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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/119900 A1

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04L 29/08* (2006.01)
H04W 4/00 (2009.01) *H04W 12/02* (2009.01)

(21) International Application Number:
PCT/EP2015/052006

(22) International Filing Date:
30 January 2015 (30.01.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors: **SCHMIDT, Mischa**; Hans-Thoma-Platz 40, 69121 Heidelberg (DE). **BOHLI, Jens-Matthias**; Römerstraße 30, 69181 Leimen (DE).

(74) Agent: **ULLRICH & NAUMANN**; Schneidmühlstraße 21, 69115 Heidelberg (DE).

(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, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, 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))*

(54) Title: METHOD AND SYSTEM FOR MANAGING ENCRYPTED DATA OF DEVICES

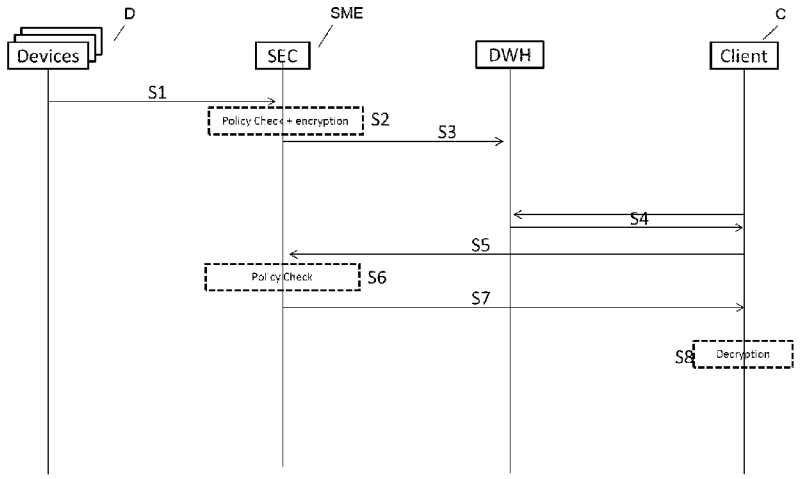

Fig. 1

(57) Abstract: The present invention relates to a method for managing encrypted data of devices (D), preferably M2M devices like sensors in buildings, using one or more computing entities (D, SME, DWH, C), comprising the steps of: a) Encrypting said data based on encryption policies using encryption keys by one or more encrypting entities (SME), b) Storing the encrypted data - ciphertext - at a storing entity (DWH), c) Requesting decryption keys to decrypt the stored ciphertext by one or more of said clients (C), d) Computing restricted decryption keys based on said access right policies for said requesting clients (C) by a security management entity (SME) and e) Providing the generated decryption keys to said requesting clients (C) for decrypting said stored ciphertext.

WO 2016/119900 A1

METHOD AND SYSTEM FOR MANAGING ENCRYPTED DATA OF DEVICES

The present invention relates to a method for managing encrypted data of devices, preferably M2M devices like sensors in buildings, using one or more computing entities.

The present invention further relates to a system for managing encrypted data of devices, preferably M2M devices like sensors in buildings, preferably for performing with a method according to one of the claims 1-13.

The present invention even further relates to a security management entity for performing with a method according to one of the claims 1-13.

Although applicable to data in general the present invention will be described with regard to data of M2M devices, in particular data of building management systems.

Building management systems monitor and control several systems in a building such as heating, air-condition, lighting, mechanical systems and various other kinds of alarms. To be able to manage the building in an automatic way the building management system collects data from many sensors installed throughout the building.

Conventional building management systems make in general use of the “cloud” for storage, where management services can be booked on demand. Therefore conventionally building data is kept outside the building and even outside the building management organization at a cloud storage or cloud service providers.

However, this causes several problems, in particular security and privacy problems: When the data is collected this data is strongly correlated with actions of persons leading to severe privacy issues in residential buildings. Also in office environments data which is collected from the sensors in the building may reveal personal preferences and habits of employees. Even further the collected data

may allow deriving confidential information of a company, for example the work load of groups and departments.

Further a security problem arises when the data is initially collected as a whole and later a focus on the relevant subset of the data is set being a source of threats, in particular when considering outsourcing of data analysis to third parties.

It is therefore an objective of the present invention to provide a method and a system for managing encrypted data of devices providing a high security while being flexible and easy to implement.

The aforementioned objective is accomplished by a method of claim 1 and a system of claim 14 as well by a security management entity of claim 15.

In claim 1 a method for managing encrypted data of devices, preferably M2M devices like sensors in buildings, using one of more computing entities is defined.

According to claim 1 the method is characterized by the steps of

a) Encrypting said data based on encryption policies using encryption keys by one or more encrypting entities,
b) Storing the encrypted data – ciphertext - at a storing entity,
c) Requesting decryption keys to decrypt the stored ciphertext by one or more of said clients,
d) Computing restricted decryption keys based on said access right policies for said requesting clients by a security management entity – SME - and
e) Providing the generated decryption keys to said requesting clients for decrypting said stored ciphertext.

In claim 14 a system for managing encrypted data of devices, preferably M2M devices like sensors in buildings, preferably for performing with a method according to one of the claims 1-13, is defined.

According to claim 14 the system is characterized by

a security management entity – SME – adapted to compute restricted decryption keys based on access right policies for requesting clients and to provide the generated decryption keys for decrypting said stored ciphertext,
one or more encrypting entities adapted to encrypt said data based on encryption policies using encryption keys,
a storing entity, preferably a cloud, adapted to store the encrypted data – ciphertext -,
one or more of said clients adapted to request decryption keys from said SME to decrypt the stored ciphertext.

In claim 15 a security management entity for performing with a method according to one of the claims 1-13 is defined.

According to claim 15 the security management entity is characterized in that said security management entity is adapted to compute restricted decryption keys based on access right policies for requesting clients and to provide the computed decryption keys for decrypting ciphertext encrypted with one or more encryption policies.

The term “entity” is to be understood in its broadest sense. In particular an “entity” may be any kind of device, preferably computing device or the like, or a plurality of devices interacting with each other, e.g. for example a storing entity may be a plurality of servers able to store data and interacting with each other to provide said storing.

The terms “clients”, “keys”, “ciphertext” and “policies” with regard to encryption and decryption may also be understood preferably throughout the description, in particular in the claims as only one client, one key, a plurality of ciphertexts or one policy.

According to the invention it has been recognized that security is enhanced since data owners stay in control while the data itself may be stored externally. In particular it has been recognized that off-the-shelf cloud storage services can be used for sensitive data while maintaining strong technical data protection.

According to the invention it has been even further recognized that flexibility is enhanced since flexible and dynamic policies and interchangeable methods for data protection can be used depending on the needs of a user, a company or the like.

According to the invention it has been further recognized that complex access policies can be realized and thus flexibility is further enhanced for example in business relations as third parties can be granted and revoked access to the encrypted data “on-the-fly”.

In other words the present invention provides a security management entity – which is in the following also called “security broker” – preferably enabling a management of encryption policies and schemes as well as encryption keys in such a way that decryption keys for decrypting partial information of the encrypted data can be generated in a flexible way. For instance the full data of the building can then be transmitted to cloud-based systems in encrypted form and a client can request decryption keys for accessing the information needed from the security broker to decrypt the data. The security broker provides for example sensors and/or encryption entities encryption keys for encrypting the data that besides conventional encryption techniques, in particular makes it possible to generate decryption keys that decrypt only partial data.

Further features, advantages and preferred embodiments are described in the following subclaims.

According to a preferred embodiment the SME acts itself as said one or more encrypting entities. This has the advantage that the security broker not only provides the encryption keys but also encrypts the data, so that a time and resource consuming transmission to other encrypting entities is avoided.

According to a further preferred embodiment prior to encryption an encryption context of the data is determined, included into said encryption policies and used for encryption of the data. This is flexible since any context or context information

can be used as encryption context and included when encrypting said data enabling context-based encryption. The number of context states per device is preferably flexible and may be expressed by a simple logic, for example comparing a message comprising the data to be encrypted with reference values or value ranges. To summarize this greatly enhances the flexibility.

According to a further preferred embodiment time information and/or range information is collected and included in said encryption context. For example for a time-based encryption said time information is determined indicating a time T. Range information can be used for range-based encryption: Value ranges for the value to be encrypted can be specified and translated into the encryption keys. Alternatively different value ranges for different devices can be specified. The term "ciphertext" is to be understood in its broadest sense as encrypted data in the description, in particular in the claims. Further the term "ciphertext" may be understood in plural, i.e. for example when different time durations are specified this may result in multiple associated ciphertexts for a single message comprising the data to be encrypted.

According to a further preferred embodiment meta-data is associated to and stored with said data at said storing entity. Meta-data enable clients to efficiently request decryption keys, etc. using the additional meta-data to specify their requests.

According to a further preferred embodiment identification and/or contact information of the SME is included into the meta-data. This enables clients to identify and contact the responsible security broker or security management entity respectively and request decryption keys to decrypt corresponding data. The meta-data comprises for example a URL to reach the responsible security broker via the clients.

According to a further preferred embodiment information representing at least one of the following: identification of devices, timestamps, tokens computed by the SME, is included into the meta-data. This information enables clients to specify their interest in data to be decrypted even more precisely and the security broker

or SME respectively may then quickly decide whether to grant or deny their requests and generate the appropriate responses. Preferably no confidential information is disclosed within the meta-data.

According to a further preferred embodiment the encryption policies and/or access right policies are requested from the SME by one or more of said encrypting entities. This enables the encrypting entities to request configuration and parameters like encryption policies and access right policies from the security broker at the time needed. This may be performed via an appropriate conventional protocol suitable for exchanging this information.

According to a further preferred embodiment when requesting decryption keys a client specifies his interest in the decryption keys using information to be compared by the SME with stored access right policies and preferably of meta-data associated with the requested data of said client. This enables to efficiently request data: The SME can answer the request by limiting the number of decryption keys using the information transmitted by the client to be compared with the policies and meta-data associated to the data and the client. Data transmission between a client and the security broker can be performed via for example URL through various conventional protocols who - depending on the configured access right policies - may or may not respond with decryption keys for deciphering the ciphertext(s). A current interest of the client may for example be only data encrypted in the last hour or the like. Comparison between the data provided by the client and requesting the decryption keys and the policies associated to the client is only successful when the information provided by the client is an eligible subset of the policies associated to the client.

According to a further preferred embodiment one or more master encryption keys are generated and used for generating said encryption keys. A master key may be provided by the security broker or may be configured into the security broker. A master key allows for example encrypting entities to derive appropriate decryption keys from said master encryption key, i.e. the master key provides in a flexible while secure way the generation of encryption keys.

According to a further preferred embodiment one ore more chains, preferably hash chains are computed and used as encryption keys and/or decryption keys. This enables in an easy way to derive the encryption and decryption keys including also time or data ranges for example.

According to a further preferred embodiment one ore more of said clients query the SME for supported access right and/or encryption policies prior to step e). This enables clients to be aware of the policies supported by the security broker or SME respectively so that the client can specify his interest in context of these policies. Thus, efficient requests by the client can be performed. Preferably either the clients can be preconfigured or use an appropriate protocol to query the security broker or SME respectively for the supported policies.

According to a further preferred embodiment the encrypting entities request the master encryption keys from said SME and compute themselves the encryption keys for encrypting said data. This enables in a very flexible way a generation/computation of the encryption keys by the entities encrypting the data.

According to a further preferred embodiment prior to encrypting data access right policies, encryption policies and/or further parameters for the different encryption schemes are configured into the SME, for example a master encryption key, eligible client identifications and/or access right policies, device identifications and the encryption policies and/or parameters for setting up encryption schemes like definition of epochs, relevant context information of other devices like sensors or the like, description of ranges of expected measurements of the data provided by the devices or the like. This enables a security broker or SME respectively to efficiently manage the encrypted data.

According to a further preferred embodiment the SME acts a policy decision entity enforcing policies associated to a requesting client when releasing decryption keys for the data in the domain of the SME/security broker.

According to a further preferred embodiment steps d) and e) are shielded from the SME by the storing entity. This enables that the storing entity acts on behalf of the

client seen from the SME and requests decryption keys from the SME and provides later the decryption keys to the requesting client on behalf of the SME. This simplifies the client since the client only needs to communicate with the storing entity.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained.

In the drawings

Fig. 1 shows a part of the steps of a method according to a first embodiment of the present invention;

Fig. 2 shows a part of a method according to a second embodiment of the present invention; and

Fig. 3 shows steps of a method according to a third embodiment of the present invention.

Fig. 1 shows a part of the steps of a method according to a first embodiment of the present invention.

In Fig. 1 an example for a call flow is depicted. An aforementioned configuration, e.g. based on CAMPUS21 or BaaS architectures for this phase is not depicted. Further the security broker/security entity SEC denoted with reference sign SME is assumed to be already configured.

In step S1 different devices D, for example sensors, deliver data for example in a message m to the SEC/SME. Based on its configuration the SEC/SME checks the

corresponding encryption policy and performs encryption of each message m into one or more ciphertexts c in a step S2. The security broker/security entity SEC acts here in this embodiment as encryption entity.

The SEC/SME then delivers the various ciphertexts c in a step S3 to a data repository, denoted with reference sign DWH along with meta-data. The data repository DHW may or may not confirm data storage to the SEC/SME.

In a further step S4 a client C requests data from the data repository DWH and receives a set of ciphertexts c along with the associated meta-data.

In a fifth step S5, the client C then contacts the SEC/SME to request decryption keys for the received ciphertexts c, preferably additionally specifying interest in deciphering entries for the last hour.

In a sixth step S6 the SEC/SME checks the client's request against configured policies and responds in a seventh step S7 with a set of decryption keys to the client C.

Only then the client C can decipher the data in an eighth step S8 or a subset of the data.

In a preferred embodiment the data repository DWH acts on the client's behalf and requests the decryption keys from the SEC/SME. This simplifies actions to be taken by the client but complicates the implementation of the storing entity DWH and places a certain trust into the storing entity DWH again. The storing entity DWH is then able to store and decrypt the data.

Fig. 2 shows a part of a method according to a second embodiment of the present invention.

In Fig. 2 the generation of hash chains g and h given the master key MK and an epoch from t_0 to t_n is shown for providing a time-based encryption.

In more detail the data collector encrypts a message dependent of the current time t. An epoch e = [t_0, . . . , t_n] is defined and within the epoch e it is possible to create a decryption key k_T for any time interval T = [t_j, . . . , t_{j+k}] ⊆ e, such that k_T can exactly decrypt only the ciphertexts c that were created at a time t ∈ T. Practically, an epoch might be one day, but could also be longer or shorter. As only one interval key per epoch e can be created, the price for the flexibility in requesting multiple intervals that comes with short epochs is the additional key overhead.

The following procedures, also called protocols, are used for setting up an encryption scheme, to encrypt data and to decrypt the data later:

Setup. To setup the scheme, an epoch e is defined, given by it's start date t_0, a time period δt and a length $n \in \mathbb{Z}$. The end time of the epoch is then given as $t_n = t_0 + n \cdot \delta t$.

Given the master key MK, two keys for the scheme are derived, denoted by $\mathrm{MK}_{t_0} = \mathrm{KDF}(\mathrm{MK}, t_0, \text{'time'})$ and $\mathrm{MK}_{t_n} = \mathrm{KDF}(\mathrm{MK}, t_n, \text{'time'})$. Two hash chains of length n are computed. The elements are computed as follows:

$$g_i = H^i(\mathrm{MK}_{t_0}) \text{ and } h_{n-i} = H^i(\mathrm{MK}_{t_n}) \text{ for } i = 0, \ldots, n,$$

where $H^i(\cdot)$ denotes the i-fold application of the hash function H, thus the first elements are given as $g_0 = \mathrm{MK}_{t_0}$ and $h_n = \mathrm{MK}_{t_n}$.

For each $t_i \in e$, the encryption key is set as $k_i = g_i \oplus h_i$. A decryption key is given by $k_T = (g_i, h_j)$ with $i \leq j$, which provides the ability to decrypt ciphertexts in the interval $T = [t_i, \ldots, t_j]$.

Encrypt. Given the key MK, the value m is at time t encrypted as

$$E^{t_i}_{\mathrm{MK}}(m) = E_{k_i}(m).$$

Decrypt. Given the ciphertext c from time t_c, a key $k_T = (g_i, h_j)$ is needed, with $i \leq c \leq j$. From g_i, and h_j, it is possible to compute g_c and h_c, by completing the hash chain as described in the setup protocol. With the key $k_c = g_c \oplus h_c$ it is possible to decrypt the ciphertext c to obtain m.

$$D^{t_c}_{k_T}(c) = E_{k_c}(c).$$

Another encryption scheme may be provided when the encryption is based on context variables. This encryption mode ties the encrypted message c to context variables at the time of encryption. Unlike the aforementioned time-based encryption and a further described encryption below based on a range the following encryption scheme does not imply any order in the set of possible contexts.

In more detail the context is given by a set Y and the following procedures are used for setting up a context-based encryption scheme, to encrypt data and to decrypt the data later:

Setup. Given is a finite set $\mathbb{Y}$. For each element $y \in \mathbb{Y}$, a key k_y is computed by

$$k_y = KDF(\mathrm{MK}, y) \forall y \in \mathbb{Y}.$$

Encrypt. When an element $m \in \mathbb{X}$ is to be encrypted, the context y is queried. Then k_y is used to encrypt the message as

$$E^y_{\mathrm{MK}}(m) = E_{k_y}(m).$$

Decrypt. Given a ciphertext $c^y = E_{k_y}(m)$ with context y, and the key k_y, the message can simply be obtained by $m = D_{k_y}(m)$.

An even further encryption scheme is based on ranges. This embodiment builds on the same principles as time-based encryption but instead of time the encryption and decryption keys are computed depending on the data to be encrypted itself. The purpose is to release partial data based on the encrypted values, e.g. to release only outliers. The plaintext space is modeled as a totally ordered finite set X, typically a discrete numerical scale. Let n denote the size of X and m0, . . . , mn−1 the elements of X in ascending order. The encryption offers the possibility to produce a key pair k_{in}, k_{out} for an interval [a, b] ⊆ X. The keys have the property, that k_{in} only decrypts the ciphertexts where c = E(m) and m ∈ [a, b]. In addition, the encryption procedure offers the possibility to decrypt the outliers only by releasing only k_{out}, i.e. k_{out} only decrypts c = E(m) for m ∉ [a, b].

Fig. 3 shows steps of a method according to a third embodiment of the present invention.

In a first step a) said data is encrypted based on encryption policies using encryption keys by one or more encrypting entities.

In a second step b) the encrypted data – ciphertext – is stored at a storing entity.

In a third step c) decryption keys are requested to decrypt the stored ciphertext by one or more of said clients,

In a forth step d) restricted decryption keys are computed based on said access right policies for said requesting clients by a security management entity – SME -.

In a firth step e) the generated decryption keys to said requesting clients for decrypting said stored ciphertext.

In summary the present invention provides inter alia the following advantages:

- Off-the-shelf cloud storage services can be used for sensitive data while maintaining strong technical data protection.
- Flexible and dynamic policies and exchangeable methods for data protection can be "plugged" in depending on the needs of the deployment scenario.
- Data owner stays in control while data itself is stored externally.
- Only few master keys need to be stored, due to use of hash-chains to realize e.g. range and time based encryption.
- Complex access policies can be realized by combining the different approaches, i.e. encryption schemes.
- Provides flexibility in business-relations as 3rd parties can be granted and revoked access to the data "on-the-fly".

In particular the present invention enables to derive a chain, e.g. a hash chain, with the elements representing a time range or a data range and using the elements as encryption and decryption keys.

The present invention further enables to use two chains representing a time or data range, one starting from the minimal value going up, one starting from the maximum value going down. Combining the elements of each of the chains enables to compute encryption and decryption keys. Further a device is presented that negotiates and manages security associations specific to requests typically occurring in an M2M system.

In particular the present invention provides a method comprising the following steps of:

1) Encrypting gateway or sensor data according to an encryption policy and keys from the security broker,
2) Encrypted data is sent to an outsourced database,
3) Building management system has access to encrypted data and requests from security broker the decryption keys to access required data.
4) The security broker generates suitably restricted decryption keys, e.g.
    a. Only access during certain time period
    b. Only access based on context, e.g. only measurements in empty rooms
    c. Only access to outliers.
5) Building management system decrypts the data and provides its service

Many modifications and other embodiments of the invention set forth herein will come to mind to the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. A method for managing encrypted data of devices (D), preferably M2M devices like sensors in buildings, using one or more computing entities (D, SME, DWH, C),
characterized by the steps of

a) Encrypting said data based on encryption policies using encryption keys by one or more encrypting entities,

b) Storing the encrypted data – ciphertext - at a storing entity (DWH),

c) Requesting decryption keys to decrypt the stored ciphertext by one or more of said clients (C),

d) Computing restricted decryption keys based on said access right policies for said requesting clients (C) by a security management entity (SME) and

e) Providing the generated decryption keys to said requesting clients (C) for decrypting said stored ciphertext.

2. The method according to claim 1, characterized in that the SME (SME) acts itself as said one or more encrypting entities.

3. The method according to one of the claims 1-2, characterized in that prior to encryption an encryption context of the data is determined and used for encryption of the data.

4. The method according to claim 3, characterized in that time information and/or range information is collected and included in said encryption.

5. The method according to one of the claims 1-4, characterized in that meta-data is associated to and stored with said data of said storing entity (DWH).

6. The method according to claim 5, characterized in that identification and/or contact information of the SME (SME) is included into the meta-data.

7. The method according to claim 5, characterized in that information representing at least one of the following: identification of devices, timestamp, tokens computed by the SME is included into the meta-data.

8. The method according to one of the claims 1-7, characterized in that the encryption policies and/or access right policies are requested from the SME (SME) by one or more of said encrypting entities.

9. The method according to one of the claims 1-8, characterized in that when requesting decryption keys a client (C) specifies his interest in the decryption keys using information to be compared by the SME (SME) with stored access right policies and preferably meta-data associated with the requested data of said client (C).

10. The method according to one of the claims 1-9, characterized in that one or more master encryption keys (MK_{t0}, ..., MK_{tn}) are generated and used for generating said encryption keys.

11. The method according to one of the claims 1-10, characterized in that one or more chains, preferably hash chains are computed and used as encryption keys and/or decryption keys.

12. The method according to claim 11, characterized in that one or more of said clients (C) query the SME (SME) for supported access right and/or encryption policies prior to step e).

13. The method according to one of the claims 1-12, characterized in that the encrypting entities request the master encryption keys (MK_{t0}, ..., MK_{tn}) from said SME (SME) and compute themselves the encryption keys for encrypting said data.

14. A system for managing encrypted data of devices (D), preferably M2M devices like sensors in buildings, using one of more computing entities (D, C, DWH, SME), preferably for performing with a method according to one of the claims 1-13,

characterized by

a security management entity – SME – (SME) adapted to compute restricted decryption keys based on access right policies for requesting clients (C) and to provide the generated decryption keys for decrypting said stored ciphertext,

one or more encrypting entities adapted to encrypt said data based on encryption policies using encryption keys,

a storing entity (DWH), preferably a cloud, adapted to store the encrypted data – ciphertext - of said SME (SME),

one or more of said clients (C) adapted to request decryption keys to decrypt the stored ciphertext,

15. A security management entity for performing with a method according to one of the claims 1-13, characterized in that said security management entity (SME) is adapted to compute restricted decryption keys based on access right policies for requesting clients (C) and to provide the computed decryption keys for decrypting ciphertext encrypted with one or more of said encryption policies.

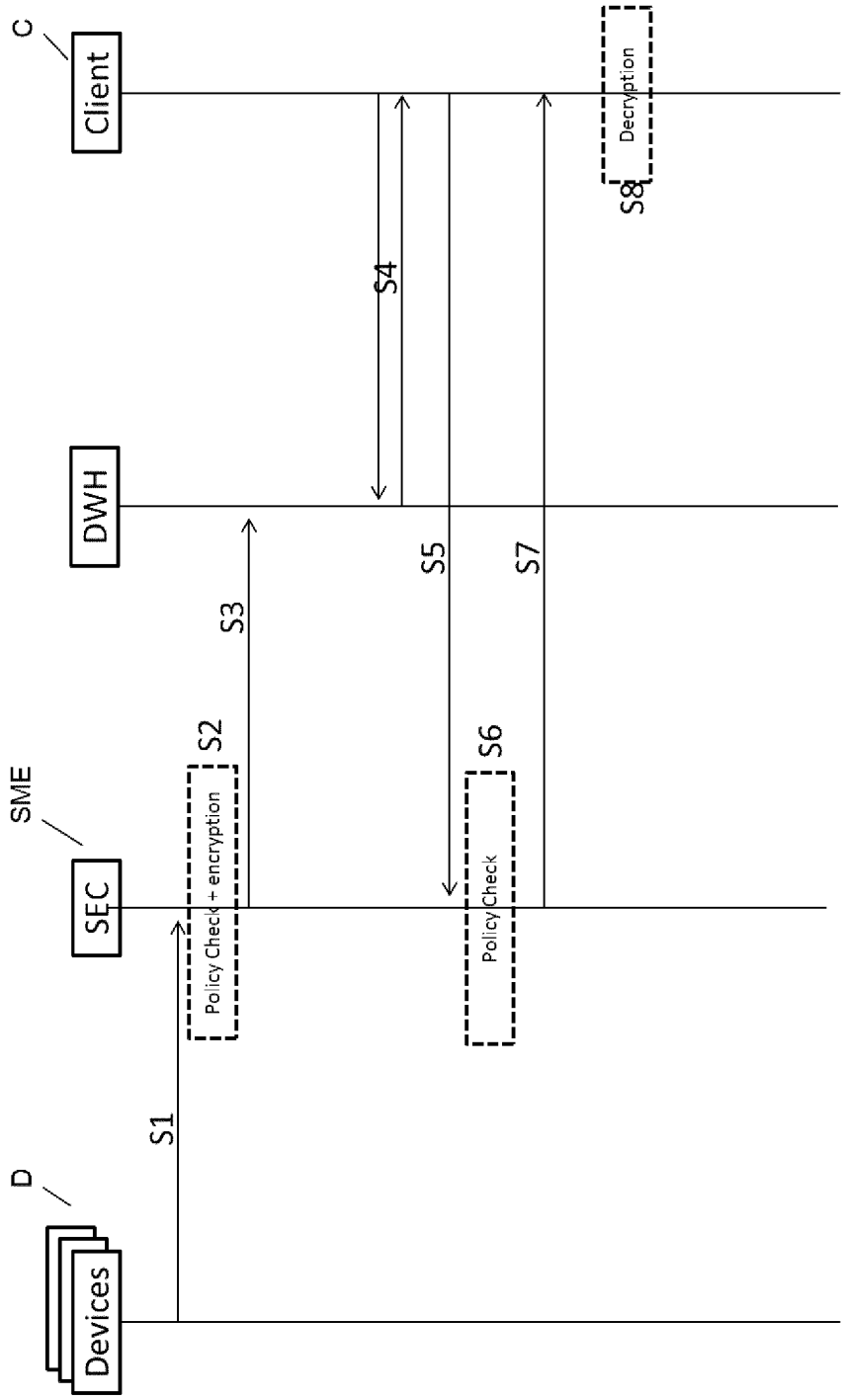
C
Client
DWH
SME
SEC
D
Devices
S1
S2
Policy Check + encryption
S3
S4
S5
S6
Policy Check
S7
S8
Decryption

Fig. 1

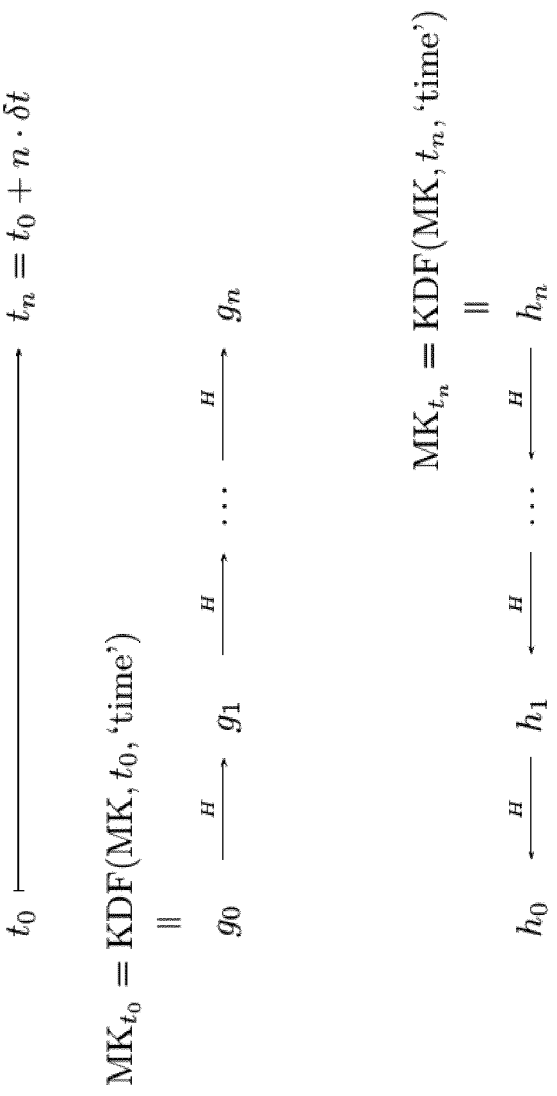
t_0
$t_n = t_0 + n \cdot \delta t$
$\mathrm{MK}_{t_0} = \mathrm{KDF}(\mathrm{MK}, t_0, \text{'time'})$
g_0 g_1 g_n
H
$\mathrm{MK}_{t_n} = \mathrm{KDF}(\mathrm{MK}, t_n, \text{'time'})$
h_0 h_1 h_n
H

Fig. 2

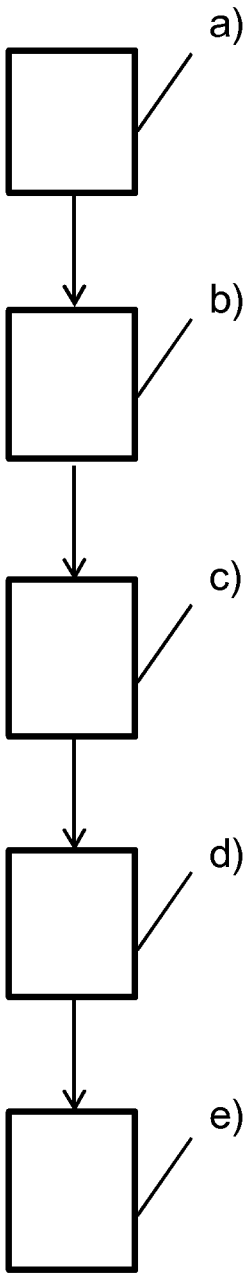

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/052006

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04W4/00 H04L29/08
ADD. H04W12/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 424 156 A1 (NIPPON TELEGRAPH & TELEPHONE [JP]) 29 February 2012 (2012-02-29) figures 1,3-5,6,9 paragraphs [0005], [0008], [0016] paragraphs [0024], [0028], [0044] paragraphs [0056], [0059], [0061] paragraphs [0062], [0068], [0071] - [0082] -----	1-15
X	EP 2 216 731 A2 (THALES HOLDINGS UK PLC [GB]) 11 August 2010 (2010-08-11) figure 2 paragraphs [0004], [0006] - [0008] paragraphs [0015] - [0017] paragraphs [0027] - [0029], [0041] paragraphs [0057] - [0064] -----	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 October 2015	20/10/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kufer, Léna

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/052006

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/141967 A1 (LANE SEAN L [US] ET AL) 16 June 2011 (2011-06-16) abstract paragraphs [0017], [0018], [0021] paragraphs [0039] - [0040]	1-15
A	WO 2014/148960 A1 (ERICSSON TELEFON AB L M [SE]) 25 September 2014 (2014-09-25) abstract paragraph [0034]	1-15
A	US 2011/237234 A1 (KOTANI SEIGO [US] ET AL) 29 September 2011 (2011-09-29) paragraphs [0112] - [0117]	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/052006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2424156 A1	29-02-2012	CN 102369687 A	07-03-2012
		EP 2424156 A1	29-02-2012
		EP 2658164 A2	30-10-2013
		EP 2658165 A2	30-10-2013
		ES 2445535 T3	03-03-2014
		ES 2516390 T3	30-10-2014
		JP 5253567 B2	31-07-2013
		KR 20110134900 A	15-12-2011
		US 2012027210 A1	02-02-2012
		WO 2010123122 A1	28-10-2010
EP 2216731 A2	11-08-2010	EP 2216731 A2	11-08-2010
		GB 2467580 A	11-08-2010
		US 2011040967 A1	17-02-2011
US 2011141967 A1	16-06-2011	US 2011141967 A1	16-06-2011
		WO 2011081872 A1	07-07-2011
WO 2014148960 A1	25-09-2014	NONE	
US 2011237234 A1	29-09-2011	CN 102823195 A	12-12-2012
		CN 102859935 A	02-01-2013
		CN 102870093 A	09-01-2013
		CN 103154966 A	12-06-2013
		EP 2550595 A1	30-01-2013
		EP 2550596 A2	30-01-2013
		EP 2550768 A1	30-01-2013
		EP 2550769 A1	30-01-2013
		JP 5516821 B2	11-06-2014
		JP 5522307 B2	18-06-2014
		JP 5747981 B2	15-07-2015
		JP 2013522793 A	13-06-2013
		JP 2013522794 A	13-06-2013
		JP 2013522795 A	13-06-2013
		JP 2013532394 A	15-08-2013
		US 2011237234 A1	29-09-2011
		US 2011238402 A1	29-09-2011
		US 2011238980 A1	29-09-2011
		US 2011239209 A1	29-09-2011
		US 2011239210 A1	29-09-2011
		US 2015248286 A1	03-09-2015
		US 2015248287 A1	03-09-2015
		US 2015261554 A1	17-09-2015
		WO 2011119297 A1	29-09-2011
		WO 2011119298 A1	29-09-2011
		WO 2011119299 A1	29-09-2011
		WO 2011119300 A2	29-09-2011