Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2510366 A1 2006/12/14

(21) 2 510 366

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2005/06/21

(41) Mise à la disp. pub./Open to Public Insp.: 2006/12/14

(30) Priorité/Priority: 2005/06/14 (US60/690,155)

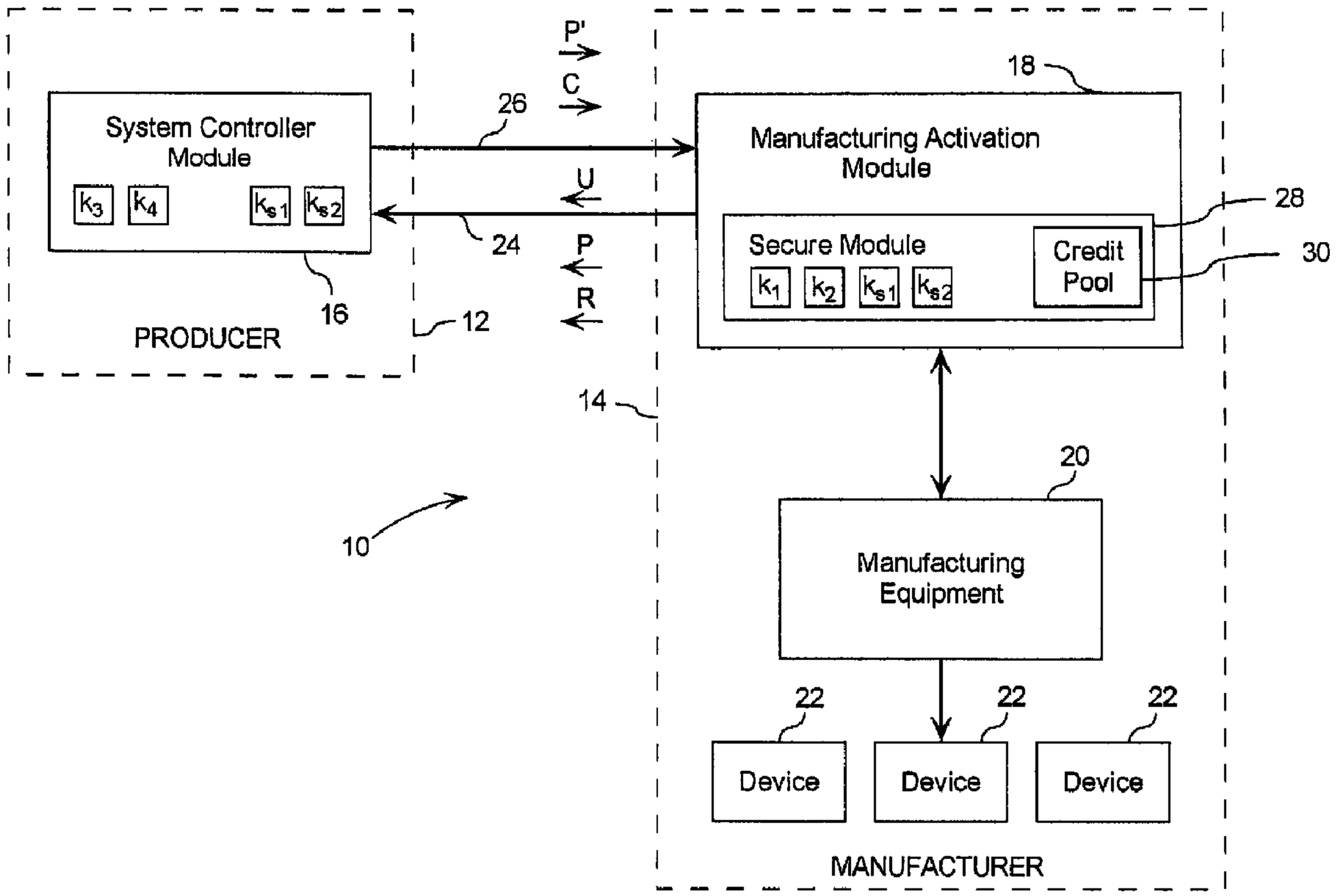
(51) Cl.Int./Int.Cl. *H04L 9/12* (2006.01),
H04L 9/00 (2006.01)

(71) Demandeur/Applicant:
CERTICOM CORPORATION, CA

(72) Inventeurs/Inventors:
NEILL, BRIAN, CA;
VADEKAR, ASHOK, CA;
XU, PATRICK, CA

(74) Agent: BLAKE, CASSELS & GRAYDON LLP

(54) Titre : SYSTEME ET METHODE D'ENREGISTREMENT A DISTANCE D'UN DISPOSITIF
(54) Title: SYSTEM AND METHOD FOR REMOTE DEVICE REGISTRATION



(57) Abrégé/Abstract:
A system and method for remote device registration, to monitor and meter the injection of keying or other confidential information onto a device, is provided. A producer who utilizes one or more separate manufacturers, operates a remote module that communicates over forward and backward channels with a local module at the manufacturer. Encrypted distribution images are sent by producer to the manufacturer and are decrypted and used in the production of devices. As distribution images are decrypted, credits from a credit pool are depleted and can be replenished by the producer through credit instructions. As

CA 2510366 A1 2006/12/14

(21) 2 510 366

(13) A1

(57) Abrégé(suite)/Abstract(continued):
distribution images are decrypted, usage records are created and eventually concatenated, and sent as usage reports back to the producer, to enable the producer to monitor and meter production at the manufacturer.

ABSTRACT

A system and method for remote device registration, to monitor and meter the injection of keying or other confidential information onto a device, is provided. A producer who utilizes one or more separate manufacturers, operates a remote module that communicates over forward and backward channels with a local module at the manufacturer. Encrypted distribution images are sent by producer to the manufacturer and are decrypted and used in the production of devices. As distribution images are decrypted, credits from a credit pool are depleted and can be replenished by the producer through credit instructions. As distribution images are decrypted, usage records are created and eventually concatenated, and sent as usage reports back to the producer, to enable the producer to monitor and meter production at the manufacturer.

SYSTEM AND METHOD FOR REMOTE DEVICE REGISTRATION

FIELD OF THE INVENTION:

[0001] The present invention relates generally to device registration, and particularly to registering end-user devices from remote locations during production thereof.

DESCRIPTION OF THE PRIOR ART

[0002] A device that participates in a cryptographically secure communication system, will typically have some type of unique and immutable information that was injected into the device at the time of manufacturing. This information could be a cryptographic key, a shared secret or some other data that may be cryptographically bound to an inherently unique attribute of the device. This injection of information is sometimes referred to as "keying" the device.

[0003] The purpose of this injected information is to ensure that the device is accepted as an authentic participant of the secured communication system at some point in the future, after the device has been distributed. The injected information enables a customer or user of the device to avoid tedious procedures required to register the device. The device may be granted access to a system based on cryptographic authentication that the information is trusted. This trust is based on the fact that it is exceptionally difficult to reproduce the trusted data outside of the manufacturing process.

[0004] These systems rely on the manufacturing process and the Original Equipment Manufacturer (OEM) to provide a root of trust for the devices, and ultimately for the entire secure communication system.

[0005] In a modern business climate comprising ever-increasing device complexity and sophistication, it is not uncommon for individual parts to be manufactured and keyed by one manufacturer for later assembly by another manufacturer. In such a situation there exists certain security implications when the producer of the device or the owner of the communication system

is not the device manufacturer. It can therefore be paramount for a device producer to ensure the integrity of the manufacturing systems that are responsible for the integrity of the producer's device.

[0006] When considering the integrity of the manufacturing process, of particular concern are issues related to the confidentiality of secret information that is used to manufacture the device, as well as ensuring that the manufacturer correctly reports the identities and the number of units manufactured to the producer. The device producer needs to obtain assurances that a manufacturer is not creating and distributing "black market" parts or devices.

[0007] Traditionally, a producer that is concerned about securing the information injection stage at a manufacturing site has little choice but to implicitly trust that a manufacturer is operating in a manner that gives due consideration to the producer's device and system security. Protective mechanisms are generally naïve, in that keying information is typically bulk encrypted and sent to the manufacturer, where, upon arrival, all of the keying information is decrypted at once, and the manufacturer is then trusted not to compromise the bulk of information.

[0008] One method to restrict access to keying information is to use an on-line client-server mechanism. With such a mechanism in place, the client at the manufacturer's facility would be connected to a network, and would make requests for keying information on a per-device basis, to a remote key-providing server under the control of the producer.

[0009] There are a number of problems with implementing a manufacturing system that relies on an off-site, remotely networked server, that provides keying information on such a just-in-time basis. The foremost problem is that an off-site server can not guarantee a minimal service level or response time to the manufacturing line if it uses a public shared packet-switched network. To prevent problems in the manufacturing line, the link should guarantee a certain level of service in terms of latency and through-put. Given modern manufacturing realities, where production lines exist in remote jurisdictions relative to the producer, such guaranteed network availability can be prohibitively expensive.

[0010] A manufacturing facility will typically not begin a production run without all of the necessary materials on hand, including data materials. Otherwise, the risk to production line delays would be too high. Any keying system used by a manufacturer, should be able to guarantee service availability and provide a suitable response. This requires local availability of all data resources and keying information before commencement of a production run.

[0011] Given that all data resources must be locally available to a production line, possibly existing on computer systems, and media that is not under direct control of the producer; the producer must consider how to ensure the confidentiality of any secret keying information.

[0012] Enough data must be locally available to commence and complete a production run. This typically entails a large repository of data to be sent in advance to the manufacturer, by the producer. In the event that the producer discovers unauthorised and contractually objectionable behaviour by the manufacturer, the producer should also consider how to prevent such a rogue manufacturer from producing black-market product, after the termination of a contract, using pre-stored keying information.

[0013] The above issue regarding objectionable behaviour on the part of the manufacturer highlights the main problem faced by the producer of the device. Once keying information is released to a manufacturer, the producer should still be able to control access to the information and enforce accurate reporting of its use. Any solution to such a problem should be able to detect and react to unauthorised manufacturing activity and be tamper-resistant, so as to thwart efforts by a manufacturer to compromise the system.

[0014] It is therefore an object of the present invention, to provide a system and method for remote device registration that obviates or mitigates at least one of the above-described disadvantages.

SUMMARY OF THE INVENTION

[0015] The present invention provides a system and method that enables a producer who wishes to use a separate entity for at least a portion of the manufacturing process, to monitor production of devices from a remote location.

[0016] In one aspect, the present invention provides a system for remotely registering devices for production thereof, the system comprising a controller module and an activation module remote from each other and connected by forward and backward communication channels, the activation module having a secure module for performing cryptographic operations. The controller module sends cryptographically protected distribution images to the activation module, which are decrypted to obtain data for insertion into the devices, the number of images decrypted by the activation module being metered remotely through control messages sent by the controller module.

[0017] In another aspect, the present invention provides a method for remotely registering devices for production thereof, the method comprising the steps of having a controller module prepare and cryptographically protect a distribution image containing data to be inserted into the devices; the controller module sending the image to at least one activation module, each of the at least one activation module having a secure module for performing cryptographic operations; each secure module extracting the data from the image and co-ordinating the use of the data for insertion into the devices; and the activation module tracking the use of the image and reporting to the controller module; wherein the controller module is located remote from the activation module.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] An embodiment of the invention will now be described by way of example only with reference to the appended drawings wherein:

[0019] Figure 1 is a schematic view of a remote device registration system;

[0020] Figure 2 is a schematic representation of a distribution image;

[0021] Figure 3 is a schematic representation of one implementation of the modules of Figure 1;

[0022] Figure 4 is a flow chart depicting the provisioning procedure of Figure 3;

[0023] Figure 5 is a flow chart depicting the credit instruction procedure of Figure 3;

[0024] Figure 6 is a flow chart depicting the distribution and keying procedure of Figure 3; and

[0025] Figure 7 is a flow chart depicting the reporting procedure of Figure 3.

DETAILED DESCRIPTION OF THE INVENTION

[0026] Referring therefore to Figure 1, a remote device registration or trusted key injection system is generally denoted by numeral 10. A producer 12 of a device 22 utilizes the services of a separate entity, in this case a manufacturer 14, for the injection of unique and immutable information into the devices 22. The information may be a cryptographic key, a shared secret, or some other data that may be cryptographically bound to an inherently unique attribute of the device 22. The producer 12 has a system controller module 16, which is a computer system that is remote to the manufacturer's facility. The system controller module 16 is responsible for packaging and conveying the key information and other information to the manufacturer 14. The system controller module 16 selectively encrypts the keying data, i.e., the keying data is partitioned into per-device data images called distribution images 40, that are described below and shown in Figure 2.

[0027] The manufacturer 14 has a manufacturer activation module 18, which is a computer system that is local to the manufacturer's facility and whose activities are metered through messages sent by the controller module 16.

[0028] The modules 16 and 18 are connected by a forward communication channel 26, and a backward communication channel 24. The channels 24 and 26 may be arbitrary communication channels and are not required to be either reliable or secure. Reliability and security over the channels 24 and 26 are provided using a combination of technical mechanisms and processes/procedures. For example, if a message sent over the forward channel 26 to the module 18 does not decrypt because it is corrupt, a user may phone an operator of the system controller module 16, and have them send the message again.

[0029] The manufacturer 14 also has equipment 20 which is used to inject the cryptographic key data into the devices 22. The manufacturer activation module 18 has a secure module 28 that comprises special trusted hardware that is configured and set-up by the producer 12 and that stores a credit pool 30. The credit pool 30 is an abstract concept representing the number of distribution images 40 that may be decrypted by the secure module 28 before the secure module 28 begins to refuse distribution image requests made by the manufacturer 14.

[0030] A general outline of the procedures used by the system 10 is shown in Figure 3. Firstly, a provisioning procedure is executed to initialize the modules 16, 18 and 28; and to establish the cryptographic keys and identification data used in the transmission of distribution images 40.

[0031] The provisioning procedure is followed by a credit instruction procedure once an initialization has been completed, which involves the transmission of credit instruction files from the controller module 16 to the activation module 18, and is used to maintain the value of the credit pool 30.

[0032] The credit instruction procedure is followed by a distribution and keying procedure which involves the decryption of distribution images 40 and the use thereof for keying the devices 22. Encrypted distribution images 40 and credit instructions, are transmitted by the producer 12 to the manufacture 14 using control messages C, over the forward communication channel 26. The control messages are special encrypted messages that, among other things, instruct the manufacturer activation module 18 to increase or decrease the credit pool 30. Thus,

credit instructions within the control message C are used by the provider 12 to control the value of the credit pool 30.

[0033] The distribution and keying procedure is followed by a reporting procedure, which involves concatenating records into a report by the secure module 28 and sending them to the controller module 16 via the backward channel 24. The activation module 18 is remotely metered by the producer 12, who governs the number of distribution images 40 available for decryption by the secure module 28. As distribution images 40 are decrypted, the credit pool 30 is diminished. Since the credit pool 30 is stored within the secure module 28, it resists tampering. In order to replenish the credit pool 30, the secure module 28 must retrieve a control message C including a positive credit instruction from the controller module 16.

[0034] Usage report messages U are sent by the activation module 18 back to the controller module 16 over the backward communication channel 24. All backward channel messages are generated, encrypted, and signed within the secure module 28. Each message is assigned a predictable identity to prevent data loss and ensure the integrity of the messages.

[0035] The reports are used to determine if the distribution of distribution images 40 should continue. If the process should not be disrupted, the credit instruction procedure may be repeated, otherwise, the manufacturing equipment 20 may be shut down until the problem is resolved.

[0036] With the system 10 in place, a producer 12 can monitor production at a manufacturing facility 14. The producer 12 actively monitors the credit pool 30 to ensure that the manufacturer 14 has a large enough credit pool 30 in order to prevent production delays. However, if the manufacturer 14 acts in bad faith, then the producer 12 has the means to force the manufacturer 14 to discontinue device production by sending a negative-valued credit instruction in a control message C, or by failing to replenish the credit pool 30 any further. This causes the credit pool 30 to diminish to zero, thus shutting down the manufacturing equipment 20.

[0037] The provisioning procedure is shown in greater detail in Figure 4, and is executed in order to initialize the system 10. The secure module 28 produces and sends a provisioning request message P to the controller module 16. This message P preferably contains the serial number of the secure module 28 being used by the activation module 18. The secure module 28 generates two cryptographic key pairs k_1, k_2 (e.g. RSA key pairs or preferably using elliptic curve cryptography (ECC)), one (k_1) for receiving encrypted messages and another (k_2) for signing outgoing messages. Preferably, the manufacturer 14 is cryptographically bootstrapped in a physically controlled environment during this exchange of key pairs k_1 and k_2.

[0038] When the controller module 16 receives the provisioning request from the activation module 18, it checks the integrity of the message and then assigns the manufacturer a "token ID". Two keys, preferably symmetric keys k_{s1} and k_{s2} (e.g. Advanced Encryption Standard (AES) keys), are generated. These keys are to be used by the modules 16 and 18 to protect the distribution images 40 on the forward channel 26 and the usage reports U on the backward channel 24.

[0039] The controller module 16 then generates a provisioning response message P' that, for example, contains the assigned token ID, public keys of the controller module's 16 encryption and signing key pairs k_3 and k_4 respectively, the forward and backward channel symmetric keys k_{s1} and k_{s2}, some initial configuration data, and a hash digest for integrity. Similar to the provisioning request message P, it is assumed that the provisioning response message P' is handled within a physically controlled environment.

[0040] The provisioning response message P' is sent to the activation module 18, and if the controller module 16 has not been initialized, it will perform all required initialization upon receiving its first provisioning request. The structure of the provisioning response may contain a member that decrypts to a separate structure that contains symmetric keys for the forward and backward channel communications between the modules 16 and 18. It shall be noted that these keys are distinct for each secure module 28 (and thus each activation module 18), and are not shared amongst a group of secure modules. Once the provisioning procedure is complete, a normal exchange of distribution images 40 and control messages C can commence.

[0041] The credit instruction procedure is shown in greater detail in Figure 5. The secure module 28 must consume a credit from the credit pool 30 to decrypt a distribution image 40. Over time, the credit pool 30 will diminish and need to be replenished with a credit instruction file sent by the controller module 16.

[0042] The controller module 16 only sends one control message to the activation module 18 at a time. One of the required files contained in this message is a credit instruction file. The file can be an encrypted set of data for a specific activation module 18 that is decrypted by the secure module 28, to a credit instruction. The credit instruction contains, e.g., the serial number of the secure module 28 and/or activation module 18, the module's token ID, a sequence number, new credit amount, and configuration data, that has all been signed by the controller module 16.

[0043] Upon receiving the control message C, the secure module 28 decrypts the credit instruction data from the control message C, and validates the signature. The secure module 28 also validates the serial number and token ID as its own, if applicable. A validation of the sequence number is then performed. The sequence number should be greater than the sequence internally stored in the secure module 28. Once validated, the secure module 28 will update its internal sequence number and set the value of the credit pool 30 to the credit value in the credit instruction.

[0044] The secure module 28 will then process any configuration messages in the control message C to update its internal configuration. Configuration messages are included in both the control messages C, and the provisioning response messages P', in order to enable the controller module 16 to push configuration data to the activation module 18, such as updates for filtering rules, keying information, credit rules etc.. Configuration data can be intended for the secure module 28 or an application running on the activation module 18. The secure module 28 looks for configuration messages of a defined type to process them. Configuration messages can be marked as private or public, and access thereto would then be controlled by the secure module 28.

[0045] A credit report R is the activation module's response to processing a credit instruction in a control message C. The credit report R may contain the serial number and token ID of the

secure module 28, the current sequence value, the current value of the credit pool 30, number of refills to date, and an error code that is set to zero if no errors occurred during credit instruction processing.

[0046] The credit report R is signed by the secure module 28 using its signing key k_2. The report R is then encrypted for the controller module 16 using the controller module's public encryption key k_3. The report R is then sent to the controller module 16.

[0047] The distribution and keying procedure is shown in greater detail in Figure 6. The distribution image 40 is first prepared by the controller module 16. The distribution image 40 is encrypted with a unique image key 42. The image key 42 is then in turn encrypted for selected modules 18 that is metered by the producer 12, and stored as individual headers 48 which are part of a collection 44 of headers 48 stored in a main header 46 of the distribution image 40.

[0048] Figure 2 also shows an exemplary message structure. For example, the distribution image 40 may contain a list of type 50 and data 52 field pairs as a basic filtering mechanism. The type field 50 contains type 58 and ID 60 information and the data field 52 contains size 54 and data 56 information. In such a structure, the data field 52 is an arbitrary byte array of a particular length.

[0049] When it is time for the activation module 18 to decrypt the distribution image 40, the activation module 18 first chooses its particular header 48 from the collection of headers 44 that were pre-appended to the distribution image 40. The header 48 and encrypted distribution image 40 are then decrypted by the secure module 28. Once the secure module 28 has the header 48 and image 40, the header 46 is decrypted using its distribution key to obtain the image key 42. The image key 42 is then used to decrypt the distribution image 40. The distribution image 40 is then validated, e.g., using a secure hashing algorithm, MAC, or digital signature; filtered; and passed back to an application of the activation module 18 in its decrypted and filtered state. The secure module 28 then produces a report record that is secured via cryptographic means, and sends the keying info extracted from the distribution image 40 to the equipment 20 for injection to the devices 22.

[0050] The secure module 28 will stop releasing keying information if the following are true: (a) the credit pool diminishes to a value of zero; or (b) the secure module 28 detects an attempt to compromise the system, due to too many errors in the distribution image decryption and validation. If the distribution of further keying information is permitted, the activation module 18 will continue to receive and process distribution images 40 using the secure module 28.

[0051] The authenticity of distribution images 40 is assumed based on the unique symmetric distribution keys k_{s1} and k_{s2} shared between the modules 16 and 18. The messages can be considered authentic once a successful integrity check is performed, e.g., after a sha-2 digest compare.

[0052] The reporting procedure is shown in greater detail in Figure 7. Usage report messages U are composed of individually encrypted records generated by the secure module 28 that are concatenated into a series of binary files. The file names of these files indicate the date that the usage report message U was created. This individual records, generated by the secure module 28 are encrypted with the backward channel encryption key k_1, and returned to an application of the activation module 18 from the secure module 28. Every distribution image decryption causes a uniquely sequenced record to be created. An operator of the controller module 16 would typically notice an absent record.

[0053] The usage report messages U are sent to the controller module 16 during the reporting process. The controller module 16 is then able to decrypt the individual records contained in the usage report message U, and validate the records. A number of validation checks may occur, the first being a cryptographic check on the validity of each record. Every record may then be decrypted with the backward channel symmetric key specific to the particular secure module 28. A sha-2 digest may then be computed on the contents of the records, and compared to the digest that was appended to the clear-text record created by the secure module 28.

[0054] Every record may also be tagged with a monotonically synchronous number. If all the record ID values, put together, are not a contiguous set, then the operator of the controller module 16 will know to track down the missing records from the particular activation module 18.

[0055] Backward channel records contain a list of applied filtering rules. This information can be saved by the producer 12 for auditing purposes.

[0056] Therefore, by utilizing a remote system controller module 16 separate from the manufacture activation module 18, the producer 12 is able to monitor and meter the activation module 18 and secure module 28, and govern the injection of keying information on the devices 22, in order to ensure that the manufacturer 14 correctly reports the identities and the number of units manufactured for the producer 12. This enables the producer 12 to have assurances that a manufacturer 14 is not creating and distributing black market products or devices 22.

[0057] With the above procedures and system 10 in place, a producer 12 can monitor production at a manufacturer 14. The producer 12, using the credit instructions in the control messages C, can meter the production of devices 22 by adding or removing available credit for use by the manufacturer 14.

[0058] It will be appreciated that the system 10 is not limited to one manufacturer 14 as shown in Figure 1, nor is each manufacturer 14 limited to one set of equipment 20. The system 10 is also not to be limited to the use of a single system controller module 16 used by the producer 12. The secure module 28 is most preferably trusted hardware in order to protect key values and the integrity of the credit pool 30. Moreover, keying information contained in the distribution image 40 does not necessarily have to be keying information, but can also be any data element that requires confidentiality and authenticity. A requirement for keying data is typical of a system 10 which wishes to enforce granularity of device activation.

What is claimed is:

1. A method for remotely registering devices for production thereof, said method comprising the steps of: having a controller module prepare and cryptographically protect distribution images containing data to be inserted into the devices; the controller module sending respective ones of the images to respective ones of at least one activation module, each of the at least one activation module having a secure module for performing cryptographic operations; each secure module extracting respective data from the respective image and co-ordinating the use of the respective data for insertion into the devices; and the activation module tracking the use of the respective images and reporting to the controller module; wherein the controller module is located remote from the activation module.

2. A method according to claim 1, further comprising a provisioning procedure executed prior to the controller module preparing and protecting the distribution image, the provisioning procedure being used to initialize the controller module, the activation module, and the secure module.

3. A method according to claim 2 wherein the provisioning procedure is initiated by having the secure module send a provisioning request to the controller module.

4. A method according to claim 3 wherein the controller module replies to the provisioning request with a provisioning response.

5. A method according to claim 4 wherein the provisioning response contains a token ID assigned by the controller module to identify the respective activation module, public encryption and signing keys of the controller module, and symmetric keys for a forward and a backward channel between the controller module and the activation module.

6. A method according to claim 1 further comprising a credit instruction procedure for establishing a credit value for a credit pool, the credit value representing the number of distribution images from which the secure module can extract data.

7. A method according to claim 6 wherein the credit instruction procedure initiates by having the controller module send a control message file to the activation module, the control message file containing credit instruction data including an updated credit value.

8. A method according to claim 7 wherein the control message is encrypted by the controller module and subsequently decrypted by the secure module upon receipt thereof, the credit instruction data being obtained through the decryption operation.

9. A method according to claim 7 wherein the credit instruction data includes a sequence number, the sequence number being internally updated by the secure module upon extraction thereof.

10. A method according to claim 6 wherein the secure module prepares and encrypts a credit report and sends the credit report to the controller module in response to the control message.

11. A method according to claim 6 wherein upon extracting the data from the distribution image, the secure module consumes a credit from the credit pool, thereby decreasing the credit value by one.

12. A method according to claim 1 wherein the secure module decrypts a header of the distribution image to obtain an image key and uses the image key to decrypt the distribution image to extract the data.

13. A method according to claim 1 wherein upon extracting the data from the distribution image, the secure module generates a report record.

14. A method according to claim 13 wherein upon a plurality of repetitions of the method, successive report records are concatenated into a report and encrypted, the report being sent to the controller module, whereby the report records are decrypted and validated, and a report summary is produced.

15. A system for remotely registering devices for production thereof, the system comprising a controller module and at least one activation module remote from one another, the controller module connected to respective ones of the at least one activation module by forward and backward communication channels, each of the at least one activation module having a secure module for performing cryptographic operations, wherein the controller module sends cryptographically protected distribution images to respective ones of the at least one activation module, which are decrypted by the secure module to obtain data for insertion into the devices, the number of images decrypted by each secure module being metered remotely through control messages sent by the controller module to respective ones of the at least one activation module.

16. A system according to claim 15 wherein the number of images are metered by maintaining a credit pool stored by the secure module, the control messages being used to update the value of the credit pool.

17. A system according to claim 15 wherein the secure module and controller module each contain symmetric keys for the forward and backward communication channels.

18. A system according to claim 15 wherein the secure module and controller module each have respective encryption and signing key pairs.

19. A system according to claim 15 wherein the distribution image has a header containing an image key, the image key being obtained by decrypting the header and the image key being used to decrypt the distribution image to obtain the data.

20. A system according to claim 15 wherein the secure module generates a report record upon extracting the data, successive report records being used to generate a report to send to the controller module.

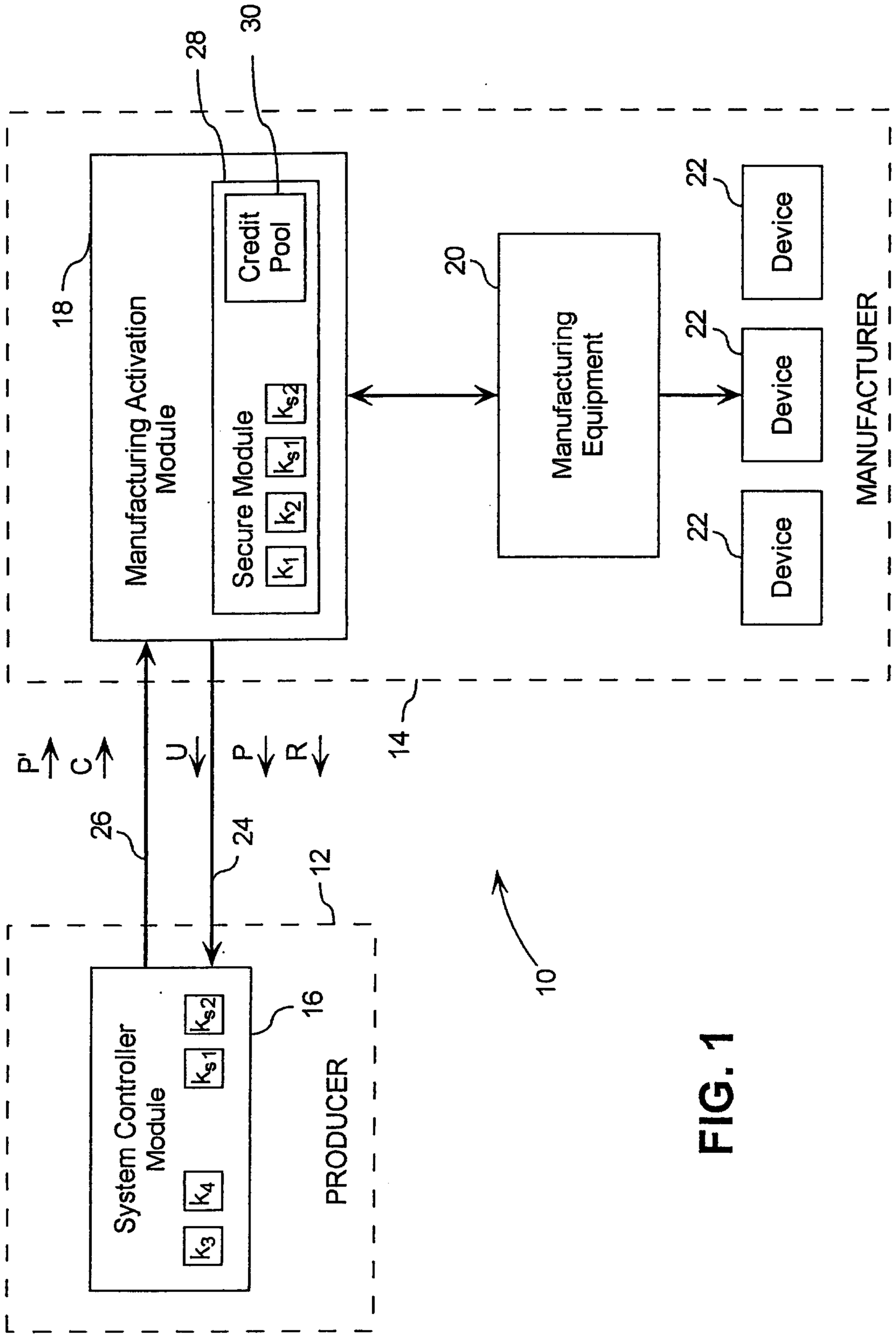

28
30
18
Manufacturing Activation Module
Secure Module
k_1
k_2
k_{s1}
k_{s2}
Credit Pool
20
Manufacturing Equipment
22
Device
22
Device
22
Device
MANUFACTURER
14
P'
C
U
P
R
26
24
12
System Controller Module
k_4
k_3
k_{s1}
k_{s2}
16
PRODUCER
10

FIG. 1

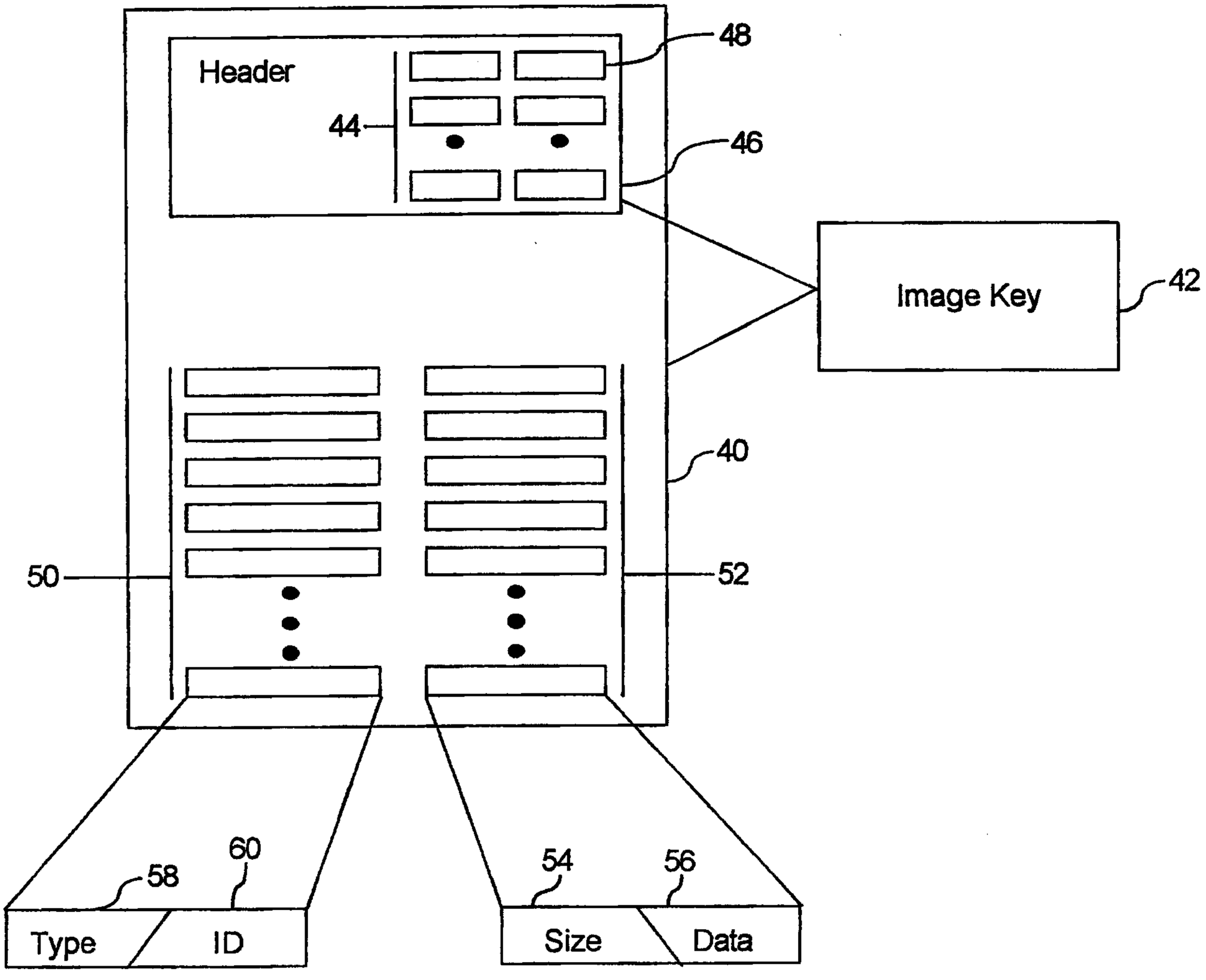

Header
44
48
46
Image Key
42
40
50
52
60
58
54
56
Type
ID
Size
Data

FIG. 2

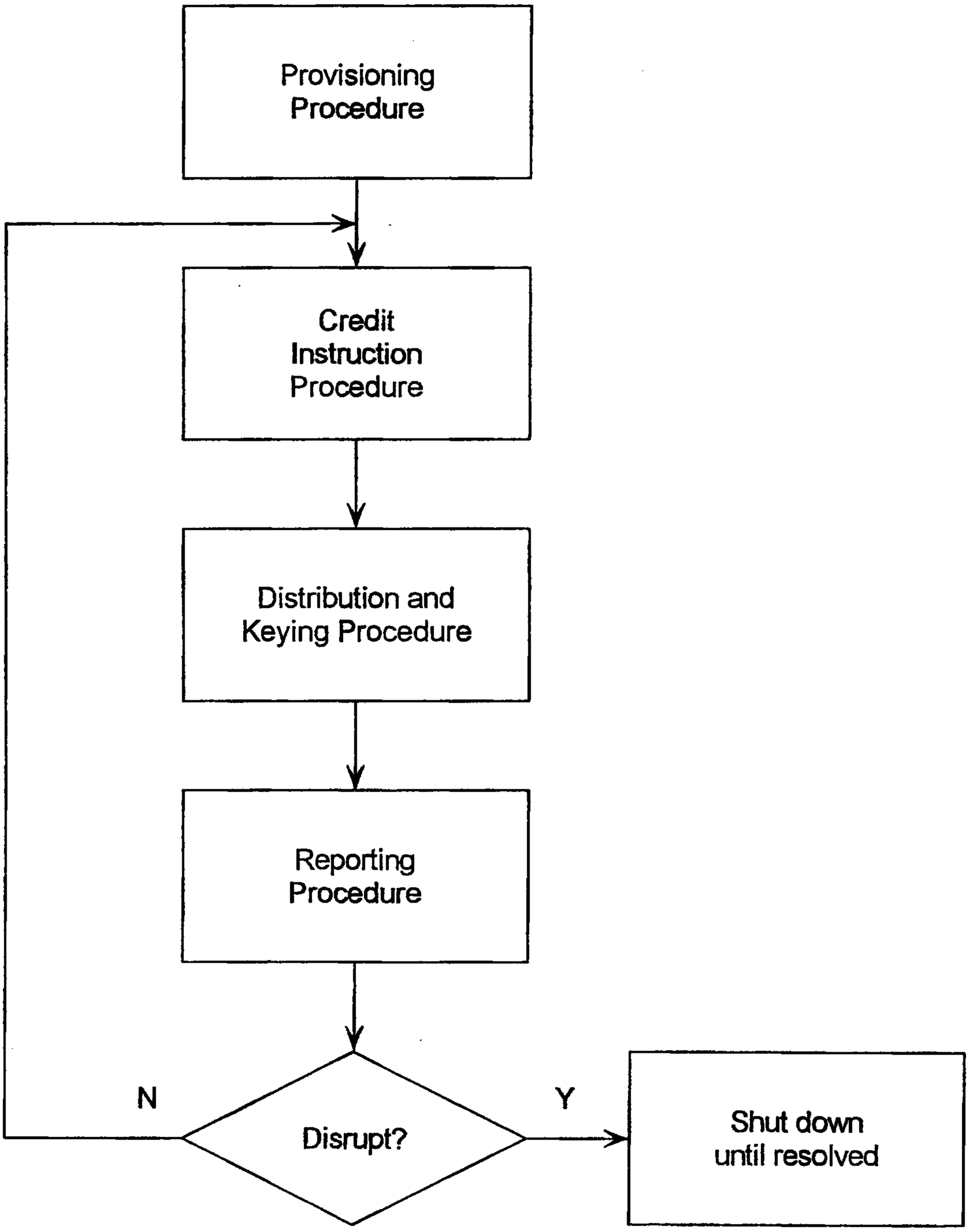

Provisioning Procedure
Credit Instruction Procedure
Distribution and Keying Procedure
Reporting Procedure
Disrupt?
N
Y
Shut down until resolved

FIG. 3

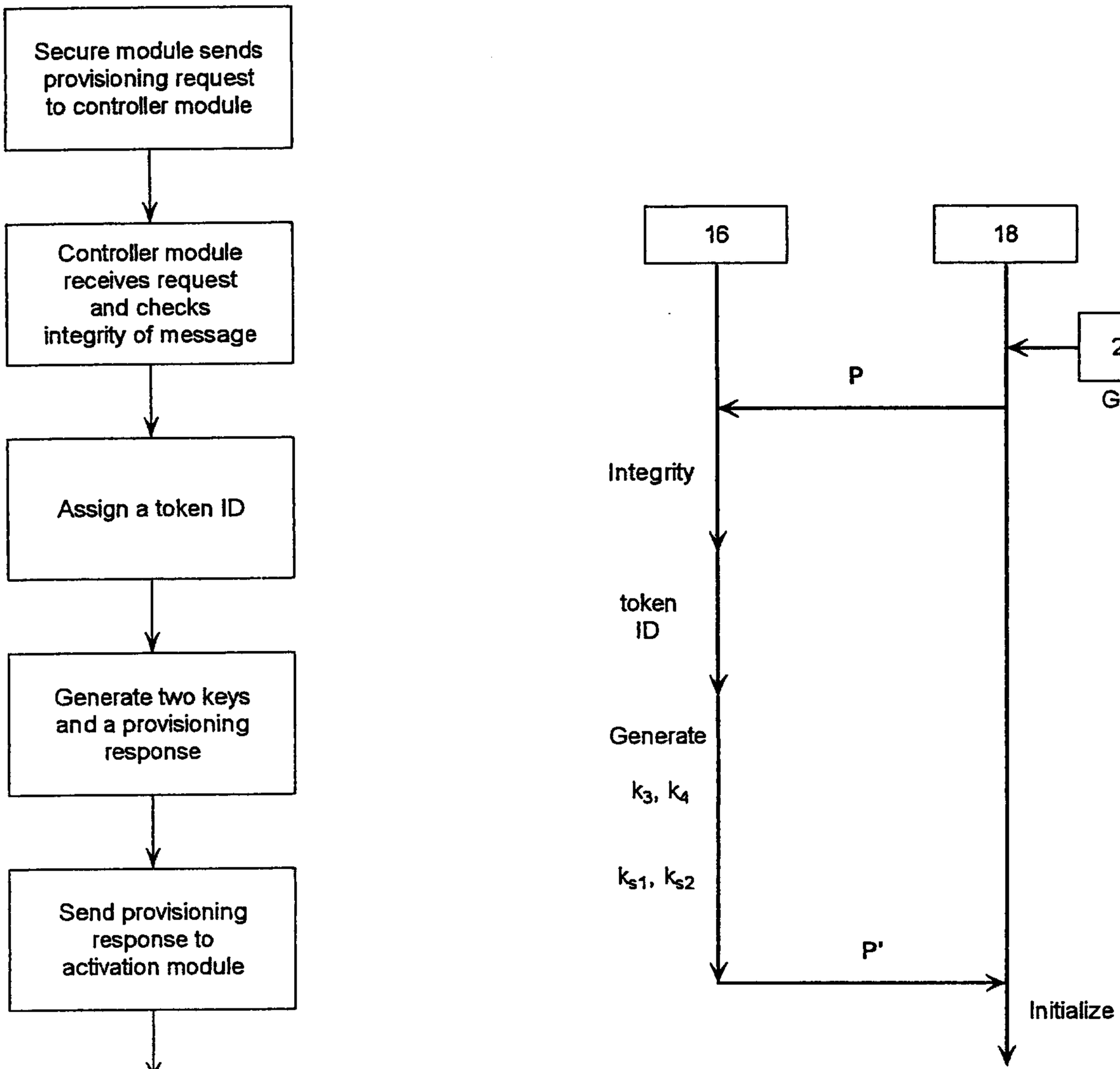

Secure module sends provisioning request to controller module
Controller module receives request and checks integrity of message
Assign a token ID
Generate two keys and a provisioning response
Send provisioning response to activation module
Initialize if necessary
16
18
28
Generate k_1, k_2
P
Integrity
token ID
Generate k_3, k_4
k_{s1}, k_{s2}
P'
Initialize

FIG.4

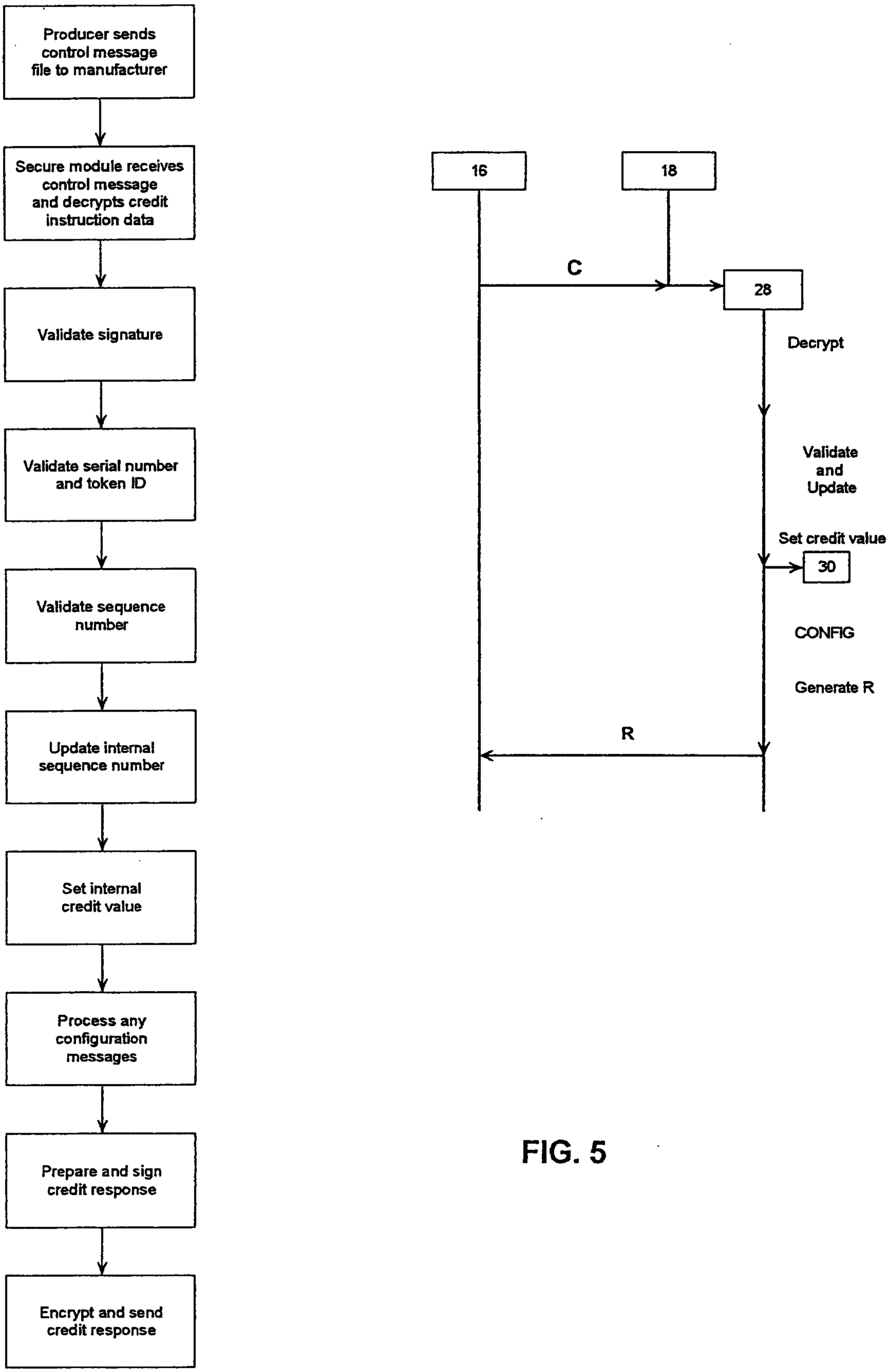

Producer sends control message file to manufacturer
Secure module receives control message and decrypts credit instruction data
Validate signature
Validate serial number and token ID
Validate sequence number
Update internal sequence number
Set internal credit value
Process any configuration messages
Prepare and sign credit response
Encrypt and send credit response
16
18
C
28
Decrypt
Validate and Update
Set credit value
30
CONFIG
Generate R
R

FIG. 5

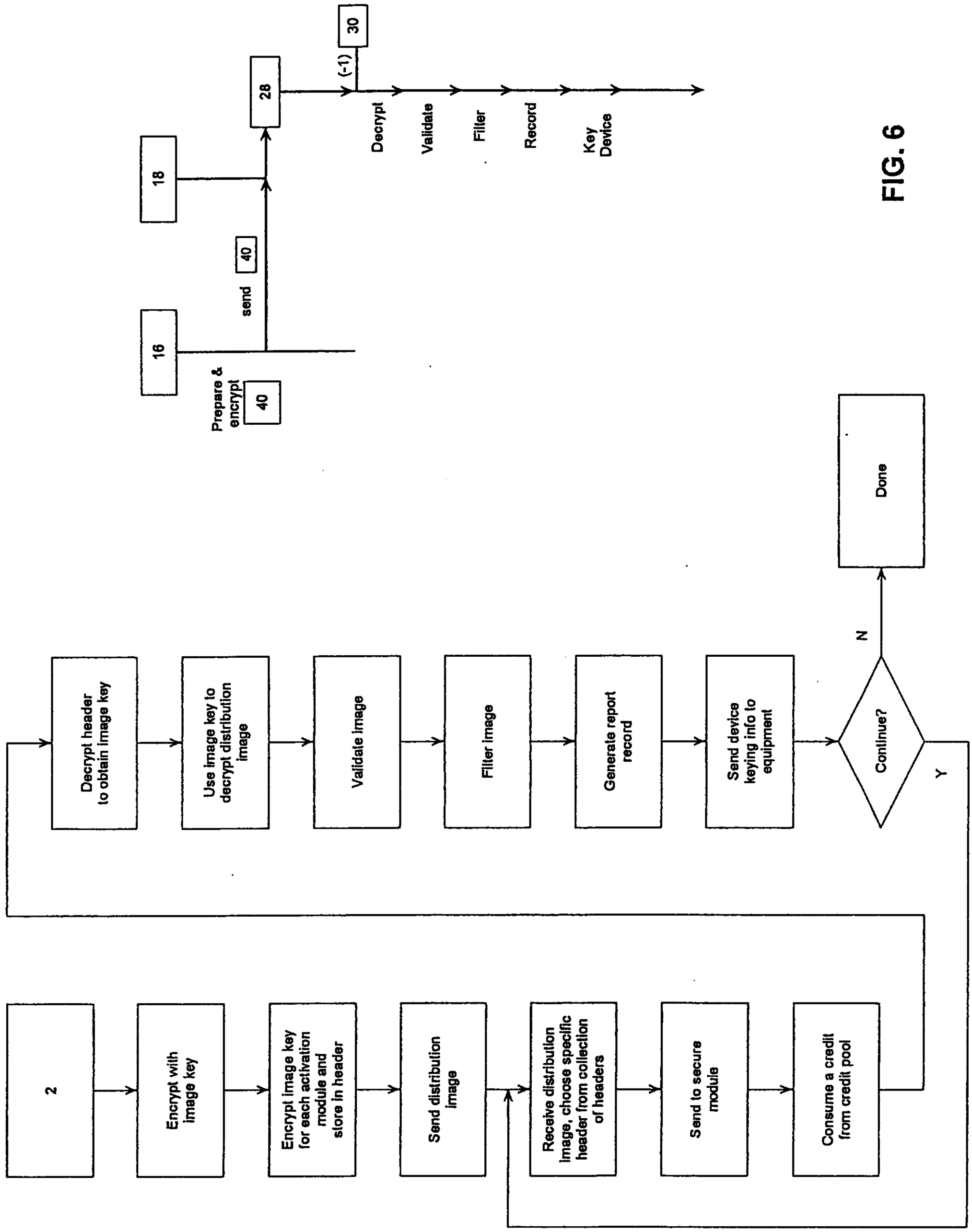

2
Encrypt with image key
Encrypt image key for each activation module and store in header
Send distribution image
Receive distribution image, choose specific header from collection of headers
Send to secure module
Consume a credit from credit pool
Decrypt header to obtain image key
Use image key to decrypt distribution image
Validate image
Filter image
Generate report record
Send device keying info to equipment
Continue?
Y
N
Done
18
16
Prepare & encrypt
40
send
40
28
30
(-1)
Decrypt
Validate
Filter
Record
Key Device

FIG. 6

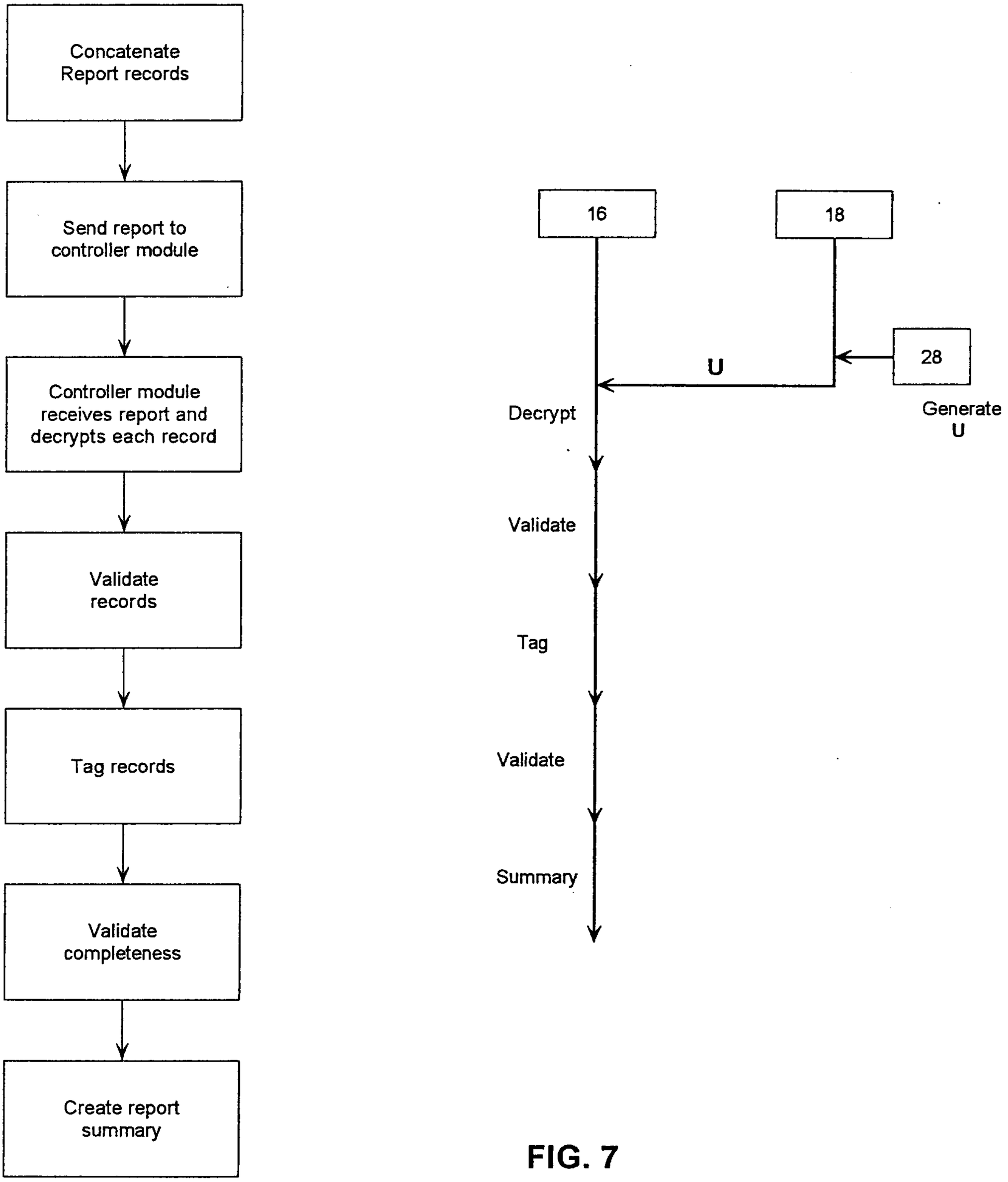
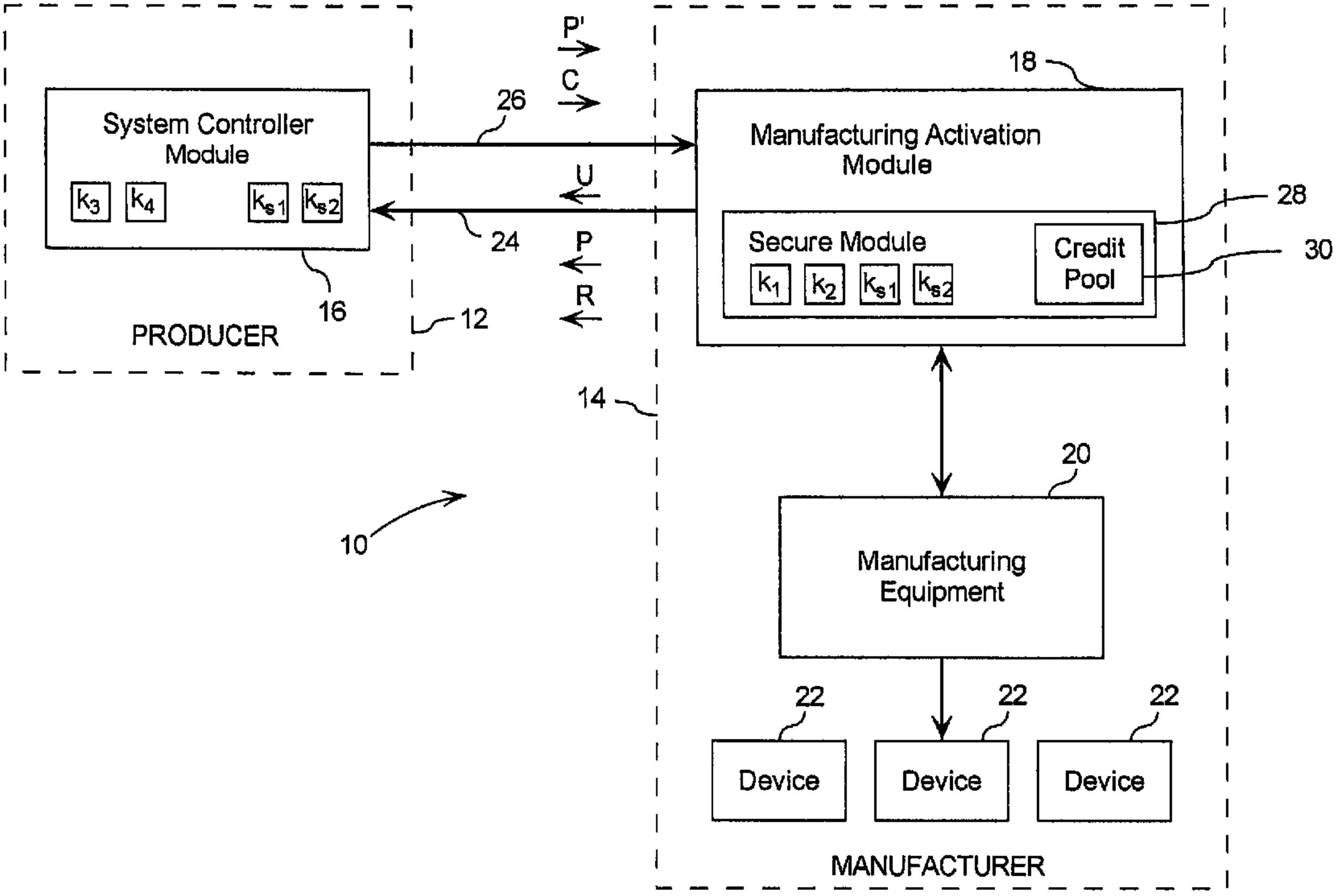

Concatenate Report records
Send report to controller module
Controller module receives report and decrypts each record
Validate records
Tag records
Validate completeness
Create report summary
16
18
28
U
Generate U
Decrypt
Validate
Tag
Validate
Summary

FIG. 7


P'
C
U
P
R
18
26
System Controller Module
k_3 k_4 k_{s1} k_{s2}
Manufacturing Activation Module
28
24
Secure Module
k_1 k_2 k_{s1} k_{s2}
Credit Pool
30
16
12
PRODUCER
14
20
Manufacturing Equipment
22
22
22
Device
Device
Device
MANUFACTURER
10