Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2907717 C 2019/10/01

(11)(21) 2 907 717

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2014/02/17
(87) Date publication PCT/PCT Publication Date: 2014/11/13
(45) Date de délivrance/Issue Date: 2019/10/01
(85) Entrée phase nationale/National Entry: 2015/09/21
(86) N° demande PCT/PCT Application No.: US 2014/016697
(87) N° publication PCT/PCT Publication No.: 2014/182359
(30) Priorité/Priority: 2013/05/07 (US13/888,747)

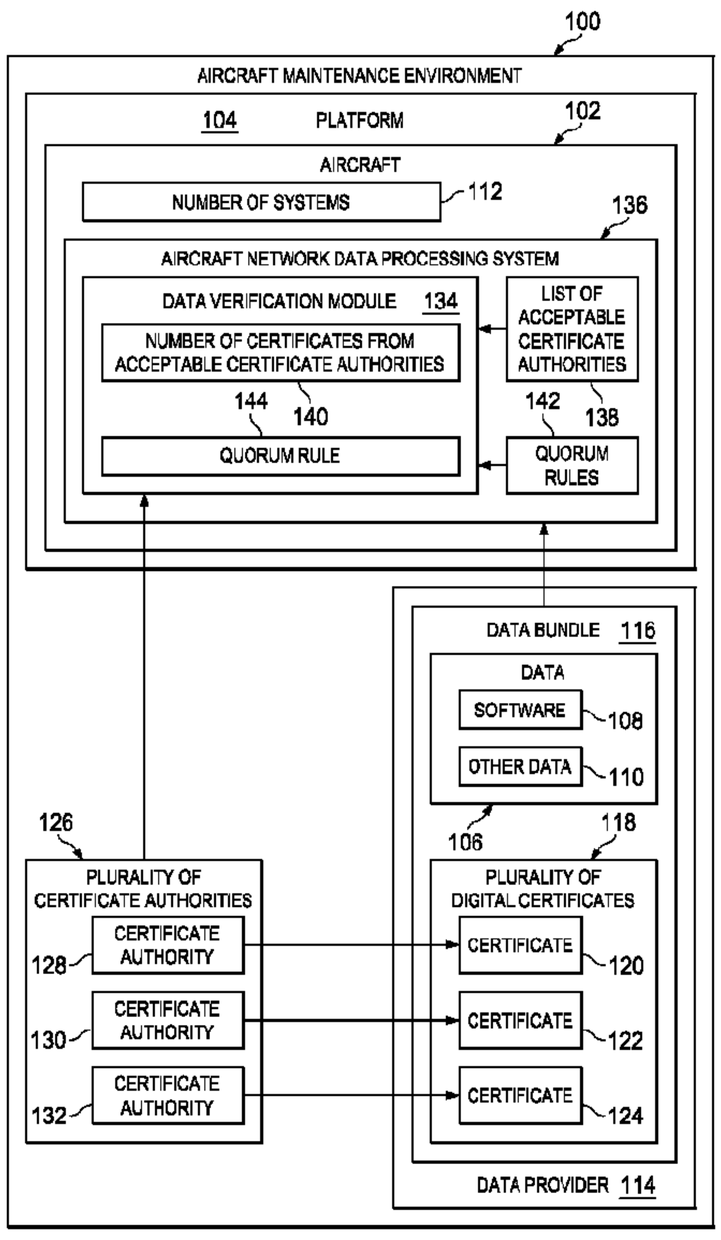
(51) Cl.Int./Int.Cl. *G06F 21/57* (2013.01), *G06F 21/64* (2013.01), *H04L 9/32* (2006.01)

(72) Inventeur/Inventor:
KIMBERLY, GREG A., US

(73) Propriétaire/Owner:
THE BOEING COMPANY, US

(74) Agent: SMART & BIGGAR

(54) Titre : VERIFICATION D'INFORMATIONS D'AVION EN REPONSE A UN CERTIFICAT NUMERIQUE COMPROMIS
(54) Title: VERIFICATION OF AIRCRAFT INFORMATION IN RESPONSE TO COMPROMISED DIGITAL CERTIFICATE



(57) Abrégé/Abstract:
A method and apparatus for verifying data for use on an aircraft. A plurality of digital certificates associated with the data are received by a processor unit. The processor unit determines whether one of the plurality of digital certificates is compromised. The processor unit selects a selected number of the plurality of digital certificates in response to a determination that the one of the plurality of digital certificates is compromised. The processor unit verifies the data for use on the aircraft using the selected number of the plurality of digital certificates.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2014 (13.11.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/182359 A1

(51) International Patent Classification:
G06F 21/57 (2013.01) *H04L 9/32* (2006.01)
G06F 21/64 (2013.01)

(21) International Application Number:
PCT/US2014/016697

(22) International Filing Date:
17 February 2014 (17.02.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/888,747 7 May 2013 (07.05.2013) US

(71) Applicant: **THE BOEING COMPANY** [US/US]; 100 North Riverside Plaza, Chicago, Illinois 60606-2016 (US).

(72) Inventor: **KIMBERLY, Greg A.**; 100 North Riverside Plaza, Chicago, Illinois 60606-2016 (US).

(74) Agents: **ASSEFA, Brook** et al.; The Boeing Company, P.O. Box 2515, MC 110-SD54, Seal Beach, California 90740-1515 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

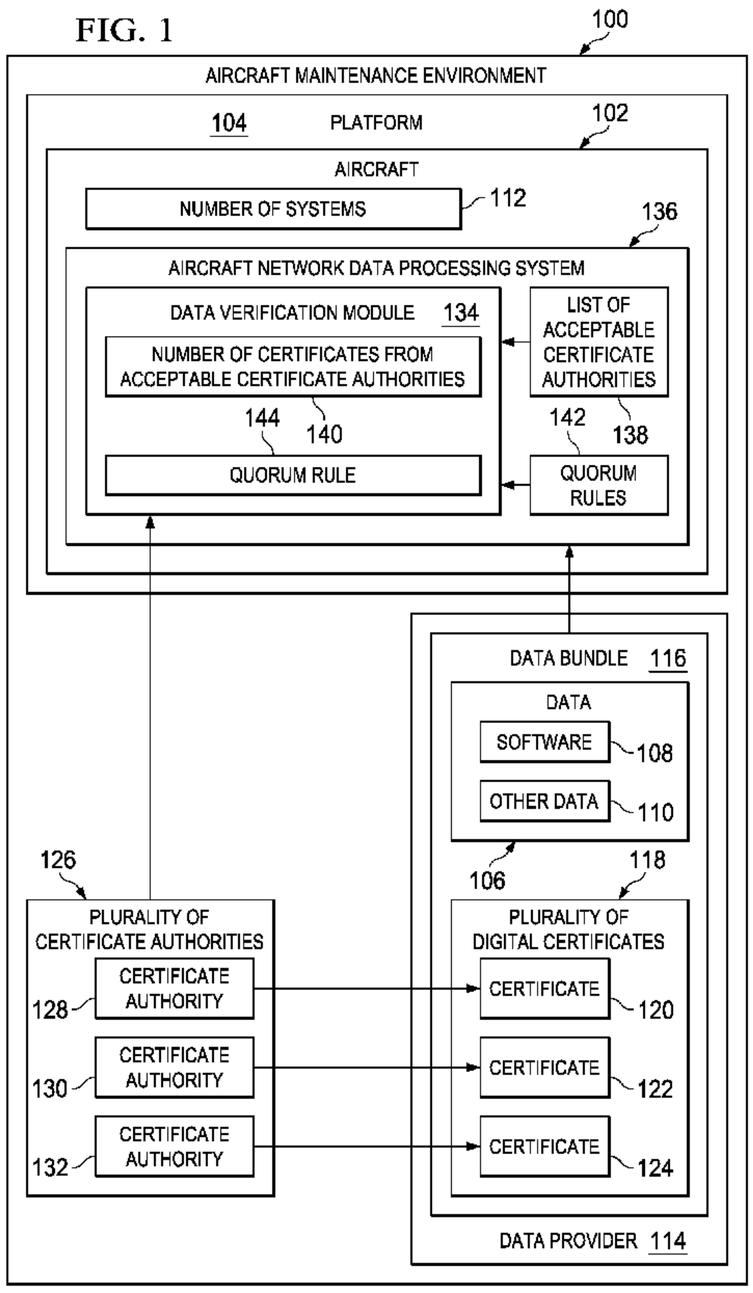
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Continued on next page]

(54) Title: VERIFICATION OF AIRCRAFT INFORMATION IN RESPONSE TO COMPROMISED DIGITAL CERTIFICATE

(57) Abstract: A method and apparatus for verifying data for use on an aircraft. A plurality of digital certificates associated with the data are received by a processor unit. The processor unit determines whether one of the plurality of digital certificates is compromised. The processor unit selects a selected number of the plurality of digital certificates in response to a determination that the one of the plurality of digital certificates is compromised. The processor unit verifies the data for use on the aircraft using the selected number of the plurality of digital certificates.

FIG. 1



WO 2014/182359 A1

WO 2014/182359 A1

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

VERIFICATION OF AIRCRAFT INFORMATION IN RESPONSE TO COMPROMISED DIGITAL CERTIFICATE

BACKGROUND

The present disclosure relates generally to systems and methods for verifying the authenticity and integrity of information used on aircraft. More particularly, the present disclosure relates to verifying the authenticity and integrity of information used on the aircraft when a digital certificate associated with the information is known or suspected to be compromised.

Modern aircraft are extremely complex. For example, an aircraft may have many types of electronic systems on-board. These systems are often in the form of line-replaceable units (LRUs). A line-replaceable unit is an item that can be removed and replaced from an aircraft. A line-replaceable unit is designed to be easily replaceable.

A line-replaceable unit may take on various forms. A line-replaceable unit on an aircraft may be, for example, without limitation, a flight management system, an autopilot, an in-flight entertainment system, a communications system, a navigation system, a flight controller, a flight recorder, a collision avoidance system, a system to support maintenance functions, or a system to support crew processes. The various line-replaceable units on an aircraft may be parts of an aircraft network data processing system.

Line-replaceable units may use software or programming to provide the logic or control for various operations and functions. Typically, software on an aircraft is treated as one or more separate parts or is combined with a hardware part and is unchangeable without changing the hardware part number. Aircraft software that is treated as an aircraft part may be referred to as a loadable aircraft software part or an aircraft software part. Aircraft software parts are parts of the configuration of an aircraft.

Aircraft operators are entities that operate aircraft. Aircraft operators also may be responsible for the maintenance and repair of aircraft. Examples of aircraft operators include airlines and military units. When an aircraft operator receives an aircraft, aircraft software parts may already be installed in the line-replaceable units on the aircraft.

An aircraft operator may also receive copies of loaded aircraft software parts in case the parts need to be reinstalled or reloaded into the line-replaceable units on the aircraft. Reloading of aircraft software parts may be required, for example, if a line-replaceable unit in which the software is used is replaced or repaired. Further, the aircraft operator also may receive updates to the aircraft software parts from time to time. These updates may include additional features not present in the currently-installed aircraft software parts and may be considered upgrades to one or more line-replaceable units. Specified procedures may be followed during loading of an aircraft software part on an aircraft such that the current configuration of the aircraft, including all of the aircraft software parts loaded on the aircraft, is known.

It may be desirable that only approved software and other data from trusted suppliers is used on an aircraft. Unapproved software and other data may include data that is corrupted, data that is infected with a virus, or other unapproved data. Unapproved software and other data may affect the operation of the aircraft in undesired ways.

Data processing networks may employ digital certificates in a public key infrastructure to ensure that only approved software and other data are used on the network. Such digital certificates also may be known as public key certificates or identity certificates. The digital certificates are issued by a certificate authority that is trusted by the network. The digital certificate identifies the source of the software or other data to the network in a manner that can be trusted. The network may use the digital certificate to determine whether or not the software or other data will be used on the network.

Current systems and methods for verifying the authenticity and integrity of software and other data for use on entirely ground-based computer networks may not be applied effectively to mobile systems, such as aircraft. The particular environment in which network data processing systems on aircraft are operated and maintained may make it difficult or impossible to use such current methods for validating software or other data for use on an aircraft network data processing system.

Accordingly, it would be desirable to have a method and apparatus that takes into account one or more of the issues discussed above as well as possibly other issues.

SUMMARY

An embodiment of the present disclosure provides a method for verifying data for use on an aircraft. A plurality of digital certificates associated with the data are received by a processor unit. The processor unit determines whether one of the plurality of digital certificates is compromised. The processor unit selects a selected number of the plurality of digital certificates in response to a determination that the one of the plurality of digital certificates is compromised. The processor unit verifies the data for use on the aircraft using the selected number of the plurality of digital certificates.

Another embodiment of the present disclosure provides an apparatus comprising a data verification module. The data verification module is configured to receive a plurality of digital certificates associated with data for use on an aircraft, determine whether one of the plurality of digital certificates is compromised, select a selected number of the plurality of digital certificates in response to a determination that the one of the plurality of digital certificates is compromised, and verify the data for use on the aircraft using the selected number of the plurality of digital certificates.

Another embodiment of the present disclosure provides a method for verifying data for use on an aircraft. A plurality of digital certificates associated with the data is received by a processor unit. The processor unit determines whether one of the plurality of digital certificates is compromised. The processor unit selects a quorum rule, wherein the quorum rule is a first quorum rule selected in response to a determination that none of the plurality of digital certificates is compromised and a second quorum rule selected in response to the determination that the one of the plurality of digital certificates is compromised. The processor unit verifies the data for use on the aircraft using a selected number of the plurality of digital certificates as defined by the quorum rule.

In another embodiment, there is provided a method for verifying data for use on an aircraft. The method involves: receiving, by a processor unit, a plurality of digital certificates associated with the data; and verifying, by the processor unit, the data for use on the aircraft using a selected number of the plurality of digital certificates.

The plurality of digital certificates may be from a plurality of certificate authorities and the method may further involve selecting the selected number of the plurality of digital certificates using a list of acceptable certificate authorities.

Verifying the data for use on the aircraft using the selected number of the plurality of digital certificates may involve determining whether at least a specified number of the selected number of the plurality of digital certificates is valid.

The specified number may be defined by a quorum rule.

The method may further involve selecting the quorum rule from a plurality of quorum rules based on a system on the aircraft on which the data will be used.

The method may further involve selecting the quorum rule from a plurality of quorum rules based on a location of the aircraft.

The data may include software for use on the aircraft.

The processor unit may be a processor unit in an aircraft network data processing system on the aircraft.

In another embodiment, there is provided an apparatus including a data verification module configured to receive a plurality of digital certificates associated with data for use on an aircraft and to verify the data for use on the aircraft using a selected number of the plurality of digital certificates.

The plurality of digital certificates may be from a plurality of certificate authorities and the data verification module may be further configured to select the selected number of the plurality of digital certificates using a list of acceptable certificate authorities.

The data verification module may be configured to determine whether at least a specified number of the selected number of the plurality of digital certificates is valid.

The specified number may be defined by a quorum rule.

The data verification module may be configured to select the quorum rule from a plurality of quorum rules based on a system on the aircraft on which the data will be used.

The data verification module may be configured to select the quorum rule from a plurality of quorum rules based on a location of the aircraft.

The data may include software for use on the aircraft.

The data verification module may be implemented in an aircraft network data processing system on the aircraft.

In another embodiment, there is provided a method for verifying data for use on an aircraft. The method involves: receiving, by a processor unit, the data for use on the aircraft; generating, by the processor unit, a plurality of digital certificates for the data; and sending the data and the plurality of digital certificates to the aircraft.

The plurality of digital certificates may be from a plurality of certificate authorities.

The data may include software for use on the aircraft.

The method may further involve: receiving the plurality of digital certificates by an aircraft network data processing system on the aircraft; and verifying, by the aircraft network data processing system, the data for use on the aircraft using a selected number of the plurality of digital certificates.

In another embodiment, there is provided a method for verifying data for use on an aircraft. The method may involve: receiving, by a processor unit, a plurality of digital certificates associated with the data; determining, by the processor unit, whether one of the plurality of digital certificates is compromised; and selecting, by the processor unit, a quorum rule. The quorum rule is a first quorum rule selected in response to a determination that none of the plurality of digital certificates is compromised and a second quorum rule selected in response to the determination that the one of the plurality of digital certificates is compromised. The method may further involve: verifying, by the processor unit, the data for use on the aircraft using a selected number of the plurality of digital certificates as defined by the quorum rule.

The plurality of digital certificates may be from a plurality of certificate authorities.

Verifying the data for use on the aircraft using the selected number of the plurality of digital certificates may involve determining whether at least a specified number of the selected number of the plurality of digital certificates is valid as defined by the quorum rule.

The first quorum rule may indicate that the specified number of the selected number of the plurality of digital certificates is less than the selected number. The second quorum rule may indicate that the specified number of the selected number of the plurality of digital certificates equals the selected number.

The data may include software for use on the aircraft.

The processor unit may be a processor unit in an aircraft network data processing system on the aircraft.

In another embodiment, there is provided a method for verifying data for use on an aircraft. The method involves: receiving, by a processor unit, a plurality of digital certificates associated with the data; verifying, for each digital certificate in the plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft; determining, by the processor unit, whether one of the plurality of digital certificates is compromised; and selecting, by the processor unit, a selected number of the plurality of digital certificates in response to the determination that the one of the plurality of digital certificates is compromised. The selected number is determined based upon a quorum rule selected from quorum rules that are based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded. The method further involves: verifying, by the processor unit, the data for use on the aircraft using the selected number of the plurality of digital certificates. Verifying the data for use on the aircraft using the selected number of the plurality of digital certificates involves determining whether at least a specified number of the selected number of the plurality of digital certificates is valid. The specified number is defined by the quorum rule. The quorum rule is composed of one, or more, of: a quorum rule for an operator of an aircraft; a quorum rule for an aircraft maintenance entity; a quorum rule for an aircraft type; a quorum rule for an aircraft system on which data will be used; a quorum rule for the number

of aircraft systems on which data will be used; and a quorum rule for use when a certificate authority is known to be, or suspected of being compromised.

In another embodiment, there is provided an apparatus, including: a data verification module configured to: receive a plurality of digital certificates associated with data for use on an aircraft; verify, for each digital certificate in the plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft; determine whether one of the plurality of digital certificates is compromised; and select a selected number of the plurality of digital certificates in response to the determination that the one of the plurality of digital certificates is compromised, the selected number being determined based upon a quorum rule selected, from quorum rules based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded. The selected number is determined on a quorum rule selected from quorum rules based on at least two of: an aircraft system on with the data will be loaded; a number of aircraft systems on which the data will be used; a location of the aircraft when the data is loaded; and when a determination is made that a certificate authority is known to be, or is suspected of being compromised. The data verification module is further configured to: verify the data for use on the aircraft using the selected number of the plurality of digital certificates. Verifying the data for use on the aircraft using the selected number of the plurality of digital certificates involves determining whether at least a specified number of the selected number of the plurality of digital certificates is valid. The specified number is defined by the quorum rule. The quorum rule is composed of one, or more, of: a quorum rule for an operator of an aircraft; a quorum rule for an aircraft maintenance entity; a quorum rule for an aircraft type; a quorum rule for an aircraft system on which data will be used; a quorum rule for the number of aircraft systems on which data will be used; and a quorum rule for use when a certificate authority is known to be, or suspected of being compromised.

In another embodiment, there is provided method for verifying data for use on an aircraft. The method involves receiving, by a processor unit, a plurality of digital certificates associated with the data: verifying, for each digital certificate in the

plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft; determining, by the processor unit, whether one of the plurality of digital certificates is compromised; and selecting, by the processor unit, a quorum rule, based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded, from quorum rules. The quorum rule is at least one of: a quorum rule for an operator of an aircraft; a quorum rule for an aircraft maintenance entity; a quorum rule for an aircraft type; a quorum rule for an aircraft system on which data will be used; a quorum rule for the number of aircraft systems on which data will be used; a quorum rule for use when a certificate authority is known to be, or suspected of being compromised; a quorum rule for use when it is determined that none of the plurality of digital certificates is compromised; and verifying, by the processor unit, the data for use on the aircraft using a selected number of the plurality of digital certificates as defined by the quorum rule.

The features and functions can be achieved independently in various embodiments of the present disclosure or may be combined in yet other embodiments in which further details can be seen with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the illustrative embodiments are set forth in the appended claims. The illustrative embodiments, however, as well as a preferred mode of use, further objectives, and features thereof will best be understood by reference to the following detailed description of illustrative embodiments of the present disclosure when read in conjunction with the accompanying drawings, wherein:

Figure 1 is an illustration of a block diagram of an aircraft maintenance environment in accordance with an illustrative embodiment;

Figure 2 is an illustration of a block diagram of quorum rules in accordance with an illustrative embodiment;

Figure 3 is an illustration of a block diagram of data verification using a plurality of digital certificates and a list of acceptable certificate authorities in accordance with an illustrative embodiment;

Figure 4 is an illustration of a block diagram of data verification using a plurality of digital certificates and quorum rules in accordance with an illustrative embodiment;

Figure 5 is an illustration of a block diagram of data verification in response to a compromised certificate authority in accordance with an illustrative embodiment;

Figure 6 is an illustration of a flowchart of a process for signing data for use on an aircraft in accordance with an illustrative embodiment;

Figure 7 is an illustration of a flowchart of a process for verifying data for use on an aircraft in accordance with an illustrative embodiment; and

Figure 8 is an illustration of a data processing system in accordance with an illustrative embodiment.

DETAILED DESCRIPTION

The different illustrative embodiments recognize and take into account a number of different considerations. "A number," as used herein with reference to items, means one or more items. For example, "a number of different considerations" means one or more different considerations.

The different illustrative embodiments recognize and take into account that current public key infrastructure systems may be structured around singular root

certificate authority-derived certificates. The use of singular certificates may create a system where misconfiguration or attack can effectively cause the system to cease to operate.

The different illustrative embodiments also recognize and take into account that an operator of an aircraft may prefer certain certificate authorities and may not trust other certificate authorities. Therefore, it may be desirable to allow an aircraft operator to use certificates from certificate authorities that are acceptable to the operator to verify software and other data for use on aircraft operated by that operator.

The different illustrative embodiments also recognize and take into account that audit techniques may exist that may make it possible to discover the compromise of a root certificate authority. It may be desirable to take into account the known or suspected compromise of a certificate authority for the verification of software or other data for use on an aircraft.

Therefore, one or more of the illustrative embodiments provide a system and method for validating the authenticity and integrity of software and other data for use on an aircraft using a plurality of digital certificates from a plurality of certificate authorities. In accordance with illustrative embodiments, software or other data may be validated for use on the aircraft if a number of the plurality of certificates associated with the data that satisfies a quorum rule is determined to be valid. The rules defining the quorum required for validation may be selected in response to a determination that a specified certificate authority may have been compromised.

Turning now to **Figure 1**, an illustration of a block diagram of an aircraft maintenance environment is depicted in accordance with an illustrative embodiment. In this example, aircraft maintenance environment **100** may be configured for the maintenance of aircraft **102**.

Aircraft **102** may be any appropriate type of aircraft. For example, without limitation, aircraft **102** may be a commercial or private passenger aircraft, a cargo aircraft, a military or other government aircraft, or any other aircraft configured for any appropriate purpose or mission. Aircraft **102** may be a fixed wing, rotary wing, or lighter than air aircraft. Aircraft **102** may be a manned aircraft or an unmanned air vehicle.

Aircraft **102** is one example of platform **104** in which an illustrative embodiment may be implemented. Platform **104** may be a vehicle or other mobile structure. For example, without limitation, platform **104** may be an aerospace vehicle

that is capable of traveling through the air, in space, or both. As another example, without limitation, platform **104** may be a vehicle that is capable of traveling on land, on the surface of water, underwater, or in any other medium or combination of media. In another illustrative embodiment, platform **104** may be a static system. For example, without limitation, platform **104** may be an industrial control system or other generally non-mobile system.

Aircraft **102** may use data **106** for operation of aircraft **102**. For example, data **106** may include software **108**, other data **110**, or various combinations of data. For example, without limitation, software **108** may include aircraft software parts for use on line-replaceable units on aircraft **102**. For example, without limitation, other data **110** may include mapping data or other data or combinations of data for use by aircraft **102**.

Data **106** may be used by number of systems **112** on aircraft **102**. For example, without limitation, number of systems **112** may include automatic pilot, flight management, communications, health management, other systems, or various combinations of systems for performing various functions on aircraft **102**.

Data **106** may be provided by data provider **114**. Data provider **114** may be any entity that has authority to provide data **106** for use on aircraft **102** or to load data **106** on aircraft **102**. For example, without limitation, data provider **114** may include a software supplier, an aircraft maintenance entity, an aircraft operator, an aircraft manufacturer, or any other entity or combination of entities authorized to provide data **106** for use on aircraft **102**. Data provider **114** may be any entity or combination of entities that is responsible for maintaining aircraft **102**. Data provider **114** may or may not be the owner of aircraft **102**. Data provider **114** may include an entity acting on behalf of the owner of aircraft **102** to provide data **106** for use on aircraft **102**.

Data provider **114** may provide data **106** in data bundle **116** for loading on aircraft **102**. For example, data bundle **116** may include data **106** along with plurality of digital certificates **118** for data **106**. In this example, without limitation, plurality of digital certificates **118** may include certificate **120**, certificate **122**, and certificate **124**. Plurality of digital certificates **118** may include any appropriate number of digital certificates. For example, plurality of digital certificates **118** may include two or more than three digital certificates.

Plurality of digital certificates **118** may be from plurality of certificate authorities **126**. For example, certificate **120** may be from certificate authority **128**.

Certificate **122** may be from certificate authority **130**. Certificate **124** may be from certificate authority **132**.

Data verification module **134** may be configured to use plurality of digital certificates **118** to verify data **106** for use on aircraft **102**. For example, data verification module **134** may be implemented in aircraft network data processing system **136** on aircraft **102**.

Data verification module **134** may be configured to use list of acceptable certificate authorities **138** to identify number of certificates from acceptable certificate authorities **140** to use to verify data **106** for use on aircraft **102**. The quantity of plurality of digital certificates **118** that must be determined to be valid in order for data **106** to be verified may be defined by quorum rules **142**. Data verification module **134** may be configured to select quorum rule **144** from quorum rules **142** for the verification of data **106** based on number of systems **112** on which data **106** will be used, location of aircraft **102** when data **106** is loaded on aircraft **102**, other factors, or various combinations of factors.

The illustration of **Figure 1** is not meant to imply physical or architectural limitations to the manner in which different illustrative embodiments may be implemented. Other components in addition to, in place of, or both in addition to and in place of the ones illustrated may be used. Some components may be unnecessary in some illustrative embodiments. Also, the blocks are presented to illustrate some functional components. One or more of these blocks may be combined or divided into different blocks when implemented in different illustrative embodiments.

Turning now to **Figure 2**, an illustration of a block diagram of quorum rules is depicted in accordance with an illustrative embodiment. In this example, quorum rules **200** may be an example of one implementation of quorum rules **142** in **Figure 1**.

Quorum rules **200** may be defined for various characteristics or conditions of an aircraft. For example, without limitation, quorum rules **200** may be defined for operator **202** of an aircraft, for aircraft maintenance entity **204**, for aircraft type **206**, for aircraft systems **208** on which data will be used, for aircraft location **210**, or for various other characteristics or combinations of characteristics of an aircraft. Specific quorum rules **200** may be defined for use in response to known or suspected certificate authority compromise **212**.

Turning now to **Figure 3**, an illustration of a block diagram of data verification using a plurality of digital certificates and a list of acceptable certificate authorities is depicted in accordance with an illustrative embodiment. For example, data verification **300** may be performed using data verification module **134** in **Figure 1**.

In this example, data bundle **302** to be verified may include certificate A **304**, certificate B **306**, and certificate C **308**. List of acceptable certificate authorities **310** may indicate that only certificates from certificate authority A **312** and certificate authority B **314** are acceptable to use for data verification **300**. In this case, certificate C **308** is not from either certificate authority A **312** or certificate authority B **314**. Therefore, certificate C **308** will not be used for data verification **300**. In this example, data bundle **302** may be verified in response to a determination of certificate A or B valid **316**.

Turning now to **Figure 4**, an illustration of a block diagram of data verification using a plurality of digital certificates and quorum rules is depicted in accordance with an illustrative embodiment. For example, data verification **400** may be performed using data verification module **134** in **Figure 1**.

In this example, data bundle **402** to be verified may include certificate A **404**, certificate B **406**, and certificate C **408**. Quorum rules **410** may indicate that data bundle **402** may be verified if at least two of three certificates is valid **412**. Therefore, in this example, data bundle **402** may be verified in response to a determination of certificates A and B valid **414**, certificates A and C valid **416**, certificates B and C valid **418**, or certificates A and B and C valid **420**.

Turning now to **Figure 5**, an illustration of a block diagram of data verification in response to a compromised certificate authority is depicted in accordance with an illustrative embodiment. For example, data verification **500** may be performed using data verification module **134** in **Figure 1**.

In this example, data bundle **502** to be verified may include certificate A **504**, certificate B **506**, and certificate C **508**. Quorum rules **510** may indicate that data bundle **502** may be verified if at least two of three certificates is valid **512**. However, in this case, available information indicates that certificate authority A is compromised **514**. Quorum rules **510** also indicate that if a certificate authority is compromised **516**, then the appropriate quorum rule to use is changed from at least two of three certificates

valid **512** to all not compromised valid **518**. Therefore, in this example, data bundle **502** may be verified only in response to a determination of certificates B and C valid **520**.

Turning now to **Figure 6**, an illustration of a flowchart of a process for signing data for use on an aircraft is depicted in accordance with an illustrative embodiment. For example, without limitation, process **600** may be performed by data provider **114** in **Figure 1**.

Data for an aircraft may be received (operation **602**). The data may be signed with a plurality of digital signatures from a plurality of certificate authorities (operation **604**). The data and the plurality of certificates then may be sent to the aircraft (operation **606**), with the process terminating thereafter.

Turning now to **Figure 7**, an illustration of a flowchart of a process for verifying data for use on an aircraft is depicted in accordance with an illustrative embodiment. In this example, process **700** may be performed by data verification module **134** in **Figure 1**.

A data bundle including a plurality of digital certificates is received (operation **702**). It may be determined whether any of the certificates are not from acceptable certificate authorities (operation **704**). If it is determined that any of the certificates are not from acceptable certificate authorities, only the certificates that are from acceptable certificate authorities may be used for verification of the data bundle (operation **706**). Otherwise, all of the received digital certificates may be used for verification (operation **708**).

An appropriate quorum rule for verification may be selected (operation **710**). It may be determined whether there is any indication that a certificate authority may have been compromised (operation **712**). An alternative quorum rule may be selected for verification in response to a determination that a certificate authority may have been compromised (operation **714**). Otherwise, the quorum rule selected in operation **710** may be used for verification (operation **716**).

It then may be determined whether the selected quorum rule is satisfied (operation **718**). If the selected quorum rule is satisfied, data authenticity and integrity may be considered to be verified (operation **720**), with the process terminating thereafter. Otherwise, data authenticity and integrity may not be verified (operation **722**), with the process terminating thereafter.

Turning now to **Figure 8**, an illustration of a data processing system is depicted in accordance with an illustrative embodiment. In this example, data processing system **800** is an example of one implementation of a data processing system on aircraft network data processing system **136** in **Figure 1**. Data processing system **800** is an example of one implementation of a data processing system on which data verification module **134** in **Figure 1** may be implemented.

In this illustrative example, data processing system **800** includes communications fabric **802**. Communications fabric **802** provides communications between processor unit **804**, memory **806**, persistent storage **808**, communications unit **810**, input/output (I/O) unit **812**, and display **814**. Memory **806**, persistent storage **808**, communications unit **810**, input/output (I/O) unit **812**, and display **814** are examples of resources accessible by processor unit **804** via communications fabric **802**.

Processor unit **804** serves to run instructions for software that may be loaded into memory **806**. Processor unit **804** may be a number of processors, a multi-processor core, or some other type of processor, depending on the particular implementation. Further, processor unit **804** may be implemented using a number of heterogeneous processor systems in which a main processor is present with secondary processors on a single chip. As another illustrative example, processor unit **804** may be a symmetric multi-processor system containing multiple processors of the same type.

Memory **806** and persistent storage **808** are examples of storage devices **816**. A storage device is any piece of hardware that is capable of storing information such as, for example, without limitation, data, program code in functional form, and other suitable information either on a temporary basis or a permanent basis. Storage devices **816** may also be referred to as computer readable storage devices in these examples. Memory **806**, in these examples, may be, for example, a random access memory or any other suitable volatile or non-volatile storage device. Persistent storage **808** may take various forms, depending on the particular implementation.

For example, persistent storage **808** may contain one or more components or devices. For example, persistent storage **808** may be a hard drive, a flash memory, a rewritable optical disk, a rewritable magnetic tape, or some combination of the above. The media used by persistent storage **808** also may be removable. For example, a removable hard drive may be used for persistent storage **808**.

Communications unit **810**, in these examples, provides for communications with other data processing systems or devices. In these examples, communications unit **810** is a network interface card. Communications unit **810** may provide communications through the use of either or both physical and wireless communications links.

Input/output unit **812** allows for input and output of data with other devices that may be connected to data processing system **800**. For example, input/output unit **812** may provide a connection for user input through a keyboard, a mouse, and/or some other suitable input device. Further, input/output unit **812** may send output to a printer. Display **814** provides a mechanism to display information to a user.

Instructions for the operating system, applications, and/or programs may be located in storage devices **816**, which are in communication with processor unit **804** through communications fabric **802**. In these illustrative examples, the instructions are in a functional form on persistent storage **808**. These instructions may be loaded into memory **806** for execution by processor unit **804**. The processes of the different embodiments may be performed by processor unit **804** using computer-implemented instructions, which may be located in a memory, such as memory **806**.

These instructions are referred to as program instructions, program code, computer usable program code, or computer readable program code that may be read and executed by a processor in processor unit **804**. The program code in the different embodiments may be embodied on different physical or computer readable storage media, such as memory **806** or persistent storage **808**.

Program code **818** is located in a functional form on computer readable media **820** that is selectively removable and may be loaded onto or transferred to data processing system **800** for execution by processor unit **804**. Program code **818** and computer readable media **820** form computer program product **822** in these examples. In one example, computer readable media **820** may be computer readable storage media **824** or computer readable signal media **826**.

Computer readable storage media **824** may include, for example, an optical or magnetic disk that is inserted or placed into a drive or other device that is part of persistent storage **808** for transfer onto a storage device, such as a hard drive, that is part of persistent storage **808**. Computer readable storage media **824** also may take the form of a persistent storage, such as a hard drive, a thumb drive, or a flash memory,

that is connected to data processing system **800**. In some instances, computer readable storage media **824** may not be removable from data processing system **800**.

In these examples, computer readable storage media **824** is a physical or tangible storage device used to store program code **818** rather than a medium that propagates or transmits program code **818**. Computer readable storage media **824** is also referred to as a computer readable tangible storage device or a computer readable physical storage device. In other words, computer readable storage media **824** is a media that can be touched by a person.

Alternatively, program code **818** may be transferred to data processing system **800** using computer readable signal media **826**. Computer readable signal media **826** may be, for example, a propagated data signal containing program code **818**. For example, computer readable signal media **826** may be an electromagnetic signal, an optical signal, or any other suitable type of signal. These signals may be transmitted over communications links, such as wireless communications links, optical fiber cable, coaxial cable, a wire, or any other suitable type of communications link. In other words, the communications link or the connection may be physical or wireless in the illustrative examples.

In some illustrative embodiments, program code **818** may be downloaded over a network to persistent storage **808** from another device or data processing system through computer readable signal media **826** for use within data processing system **800**. For instance, program code stored in a computer readable storage medium in a server data processing system may be downloaded over a network from the server to data processing system **800**. The data processing system providing program code **818** may be a server computer, a client computer, or some other device capable of storing and transmitting program code **818**.

The different components illustrated for data processing system **800** are not meant to provide architectural limitations to the manner in which different embodiments may be implemented. The different illustrative embodiments may be implemented in a data processing system including components in addition to and/or in place of those illustrated for data processing system **800**. Other components shown in **Figure 8** can be varied from the illustrative examples shown. The different embodiments may be implemented using any hardware device or system capable of running program code. As one example, data processing system **800** may include

organic components integrated with inorganic components and/or may be comprised entirely of organic components excluding a human being. For example, a storage device may be comprised of an organic semiconductor.

In another illustrative example, processor unit **504** may take the form of a hardware unit that has circuits that are manufactured or configured for a particular use. This type of hardware may perform operations without needing program code to be loaded into a memory from a storage device to be configured to perform the operations.

For example, when processor unit **804** takes the form of a hardware unit, processor unit **804** may be a circuit system, an application specific integrated circuit (ASIC), a programmable logic device, or some other suitable type of hardware configured to perform a number of operations. With a programmable logic device, the device is configured to perform the number of operations. The device may be reconfigured at a later time or may be permanently configured to perform the number of operations. Examples of programmable logic devices include, for example, a programmable logic array, a programmable array logic, a field programmable logic array, a field programmable gate array, and other suitable hardware devices. With this type of implementation, program code **818** may be omitted, because the processes for the different embodiments are implemented in a hardware unit.

In still another illustrative example, processor unit **804** may be implemented using a combination of processors found in computers and hardware units. Processor unit **804** may have a number of hardware units and a number of processors that are configured to run program code **818**. With this depicted example, some of the processes may be implemented in the number of hardware units, while other processes may be implemented in the number of processors.

In another example, a bus system may be used to implement communications fabric **802** and may be comprised of one or more buses, such as a system bus or an input/output bus. Of course, the bus system may be implemented using any suitable type of architecture that provides for a transfer of data between different components or devices attached to the bus system.

Additionally, communications unit **810** may include a number of devices that transmit data, receive data, or transmit and receive data. Communications unit **810** may be, for example, a modem or a network adapter, two network adapters, or some combination thereof. Further, a memory may be, for example, memory **806**, or a cache,

such as found in an interface and memory controller hub that may be present in communications fabric **802**.

The description of the different illustrative embodiments has been presented for purposes of illustration and description and is not intended to be exhaustive or to limit the embodiments in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. Further, different illustrative embodiments may provide different features as compared to other illustrative embodiments. The embodiment or embodiments selected are chosen and described in order to best explain the principles of the embodiments, the practical application, and to enable others of ordinary skill in the art to understand the disclosure for various embodiments with various modifications as are suited to the particular use contemplated.

EMBODIMENTS IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for verifying data for use on an aircraft, comprising:

receiving, by a processor unit, a plurality of digital certificates associated with the data;

verifying, for each digital certificate in the plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft;

determining, by the processor unit, whether one of the plurality of digital certificates is compromised;

selecting, by the processor unit, a selected number of the plurality of digital certificates in response to the determination that the one of the plurality of digital certificates is compromised, the selected number being determined based upon a quorum rule selected from quorum rules that are based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded;

verifying, by the processor unit, the data for use on the aircraft using the selected number of the plurality of digital certificates;

wherein verifying the data for use on the aircraft using the selected number of the plurality of digital certificates comprises determining whether at least a specified number of the selected number of the plurality of digital certificates is valid; and

wherein the specified number is defined by the quorum rule, the quorum rule being composed of one, or more, of:

a quorum rule for an operator of an aircraft;

a quorum rule for an aircraft maintenance entity;

a quorum rule for an aircraft type;

a quorum rule for an aircraft system on which data will be used;

a quorum rule for the number of aircraft systems on which data will be used; and

a quorum rule for use when a certificate authority is known to be, or suspected of being compromised.

2. The method of claim **1**, wherein the plurality of digital certificates is from a plurality of certificate authorities.

3. The method of claim **1** or **2**, further comprising:

selecting the quorum rule from a plurality of quorum rules in response to the determination that the one of the plurality of digital certificates is compromised.

4. The method of any one of claims **1** to **3**, wherein the data comprises software for use on the aircraft.

5. The method of any one of claims **1** to **4**, wherein the processor unit is a processor unit in an aircraft network data processing system on the aircraft.

6. An apparatus, comprising:

a data verification module configured to:

receive a plurality of digital certificates associated with data for use on an aircraft;

verify, for each digital certificate in the plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft;

determine whether one of the plurality of digital certificates is compromised;

select a selected number of the plurality of digital certificates in response to the determination that the one of the plurality of digital certificates is compromised, the selected number being determined based upon a quorum rule selected, from quorum rules based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded; and

the selected number being determined on a quorum rule selected from quorum rules based on at least two of:

an aircraft system on with the data will be loaded;

a number of aircraft systems on which the data will be used;

a location of the aircraft when the data is loaded; and

when a determination is made that a certificate authority is known to be, or is suspected of being compromised;

verify the data for use on the aircraft using the selected number of the plurality of digital certificates;

wherein verifying the data for use on the aircraft using the selected number of the plurality of digital certificates comprises determining whether at least a specified number of the selected number of the plurality of digital certificates is valid; and

wherein the specified number is defined by the quorum rule, the quorum rule being composed of one, or more, of:

a quorum rule for an operator of an aircraft;

a quorum rule for an aircraft maintenance entity;

a quorum rule for an aircraft type;

a quorum rule for an aircraft system on which data will be used;

a quorum rule for the number of aircraft systems on which data will be used; and

a quorum rule for use when a certificate authority is known to be, or suspected of being compromised.

7. The apparatus of claim **6**, wherein the plurality of digital certificates is from a plurality of certificate authorities.

8. The apparatus of claim **6** or **7**, wherein the data verification module is configured to select the quorum rule from a plurality of quorum rules in response to the determination that the one of the plurality of digital certificates is compromised.

9. The apparatus of claim **6**, wherein the data comprises software for use on the aircraft.

10. The apparatus of claim **6**, wherein the data verification module is implemented in a processor unit in an aircraft network data processing system on the aircraft.

11. A method for verifying data for use on an aircraft, the method comprising:

receiving, by a processor unit, a plurality of digital certificates associated with the data:

verifying, for each digital certificate in the plurality of digital certificates, an issuer of the digital certificate as being in a list of acceptable certificate authorities, in a processing system on the aircraft;

determining, by the processor unit, whether one of the plurality of digital certificates is compromised;

selecting, by the processor unit, a quorum rule, based upon a number of aircraft systems on which the data will be used and a location of the aircraft when the data is loaded, from quorum rules wherein the quorum rule is at least one of:

a quorum rule for an operator of an aircraft;

a quorum rule for an aircraft maintenance entity;

a quorum rule for an aircraft type;

a quorum rule for an aircraft system on which data will be used;

a quorum rule for the number of aircraft systems on which data will be used;

a quorum rule for use when a certificate authority is known to be, or suspected of being compromised;

a quorum rule for use when it is determined that none of the plurality of digital certificates is compromised; and

verifying, by the processor unit, the data for use on the aircraft using a selected number of the plurality of digital certificates as defined by the quorum rule.

12. The method of claim **11**, wherein the plurality of digital certificates is from a plurality of certificate authorities.

13. The method of claim **11**, wherein verifying the data for use on the aircraft using the selected number of the plurality of digital certificates comprises determining whether at least a specified number of the selected number of the plurality of digital certificates is valid as defined by the quorum rule.

14. The method of claim **13**, wherein:

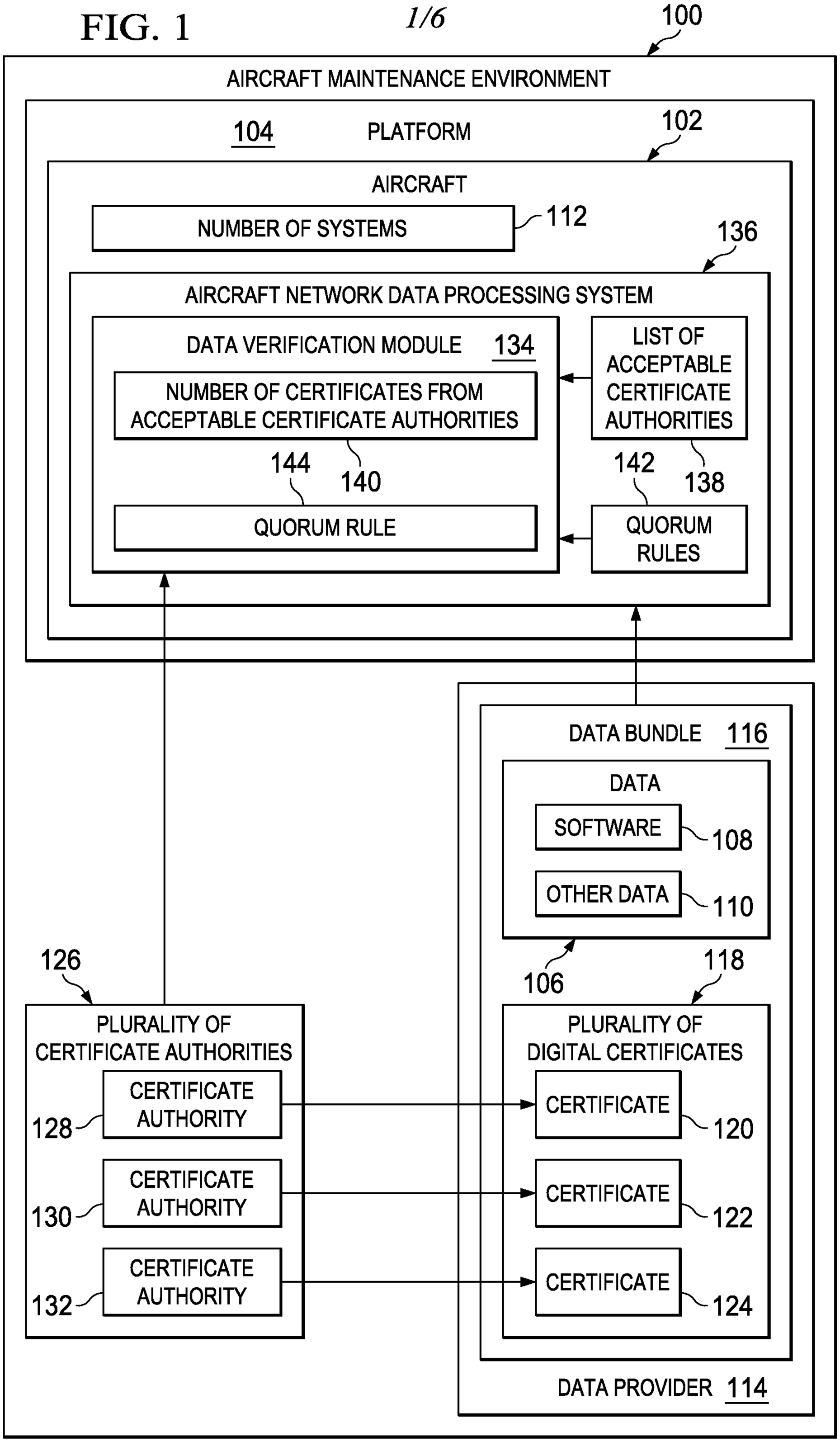
the first quorum rule indicates that the specified number of the selected number of the plurality of digital certificates is less than the selected number; and

the second quorum rule indicates that the specified number of the selected number of the plurality of digital certificates equals the selected number.

15. The method of claim **11**, wherein the data comprises software for use on the aircraft.

16. The method of claim **11**, wherein the processor unit is a processor unit in an aircraft network data processing system on the aircraft.

FIG. 1


100
AIRCRAFT MAINTENANCE ENVIRONMENT
104
PLATFORM
102
AIRCRAFT
NUMBER OF SYSTEMS
112
136
AIRCRAFT NETWORK DATA PROCESSING SYSTEM
DATA VERIFICATION MODULE
134
NUMBER OF CERTIFICATES FROM ACCEPTABLE CERTIFICATE AUTHORITIES
144
140
QUORUM RULE
LIST OF ACCEPTABLE CERTIFICATE AUTHORITIES
142
138
QUORUM RULES
DATA BUNDLE
116
DATA
SOFTWARE
108
OTHER DATA
110
106
118
PLURALITY OF DIGITAL CERTIFICATES
CERTIFICATE
120
CERTIFICATE
122
CERTIFICATE
124
126
PLURALITY OF CERTIFICATE AUTHORITIES
128
CERTIFICATE AUTHORITY
130
CERTIFICATE AUTHORITY
132
CERTIFICATE AUTHORITY
DATA PROVIDER
114

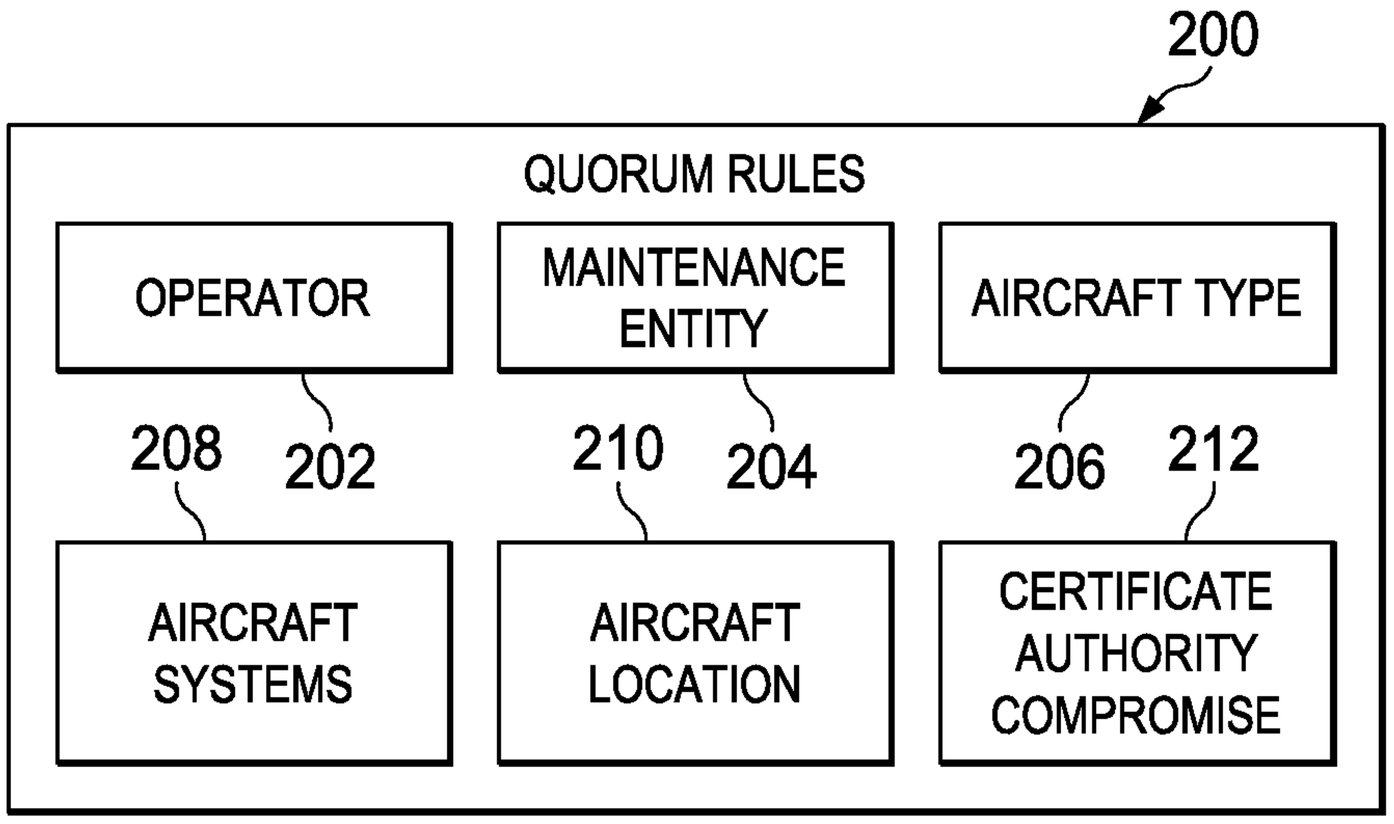

200
QUORUM RULES
OPERATOR
MAINTENANCE ENTITY
AIRCRAFT TYPE
208
202
210
204
206
212
AIRCRAFT SYSTEMS
AIRCRAFT LOCATION
CERTIFICATE AUTHORITY COMPROMISE

FIG. 2

310
LIST OF ACCEPTABLE CERTIFICATE AUTHORITIES
312
CERTIFICATE AUTHORITY A
314
CERTIFICATE AUTHORITY B
302
DATA BUNDLE
304
CERTIFICATE A
CERTIFICATE B
306
CERTIFICATE C
308
DATA VERIFICATION
300
CERTIFICATE A OR B VALID
316

FIG. 3

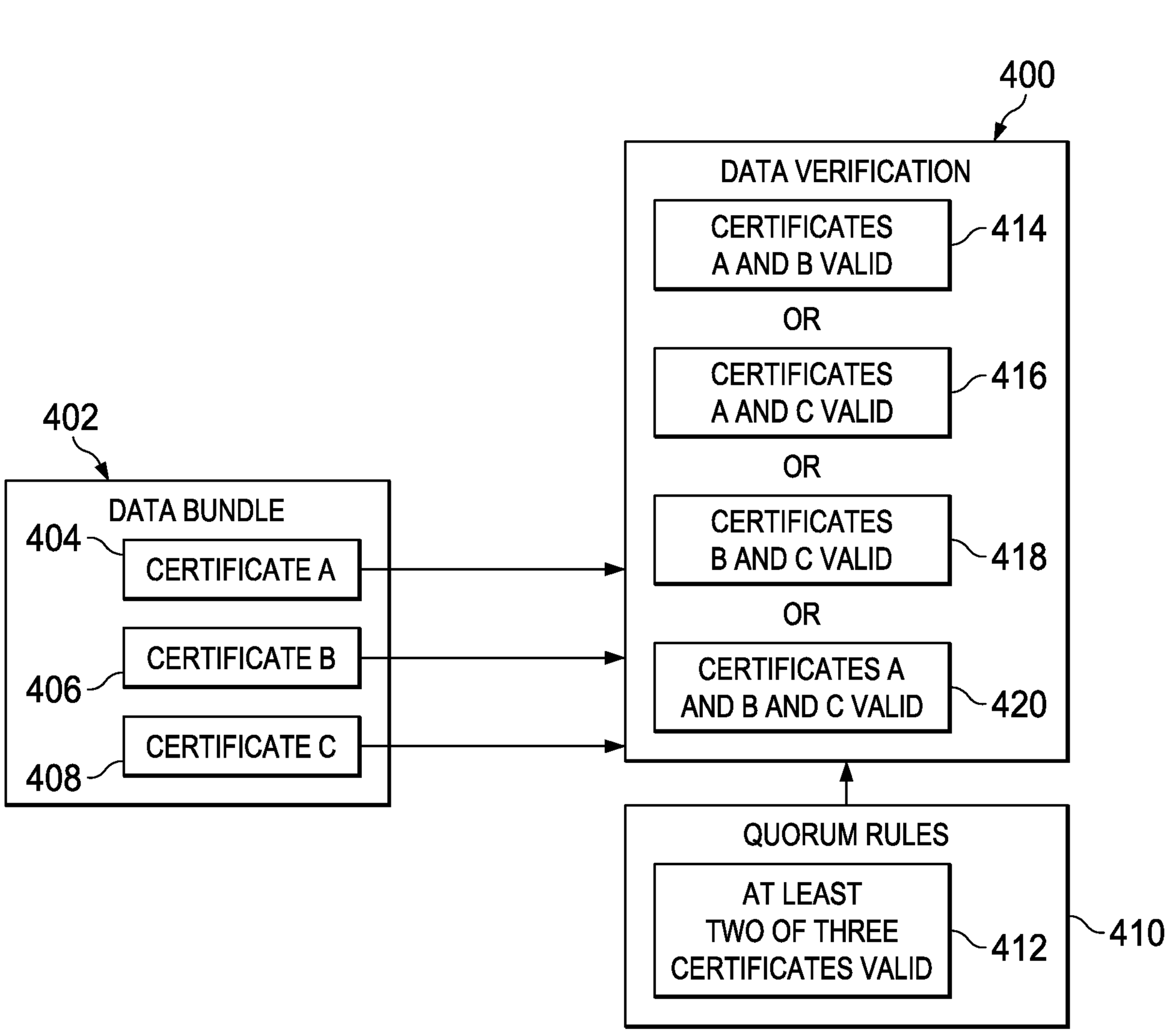

400
DATA VERIFICATION
CERTIFICATES A AND B VALID
414
OR
CERTIFICATES A AND C VALID
416
OR
CERTIFICATES B AND C VALID
418
OR
CERTIFICATES A AND B AND C VALID
420
402
DATA BUNDLE
404
CERTIFICATE A
CERTIFICATE B
406
CERTIFICATE C
408
QUORUM RULES
AT LEAST TWO OF THREE CERTIFICATES VALID
412
410

FIG. 4

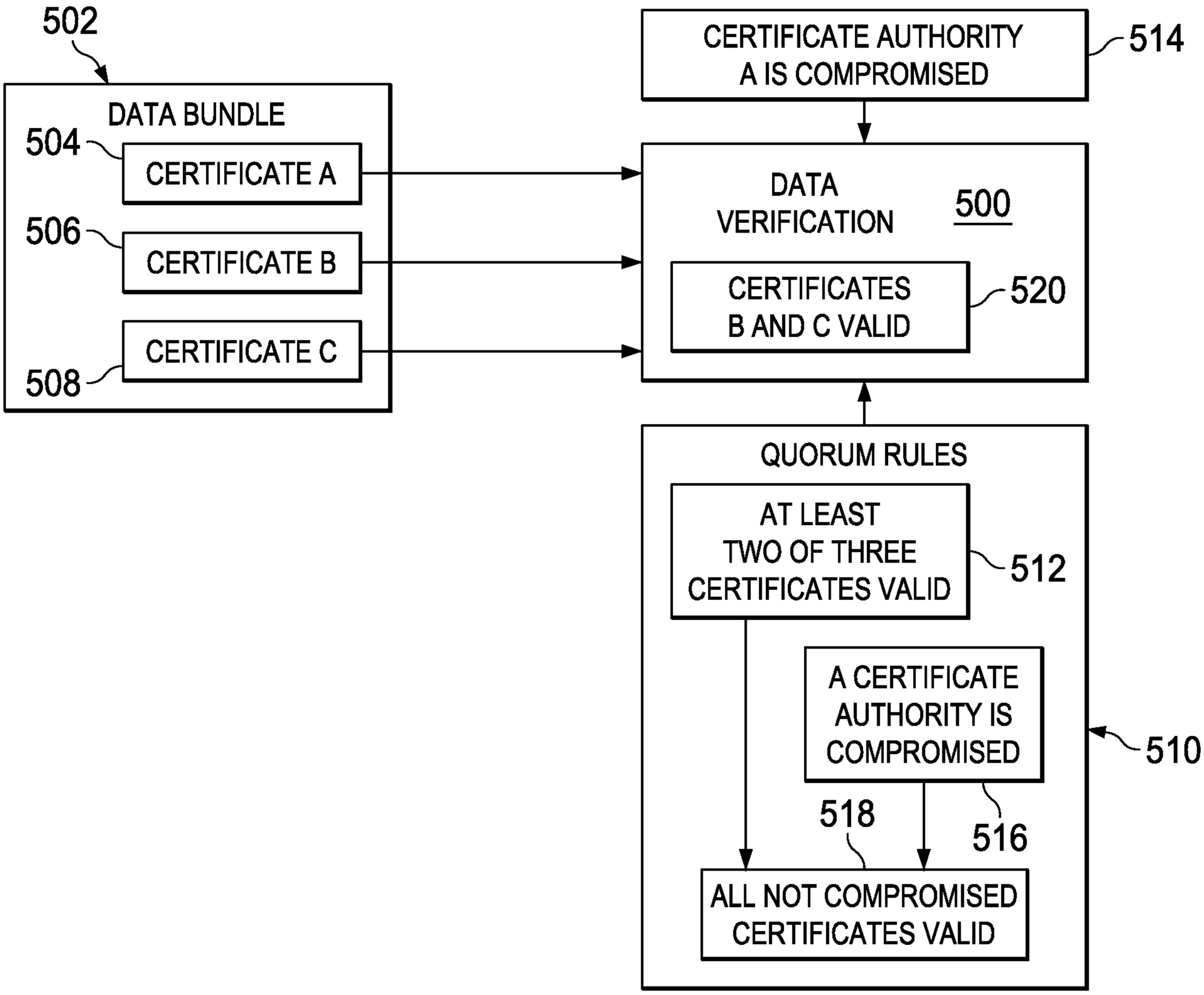

502
DATA BUNDLE
504
CERTIFICATE A
506
CERTIFICATE B
CERTIFICATE C
508
CERTIFICATE AUTHORITY A IS COMPROMISED
514
DATA VERIFICATION
500
CERTIFICATES B AND C VALID
520
QUORUM RULES
AT LEAST TWO OF THREE CERTIFICATES VALID
512
A CERTIFICATE AUTHORITY IS COMPROMISED
518
516
ALL NOT COMPROMISED CERTIFICATES VALID
510

FIG. 5

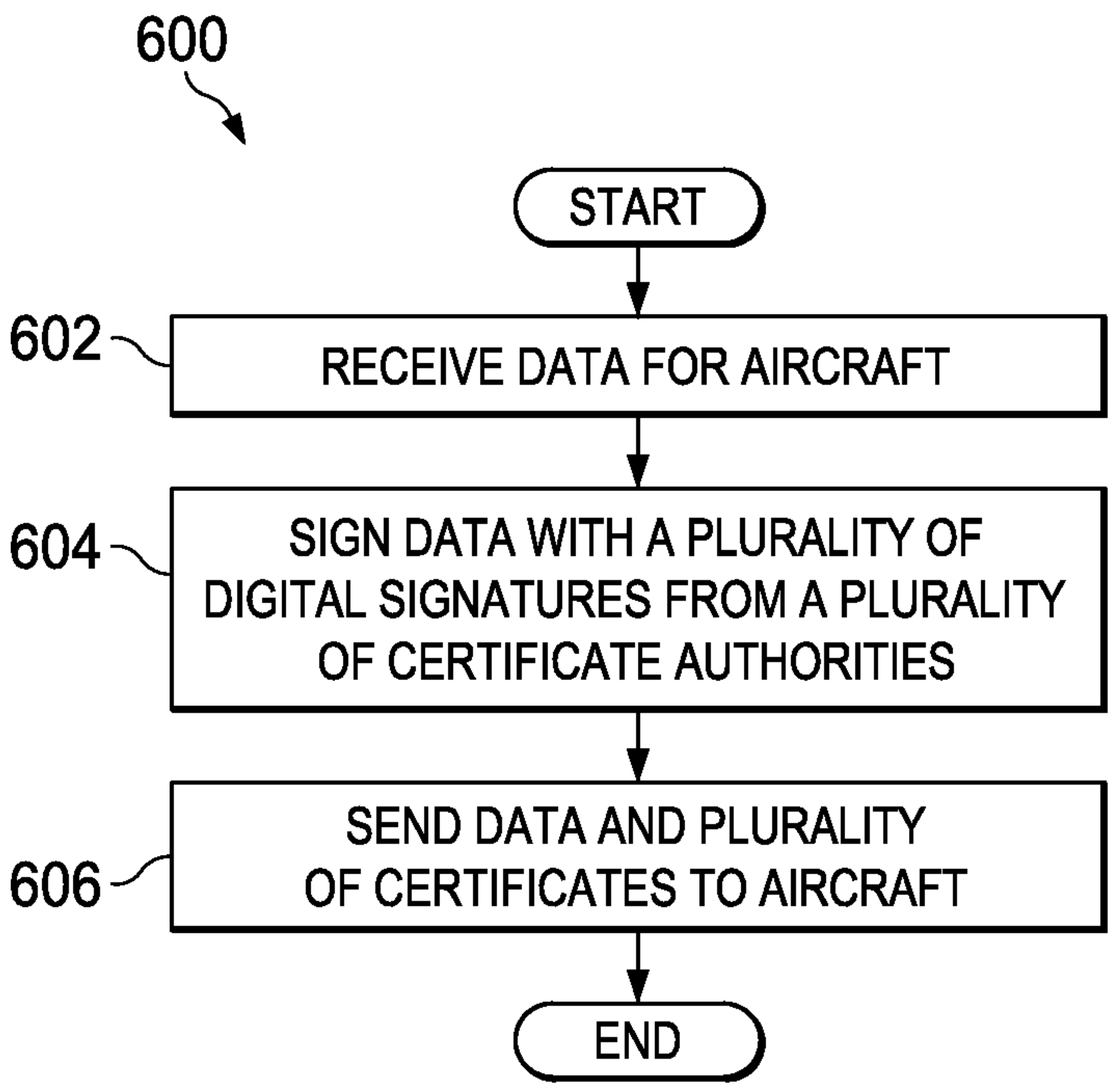

600
START
602
RECEIVE DATA FOR AIRCRAFT
604
SIGN DATA WITH A PLURALITY OF DIGITAL SIGNATURES FROM A PLURALITY OF CERTIFICATE AUTHORITIES
606
SEND DATA AND PLURALITY OF CERTIFICATES TO AIRCRAFT
END

FIG. 6

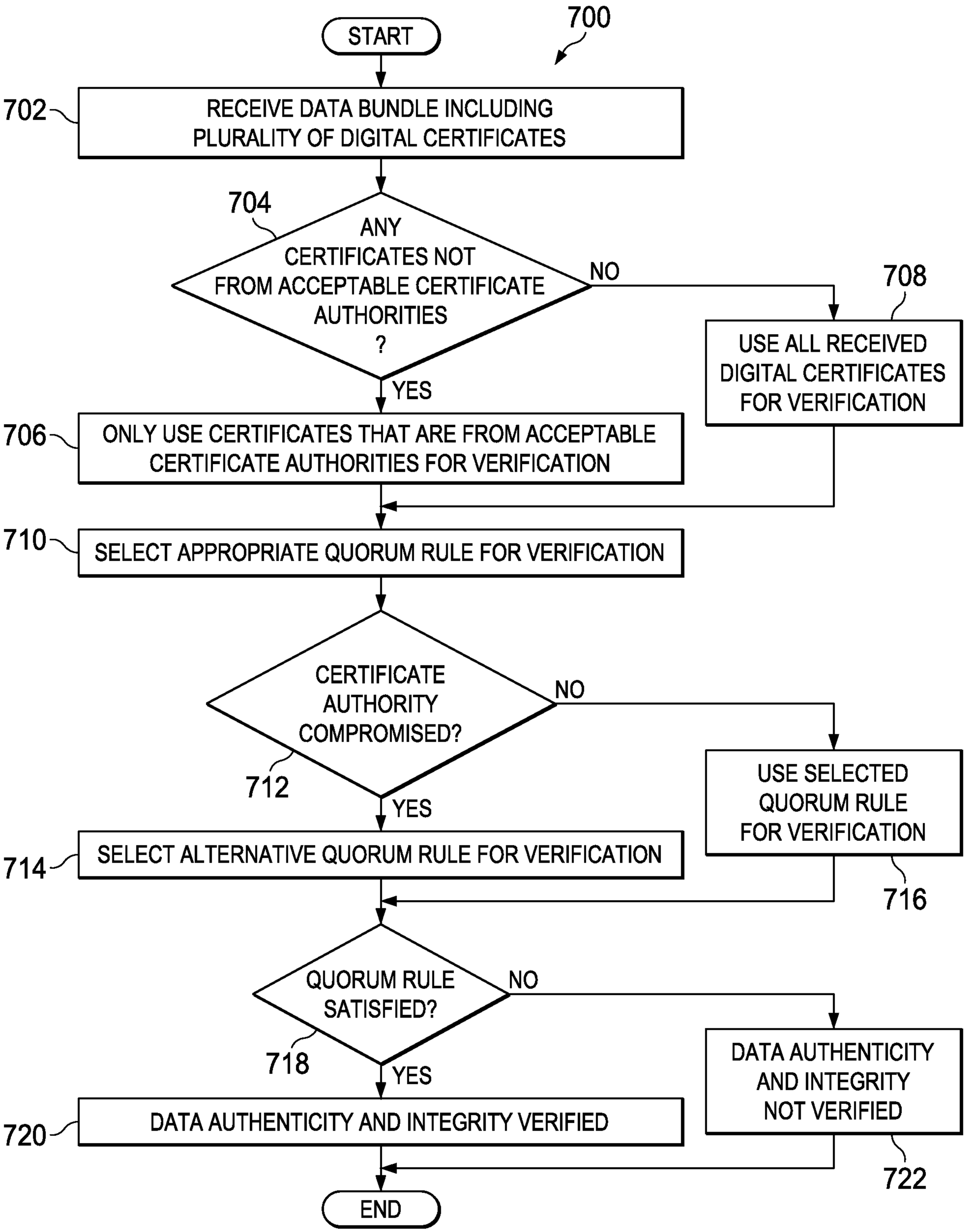
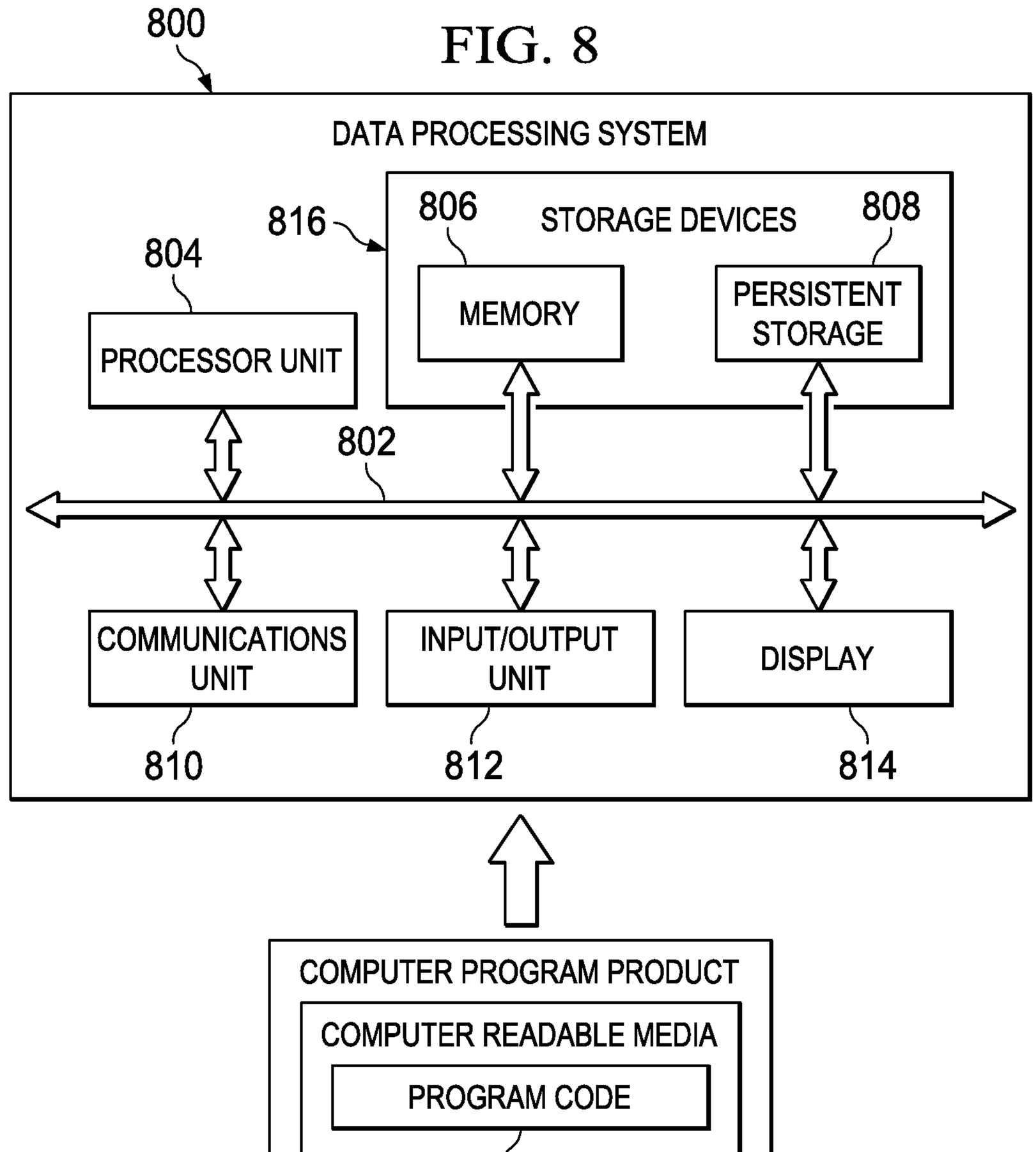
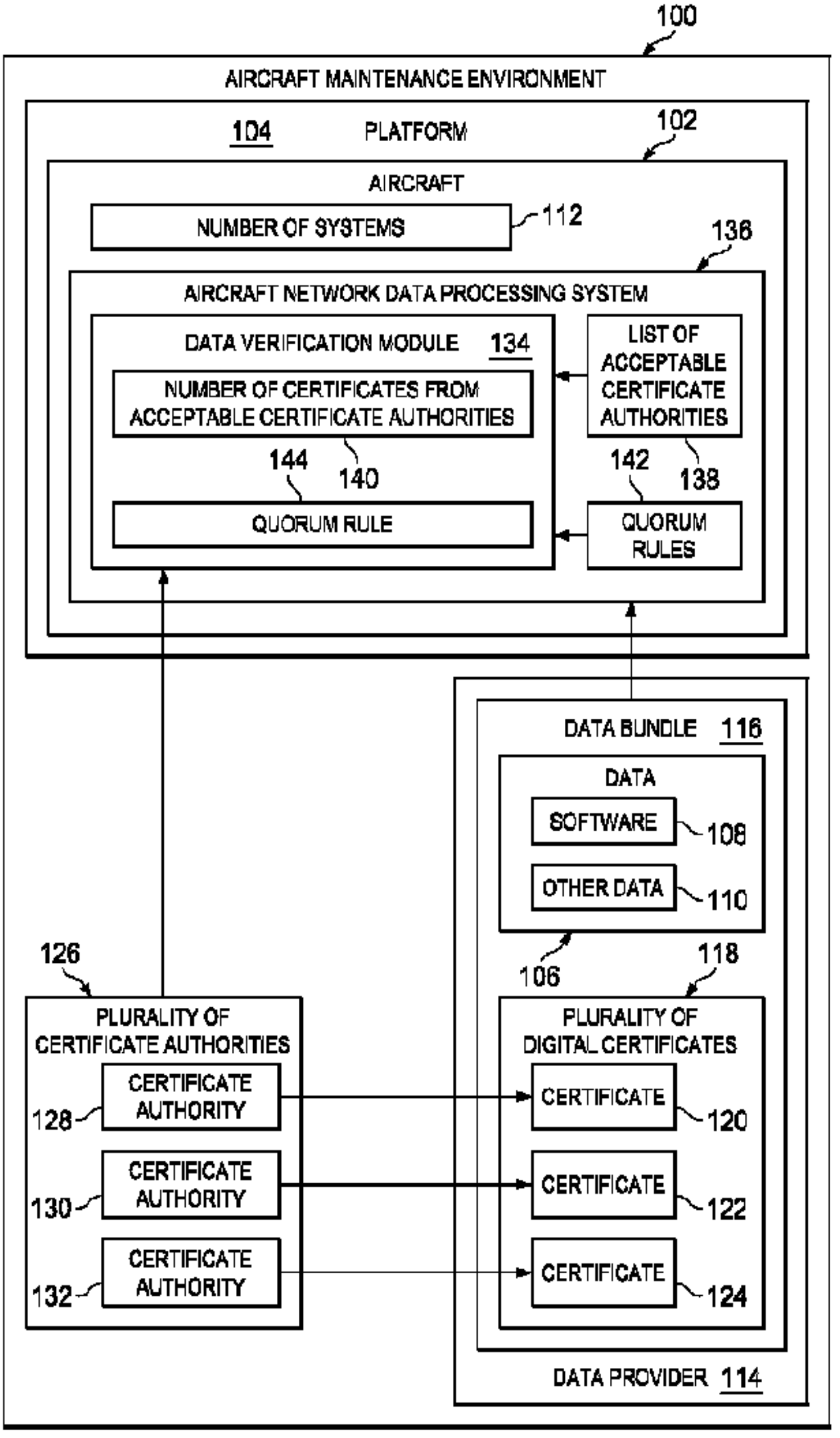

700
START
702
RECEIVE DATA BUNDLE INCLUDING PLURALITY OF DIGITAL CERTIFICATES
704
ANY CERTIFICATES NOT FROM ACCEPTABLE CERTIFICATE AUTHORITIES ?
NO
708
USE ALL RECEIVED DIGITAL CERTIFICATES FOR VERIFICATION
YES
706
ONLY USE CERTIFICATES THAT ARE FROM ACCEPTABLE CERTIFICATE AUTHORITIES FOR VERIFICATION
710
SELECT APPROPRIATE QUORUM RULE FOR VERIFICATION
CERTIFICATE AUTHORITY COMPROMISED?
NO
712
USE SELECTED QUORUM RULE FOR VERIFICATION
YES
714
SELECT ALTERNATIVE QUORUM RULE FOR VERIFICATION
716
QUORUM RULE SATISFIED?
NO
718
DATA AUTHENTICITY AND INTEGRITY NOT VERIFIED
YES
720
DATA AUTHENTICITY AND INTEGRITY VERIFIED
722
END

FIG. 7

FIG. 8


800
DATA PROCESSING SYSTEM
816
806
STORAGE DEVICES
808
804
MEMORY
PERSISTENT STORAGE
PROCESSOR UNIT
802
COMMUNICATIONS UNIT
INPUT/OUTPUT UNIT
DISPLAY
810
812
814
COMPUTER PROGRAM PRODUCT
COMPUTER READABLE MEDIA
PROGRAM CODE
818
COMPUTER READABLE STORAGE MEDIA
824
826
822
COMPUTER READABLE SIGNAL MEDIA
820


100
AIRCRAFT MAINTENANCE ENVIRONMENT
104
PLATFORM
102
AIRCRAFT
NUMBER OF SYSTEMS
112
136
AIRCRAFT NETWORK DATA PROCESSING SYSTEM
DATA VERIFICATION MODULE
134
NUMBER OF CERTIFICATES FROM ACCEPTABLE CERTIFICATE AUTHORITIES
144
140
QUORUM RULE
LIST OF ACCEPTABLE CERTIFICATE AUTHORITIES
142
138
QUORUM RULES
DATA BUNDLE
116
DATA
SOFTWARE
108
OTHER DATA
110
106
118
126
PLURALITY OF CERTIFICATE AUTHORITIES
CERTIFICATE AUTHORITY
128
CERTIFICATE AUTHORITY
130
CERTIFICATE AUTHORITY
132
PLURALITY OF DIGITAL CERTIFICATES
CERTIFICATE
120
CERTIFICATE
122
CERTIFICATE
124
DATA PROVIDER
114