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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
09 June 2022 (09.06.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/118281 A1

(51) International Patent Classification:
G06F 21/36 (2013.01) *H04W 12/77* (2021.01)
H04L 9/00 (2022.01) *G06F 21/62* (2013.01)

(21) International Application Number:
PCT/IB2021/061318

(22) International Filing Date:
03 December 2021 (03.12.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01543/20 04 December 2020 (04.12.2020) CH

(71) Applicant: **VEREIGN AG** [CH/CH]; Kolinplatz 10, 6300 Zug (CH).

(72) Inventors: **GREVE, Georg**; Weinmanngasse 88, 8700 Küsnacht (CH). **BODUROV, Gospodin**; Luiben Karavelov 38 str, 8000 Burgas (BG).

(74) Agent: **P&TS SA (AG, LTD.)**; Av. J.-J. Rousseau 4, P.O. Box 2848, 2001 Neuchâtel (CH).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: A METHOD AND A SYSTEM FOR SECURELY SHARING DATASETS VIA GLYPHS

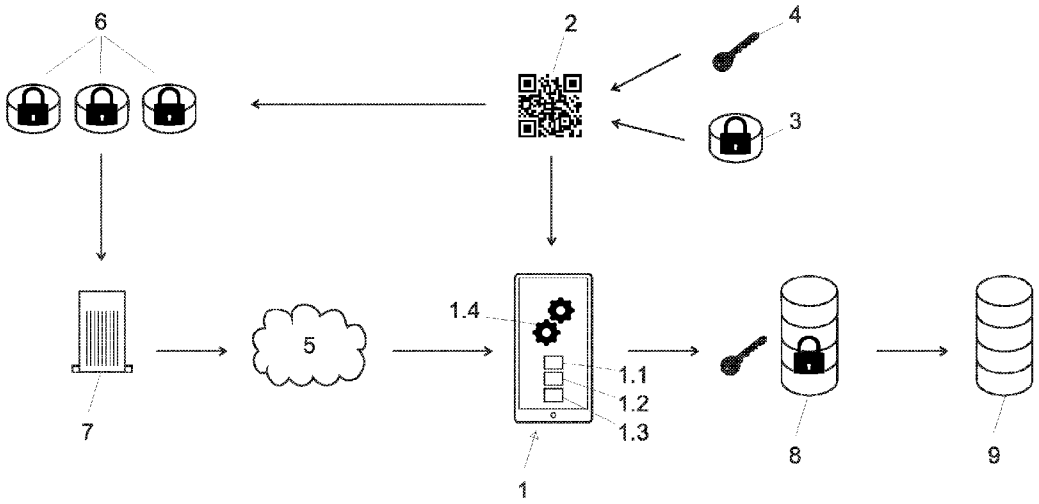

Fig. 5

(57) Abstract: The present disclosure concerns a method for securely sharing a dataset via a glyph comprising: - splitting said dataset into at least two data subsets using a splitting module, - generating a payload for the glyph using a first data subset from the at least two data subsets, - storing all the at least two data subsets but the first data subset in a key value database with a hash value obtained from the payload as storage key, - generating the glyph representing the payload and sharing the glyph via an output medium.The present disclosure also concerns a method for interpreting a glyph, comprising via an image capture device, scanning said glyph to retrieve a payload,deriving a first data subset from said payload,retrieving at least one data subset in a key-value database using a hash of the payload as storage key,assembling said data subsets into said dataset, deserializing said dataset. The present disclosure also concerns a system for securely sharing a dataset via a glyph comprising:- a processor an image capture device; - a storage for storing a key

WO 2022/118281 A1

[Continued on next page]

(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))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

value database and a computer program arranged for casing said processor to carry out the methods of any of the previous claims when said program is executed. Finally, the present disclosure concerns a data storing medium comprising a computer program arranged for causing a data processing system to carry out the described methods when said computer program, is executed.

A method and a system for securely sharing datasets via glyphs

Field of invention

[0001] The present disclosure concerns a method and a system for securely sharing datasets via glyphs.

Background of the invention

[0002] Data sharing via glyphs such as barcodes or QR-codes refers to the standard protocol of giving a user an access to some data after he has read a glyph with an appropriate image capture device such as a smartphone with a camera. The data can be contained in the glyph itself, which holds for small datasets since only a limited amount of data can be encoded in such glyphs, but the glyph can also be used, for example, as a way of accessing a server storing data of arbitrary size by providing a URL to the user.

[0003] The security of such data sharing systems is obviously of utmost importance as the data can contain for example medical or bank information about a patient or a customer. In existing such systems, the security of the data is ensured by an encryption of the datasets themselves and/or by a control of the user identity by means of a password, or more generally by a multi-factor authentication, independently of the glyph. In other words, a sufficiently skilled informatic pirate could access the data by decrypting the data after having obtained say the password of a user, without having knowledge of the glyph.

[0004] US 2016/117448 A1 describes a system for managing medical data in which a patient can request a doctor to share medical data by providing a QR-code that the doctor can scan with an appropriate device such as a smartphone. In this case, the QR-code only contains the request from the patient to the doctor and no confidential information. The authentication of the user can be required by the module providing the medical data. The

security of the medical data accessible by this procedure entirely relies on the authentication of the user and the encryption of the data.

[0005] US 2015/358164 A1 discloses a method and a system for validating and verifying documents by first encrypting a dataset with a private key, and generating a glyph representing the encrypted dataset. This glyph is then overlayed on a digital image of a document related to the dataset. A user may then scan the glyph with a mobile device to recover the encrypted dataset and decrypt it. The size of the dataset is therefore limited by the maximum payload of the glyph.

[0006] EP 2 509 275 A1 discloses an authentication method based on the use of a password, a private key QR-code and a matching public key QR-code, both QR-codes being generated from URLs and PKIs private/public keys.

[0007] US 2007/170250 A1 discloses a method for copy protection of digital documents. The method is based on the generation of a glyph based on an encrypted ID of the digital document (the ID is constructed from copy protection data such as a password or a copy count that are related to the digital document). The glyph is then incorporated to the digital document and a thumb print of the document content and adds it to the document. Finally, a watermark is added to the digital document and a hardcopy is printed.

Brief summary of the invention

[0008] It is an aim of the present disclosure to present a method for securely sharing datasets via a glyph.

[0009] Another aim is to present a method for interpreting a glyph.

[0010] A third aim of the present disclosure is to provide a system for securely sharing a dataset via a glyph.

[0011] According to one aspect, those aims can be achieved with a method for securely sharing a dataset via a glyph comprising:

splitting said dataset into at least two data subsets using a splitting module,

generating a payload for the glyph using a first data subset from the at least two data subsets,

storing all the at least two data subsets but the first data subset in a key value database with a hash value obtained from the payload as storage key,

allowing storage of the second and subsequent data sets in a public repository without reducing the integrity and security of the encoded data,

generating the glyph representing the payload and

sharing the glyph via an output medium.

[0012] The method may comprise a preliminary step of encrypting a dataset into an encrypted dataset using an encryption parameter.

[0013] The encryption parameter may comprise a symmetric encryption key.

[0014] The encryption parameter may comprise a symmetric encryption key and an initialization vector.

[0015] The encryption parameter may be encrypted using a second encryption parameter of comparatively small size.

[0016] The payload for the glyph may be generated using said first dataset and said encryption parameter.

[0017] The payload may be generated with said first data subset and said second encryption parameter.

[0018] The method may comprise a step of storing said encrypted encryption parameter in said key-value database with a hash value obtained from the payload as storage key.

[0019] The splitting of the dataset may be operated using a cryptographic splitting module.

[0020] The output medium may consist of a computer or a mobile screen device.

[0021] According to another aspect, those aims can be achieved by a method for interpreting a glyph, comprising

via an image capture device, scanning said glyph to retrieve a payload,

deriving a first data subset from said payload,

retrieving at least one data subset in a key-value database using a hash of the payload as storage key,

assembling said data subsets into said dataset.

[0022] The above method may comprise a final step of deserializing said dataset after the assembling step.

[0023] The dataset may be an encrypted dataset. In that case, the method may include a decryption step comprising:

deriving an encryption parameter from said payload,

decrypting the encrypted dataset using the encryption parameter to obtain a decrypted dataset.

[0024] The method may include a decryption step comprising:

deriving a second encryption parameter from said payload,

retrieving an encrypted encryption parameter in a key-value database using a hash of the payload, as storage key,

decrypting said encrypted encryption parameter using said second encryption parameter to obtain an encryption parameter,

decrypting the encrypted dataset using the encryption parameter to obtain a decrypted dataset.

[0025] The data subsets of the second method may have been obtained from said dataset by applying a cryptographic splitting algorithm.

[0026] The method may include a step of authenticating with a multi-factor authentication to access said at least one data subset in said key-value database.

[0027] The glyph of both methods may consist of a barcode or matrix code.

[0028] The previously described methods may comprise a step of revoking said glyph by deleting said data subsets from said key-value database.

[0029] The previously described methods may comprise a step of revoking said glyph by deleting said encryption parameter and/or said second encryption parameter.

[0030] According to another aspect, the aforementioned aims can be achieved with a system for securely sharing a dataset via a glyph comprising:

a processor,

an image capture device,

a storage for storing a key value database and a computer program arranged for casing said processor to carry out the methods of any of the previous claims when said program is executed.

[0031] According to another aspect, the aforementioned aims can be achieved with a data storing medium comprising a computer program arranged for causing a data processing system to carry out any of the methods described above when said computer program is executed.

Brief description of the drawings

[0032] The invention will be better understood with the aid of the description of an embodiment given by way of example and illustrated by the figures, in which:

- Fig. 1 illustrates a flowchart of an example of method for generating and sharing a dataset using a glyph according to the invention.

- Fig. 2 illustrates a flowchart of another example of method for generating and sharing a dataset using a glyph according to the invention.

- Fig. 3 illustrates a flowchart of an example of a method for interpreting a glyph according to the invention.

- Fig. 4 illustrates a flowchart of an example of method for interpreting a glyph according to the invention.

- Fig. 5 illustrates schematically a system for carrying out a method according to the invention.

Detailed description of the disclosure

[0033] As illustrated with the Flowchart of Fig. 1, an embodiment of a method for generating and sharing a dataset 9 using a glyph 2 can comprise the following main steps:

10. Splitting a dataset 9 into at least two data subsets 3, 6.

20. Generating a payload using the first data subset 3.

30. Storing all data subsets but the first data subset 6 in a key-value database with a hash value of the payload as storage key.

40. Generating a glyph 2 encoding the payload.

50. Sharing the glyph 2 via an output medium.

Dataset

[0034] In the context of this disclosure, a dataset 9 may comprise data of any kind and of any size. In particular, the dataset 9 can include medical data, electronic record data, tracking data, email data, etc.

[0035] In a particular embodiment in which the structure of the dataset 9 is particularly complex, a preliminary step of serializing 60 the dataset 9 into a byte stream can be applied.

Glyph

[0036] In the present disclosure, a glyph 2 is meant to be a symbol which is used to convey information to other devices when the glyph 2 is scanned. Examples of glyphs comprise one-dimensional barcodes, two-dimensional codes such as quick-response codes (QR codes) or data matrices.

[0037] A glyph 2 therefore comprises a symbol and a payload, i.e. an information that is encoded in the symbol. The payload represents a relatively small amount of information with respect to the entire dataset 9 that is to be shared as the storage capacity of glyphs is fairly limited. In the case of QR-codes, the storage capacity is at most 7089 numeric characters.

[0038] In a particular embodiment illustrated in Fig. 5, the glyph 2 is a QR-code and the payload is a URL deploying a web application used to visualize and process the dataset 9.

[0039] This means the payload can also be shared as a URL where glyphs may be inconvenient, for example via social media or other (primarily) text-based channels, including email.

Encryption of dataset

[0040] In a particular embodiment the method described above comprises an encryption step 70, 80 before the splitting 10 of the dataset 9. During this encryption step, the dataset 9 is encrypted using an encryption parameter which can comprise an encryption key, a combination of an

encryption key and an initialisation vector or any other suitable encryption protocol.

[0041] An embodiment of this method comprising an encryption step is illustrated with the Flowchart of Fig. 2. The method comprises the following:

60. Serializing the dataset.

70. Encrypting the dataset into an encrypted dataset using an encryption parameter.

80. Encrypting the encryption parameter using a comparatively small second encryption parameter.

10. Splitting the dataset into at least two data subsets.

20. Generating a payload using the first data subset and the second encryption parameter.

30. Storing all data subsets but the first data subset and the encrypted encryption parameter in a key-value database with a hash value of the payload P as storage key.

90. Encrypting the payload with a symmetric encryption key.

40. Generating a glyph encoding the encrypted payload.

50. Sharing the glyph via an output medium.

[0042] In an alternative embodiment the order of the steps is such that the splitting step and the payload generation step are applied before the encryption. In this case, the method comprises the following steps:

60. Serializing the dataset.

10. Splitting the dataset into at least two data subsets.

20. Generating a payload using the first data subset and the second encryption parameter.

70. Encrypting the dataset into an encrypted dataset using an encryption parameter.

80. Encrypting the encryption parameter using a comparatively small second encryption parameter.

30. Storing all data subsets but the first data subset and the encrypted encryption parameter in a key-value database with a hash value of the payload P as storage key.

90. Encrypting the payload with a symmetric encryption key.

40. Generating a glyph encoding the encrypted payload.

50. Sharing the glyph via an output medium.

[0043] The order of the steps of storing the data subsets in a key-value database and of encrypting the payload may also be interchanged so that it is a hash-value of the encrypted payload that is used as storage key for the key-value database.

[0044] The encryption parameter can be a symmetric encryption key 4 such as an AES-128, AES-192 or AES-256 encryption key. This symmetric key 4 can be provided by a suitable service or app used to treat the dataset 9, or it can be provided by a web service which is also available at the time of decryption.

[0045] If the encryption protocol involves a comparatively larger encryption parameter which is too large to be encoded in the glyph 2, an additional encryption step can be operated to produce an encrypted

encryption parameter. The large encryption parameter is encrypted using a comparatively small encryption parameter which will be encoded in the glyph 2 while the encrypted encryption parameter is stored in a key-value database as explained thereafter. This solution allows the use of larger encryption keys or encryption parameters which leads to an increased level of security of the method.

[0046] In a particular embodiment, the dataset 9 is encrypted into an encrypted dataset 8 using an encryption parameter of comparatively large size, for example an AES-GCM encryption protocol involving a symmetric encryption key and an initialisation vector that are too large to be encoded in a glyph 2 such as a QR-code. In this case, the encryption parameter may be itself encrypted using a symmetric encryption key such as for example a symmetric AES key of 256 bits. The resulting encrypted encryption parameter is stored in a key-value database with the other data subsets 6 as explained thereafter, while the key is sufficiently small to be encoded in a glyph 2. The AES-GCM encryption protocol mentioned above is only one example and any other encryption protocol needing large encryption data may be used in the present invention.

[0047] In another embodiment in which the size of the dataset 9 is comparatively small or of type or structure that can be guessable, the dataset 9 can be salted or randomly padded to arbitrarily increase its size before the aforementioned encryption step.

[0048] In another particular embodiment, the dataset 9 comprises email information such as for example

the name and email address of the sender,
the subject of the message,
the names and email addresses of all recipients,
the date of the message,
the names, sizes and signatures of the attachments.

The dataset is encrypted as explained above using an encryption parameter which is itself encrypted by a hardware security module service (HSM service) using a public symmetric encryption key. The encrypted dataset is

then split so that a first data subset, called the head and a second data subset, called the tail. A payload is then generated using the head and the public symmetric encryption key and optionally this payload is also itself encrypted with a public symmetric key. The tail is stored in a key-value database with a hash value of the payload as storage key. A QR-code encoding the payload is then generated and shared via a computer or smartphone screen. This embodiment of the method can be used to provide a secure signature to an email by integrating the QR-code into the email.

Dataset splitting

[0049] The method described above comprises a first step of splitting a dataset 9 into at least two data subsets 3, 6 using a splitting module. The dataset 9 can be split in an arbitrary number of data subsets.

[0050] In a particular embodiment, the dataset 9 is split into two data subsets, the first data subset consisting of the first half of the number of bytes of the dataset 9, and the second data subset consisting of the rest of the bytes of the dataset 9. Any other splitting by slicing the dataset 9 at regular intervals can be considered.

[0051] For security purposes, it is often desirable to make the reassembling of the data subsets difficult for anyone who should not have access to the data. Therefore, the splitting can be made using a cryptographic splitting module. In a particular embodiment, a dataset 9 is first divided into an arbitrary number of portions that are then reassembled by an algorithm that is kept secret, into at least two data subsets 3, 6. Without knowing the algorithm, no one is able to reassemble the data subsets 3, 6 into the original dataset 9.

Generating payload

[0052] According to the method described above, a payload for the glyph 2 is then generated using the first data subset 3 obtained during the data splitting step 10.

[0053] In a particular embodiment in which the dataset 9 has been encrypted with an encryption parameter which is an encryption key 4 of a comparatively small size allowing its encoding in the glyph 2, the payload is generated using both the first encrypted data subset 3 and the encryption key 4.

[0054] In another particular embodiment in which the encrypted dataset 8 has been encrypted using an encryption protocol that needs a comparatively large encryption parameter, the encryption parameter itself can be encrypted into an encrypted encryption parameter using an encryption key. In this case, the payload is generated using the first encrypted data subset 3 and the encryption key.

[0055] In an embodiment, the payload can be further encrypted into an encrypted payload using a public symmetric encryption key. This public encryption key is generated by the service or the application that will process the encrypted payload after a scan of the glyph 2 encoding the encrypted payload.

Storing in a key-value database

[0056] The method described above also comprises a step of storing 20 the at least two data subsets but the first data subset 6 into a key-value database. A key-value database is a database with a hash table data structure. In other words, the database is organised as a collection of records having different fields which themselves contain the data. The data are stored and retrieved using a storage key that identifies uniquely a record in the database. The storage key is constructed as a hash value of the payload that has been generated during the previous step of the method. In other words, it is necessary for a user to know the payload in order to retrieve the data stored in the key-value database. The data may

be stored in an in-memory (RAM) database or alternatively on a solid-state drive or a hard-disk drive.

[0057] In a particular embodiment, the data may also be stored utilizing a single public cloud infrastructure and delivered at scale using a Content Delivery Network (CDN) and other authentication-less methods of content delivery at no loss of integrity, security or confidentiality due to the inability of the attacker to reversely-attribute each data set so stored to its QR code in combination with the nature of the encryption of the payload.

[0058] In a particular embodiment, the key-value database is distributed over several different cloud storage comprising for example content delivery networks (CDN), to further increase the protection of the stored data by fragmenting the data over several different storages.

[0059] In another embodiment, the access to the key-value database requires successful multi-factor authentication. For example, a user has to introduce a correct Time-based One-time Password (TOTP), HMAC-based One-time Password algorithm (HOTP), personal password or a randomly generated code sent to the user's smartphone.

Generating and sharing glyph

[0060] The method described above comprises a final step of generating 40 and sharing 50 a glyph 2 that provides an access to the payload. Any kind of glyph generator can be using so that the present method can be easily implemented on top of existing suitable devices.

[0061] In a particular embodiment, the glyph 2 is generated so that the encoded information is of the form

https://URL/payload

where URL is a uniform resource locator of an application for sharing and visualizing the data encoded in the glyph. This URL may be a locally executed web application and can be distributed via a content delivery network. It may also be an application programming interface (API) of a

web service or application configured for receiving and/or processing the dataset D.

[0062] In another embodiment, the glyph 2 is generated so that the encoded information only consists of the payload. This is useful when the glyph 2 should only be used by a specialized mobile application.

[0063] The glyph 2 can then be shared via an output medium. Output media comprise for example mobile device screens, computers or physical devices on which a glyph 2 can be printed.

[0064] The present disclosure also concerns a method for interpreting a glyph 2, comprising

via an image capture device 1.1, scanning said glyph 2 to retrieve a payload,

deriving a first data subset 3 from said payload,

retrieving at least one data subset 6 in a key value database using a hash of the payload as storage key,

assembling said data subsets 3, 6 into said dataset 9,

[0065] The first step of the method for interpreting a glyph 2 comprises the use of an image capture device 1.1 to scan a glyph. Such devices include cameras of mobile phones or tablets, or any other wireless communication device having an image capture capability.

[0066] The scan of the glyph 2 leads to a retrieving of a payload encoded in the glyph 2 and from the retrieved payload a first data subset 3 is derived. Using a hash of the payload as storage key, at least one data subset 6 is retrieved in a key-value database. Finally, the data subsets 3, 6 are reassembled into a dataset 9.

[0067] An embodiment of this method for interpreting a glyph 2 is illustrated by the Flowchart of Fig. 3. This embodiment comprises the following basic steps:

11. Scanning a glyph 2 with an image capture device 1.1. to retrieve a payload.

21. Deriving a first data subset 3 from the payload .

31. Retrieving at least one data subset 6 in a key-value database using a hash of the payload as storage key.

41. Assembling said data subsets 3, 6 into a dataset 9.

[0068] As the payload may have been encoded in the glyph 2 in encrypted form, an additional step of decrypting 51 the payload may be comprised in the method. This decryption step 51 can be performed by the service or application which is used to treat and process the data.

[0069] In a particular embodiment, the assembling step 41 requires using an encryption key as the data subsets may have been determined by cryptographic splitting as mentioned above. In particular, the data subsets 3, 6 may have been determined by slicing a dataset 9 into regular portions or by applying any other data splitting algorithm.

[0070] A decryption step of the reassembled dataset 8 may be needed in case of an encryption of the dataset 9. This decryption step comprises:
deriving an encryption key from the payload,
decrypting said dataset 8 using the encryption key.

[0071] In another embodiment, a decryption step of the reassembled dataset 8 may be needed if said dataset 9 has been encrypted with an encryption protocol needing large size encryption parameter as described above.

[0072] In this case, the decryption step comprises:
deriving an encryption key from the payload,
retrieving an encrypted encryption parameter in key-value database using a hash of the payload as storage key,

decrypting said encrypted encryption parameter using said encryption key to obtain a decrypted encryption parameter,

decrypting assembled dataset 8 using encryption parameter.

[0073] An embodiment of a method for interpreting a glyph 2 including the previous encryption step is illustrated by the Flowchart of Fig. 4. This embodiment comprises in particular the following:

11. Scanning a glyph 2 with an image capture device 1.1 to retrieve an encrypted payload.

51. Decrypting the encrypted payload into a payload.

21. Deriving a first data subset 3 and an encryption parameter.

31. Retrieving at least one data subset 6 and an encrypted encryption parameter in a key-value database using a hash of the payload as storage key.

61. Decrypting the encrypted encryption parameter using the encryption parameter.

41. Assembling said data subsets 3, 6 into an encrypted dataset 8.

71. Decrypting encrypted dataset 8 using the encryption parameter into a dataset 9.

81. Deserialize dataset 9.

[0074] The decryption step is typically needed when the dataset 9 has been encrypted using an AES-GCM encryption protocol in which the encryption parameter comprises a large encryption key and initialization vector. In this case, the encryption parameter can be further encrypted with a symmetric encryption key of comparatively small size which is stored in the payload.

[0075] Both decryption steps mentioned above may include an additional sub step of decrypting a dataset that have been encrypted by padding.

[0076] In a particular embodiment, the step of retrieving the data subsets 6 stored in the key-value database requires a multi-factor authentication. As an additional security layer, the key-value database may also have been distributed over a plurality of clouds or content delivery networks.

[0077] In another embodiment, a deserializing 81 of the reassembled dataset 9 may be needed to recover the original data structure.

Revoking glyphs

[0078] A mechanism for revoking a glyph 2 is also provided in the method. Indeed, it can be necessary for various reasons to be able to restrict the access to the dataset 9 from a glyph 2.

[0079] In a particular embodiment, a step of deleting the data subsets 6 stored in the key-value database is added to the method.

[0080] In another particular embodiment, a step of deleting/forgetting all the encryption parameters that have been used to encrypt the dataset 9 and/or encryption parameter and/or the payload is added to the method.

System

[0081] The present invention is further related to a system for securely sharing a dataset 9 via a glyph 2 comprising:

a processor 1.2

an image capture device 1.1

a storage 7 for storing a key value database and a computer program 1.4 arranged for casing said processor 1.2 to carry out the methods described above when said program 1.4 is executed.

[0082] In a particular embodiment illustrated in Fig. 5, a system adapted for carrying out the previous methods can comprise a user equipment 1, such as a smartphone, a tablet, a computer, etc including a camera 1.1, a processor 1.2 and a memory 1.3. A glyph 2 can be scanned using the camera 1.1. A program 1.4 stored in the memory 1.3 causes the processor 1.2 to derive a payload constructed with an encrypted data subset 3 and a symmetric encryption key 4. The program 1.4 also retrieves via a suitable network 5 such as a local network, Internet, a mobile network or any other type of adapted network, at least one encrypted data subset 6 in a key-value database that is stored in a server 7. The program then proceeds to an assembling of the encrypted data subsets 8 and to a decryption of the assembled dataset to recover a decrypted dataset 9.

[0083] The user equipment 1 of Fig. 5, or another user equipment, can also be used for generating and sharing a glyph 2, using a program in memory 1.3 arranged for causing the processor 1.2 to carry out the steps of any of the above mentioned or claimed methods.

[0084] The present disclosure is also related to a data storing medium comprising a computer program 1.4 arranged for causing a data processing system to carry the methods described above when said computer program1.4, is executed.

[0085] The data storing medium may be any memory storing a computer program arranged for causing a processor to carry out the methods for securely sharing a dataset 9 with a glyph 2 and/or interpreting a glyph 2 described above.

Additional Features and Terminology

[0086] Many other variations than those described herein will be apparent from this disclosure. For example, depending on the embodiment, certain acts, events, or functions of any of the algorithms described herein can be performed in a different sequence, can be added, merged, or left out altogether (for example, not all described acts or events are necessary

for the practice of the algorithms). Moreover, in certain embodiments, acts or events can be performed concurrently, for instance, through multi-threaded processing, interrupt processing, or multiple processors or processor cores or on other parallel architectures, rather than sequentially. In addition, different tasks or processes can be performed by different machines or computing systems that can function together.

[0087] The various illustrative logical blocks, modules, and algorithm steps described herein can be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. The described functionality can be implemented in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the disclosure.

[0088] The various illustrative logical blocks and modules described in connection with the embodiments disclosed herein can be implemented or performed by a machine, a microprocessor, a state machine, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a FPGA, or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A hardware processor can include electrical circuitry or digital logic circuitry configured to process computer-executable instructions. In another embodiment, a processor includes an FPGA or other programmable device that performs logic operations without processing computer-executable instructions. A processor can also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. A computing environment can include any type of computer system, including, but not limited to, a computer system based on a microprocessor,

a mainframe computer, a digital signal processor, a portable computing device, a device controller, or a computational engine within an appliance, to name a few.

[0089] The steps of a method, process, or algorithm described in connection with the embodiments disclosed herein can be embodied directly in hardware, in a software module stored in one or more memory devices (data storing mediums) and executed by one or more processors, or in a combination of the two. A software module can reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of non-transitory computer-readable data storage medium, media, or physical computer storage known in the art. An example of data storing medium can be coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium can be integral to the processor. The storage medium can be volatile or nonvolatile. The processor and the storage medium can reside in an ASIC.

[0090] Conditional language used herein, such as, among others, "can," "might," "may," "e.g.," and the like, unless specifically stated otherwise, or otherwise understood within the context as used, is generally intended to convey that certain embodiments include, while other embodiments do not include, certain features, elements or states. Thus, such conditional language is not generally intended to imply that features, elements or states are in any way required for one or more embodiments or that one or more embodiments necessarily include logic for deciding, with or without author input or prompting, whether these features, elements or states are included or are to be performed in any particular embodiment. The terms "comprising," "including," "having," and the like are synonymous and are used inclusively, in an open-ended fashion, and do not exclude additional elements, features, acts, operations, and so forth. Also, the term "or" is used in its inclusive sense (and not in its exclusive sense) so that when used, for example, to connect a list of elements, the term "or" means one, some, or all of the elements in the list. Further, the term "each," as used herein,

in addition to having its ordinary meaning, can mean any subset of a set of elements to which the term "each" is applied.

Claims

1. A method for securely sharing a dataset (9) via a glyph comprising:
splitting said dataset (9) into at least two data subsets using a splitting module,
generating a payload for the glyph using a first data subset (3) from the at least two data subsets,
storing all the at least two data subsets but the first data subset (6) in a key value database with a hash value obtained from the payload as storage key,
generating the glyph (2) representing the payload and
sharing the glyph (2) via an output medium.

2. A method according to claim 1, further comprising a preliminary step of encrypting a dataset (9) into an encrypted dataset (8) using an encryption parameter.

3. A method according to claim 2, wherein said encryption parameter comprises a symmetric encryption key (4).

4. A method according to claim 2, wherein said encryption parameter comprises a symmetric encryption key and an initialization vector.

5. A method according to any of the claims 2 or 4, wherein said encryption parameter is encrypted using asymmetric (public-private-key) cryptographic parameter utilizing a Hardware Security Module (HSM), token or web service providing this kind of function.

6. A method according to any of the claims 2 ,4 or 5, wherein said encryption parameter and/or said asymmetric cryptographic parameter are encrypted using a second encryption parameter of comparatively small size.

7. A method according to any of the claims 2 through 5, wherein said payload for the glyph (2) is generated using said first dataset (3) and said encryption parameter.

8. A method according to claim 6, wherein said payload is generated with said first data subset (3) and said second encryption parameter.

9. A method according to claim 8, further comprising a step of storing said encrypted encryption parameter in said key value database with a hash value obtained from the payload as storage key.

10. A method according to any of the preceding claims, wherein said splitting of the dataset (9) is made using a cryptographic splitting module.

11. A method according to any of the preceding claims, wherein said output medium consisting of a computer or a mobile screen device.

12. A method for interpreting a glyph, comprising
via an image capture device (1.1), scanning said glyph to retrieve a payload,
deriving a first data subset (3) from said payload,
retrieving at least one data subset (6) in a key-value database using a hash of the payload as storage key,
assembling said data subsets into said dataset (9).

13. A method according to claim 12, wherein said dataset (9) is an encrypted dataset (8).

14. A method according to claim 13, further comprising a decryption step comprising:
deriving an encryption parameter (4) from said payload,
decrypting said encrypted dataset (8) using the encryption parameter (4) to obtain said dataset (9).

15. A method according to claim 13, further comprising a decryption step comprising:
deriving a second encryption parameter from said payload,
retrieving an encrypted encryption parameter in a key-value database using a hash of the payload as storage key,

decrypting said encrypted encryption parameter using said second encryption parameter to obtain an encryption parameter,

decrypting said encrypted dataset (8) using the encryption parameter to obtain said dataset (9).

16. A method according to any of the claims 12 to 15, wherein said data subsets have been obtained from said dataset (9) by applying a cryptographic splitting algorithm.

17. A method according to any of the claims 12 to 16, further comprising a step of authenticating with a multi-factor authentication to access said at least one data subset in said key-value database.

18. A method according to any of the preceding claims, wherein said glyph (2) consists of a barcode or matrix code.

19. A method according to any of preceding claims, further comprising a step of revoking said glyph by deleting said data subsets from said key-value database.

20. A method according to any of the preceding claims, further comprising a step of revoking said glyph by deleting said encryption parameter and/or said second encryption parameter.

21. A system for securely sharing a dataset (9) via a glyph comprising:

a processor (1.2)

an image capture device (1.1)

a storage (7) for storing a key value database and a computer program (1.4) arranged for causing said processor (1.2) to carry out the methods of any of the previous claims when said program (1.4) is executed.

22. A data storing medium (1) comprising a computer program (1.4) arranged for causing a data processing system to carry out the methods of any of the claims 1 to 20 when said computer program, is executed.

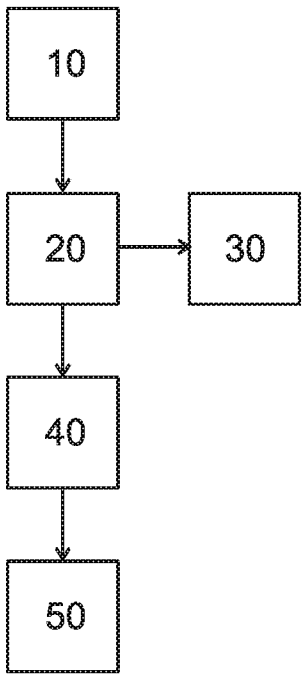

Fig. 1

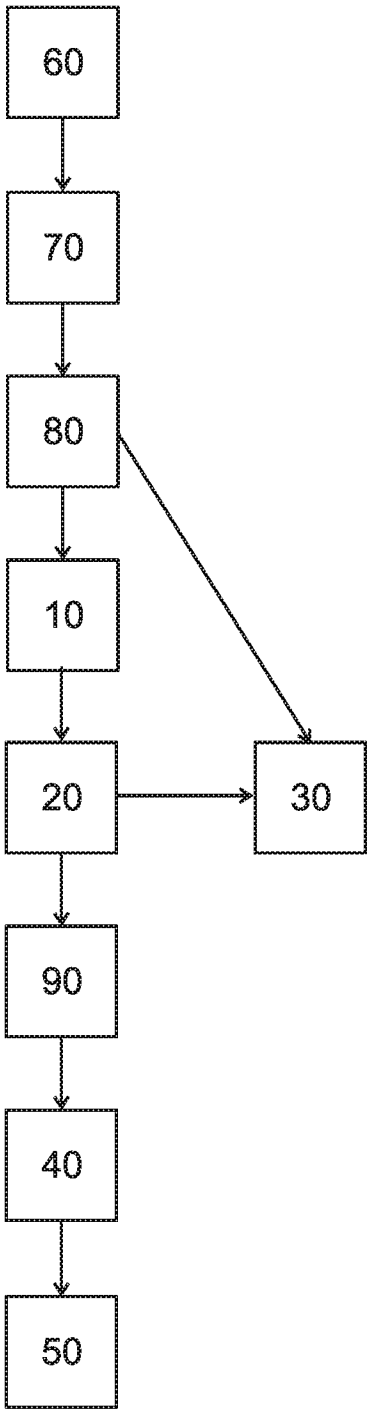

Fig. 2

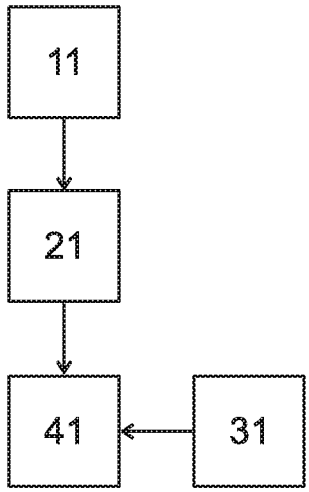

Fig. 3

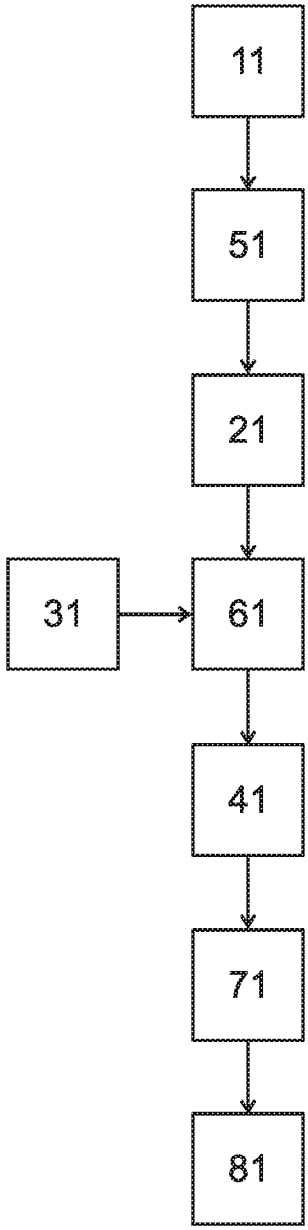

Fig. 4

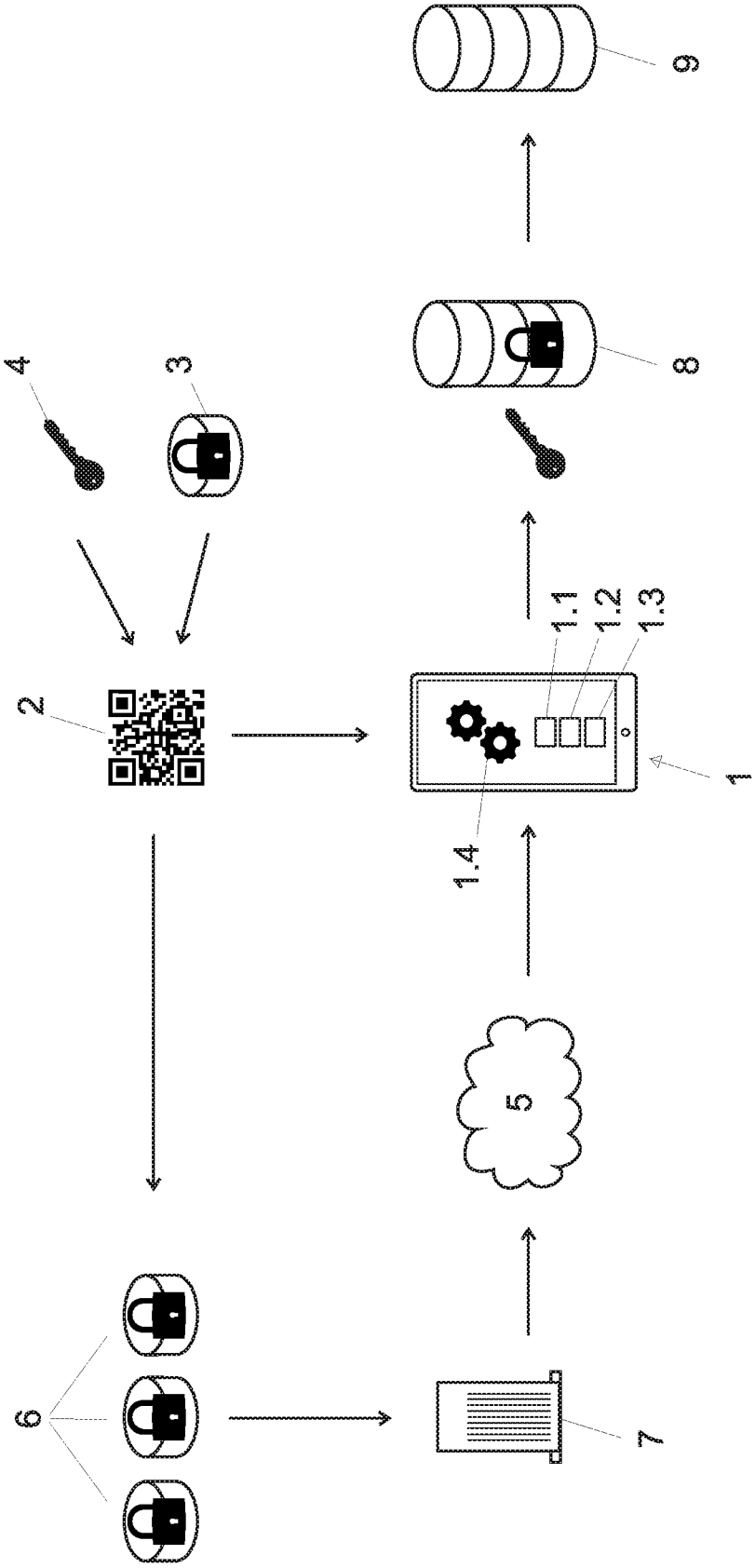

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2021/061318

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/36 H04L9/00 H04W12/77 G06F21/62
ADD.

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)
H04L G06F H04W

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	US 2015/358164 A1 (CARTER PAUL L [NZ]) 10 December 2015 (2015-12-10) abstract paragraphs [0004] - [0007] paragraphs [0019] - [0026] paragraphs [0034] - [0054] paragraphs [0064] - [0070] claims 1-27 figures 1-7 ----- -/--	1-22

[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
18 February 2022	28/02/2022

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	Bichler, Marc

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2021/061318

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 509 275 A1 (BUNTINX [BE]) 10 October 2012 (2012-10-10) abstract paragraphs [0006] - [0016] paragraphs [0032] - [0052] paragraphs [0083] - [0098] paragraphs [0109] - [0122] claims 1-19 figures 1-16b	1-22
A	US 2007/170250 A1 (BYSTROM TOMAS [GB] ET AL) 26 July 2007 (2007-07-26) abstract paragraphs [0007] - [0011] paragraphs [0027] - [0038] paragraphs [0042] - [0049] claims 1-10 figures 1-5	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2021/061318

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015358164 A1	10-12-2015	US 2015358164 A1	10-12-2015
		US 2017134167 A1	11-05-2017
EP 2509275 A1	10-10-2012	AU 2012239057 A1	14-11-2013
		BE 1019683 A3	04-09-2012
		BR 112013025752 A2	02-05-2018
		CA 2832171 A1	11-10-2012
		CN 103493460 A	01-01-2014
		EP 2509275 A1	10-10-2012
		EP 2695354 A1	12-02-2014
		JP 2014515142 A	26-06-2014
		RU 2013147885 A	10-05-2015
		SG 193987 A1	29-11-2013
		US 2014026204 A1	23-01-2014
		WO 2012136366 A1	11-10-2012
		ZA 201308105 B	25-06-2014
US 2007170250 A1	26-07-2007	NONE	