(54) Titre : CONTROLE DE L'ACCES A DES DONNEES CLINIQUES ANALYSEES PAR DES RESSOURCES INFORMATIQUES A DISTANCE
(54) Title: CONTROLLING ACCESS TO CLINICAL DATA ANALYZED BY REMOTE COMPUTING RESOURCES

(57) Abrégé/Abstract:
A method for controlling access to data being processed by a remote computing resource includes issuing a public encryption key for a data creator from a public certificate authority, detecting an encounter with a data owner, creating private encryption keys for the data creator and the data owner in response to detecting the encounter, encrypting data being sent to the remote computing resource with the public encryption key, the data creator's private encryption key, and the data owner's private encryption key, decrypting the data based on public verification of the public encryption key and local verification of the data creator's private encryption key and the data owner's private encryption key at the remote computing resource, and controlling the data creator's access to the data by altering the permission of at least one of the public encryption key and data creator's private encryption key.

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

[Continued on next page]

(54) Title: CONTROLLING ACCESS TO CLINICAL DATA ANALYZED BY REMOTE COMPUTING RESOURCES

FIGURE 4

(57) Abstract: A method for controlling access to data being processed by a remote computing resource includes issuing a public encryption key for a data creator from a public certificate authority, detecting an encounter with a data owner, creating private encryption keys for the data creator and the data owner in response to detecting the encounter, encrypting data being sent to the remote computing resource with the public encryption key, the data creator's private encryption key, and the data owner's private encryption key, decrypting the data based on public verification of the public encryption key and local verification of the data creator's private encryption key and the data owner's private encryption key at the remote computing resource, and controlling the data creator's access to the data by altering the permission of at least one of the public encryption key and data creator's private encryption key.
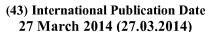
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

CONTROLLING ACCESS TO CLINICAL DATA ANALYZED BY REMOTE COMPUTING RESOURCES

The present application relates to analyzing clinical data by remote computing resources. It finds particular application in conjunction with systems and
5   methods for controlling healthcare provider access to clinical data analyzed by remote computing resources and will be described with particular reference thereto. However, it is to be understood that it also finds application in other usage scenarios and is not necessarily limited to the aforementioned application.

It is essential to ensure that information being transmitted by and between the
10 clinical resources is securely protected. Because patient medical information is confidential and protected by Federal and State laws and regulations, such as HIPAA in the US, it is important that the communicated clinical data is protected during its transmission and storage. The security of communications between clinical resources is typically enabled by controlling access to the clinical data. Specifically, the communication clinical data is
15 encrypted to protect the content of transmitted messages so that intruders cannot read or modify the clinical data. With the growth of remote computing resources, most modern healthcare communication architectures tend to be open, interconnected environments. Sensitive clinical data no longer reside on mainframes physically isolated within a healthcare provider, where physical security measures can be taken to defend the data and
20 the system. Clinical data is rather kept in an environment where data is outsourced to or processed on remote computing resource in order to allow de-centralized access for family doctors, medical specialists and even non-medical care providers. In order to allow sharing of clinical data among different healthcare providers or with external parties, it is advantageous to provide end-to-end security techniques such that trusted parties are allowed
25 access to the clinical data on the network, and that the owner of the data has the ability to limit what data is accessible to others.

The present invention provides a new and improved apparatus and method which overcomes the above-referenced problems and others.

30   In accordance with one aspect, a method for controlling access to data being processed by a remote computing resource is provided. The method including the steps of issuing a public encryption key for a data creator from a public certificate authority, detecting an encounter with a data owner, creating private encryption keys for the data creator and the data owner in response to detecting the encounter, encrypting data being sent

to the remote computing resource, decrypting the data based on public verification of the public encryption key and local verification of the data creator's private encryption key and the data owner's private encryption key at the remote computing resource, and controlling the data creator's access to the data by altering the permission of at least one of the public

5   encryption key and data creator's private encryption key.

In accordance with another aspect, a system for controlling access to data being processed by a remote computing resource is provided. The system includes a public certificate authority which issues a public encryption key to the data creator. A data creator collects data from a data owner and encrypts the data with the public encryption key, a data

10   creator private encryption key and a data owner encryption key. The remote computing resource decrypts the data based on public verification of the public encyrption key and local verification of the data creator's private encryption key and the data owner's private encryption key at the remote computing resource and includes a local private certification authority which creates a data creator private encryption key and a data owner encryption key

15   in response to detecting a data owner encounter at the remote computing resource. The data owner controls the data creator's access to the data by altering the permission of at least one of the public encryption key and data creator's private encryption key.

In accordance with another aspect, a method for controlling access to data being processed by a remote computing resource is provided. The method includes issuing a

20   public encryption key for a data creator from a public certificate authority, creating private encryption keys for the data creator and the data owner in response to detecting the encounter, encrypting data being sent to the remote computing resource with at least one of the public encryption key, the data creator's private encryption key, and the data owner's private encryption key, and decrypting and storing the data based on public verification of the public

25   encryption key and local verification of at least one of the data creator's private encryption key and the data owner's private encryption key at the remote computing resource.

According to one aspect of the present invention, there is provided a method for controlling access to data being processed by a remote computing resource, the method comprising: issuing a first encryption key for a data creator from a first certificate authority located outside the remote computing resource; detecting an encounter with a data owner;

5   creating, by a second certificate authority of the remote computing resource, a second encryption key for the data creator and an encryption key for the data owner in response to detecting the encounter; the data creator encrypting data being sent to the remote computing resource with the first encryption key, the data creator's second encryption key, and the data owner's encryption key; decrypting and storing the data based on verification of the first

10   encryption key by a verification authority located outside the remote computing resource and based on a verification of at least one of the data creator's second encryption key and the data owner's encryption key at the remote computing resource; and controlling the data creator's access to the data by altering the permission of at least one of the data creator's first and second encryption key.

15   According to another aspect of the present invention, there is provided a system for controlling access to data being processed by a remote computing resource, the system comprising: a first certificate authority located outside the remote computing resource, which issues a first encryption key to a data creator; the data creator being configured to collect data from a data owner and encrypt the data with the first encryption key, a data

20   creator's second encryption key and a data owner's encryption key; the remote computing resource being configured to decrypt and store the data based on a verification of the first encryption key by a verification authority located outside the remote computing resource and based on a verification of the data creator's second encryption key and the data owner's encryption key at the remote computing resource and includes: a second certification authority

25   which creates the data creator second encryption key and the data owner's encryption key in response to detecting a data owner encounter at the remote computing resource; wherein the data owner controls the data creator's access to the data by altering the permission of at least one of the data creator's first and second encryption key.

One advantage resides in providing a patient or data owner the ability to control access to clinical data being analyzed.

Another advantage resides in the ability to extend or rescind permission to access clinical data analyzed by remote computing resources.

Still further advantages of the present invention will be appreciated to those of ordinary skill in the art upon reading and understanding the following detailed description.

5   The invention may take form in various components and arrangements of components, and in various steps and arrangements of steps. The drawings are only for purposes of illustrating the preferred embodiments and are not to be construed as limiting the invention.

FIGURE 1 is a block diagram of an IT infrastructure in accordance with the

10   present application.

FIGURE 2 is a block diagram of a system for issuing public and private keys to healthcare providers and patients in accordance with the present application.

FIGURE 3 is a block diagram of a system for verifying public and private keys issued to healthcare providers and patients in accordance with the present application.

15   FIGURE 4 is a flowchart diagram of a method for transmitting data from a data creator to a cloud in accordance with the present application.

FIGURE 5 is a flowchart diagram of a method for transmitting data from a cloud to a data creator in accordance with the present application.

20   With reference to FIGURE 1, a block diagram illustrates one embodiment of an information technology (IT) infrastructure **10** of a system for controlling access to clinical data analyzed by a remote computing resource. The IT infrastructure **10** suitably includes one or more healthcare systems and providers **12**, a remote computing resource **14**, and the like, interconnected via a communications network **16**. It is contemplated that the communications

25   network **16** includes one or more of the Intranet, a local area network, a wide area network, a wireless network, a wired network, a cellular network, a data bus, a personal area network, and the like. The healthcare provider **12** collects clinical data related to a patient **18** cared for by the healthcare system or medical institution which is analyzed by the remote computing resource **14**, which in one embodiment is located in a cloud infrastructure. In other

30   embodiments the system may be located at a single location. In yet another embodiment may exist in a secure environment, but data transmission is over public media or shared infrastructure.

As used herein, "cloud" may refer to a collection of resources (e.g., hardware, data and/or software) provided and maintained by an off-site or off-premise party (e.g., third

party), wherein the collection of data and resources can be accessed by an identified user via a network. The resources can include data storage services, data processing services (e.g., applications), and many other services that are conventionally associated with and reside within personal computers, local or "on-premise" servers, having at least one processing device such as a microprocessor, graphics processor among other processing devices and associated components. In general, cloud computing may be employed to perform services in a dissociative way, i.e., the client may not know where the service is performed as long as the service is performed with the expected quality of service.

As used herein, "clinical data" may refer to data collected from a patient or from a medical institution in any number of conventional ways. For example, clinical data may be collected in the field by a healthcare provider such as a physician or clinician. Alternatively, a patient may be admitted to a healthcare provider such as a hospital or an emergency clinic and related clinical data may be collected by, for example, admissions or administration at the healthcare provider. Clinical data may be collected by other medical devices, such as, patient monitors including various subsystems for each vital sign such as SpO2, temperature, blood pressure, heart rate, etc., various imaging equipment, pacemaker monitors and interrogation devices, laboratory equipment, and other clinical data collection systems. Clinical data may also be collected by a patient's home monitoring systems, which may report physical, chemical, electrical or other patient's clinical parameters. Data collection used herein may be episodic, based on a predefined event or stochastic process, periodic, such as every 4 hours, or continuous. Data collection may be real time, near real-time or previously acquired and later uploaded.

The healthcare system, application, process, or provider (referred to as healthcare provider here forward) **12** creates data on behalf of the data owner, or processes the collected clinical data and securely transmits the clinical data to the remote computing resource **14** for analysis. After receiving the clinical data, the remote computing resource **14** processes the clinical data and generates one or more results from the analysis. For example, the remote computing resource **14** may compare the patient's clinical data with baseline clinical data, demographic data, all of which may be stored in or accessible by the remote computing resource **14**. The analysis may also include the generation of one or more reports by the remote computing resource **14**, which may include performance reports, clinical recommendations or advisories, or chronological graphical reports, including charts indicating healthy and unhealthy results in clear and easy to read display formats, for example. In an exemplary embodiment, result data corresponding to the results are securely

transmitted back to healthcare system, provider, or actual data owner **12** for further processing.

To securely transmit the clinical and result data, the healthcare provider **12** and the remote computing resource **14** encrypt the clinical and result data to maintain the security and integrity of the data transmitted within the IT infrastructure **10**. Because patient medical information is confidential and protected by Federal and State laws and regulations, such as HIPAA in the US, it is important that the communicated clinical data is protected during its transmission. The present application provides systems and methods for ensuring that all clinical data is protected while they are transmitted and that only usable by parties and processes that possess the specific set of public and private encryption keys to access such data. The transmitted data may be encrypted or scrambled, and various user access validation steps may be incorporated to protect the integrity of the data and the privacy of the patient. For example, the clinical data is encrypted before it is transmitted from the healthcare system or provider **12** to the remote computing resource **14**. Once at the remote computer resource **14**, the clinical data is decrypted and processed for analysis. The result data from the analysis is then encrypted again and transmitted back to the healthcare provider **12** from the remote computing resource **14** where it is decrypted for further processing.

To further maintain security and integrity of the data, public and private encryptions keys are issued to the healthcare system or provider **12** and data owner or patient (referred to as patient here forward) **18** respectively to control access to the data analyzed by remote computing resources. With reference to FIGURE 2, a system for issuing public and private keys to the healthcare provider **12** and patient **18** is illustrated. When the healthcare provider **12** subscribes to the remote computer resource **14** for the processing of clinical data, the healthcare provider requests a public encryption key from a public certificate authority **20**. After the health provider **12** is verified, the public certificate authority (PuK Authority) **20** issues a public encryption key **22** to the healthcare provider **12**. When a patient is introduced to the healthcare provider **12**, the communication of collected clinical data for processing by the remote computing resource **14** creates a patient encounter for the patient **18**. In response to detecting a new patient encounter, a local private certificate authority **24** (PrK Authority) issues private encryption keys **26, 28** for healthcare provider **12** and the patient **18** respectively. In one embodiment, the private encryption keys **26, 28** for healthcare provider **12** and the patient **18** are held in escrow at the healthcare provider location until data identified for transmission for the healthcare provider and patient is identified. In another

embodiment, the private encryption keys **26, 28** for healthcare provider **12** and the patient **18** are held in escrow at the remote computing resource **14**.

To provide additional security and enable the user to control access, the clinical and results data are encrypted with the public encryption key **22**, the healthcare provider's private encryption key **26**, and the patient's private encryption key **28**. For example, before the clinical data is transmitted from the healthcare provider **12** to the remote computing resource **14**, the clinical data is encrypted with the public encryption key **22**, the healthcare provider's private encryption key **26**, and the patient's private encryption key **28**. Likewise, before the results data is transmitted from the remote computing resource **14** to the healthcare provider **12**, the result data is encrypted with the public encryption key **22**, the healthcare provider's private encryption key **26**, and the patient's private encryption key **28**.

After the clinical data is encrypted and transmitted from the healthcare provider **12** to the remote computing resource **14**, the remote computing resource **14** decrypts the clinical data based on a verification of the public encryption key **22**, the healthcare provider's private encryption key **26**, and/or the patient's private encryption key **28**. Likewise, after encrypted result data is transmitted from the remote computing resource **14** to the healthcare provider **12**, the healthcare provider **12** decrypts the result data based on a verification of the public encryption key **22**, the healthcare provider's private encryption key **26**, and/or the patient's private encryption key **28**. With reference to FIGURE 3, a system for verifying public and private keys of the healthcare provider **12** and patient **18** is illustrated. Specifically, the decryption of the clinical and result data is based on verification of the validity of public encryption key **22** by a public verification authority **30** (PuK Verification) located outside the cloud infrastructure and verification of the validity of the healthcare provider's private encryption key **26**, and/or the patient's private encryption key **28** by a private verification authority **32** located within the cloud infrastructure. As described above, the encryption session is based on the public encryption key **22** and both the healthcare provider private encryption key **26** and the patient's private encryption key **28**. The decryption session is based on the verification of the validity of the healthcare provider's public encryption key **22** and private encryption key **26** and/or the patient's private encryption key **28**. Thus access to the clinical and report data is controlled by the verification of the validity of the public encryption key and the healthcare provider's private encryption key.

The additional encryption and verification protection also enables the patient to control access to the clinical data and results. Specifically, the patient **18** can authorize

parties to use the existing clinical and result data by sharing the patient's private encryption key **28** with the party. Such an action does not require the healthcare provider **12** permission. In order to provide access of the clinical and results data to a party, the party would utilize its own public encryption key and the patient's private encryption key **28** to encrypt/decrypt the clinical and result data. It should also be appreciated that patient **18** can de-authorize access of the clinical and result data to the healthcare provider **12** or other parties. The patient can de-authorize application use of the existing clinical and result data, or any sub part of it by notifying the local verification authority **32** and referencing which public keys are no longer permitted to access the clinical and result data or sub part thereof.

In another embodiment, business rules based on local verification authority are established for requiring the patient's permission for which parties are permitted or rescinded from accessing particular data. For example, the local verification authority **32** includes a table of the parties that request access to the patient's data. The table enables the patient **18** to edit and match the privileges of parties to particular data sets. Further, additional business rules can be created on the patient's request to destroy aspects of the data that require the patient's permission. For example, the healthcare provider **12** will have access to data sets which they generate if the data is being utilized for performance calculations. The business rules would delete all sensitive personal information from the data and thus would not require data owner permission to access the data. Likewise, if the data does not include sensitive personal information and is suitable for secondary use (performance calculations and the like) the local verification authority requires a party to have a public encryption key to access the data.

The components of the IT infrastructure **10** suitably include processors executing computer executable instructions embodying the foregoing functionality, where the computer executable instructions are stored on memories associated with the processors. It is, however, contemplated that at least some of the foregoing functionality can be implemented in hardware without the use of processors. For example, analog circuitry can be employed. Further, the components of the IT infrastructure **10** include communication units providing the processors an interface from which to communicate over the communications network **16**. Even more, although the foregoing components of the IT infrastructure **10** were discretely described, it is to be appreciated that the components can be combined.

FIGURE 4 illustrates a flowchart diagram of a method for transmitting data from a data creator to a cloud. In a step **100**, a data creator requests a public encryption key from a certificate authority. The request is created when the data creator subscribes to the

system using the created data. In a step **102**, the certificate authority issues a public key (PuK) to the data creator. In a step **104**, an encounter is created for a data owner. In a step **106**, a local certificate authority in the cloud creates private keys (PrK) for the data creator and the data owner. In a step **108**, the data is created and encoded with the creation authority public key (PuK) and both private keys (PrK) for the data creator and the data owner. In a step **110**, the data is encrypted and transmitted to the cloud. In a step **112**, the cloud decrypts the data based on a verification authority for the public key (PuK) and on an internal verification authority for the private keys (PrK) for the data creator and the data owner.

FIGURE 5 illustrates a flowchart diagram of a method for transmitting data from a cloud to a data creator. In a step **120**, a data requestor calls to a cloud with a public key (PuK) and a data request. In a step **122**, a verification authority notifies the cloud of the validity of the public key (PuK). In a step **124**, the data is encoded with a public key from a certificate authority and private keys for both the data creator and data owner from a local certificate authority in the cloud. In a step **126**, data is sent to the data requestor from the cloud. In a step **128**, the data requestor decrypts the data based on a verification authority for the public key (PuK) and on an internal verification authority for the private keys (PrK) for the data creator and the data owner.

As used herein, a memory includes one or more of a non-transient computer readable medium; a magnetic disk or other magnetic storage medium; an optical disk or other optical storage medium; a random access memory (RAM), read-only memory (ROM), or other electronic memory device or chip or set of operatively interconnected chips; an Internet/Intranet server from which the stored instructions may be retrieved via the Internet/Intranet or a local area network; or so forth. Further, as used herein, a processor includes one or more of a microprocessor, a microcontroller, a graphic processing unit (GPU), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA), and the like; a user input device includes one or more of a mouse, a keyboard, a touch screen display, one or more buttons, one or more switches, one or more toggles, and the like; and a display device includes one or more of a LCD display, an LED display, a plasma display, a projection display, a touch screen display, and the like.

The invention has been described with reference to the preferred embodiments. Modifications and alterations may occur to others upon reading and understanding the preceding detailed description. It is intended that the invention be constructed as including all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

CLAIMS:

1.   A method for controlling access to data being processed by a remote computing resource, the method comprising:

          issuing a first encryption key for a data creator from a first certificate authority
5   located outside the remote computing resource;

          detecting an encounter with a data owner;

          creating, by a second certificate authority of the remote computing resource, a second encryption key for the data creator and an encryption key for the data owner in response to detecting the encounter;

10   the data creator encrypting data being sent to the remote computing resource with the first encryption key, the data creator's second encryption key, and the data owner's encryption key;

          decrypting and storing the data based on verification of the first encryption key by a verification authority located outside the remote computing resource and based on a
15   verification of at least one of the data creator's second encryption key and the data owner's encryption key at the remote computing resource; and

          controlling the data creator's access to the data by altering the permission of at least one of the data creator's first and second encryption key.

2.   The method according to claim 1, wherein a counter includes the collection of
20   clinical data.

3.   The method according to claim 1, further including:

          requesting access to the data stored in the remote computing resource for a third party data requestor with an encryption key created by the first certificate authority and a data request.

4.   The method according to claim 3, further including:

   decrypting the data for the third party data requestor based on a verification of being the third party data requestor's encryption key and a verification of at least one of the data creator's second encryption key and the data owner's encryption key at the remote computing resource.

5.   The method according to claim 3, further including:

   providing access of the data stored in the remote computing resource for at least one of the data creator and third party data requestor.

6.   The method according to claim 5, wherein providing access to the data further includes:

   encrypting data being accessed by the at least data creator and third party requestor with the encryption key issued by the first certificate authority for the data creator or the third party, the data creator's second encryption key, and the data owner's encryption key.

7.   A non-transitory computer readable medium containing software which, when loaded into a processor, programs the processor to perform the method according to claim 1.

8.   A system for controlling access to data being processed by a remote computing resource, the system comprising:

   a first certificate authority located outside the remote computing resource, which issues a first encryption key to a data creator;

   the data creator being configured to collect data from a data owner and encrypt the data with the first encryption key, a data creator's second encryption key and a data owner's encryption key;

   the remote computing resource being configured to decrypt and store the data based on a verification of the first encryption key by a verification authority located outside

the remote computing resource and based on a verification of the data creator's second encryption key and the data owner's encryption key at the remote computing resource and includes:

a second certification authority which creates the data creator second encryption key and the data owner's encryption key in response to detecting a data owner encounter at the remote computing resource;

wherein the data owner controls the data creator's access to the data by altering the permission of at least one of the data creator's first and second encryption key.

9.   The system according to claim 8, wherein the encounter includes the collection of clinical data.

10.   The system according to claim 8, wherein a third party data requests access to the data in the remote computing resource with an encryption key issued for the third party by the first certification authority and a data request.

11.   The system according to claim 10, wherein upon access to the data, the third party data requestor decrypts the data for the third party data requestor based on a verification of the encryption key issued for the third party by the first certification authority and a verification of at least one of the data creator's second encryption key and the data owner's encryption key at the remote computing resource.

12.   The system according to claim 8, wherein the remote computing resource provides access of the data stored in the remote computing resource for at least one of the data creator and third party data requestor.

13.   The system according to claim 11, wherein the remote computing resource encrypts data being accessed by the at least data creator and third party requestor with the encryption key issued by the first certification authority for the data creator or the third party, the data creator's second encryption key, and the data owner's encryption key.

14.   The system according to claim 8, wherein the data is streamed episodically, periodically, or continuously.

15.   The system according to claim 8 wherein the stored data includes real-time clinical data, near real time clinical data, and historical clinical data.

FIGURE 1

PrK Verification

PuK Verificaiton

PuK Authority

PrK Authority

Requests PrK for site (at enrollment and for Patient at admission)

Requests PuK

PuK issued by Aut

PrK issued by cloud

PrK Issued by Cloud

Healthcare Provider

Patient

FIGURE 2

FIGURE 3

Verifies the validity of the public keys

PuK Verificaiton

Verified PuK

PuK Verification

Encryption session based on Health Care Center public key, and both the data generator (Health Care Center) and data owner (patient) private keys

22
26
28

32

PrK Verification

PuK for site

PrK for site

PrK for Pt

Verifies the validity of the private keys and keeps track of authorized use of data based on private key app permission

30

20

PuK Authority

12

22
26

18
28

Healthcare Provider

Patient

FIGURE 5

120 — A data requestor calls to a cloud with a public key (PuK) and a data request

122 — A verification authority notifies the cloud of the validity of the public key (PuK)

124 — Data is encoded with a public key from a certificate authority and private keys for both the data creator and data owner from a local certificate authority in the cloud

126 — Data is sent to the data requestor from the cloud

128 — The data requestor decrypts the data based on a verification authority for the public key (PuK) and on an internal verification authority for the private keys (PrK) for the data creator and the data owner

FIGURE 4

100 — A data creator requests a public encryption key from a certificate authority

Done when they subscribe to the system using the data.

102 — The certificate authority issues a public key (PuK) to the data creator

104 — An encounter is created for a data owner

106 — A local certificate authority in the cloud creates private keys (PrK) for the data creator and the data owner

108 — The data is created and encoded with the creation authority public key (PuK) and both private keys (PrK) for the data creator and the data owner

110 — Data is encrypted and transmitted to the cloud

112 — The cloud decrypts the data based on a verification authority for the public key (PuK) and on an internal verification authority for the private keys (PrK) for the data creator and the data owner

```
                    ┌─────────────────────┐  100
                    │ A data creator requests a│          Done when they
                    │  public encryption key  │          subscribe to the
                    │  from a certificate    │           system using the
                    │       authority        │           data.
                    └───────────┬─────────┘
                                │
                    ┌───────────▼─────────┐  102
                    │ The certificate authority│
                    │  issues a public key (PuK)│
                    │     to the data creator │
                    └───────────┬─────────┘
                                │
                    ┌───────────▼─────────┐  104
                    │  An encounter is created │
                    │     for a data owner    │
                    └───────────┬─────────┘
                                │
            ┌───────────────────▼──────────────────┐  106
            │ A local certificate authority in the   │
            │ cloud creates private keys (PrK) for    │
            │  the data creator and the data owner   │
            └───────────────────┬──────────────────┘
                                │
        ┌───────────────────────▼──────────────────────┐  108
        │ The data is created and encoded with the       │
        │ creation authority public key (PuK) and         │
        │ both private keys (PrK) for the data            │
        │ creator and the data owner                      │
        └───────────────────────┬──────────────────────┘
                                │
                    ┌───────────▼─────────┐  110
                    │  Data is encrypted and   │
                    │  transmitted to the cloud │
                    └───────────┬─────────┘
                                │
    ┌───────────────────────────▼────────────────────────────┐  112
    │ The cloud decrypts the data based on a                    │
    │ verification authority for the public key (PuK) and        │
    │ on an internal verification authority for the              │
    │ private keys (PrK) for the data creator and the            │
    │ data owner                                                 │
    └────────────────────────────────────────────────────────┘
```