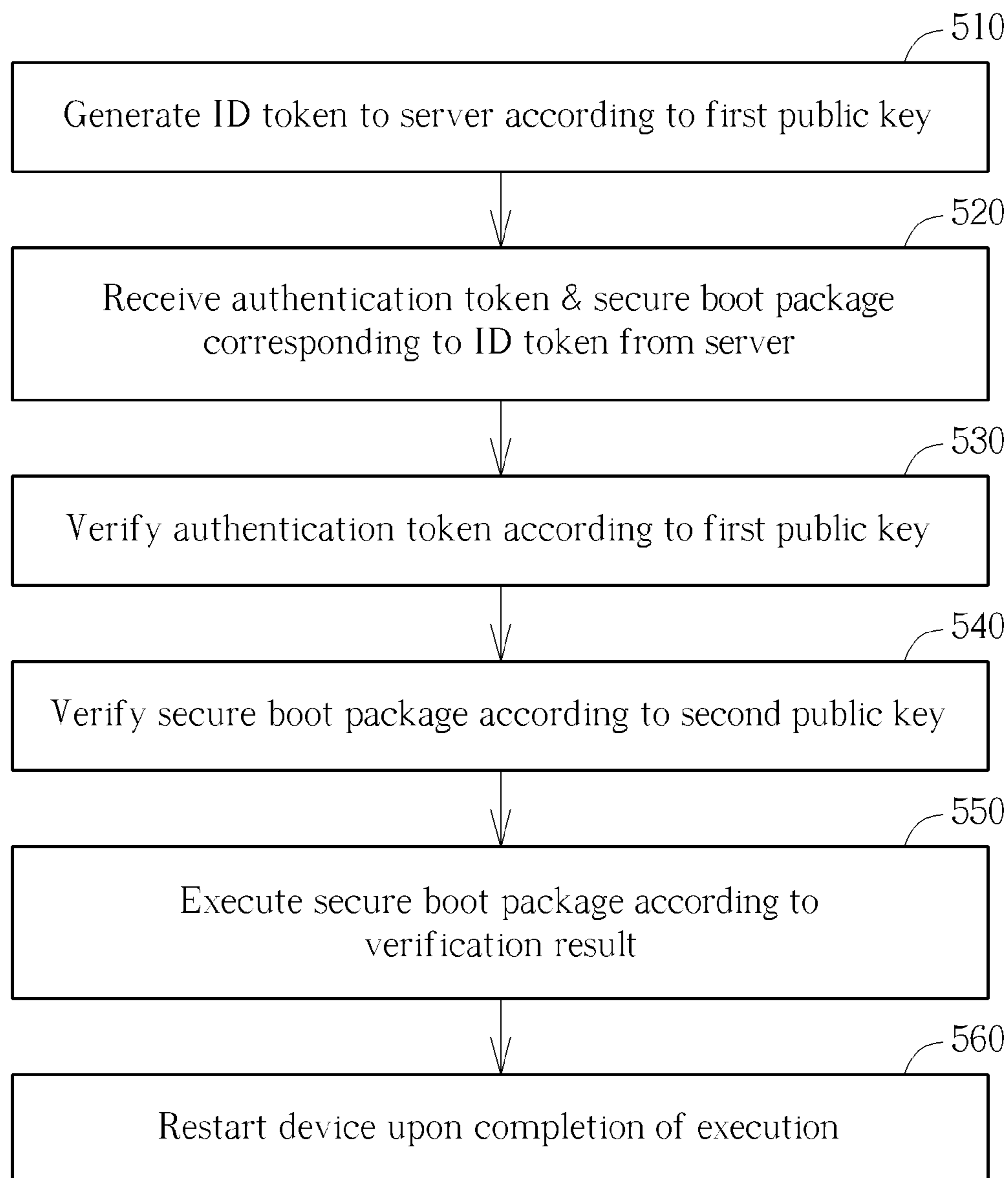


FIG. 5

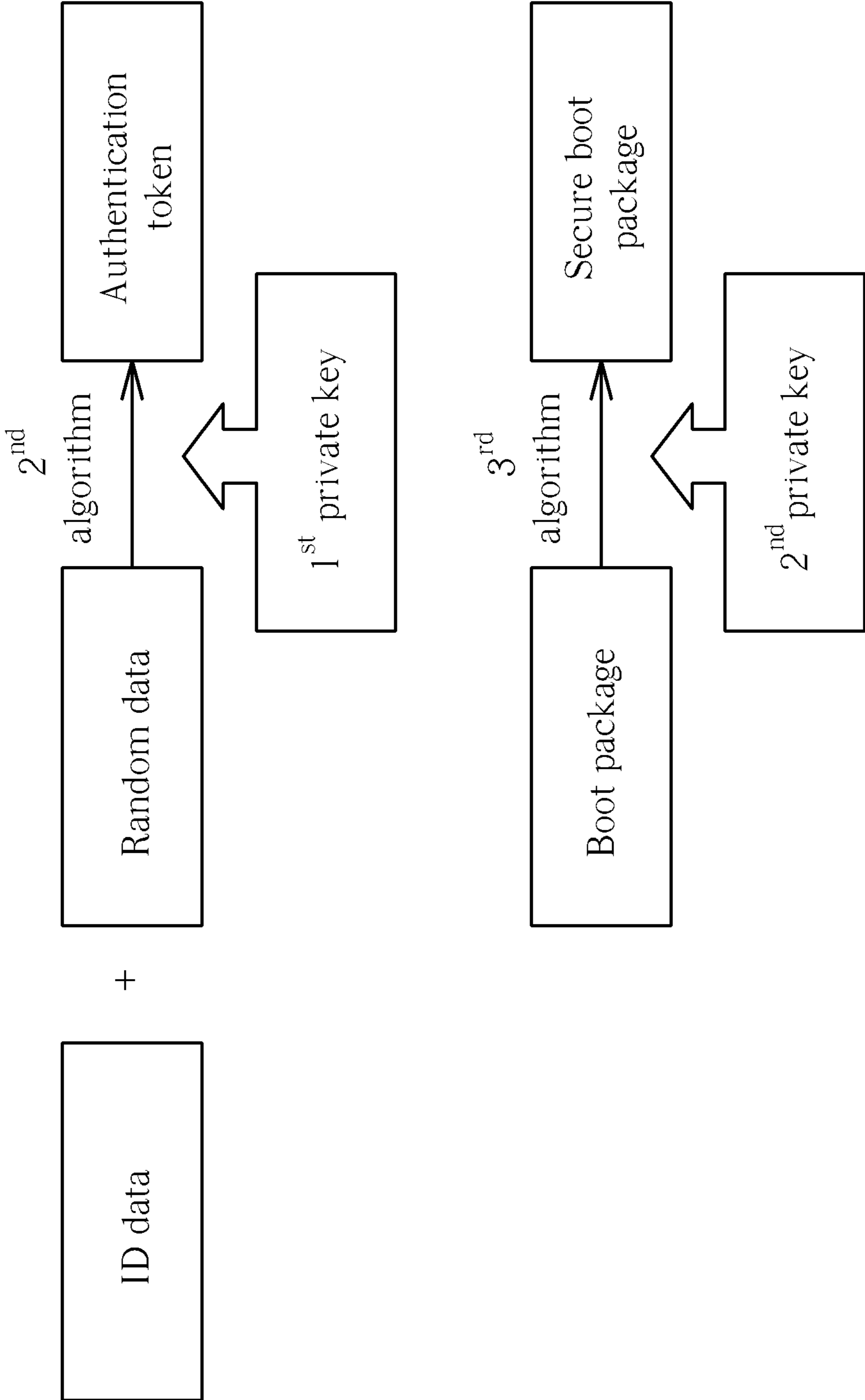


FIG. 6



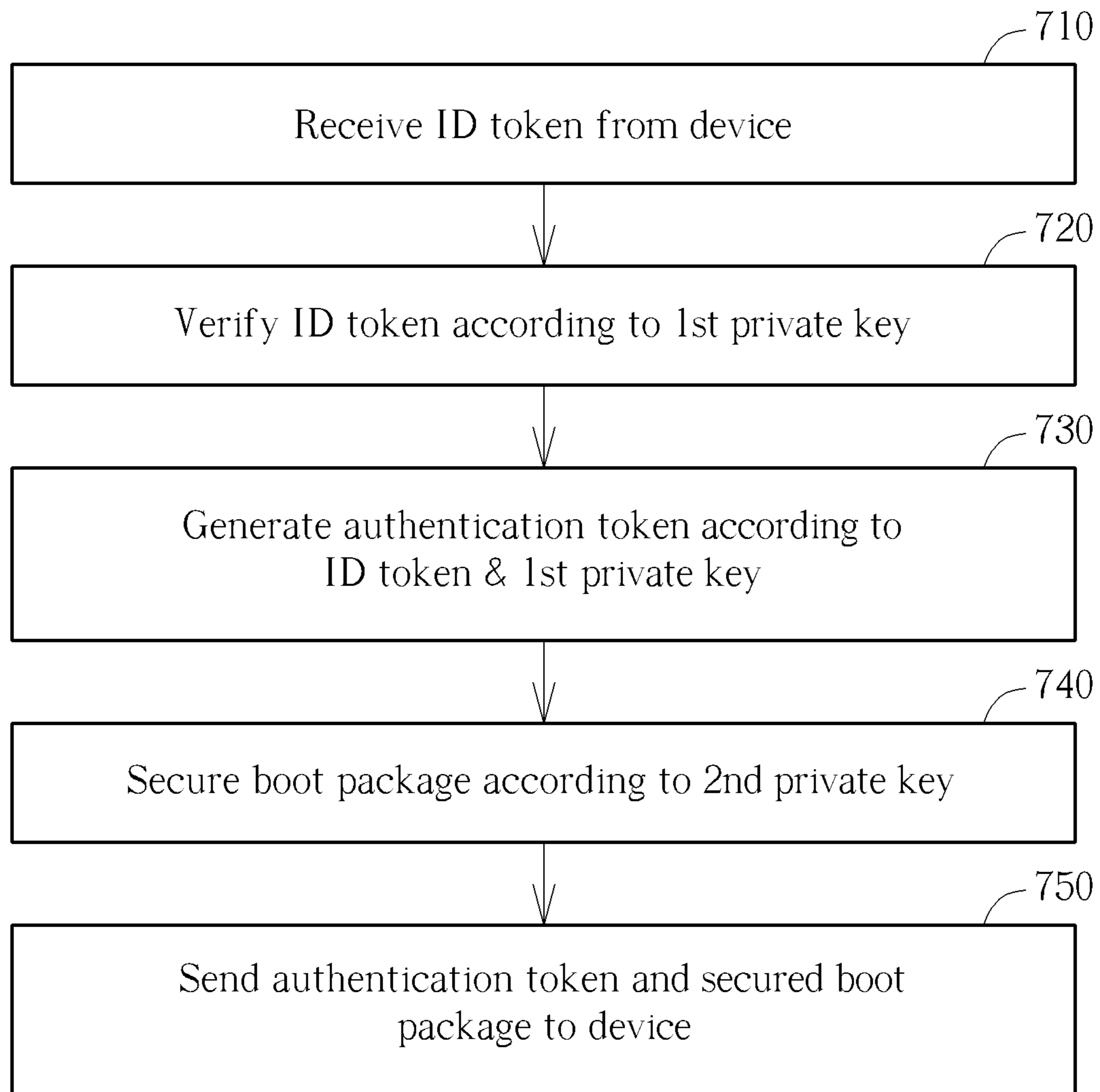


FIG. 7

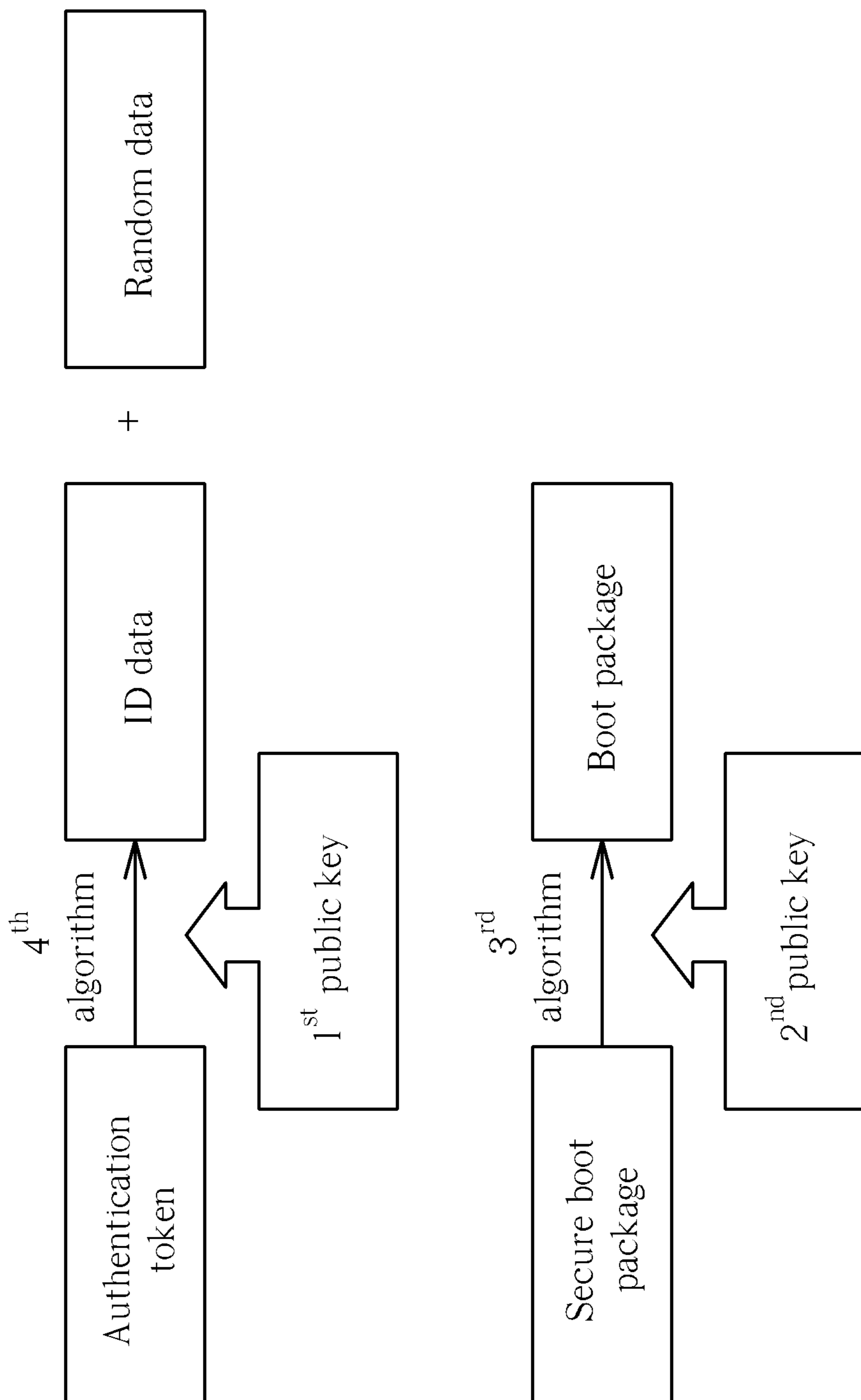


FIG. 8

# SYSTEM AND METHOD FOR TEMPORARY SECURE BOOT OF AN ELECTRONIC DEVICE

## CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority of U.S. Provisional No. 61/565,955 filed on Dec. 1, 2011.

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

The invention relates to system and method of temporary secure boot process of an electronic device. More particularly, the invention relates to a temporary secure boot process by use of unique device information.

### 2. Description of the Prior Art

Electronic devices are installed with an operating system. Normally in a boot up process, a bootloader would initiate components of the electronic device and load the operating system so that a user may operate the electronic device to perform various functions. Some user specific data or user-installed programs are also controlled by the operation system. However, when the electronic device encounters error or is sent to the care center for examination, user might not wish to reveals personal data/files during examination, or the electronic device may not be able to boot up as normal.

## SUMMARY OF THE INVENTION

The invention discloses system and method of temporary secure boot process of an electronic device. A method of temporary secure boot process according to an embodiment of the invention comprises: generating a first token according to an identification data of the electronic device; sending a request along with the first token to a service provider, the request corresponding to a boot package; receiving a second token and a boot package from the service provider; verifying the second token and the boot package; and executing the boot package according to verification result.

Another embodiment of the invention comprises: an electronic device, configured to execute at least an operating system by a processor. The processor comprises: a token generator, configured to generate a first token according to a first key; a token verification unit, configured to verify a second token according to the first key of a first key pair; a boot package execution unit configured to execute a secure boot package according to the verification of the second token; and a key pair unit configured to store at least the first key, the first key being one key of a first key pair. The system further comprises a communication interface unit within the electronic device configured to transmit the first token and receive the second token and the secure boot package; and a service provider configured to verify the first token and to generate the second token according to a second key of the first key pair and the secure boot package according to a third key of a second key pair according to the verification of the first token.

Yet in another embodiment of the invention discloses method for boot package processing. The method comprises: receiving a first token along with a request from an electronic device; verifying an identity of the electronic device according to the first token; in response to the identity being confirmed, generating a second token comprising at least partial content of the first token; securing a boot package corre-

sponding to the request by the second token; and sending the second token and the secured boot package to the electronic device.

These and other objectives of the present invention will no doubt become obvious to those of ordinary skill in the art after reading the following detailed description of the preferred embodiment that is illustrated in the various figures and drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a data authentication system according to an embodiment of the invention.

FIG. 2 illustrates a block diagram of the electronic device according to an embodiment of the invention.

FIG. 3 illustrates a secure boot method according to an embodiment of the invention.

FIG. 4 illustrates identification token generation according to an embodiment of the invention.

FIG. 5 depicts an embodiment of boot package processing flow according to an embodiment of the invention.

FIG. 6 illustrates embodiment of authentication token and secure boot package generation according to an embodiment of the invention.

FIG. 7 illustrates embodiment of secure boot package processing flow of the service provider of the invention.

FIG. 8 depicts an embodiment of boot package verification flow of the electronic device of the invention

## DETAILED DESCRIPTION

The invention discloses system and method for temporary secure boot processing of an electronic device. The electronic device may send request to a service provider for providing a boot package that can only be executed temporarily. To ensure security of the request, the electronic device may generate a token along with the request. In response to the request, the service provider may verify the token to determine identity of request sender. Once confirmed, the service provider sends a secure boot package along with another token. The electronic device also verifies the token and the secure boot package to confirm the identity of the service provider. The electronic device and the service provider may generate the tokens according to particular information held by the two parties only. In addition, to avoid such information being stolen by malicious party, the electronic device may process the request and the token in a secure domain that cannot be accessed by unauthorized user.

Please refer to FIG. 1, which illustrates a secure boot processing system according to an embodiment of the invention. As illustrated, the system comprises an electronic device **100** and a service provider **200**. The electronic device **100** may be a handheld device such as mobile phone, tablet, game console, PDA, and/or other kinds. The electronic device **100** may also be a personal computer, desktop computer, laptop computer. In some circumstances, user might wish to boot up the electronic device **100** without affecting operating system or revealing personal data, for example the electronic device is sent to care center for inspection. User might lock the electronic device **100** with some security mechanism, such as password or unlock pattern. In order to preserve privacy of user but still be able to inspect the functionality of the electronic device **100**, another boot package may be executed temporarily in a secure domain and be removed upon completion of execution. To obtain the temporary boot package, the electronic device may send a request to the service provider **200** for downloading the temporary boot package, such as

manufacturer of the electronic device **100**. The electronic device **100** may send an identification (ID) token which contains unique information corresponding to the electronic device **100** along with the request to the service provider **200**. The request and the ID token may also be stored in a memory device, such as SD or micro SD card, and be transmitted to the service provider via another electronic device, such as a personal computer. User may communicate with the service provider **200** through the other electronic device, for example logging on the service provider and uploading the ID token via a personal computer.

The service provider **200** may verify identity of the electronic device **100** and record the activity for security reason. In response to the request and confirmation of the ID token, the service provider **200** may send back a secure boot package along with an authentication token to the electronic device **100**. The authentication token is also verified by the electronic device **100** so as to confirm the identity of boot package sender. Once confirmed, the electronic device **100** may execute the boot package temporarily and reboot by normal procedure when the execution of the boot package finishes. Similarly, the boot package and the authentication token may be received by the other electronic device that sends the request and be stored in a storage device that can be accessed by the electronic device **100**. For example, when the service provider **200** verifies the ID token sent by a logged-in user, the user then may access the secure boot package and the authentication token by downloading them and storing in the SD/micro SD card or hard-disk memory of a personal computer. The electronic device **100** can access the files from the SD or micro SD card or by connecting to the personal computer via USB connection.

Next please refer to FIG. 2, which illustrates a block diagram of the electronic device **100** according to an embodiment of the invention. The electronic device **100** comprises, among others, a processor **110** and a communication interface **170**. The processor **110** is configured to execute at least an operating system and a plurality of applications in normal domain (not shown) and private programs in a secure domain **120**. The secure domain **120** may be configured to execute applications and/or programs with security demand. In the embodiment of the invention, the secure domain **120** may comprise, among others, a token generator **130**, a token verification unit **140**, a boot package execution unit **150**, and a key pair unit **160**. The token generator **130** is configured to generate the ID token sent to the service provider **200**, and the token verification unit **140** is configured to verify the authentication token received from the service provider **200**. The token generator **130** generates the ID token from unique information of the electronic device **100**, such as identification data. The identification data may be device serial number, IMEI number, MAC address, IMSI number, and/or other information that is unique and can be used to specify the electronic device **100**. Furthermore, to provide better security, the ID token is generated by combining other data generated in random. The unique information and the random data may be processed by a predetermined algorithm and secured by a key that is known to the electronic device **100** and the service provider **200** only. The predetermined algorithm may be an encryption algorithm known in the art.

The token verification unit **140** verifies the authentication token according to another predetermined algorithm, which may be a decryption algorithm known in the art. Both the electronic device **100** and the service provider **200** may possess at least one pair of keys used for encryption and decryption. The key pair is stored in the key pair unit **160**. The keys may be stored during manufacturing stage or obtained by a

secure procedure, and different electronic device **100** may hold different pair of keys. The key pair may be RSA public and private key pair. The electronic device **100** holds the public key while the service provider **200** holds the private key. The ID token may be generated by encrypting the identification data and the random data by the public key of the electronic device **100**, and be verified by the service provider **200** by using the private key for decryption. Therefore, the token generator **130** and the service provider **200** may share corresponding pair of algorithms for encryption and decryption respectively. Similarly, the token verification unit **140** shares corresponding pair of algorithms for decryption with the service provider **200**. Details of the token generation and verification will be described later.

The boot package execution unit **150** is configured to execute the boot package received from the service provider **200** upon verification of the authentication token being confirmed. To provide better security, the boot package may be further secured by a key, and the boot package execution unit **150** may verify the secure boot package prior to execution. In this case, as described above, the boot package execution unit **150** may access corresponding key in the key pair unit **160** and use corresponding algorithms for boot package protection. Similar to the tokens, the service provider **200** may secure the boot package by signing or encrypting with a private key and the boot package execution unit **150** may verify the secure boot package by corresponding public key. For example, the boot package may be signed with a signature generated from the private key of the service provider **200**. The boot package may be designated to perform specific tasks, such as file system backup, customization, system check and/or others. The electronic device **100** may send request of particular boot package for specific purpose.

The electronic device **100** also comprises a communication interface **170** which is configured to communicate with the service provider **200**. The communication interface may transit the ID token, authentication token and boot package between the electronic device **100** and the service provider **200** via suitable transmission protocol. The transmission protocol may be wired or wireless protocol. The communication interface **170** may be configured to communicate with another electronic device, such as a personal computer. The tokens and boot package are transmitted between the electronic device **100** and the service provider **200** via the other electronic device. For example, the communication interface may be a USB interface or memory interface.

FIG. 3 illustrates a secure boot method according to an embodiment of the invention. The method may be implemented by the system shown in FIG. 1. The method starts from generating an ID token by the electronic device **100** in step **310**. The ID token is generated according to some unique data possessed by the electronic device **100** and encrypted by one key of a first key pair. Then the ID token is sent from the electronic device **100** to the service provider **200** in step **320**. The ID token may be attached to a request for demanding a boot package or combined within the request. The service provider **200** may verify the ID token to confirm identity of requesting device and whether it is reliable (step **330**). The ID token may be verified by another key of the key pair. In response to confirmation of the ID token, the service provider **200** generates an authentication token which comprises information that should be verified by the receiver (i.e. the electronic device **100** in this embodiment) in step **340**. Then the service provider **200** sends the authentication token along with secure boot package to the electronic device **100** (step **350**). The authentication token may be generated from the content within the ID token and encrypted by another key of

## 5

the first key pair. In other embodiments, the authentication token may further comprise other information that needs to be verified by the receiver and be processed by other operations, such as SHA. Upon receiving the authentication token, the electronic device first verifies the authentication token in step 360. Similarly, the authentication token may be verified by the key held by the electronic device 100. The electronic device 100 also verifies the secure boot package according to a key, which may be one of another key pair shared by the electronic device 100 and the service provider 200 (step 370). If both the authentication token and the secure boot package are confirmed, the secure boot package is executed in a secure domain for temporarily booting up the electronic device 100 to perform specific task in step 380. Upon completion of the execution of the secure boot package, the electronic device 100 will be restarted by normal boot procedure in step 390. While restarting, the secure boot package may be erased from the electronic device 100 and thus cannot be executed again.

In below token generations and verifications will be described in further details. FIG. 4 illustrates identification token generation according to an embodiment of the invention. As shown in FIG. 4, the identification token is generated from identification data of the electronic device 100 and random data. The identification data may be device serial number, IMEI number, MAC address, IMSI and/or other data that is unique and can be used to identify the electronic device 100. The random data can only be used for once to ensure security. The random data may also be used to hide the identification data from stealing. In one embodiment of the invention, the length of the random data is longer than the identification data. Therefore, identification token of each request would be different for each request and is only valid to corresponding request. The ID data and random data are processed by a first algorithm according to a first public key of a key pair. For each key pair, a public key is held by the electronic device 100 and the private key is held by the service provider 200. The electronic device 100 may not know the private key, but it can be verified by the public key as known in the art. The first algorithm may be any kind of encryption algorithm, such as RSA encryption.

Next please refer to FIG. 5, which depicts an embodiment of boot package processing flow of the electronic device 100. The processing flow starts from step 510, an identification token is generated according to a first public key and sent to the service provider 200 along with a request for boot package. The ID token may be generated according to FIG. 4. The first public key is one of a key pair comprising the first public key and a corresponding first private key. The first public key is held by the electronic device 100 and the first private key is held by the service provider 200. One or more key pairs may be shared by the electronic device 100 and the service provider 200. Next an authentication token and a secure boot package corresponding to the ID token are received from the service provider 200 (step 520). The ID token, authentication token and the secure boot package may be transmitted via wireless protocol and/or accessed via a storage device. For example, the authentication and the secure boot package may be downloaded and stored in an SD card or micro SD card. The electronic device 100 then verifies the authentication token according to the first public key in step 530. The authentication token may be verified by decrypting the authentication token by the first public key and confirming the content within. Upon confirmation of the authentication token, the electronic device next verifies the secure boot package according to a second public key in step 540. Similarly, the second public key may correspond to a second private key used to sign or encrypt the secure boot package. Next the

## 6

secure boot package is executed according to the verification result in step 550. If the verification fails, the secure boot package would not be executed and be discarded. If verification is successful, the secure boot package is executed in a secure domain of the electronic device 100. Upon completion of the boot package execution, the electronic device 100 is restarted by normal boot-up procedure and enters the operating system. The identification token and secure boot package may be erased from the electronic device 100. Please note that the random data used to generate the ID token will be cleared as well and cannot be used again.

FIG. 6 illustrates embodiment of authentication token and secure boot package generation of the service provider 200. As described above, authentication token is generated upon confirmation of ID token received from the electronic device 100. Content of the ID token may be used to generate the authentication token so that it can only be verified by the sender of the ID token. In this embodiment, ID data and random data of the electronic device 100 is used to generate the authentication token according to a second algorithm and a first private key. The first private key is in pair with the first public key of FIG. 4, and the second algorithm may be any kind of encryption algorithm as well. In another embodiment of the invention, other data may be combined into the authentication token as well, for example other data that need to be verified. Yet in another embodiment of the invention, the content of the authentication token may be preprocessed before encryption, such as hash operation. The boot package requested by the electronic device 100 is processed by a third algorithm and a second private key to generate a secure boot package too. The second private key is in pair with a second public key held by the electronic device 100 and the third algorithm may be any suitable encryption/compression algorithm or used as a signature. In the embodiment of FIG. 4 and FIG. 6, the key pair may be distributed to the electronic device 100 during manufacturing stage or be requested by certain secure registration procedure to the service provider 200, and be stored in a secure memory that can only be accessed in secure domain.

FIG. 7 illustrates embodiment of secure boot package processing flow of the service provider 200 of the invention. First, an ID token along with a request is received by the service provider 200 in step 710. The request may demand for a boot package of a specific task. Prior to sending the boot package, the ID token is verified according to a first private key in step 720. The ID token comprises information of the request sender's identity and should be generated by a first public key in pair with the first private key. Furthermore, the ID token may be checked to confirm whether the request sender is associated with the service provider 200, for example manufactured by the service provider 200, registered to the service provider 200, and/or other relationships. The service provider 200 may also record an event corresponding to the request. The event may comprise information of the identity of requesting device, time of request received, type of request and confirmation result, etc.

In response to the identification token is confirmed, the service provider 200 generates an authentication token according to content of the ID token and the first private key in step 730. To make sure the response from the service device 200 is sent to the right requesting device, the authentication token may comprise the ID data and the random data within the ID token so that it can only be verified by the requesting device that generates these data. To provide better protection, the ID data and random data may be pre-processed by operations such as hash operation prior to encrypting by the first private key. In other embodiment of the invention, the authen-

7

tication token may also comprise other information that is necessary. Then the boot package corresponding to the request is secured according to a second private key in step 740. The boot package may be signed with a signature generated by the second private key for example. The authentication token is then sent to the requesting device along with the secured boot package in step 750. In one embodiment of the invention, the token and secured boot package may be sent via wireless protocol. In another embodiment of the invention, the authentication token and boot package may be stored in a storage device that can be accessed by the electronic device 100, such as an SD card.

FIG. 8 depicts an embodiment of boot package verification flow of the electronic device 100 of the invention. Upon receiving the authentication token and the secure boot package, the electronic device 100 needs to verify both of them prior to execution so that it can be ensured the boot package is received from a trusted service provider. The authentication token is processed by a fourth algorithm according to a first public key. The fourth algorithm may be a decryption algorithm corresponding to the second algorithm of FIG. 6, and the first public key is in pair with the first private key. As a result, the authentication token may be decrypted into identification data and random data. The electronic device 100 may compare the decrypted identification data with its own identification to confirm the authentication token is sent from the service provider and it is the right recipient. The decrypted random data may also be compared with the random data of FIG. 4. The secure boot package is processed by a fifth algorithm according to a second private key to confirm the boot package. The fifth algorithm may be a decryption/decompression algorithm corresponding to the third algorithm of FIG. 6 and the second public key is in pair with the second private key. Please note that the public key of the key pairs is held by the electronic device 100 and the private key is held by the service provider 200. In yet another embodiment of the invention, the second key pair may be encrypted within the authentication token and the electronic device 100 can only obtain the second public key in response to confirmation of the authentication token. In the case that the service provider provides boot packages to multiple electronic devices 100, the key pair is different for each electronic device. The algorithms and keys used for token generation and verification may be stored in a secure domain of the electronic device 100 during manufacturing stage or be requested by certain registration process.

In one embodiment of the invention, the electronic device may be a handheld device such as smart phone, tablet, game console, PDA, multimedia player and/or other devices. In one embodiment of the invention, the temporary secure boot process may be initiated by specific user input, such as long press of power button and home key during device boot up. Yet in another embodiment of the invention, the temporary secure boot process may be executed by a boot loader in a secure domain or other software implemented by TrustZone technology, the tokens and boot package may be transmitted via wireless transmission or via hardwire connection to a storage device, such as SD card, USB external memory, etc.

Those skilled in the art will readily observe that numerous modifications and alterations of the device and method may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.

What is claimed is:

1. A method of temporary secure boot process of an electronic device, comprising:

8

generating a first token according to an identification data of the electronic device;  
 sending a request along with the first token to a service provider, the request corresponding to a boot package;  
 receiving a second token and the boot package from the service provider;  
 verifying the second token and the boot package; and  
 executing the boot package according to verification result;  
 wherein the generating of the first token comprises:

generating random data; and  
 encrypting the identification data and the random data according to a first key.

2. The method of claim 1, further comprising:  
 upon completion of the execution, erasing the boot package and then restarting the electronic device.

3. The method of claim 1, wherein the verifying of the second token and the boot package comprises:  
 decrypting the second token by the first key;  
 confirming content of the second token with the identification data; and

in response to the second token being confirmed, verifying the boot package by a second key.

4. The method of claim 3, further comprises clearing the random data from the electronic device.

5. The method of claim 1, wherein the identification data is one of the following: device serial number, IMEI number, MAC address and IMSI number.

6. The method of claim 1, wherein the executing of boot package is executed in a secure domain of the electronic device.

7. A system for temporary boot up process, comprising:  
 an electronic device, configured to execute at least an operating system by a processor, the electronic device comprises:

a token generator, configured to generate a first token by encrypting an identification data of the electronic device and a random data according to a first key;

a token verification unit, configured to verify a second token according to the first key of a first key pair;

a boot package execution unit, configured to execute a secure boot package according to the verification of the second token; and

a key pair unit, configured to store at least the first key, the first key being one key of a first key pair.

8. The system of claim 7, further comprising:  
 a communication interface unit within the electronic device, configured to transmit the first token and receive the second token and the secure boot package; and

a service provider, configured to verify the first token and to generate the second token according to a second key of the first key pair and to generate the secure boot package according to a third key of a second key pair according to the verification result of the first token.

9. The system of claim 7, wherein the service provider is further configured to generate the second token by encrypting content of the first token according to the second key, and to generate the secure boot package by signing a boot package with the third key.

10. The system of claim 7, wherein the boot package execution unit is further configured to verify the secure boot package according to a fourth key of a second key pair.

11. The system of claim 10, wherein the first key pair is a RSA key pair, the first key is a public key and the second key is a private key; the second key pair is another RSA key pair, the fourth key is a public key and the third key is a private key.

9

12. The system of claim 10, wherein the fourth key is encrypted within the second token by the service provider, and is obtained by the electronic device by decrypting the second token.

13. The system of claim 7, wherein the secure boot package is downloaded into a storage device accessible by the electronic device.

14. The system of claim 7, wherein the processor is further configured to erase the secure boot package and restart the electronic device upon execution completion of the secure boot package, and execute the operating system.

15. The system of claim 7, wherein the token generator, the token verification unit, the boot package execution unit and the key pair unit are implemented in a secure domain of the electronic device, the secure domain is unable to be accessed by the operating system.

16. A method for boot package processing, comprising:  
receiving a first token along with a request from an electronic device;

10

verifying an identity of the electronic device according to the first token;

in response to the identity being confirmed, generating a second token comprising at least partial content of the first token;

securing a boot package corresponding to the request; and sending the second token and the secured boot package to the electronic device;

wherein the step of verifying the identity of the electronic device further comprises decrypting the first token to obtain an identification data of the electronic device and a random data according to a second key of a first key pair,

wherein the first token is generated by a first key of the first key pair.

17. The method of claim 16, wherein the step of generating the second token further comprises encrypting at least the identification data and the random data by the first key.

\* \* \* \* \*