METHOD AND SYSTEM FOR PROTECTING SENSITIVE INFORMATION AND PREVENTING UNAUTHORIZED USE OF IDENTITY INFORMATION

Inventor: Lingyan Shu, Metairie, LA (US)

Correspondence Address:
Lingyan Shu
4017 Richland Ave
Metairie, LA 70002 (US)

Appl. No.: 12/587,810
Filed: Oct. 13, 2009

Related U.S. Application Data
Continuation of application No. 10/653,846, filed on Sep. 2, 2003, now Pat. No. 7,603,320.
Provisional application No. 60/407,540, filed on Aug. 31, 2002.

Publication Classification
Int. Cl. H04L 9/32 (2006.01) G06F 21/00 (2006.01)

U.S. Cl.: 726/7

ABSTRACT
This invention features a method and system for protecting sensitive information and preventing the unauthorized use of identity information by third parties. Virtual identifiers that identify an information holder whose sensitive information is involved in the process, are dynamically created by an entity called processing entity. The virtual identifiers are usually linked to a static identity of the information holder through a data management mechanism, such as a database system. A virtual identifier could serve for multiple functions. Usually, validity attributes that indicate when and for how long a virtual identifier is valid for the different functions, are associated with the virtual identifier. When the information holder interacts with a third party in a process that involves the information holder’s sensitive information, the information holder uses virtual identifiers. Then, through a device connected to a network including wireless devices, telephone or a mail service, the party either passes along the virtual identifiers to other parties or submits requests along with the virtual identifiers to the processing entity which could map the virtual identifiers to the static identity information and uses the static information to realize the requests.

Diagram:

- Create a virtual identifier and another identifier for displaying in or on a medium
- Link the virtual identifier and the other corresponding identifier to static information
- Use the medium
- Send virtual identifier and the other corresponding identifier to the processing entity
- Processing entity maps the virtual identifier to the static information
- Processing entity verifies if the medium and information it carries is valid
  - Yes: Confirm validity
  - No: Acknowledge invalidity
create virtual identifier

link virtual identifier to static information

issue virtual identifier

use virtual identifier when information holder dealing with third parties

use virtual identifier when third parties dealing with each other

map virtual identifier to static information

Fig. 1
create virtual identifier

link virtual identifier to static information

issue virtual identifier

use virtual identifier when information holder dealing with third parties

use virtual identifier when third parties dealing with each other

map virtual identifier to static information

update said virtual identifier's validity attributes

Fig. 2
1. Create virtual identifier

2. Link virtual identifier to static information

3. Issue virtual identifier

4. Use virtual identifier when information holder dealing with third parties

5. Use virtual identifier when third parties dealing with each other

6. Map virtual identifier to static information

7. Update said virtual identifier's validity attributes

8. Verify if said virtual identifier is valid
   - Yes: Process said party's request
   - No: Acknowledge invalidity

---

Fig. 3
information holder registers with processing entity

processing entity stores registration information

information holder contacts processing entity

processing entity authenticates the information holder

processing entity creates virtual identifier

processing entity links virtual identifier to static information

processing entity issues virtual identifier

information holder uses virtual identifier with non-information-destination

non-information-destination and processing entity get in touch with each other and processing entity gets the virtual identifier from the non-information-destination

processing entity maps the virtual identifier to static information

processing entity verifies if the virtual identifier is valid

Yes

processing entity processes request

No

processing entity acknowledges invalidity

processing entity passes result to the non-information-destination

Fig. 4
information holder registers with processing entity

Information destination registers with processing entity

processing entity stores registration information

information holder contacts processing entity

processing entity authenticates said information holder

processing entity creates virtual identifier

processing entity links virtual identifier to static information

processing entity issues virtual identifier

information holder uses virtual identifier with Non-information-destination

information destination is given a virtual identifier

information destination and processing entity get in touch with each other

processing entity maps virtual identifier to a static identifier

verifies if the virtual identifier is valid

processing entity processes for information destination

processing entity acknowledges invalidity

processing entity passes information to information destination

Fig. 5
create a virtual identifier and another identifier for displaying in or on a medium

link the virtual identifier and the other corresponding identifier to static information

use the medium

send virtual identifier and the other corresponding identifier to the processing entity

processing entity maps the virtual identifier to the static information

processing entity verifies if the medium and information it carries is valid

Yes

confirm validity

No

acknowledge invalidity
Create a virtual account number for each check number

link virtual account number and the corresponding check number to static account number

issue the checks

account holder writes the checks to third parties

send virtual account number and the corresponding check number of a written check to the processing entity

processing entity maps the virtual account number to the static account number

processing entity verifies if the check is valid

Yes

confirm validity

No

acknowledge invalidity

Fig. 7
Credit card number --- (C.C.N.) holder registers with C.C.N. holder gives processing entity virtual Credit Card number to... Contacts the processing entity with the virtual credit card number C.C.N. holder applies for a virtual credit card number

processing entity authenticates applicant No

processing entity maps the virtual Credit card number to the C.C.N.

if mapping Successful processing entity acknowledges virtual Card number is valid invalidity if said applicant passes

the status of the virtual Credit card processing entity number C.C.N. holder

processes virtual Card number to the C.C.N. holder

Fig. 8
third party contacts the processing entity

processing entity requests for a virtual social security number (V.S.S.N.)

processing entity creates a V.S.S.N.

processing entity links the V.S.S.N. to the S.S.N.

processing entity issues the V.S.S.N. to the S.S.N. holder

The S.S.N. holder gives the V.S.S.N. to a third party

third party requests for information with the V.S.S.N.

processing entity maps the V.S.S.N. to the S.S.N.

if mapping is successful

processing entity acknowledges invalidity

processing entity gets information from an information source using the S.S.N.

processing entity gives the result to the third party

processing entity changes the status of the V.S.S.N.

processing entity acknowledges invalidity

if V.S.S.N. is valid

Yes

No

Fig. 9
METHOD AND SYSTEM FOR PROTECTING SENSITIVE INFORMATION AND PREVENTING UNAUTHORIZED USE OF IDENTITY INFORMATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of a prior application entitled “Method And System For Protecting Sensitive Information And Preventing Unauthorized Use Of Identity Information”, which was assigned Ser. No. 10/653,846 and filed 2003 Sep. 2, now U.S. Pat. No. 7,603,520 and which claims the benefit of a provisional patent application Ser. No. 60/407,540, filed 2002 Aug. 31.

FIELD OF THE INVENTION

[0002] This invention relates generally to methods and systems for protecting sensitive information, particularly identity information from being disclosed, collected, mismanaged, or misused during transactions that involve multiple parties.

BACKGROUND OF THE INVENTION

[0003] Currently, the extensive and unprotected use of one's identity information makes it very hard to prevent such identity information from being collected, misused or mishandled. For example, people are required to disclose their social security numbers and dates of birth to landlords when applying for renting a property, to disclose the same information to loan officers when applying for loans, to disclose the information to service representatives when applying for cellular phone services, etc. One needs to disclose one's credit card information to the person on the other end of the telephone line when making a hotel reservation or when reserving a rental boat. When shopping on-line or off-line with credit cards, credit card numbers along with other personal information need to be disclosed. People have no control over how the disclosed information will be managed and used. Even worse, people are vulnerable to information collection attacks. People are sent credit card application invitations with good offers. All they need to do to apply for a credit card is to fill in their social security numbers, dates of birth and other personal information. Yet, these invitations may come from an entity that is trying to collect personal information. Because of the unprotected and extensive use of identity information, identity theft has become a serious problem that can affect anyone. Another problem with the extensive use of sensitive information is that people can lose privacy without even knowing it. Vendors can collect an individual's shopping lists and use them to get other information about the individual. Also, the more one uses his/her sensitive information over the transmission media, the more susceptible the information is to being intercepted and collected. In U.S. Pat. No. 5,884,272, a method and system for establishing anonymous communications between two parties are described. In this prior art, a central database is used to store the two parties' identities and data, as well as the rules for releasing the data. The two parties could get each other's information without having to disclose its own identity. This prior art is for establishing anonymous communications between only two parties and requires that the data and/or information sources related to both parties be centralized.

[0004] In U.S. Pat. No. 6,029,890, a user-specified credit card system is described. In this prior art, a central bank control system is used to transmit a user's request for a one-time credit card number to a credit provider and transmit back a one-time credit card number from the credit provider after the request is validated by the credit provider. This prior art would achieve the object of not giving out a static credit card number to the vendors. However, it requires a fairly large amount of changes to the current financial networks, including credit card approval and ATM networks to implement the central bank control system in this prior art. It also requires changes to each credit provider's business processes at a low level which is more difficult than making changes at a higher level. Therefore, it is costly and not easy to implement this prior art. In another prior art, U.S. Pat. No. 5,890,137, a method of credit card payment settlement in an on-line shopping system is described. In this method, a service center sends order data including the credit card information via a settlement network. The approval center pays the price to the service center. Then, service center sends the order information to the shopping system. This way the credit card information is not transmitted in public networks, such as the Internet. This prior art too, requires a large amount of changes to the existing business processes.

OBJECTS OF THE INVENTION

[0005] It is an object of the present invention to obviate the disadvantages of the prior art; It is an object of the present invention to provide a method and system for preventing sensitive information from being disclosed to certain parties, especially the parties whose credibility is uncertain, during transaction processes that involve multiple parties; It is an object of the present invention to provide a method and system for preventing unauthorized use of one's identity information by a third party; It is a further object to make it easy and cost-effective for the current business processes to adapt to the present invention.

SUMMARY OF THE INVENTION

[0006] An embodiment of the present invention provides a method and system for protecting sensitive information, more particularly identity information during multi-party transaction processes. This method prevents sensitive information from being disclosed to certain parties, especially the parties whose credibility is uncertain. This method provides a way to prevent sensitive information from being collected illegally or being collected and used without authorization. An entity called processing entity creates virtual identifiers for an information holder whose sensitive information is involved in the process. A virtual identifier identifies an information holder and is usually temporary and has validity attributes. It usually maps to a static identity of the information holder. The processing entity stores the information about the virtual identifiers. Usually, the virtual identifiers are issued to the information holder. The information holder uses a virtual identifier when interacting with third parties. The third parties also use the virtual identifiers when interacting with other parties concerning the information holder. Such a system comprises a processing entity which creates and processes virtual identifiers, a data management system for storing and retrieving data, and a communication component which includes the different interfaces for the communications between different parties.
This method eliminates the necessity of disclosing sensitive information, particularly identity information, to parties whose credibility is uncertain. Furthermore, this method greatly reduces the need of using one’s static identity information in the processes that are prone to eavesdropping and interception, such as Internet transactions, telephone transactions, and mail transactions. This method allows for one-time or multiple-time identification, therefore the virtual identifiers can serve the different functions the static identifiers serve currently and effectively protects the information holder from identity collection attacks and identity theft attacks. Yet, this method is easy to implement and does not require fundamental changes to the current business processes.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating the steps of the first embodiment described in the DETAILED DESCRIPTION;
FIG. 2 is a block diagram illustrating an embodiment of the present invention;
FIG. 3 is a block diagram illustrating an embodiment of the present invention;
FIG. 4 is a flow diagram illustrating an embodiment of the present invention;
FIG. 5 is a flow diagram illustrating an embodiment of the present invention;
FIG. 6 is a flow diagram illustrating an embodiment of the present invention in which a virtual identifier and another corresponding identifier are displayed in or on a medium;
FIG. 7 is a flow diagram illustrating an embodiment of the present invention in which a virtual identifier is a virtual account number and its corresponding identifier is a check number;
FIG. 8 is a flow diagram illustrating an embodiment of the present invention in which a virtual identifier is a virtual credit card number;
FIG. 9 is a flow diagram illustrating an embodiment of the present invention in which a virtual identifier is a virtual social security number;
FIG. 10 is a block diagram illustrating the components of an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The following terms are used in the description of this invention.
Information destination—entity that has to use the information directly to serve its function.
Non-information-destination—entity that uses the information indirectly to serve its function.
Information holder—entity whose sensitive information is needed in the processes that involve multiple parties.
Information source—entity that has sensitive information of an information holder. An information destination and an information source can reside in the same entity.
Virtual identifier—A virtual identifier comprises information that identifies an information holder. A virtual identifier usually corresponds to a static identity of an information holder. It is usually valid for a stated period of time for each of its specified functions. It can be valid for a one-time use or for multiple-time uses. A possible virtual identifier string comprises a field that identifies the information holder, a field that indicates an information source and a field of a randomly generated string.
Processing entity—entity that creates, manages and processes virtual identifiers. A processing entity can reside in the same system as an information source and/or an information-destination. A processing entity usually resides in a server computer system.
Where indicated, these terms are used interchangeably with some other terms through out the specification.
FIG. 1 is a block diagram illustrating the general steps of an embodiment of this invention. A processing entity creates virtual identifiers for an information holder. The processing entity links the virtual identifiers to the static information of the information holder, through a data management mechanism such as database tables. The processing entity links other related information, such as the validity attributes of a virtual identifier, to the virtual identifier, usually through a data management mechanism or through adding the validity attributes to the virtual identifier string. Virtual identifiers are used when the information holder deals with third parties, particularly non-information-destination entities. The third parties use the virtual identifiers when dealing with each other concerning the information holder. At certain point of the process, virtual identifiers are mapped to the static information through a data management technique, such as a database query. Static sensitive information, particularly static identity information is not circulated in the process. Consequently, the static information is protected against collection and fraud. A variant of this embodiment is to add the following step:
Update the virtual identifier’s validity attributes. For example, marking the virtual identifier as invalid.
FIG. 2 illustrates this variation. In FIG. 3, the step of verifying the virtual identifiers after they are submitted to the processing entity is added.
FIG. 4 is a flowchart illustrating the general steps of an embodiment. An information holder registers with a processing entity. The processing entity stores the information in a computer system using data management mechanisms such as database systems. For security purpose, the information can be encrypted by the processing entity before being stored. Then each time when the information holder needs a virtual identifier, he/she/it contacts the processing entity through a device that is connected to a network, a telephone or mail. The processing entity authenticates the user (user is used interchangeably with information holder through out the Specification) through an authentication protocol, such as a user id and password pair. If the authentication is successful, the user is prompted to input the validity terms as the validity attributes for the virtual identifier. For example, the user can specify that the virtual identifier is valid for only one-time use within the current week. The processing entity then creates a virtual identifier that can uniquely identify the user. The processing entity links the virtual identifier to the static identity information through data management mechanisms such as database systems. The processing entity issues the virtual identifier to a third party specified by the user or to the user. In the latter case, the user can then give this virtual identifier to a non-information-destination entity in a process. Then the non-information-destination gets in touch with the processing entity and requests for service. The non-information-destination gives the virtual identifier to the processing entity. The processing entity maps the virtual identifier to the static
identity information. The processing entity verifies, based on the validity information, if the virtual identifier is valid. If it is valid, the processing entity processes the request, which may mean using the static identity information to contact an information source to get information. Then the non-information-destination is given the result. Depending on how the virtual identifier’s validity was specified, the processing entity changes the status of the virtual identifier after each use of it.

FIG. 5 is a flowchart of another embodiment of this invention. In this embodiment, the non-information-destination entity gives the virtual identifier to an information destination. Then the information destination and the processing entity get in touch with each other. The processing entity maps the virtual identifier to the static identity and verifies if the virtual identifier is valid. If it is valid, then the processing entity processes for the information destination, which could include using the static identity information to get information from an information source. The processing entity and the information source could reside in the same computer system.

FIG. 6 is a flowchart of another embodiment of this invention. It is a method of preventing forgery. A processing entity creates virtual identifiers and another corresponding identifier for each virtual identifier and links them to the static identity information using data management mechanisms such as a database system. Validity attributes for the virtual identifier are also linked to the static information. Each virtual identifier contains a part that is randomly generated by a random number generator as part of the procedure. The virtual identifiers, their corresponding other identifiers and the validity attributes are stored in a database system. Then the virtual identifiers and their corresponding other identifiers are displayed in or on a medium. Each such medium uses a different virtual identifier. In each use of a medium, the virtual identifier and the corresponding other identifier are collected by the processing entity. The processing entity maps the virtual identifier to the static identity information and verifies if the virtual identifier matches the corresponding identifier based on the stored information. It also verifies if the virtual identifier is valid based on the validity terms of the virtual identifier. If it is valid, a validity confirmation is sent to the requesting party. If it is invalid, an invalidity acknowledgement is sent to the requesting party.

FIG. 7 is a flowchart of another embodiment of this invention. It is a method of protecting account numbers against collection and fraud when checks are used. The account holder requests for checks through a network connected communication device, e.g., a client computer that has Internet access, a telephone, mail service or in person. A processing entity creates virtual account numbers and links them to the static account number using data management mechanisms such as a database system. The default validity term for the virtual account numbers could be that each virtual account number is valid for one time for cashing and for the time periods specified by the financial institute for shipping, direct-deposit, automatic-drafting, etc. Each virtual account number contains a part that is randomly generated by a random number generation function or procedure. The virtual account numbers, their corresponding check numbers and the validity terms are stored in a database system. Then the virtual account numbers and their corresponding check numbers are printed on checks. Each check uses a different virtual account number. Then the checks are issued to the account holder. The account holder uses the checks the way it is done now. In each use, the virtual account number and the corresponding check number of a written check are collected by the processing entity. The processing entity maps the virtual account number to the static account number and verifies if the virtual account number matches the check number based on the stored information. It also verifies if the virtual account number is valid based on the validity terms of the virtual account number. If it is valid, a validity confirmation is sent to the requesting party. If it is invalid, an invalidity acknowledgement is sent to the requesting party. A variation of this method is to include the static account number in a virtual account number. In this method, the static account number is not protected from being disclosed. However, it prevents forged checks from being cashed.

FIG. 8 is a flowchart illustrating this method. A credit card holder registers with a processing entity. This is done through a device connected to a network, a telecommunication device, such as a telephone, or mail. The processing entity stores the information securely in a database system. A user id and password are created during registration. The credit card holder can then contact the processing entity through a device connected to a network, or a telecommunication device, to get virtual credit card numbers. After an authentication procedure, i.e., verifying the user’s id and password, the processing entity prompts the user to specify the validity terms of the virtual card number. The processing entity then creates a virtual credit card number and links it to the static credit card number, and then issues the virtual card number to the user. The credit card holder can then use virtual credit card number when dealing with a goods or services provider. The provider submits the transaction with the virtual credit card number to the processing entity. The processing entity maps the virtual credit card number to the static credit card number through a database system and checks the validity of the virtual credit card number that is being submitted. If the virtual card number is valid, the processing entity attaches the static credit card information to the transaction and submits the transaction to the credit card approval network or credit card issuer. The processing entity gets the approval result and passes it to the goods or services provider. A credit card refund can be processed in the same way. The services or goods provider submits the refund transaction with the virtual card number to the processing entity. If the processing entity determines that this is a refund and the virtual card number is valid for tracking, it attaches the static credit card number to the transaction and submits the transaction to the credit card approval network or credit card issuer. The processing entity then passes the confirmation result to the provider. A virtual credit card number can be valid for only one day and only for one purchasing, but it can be valid for tracking or automatic billing, etc. for a much longer term, such as three years or longer.

FIG. 9 illustrates this method. In this method, a social security number holder requests for a virtual social security number from a processing entity through a device connected to a network or a telephone. The processing entity prompts the user to select validity terms and creates a virtual social security number. The processing entity links the virtual social security number to the static social security number and with the validity terms. The processing entity then issues the virtual social.
security number to the user. The user uses the virtual social security number when dealing with third parties, particularly non-information-destination entities. When a third party needs to get information about the social security number holder, the third party submits the virtual social security number to the processing entity. The processing entity maps the virtual social security number to the static social security number through a database system and determines the validity of the virtual social security number. If it is valid, the processing entity gets the results and passes them to the third party. On the other hand, a third party can report to an information source through a processing entity using a virtual social security number. The processing entity maps the virtual social security number to the static social security number, attaches the static social security number to the report, and then passes it to the information source through a network connection. Or the third party could report to an information source directly with the virtual social security number. The information source then could get the static social security number through the processing entity.

FIG. 10 illustrates the components of an embodiment of this invention. The processing entity which usually resides in a server computer system is the main component. The processing entity creates, manages and processes virtual identifiers. Through the different communication interface components, the processing entity communicates with information holders, information sources, information destinations and non-information-destinations. The data management component links, stores and retrieves data and information.

Many embodiments of this invention comprise all or some of the following processes.

Registration Process:

When registering through a computer network, such as Internet, or a telephone, an information holder is prompted to create or given a user id. Then based on the authentication protocol used by the processing entity, the information holder needs at least another element for an authenticated handshake with the processing entity when requesting for virtual identifiers in the future. For example, if the authentication protocol uses a user id and password pair to verify a user, the information holder needs a password. If the authentication procedure uses cryptographic techniques, the information holder needs encryption/decryption keys. In this Specification, we use the user id and password pair scheme. After successfully getting the user id and password, the information holder provides his/her/its static information to the processing entity. For a higher security requirement, a secure communication link is used in the registration. The processing entity securely stores the information. When registering through a mail service, the user fills out the form with static information and then mails the form to the processing entity. The processing entity creates a user id and an initial password for the user.

Request for Virtual Identifier Process:

An information holder gets in touch with a processing entity through a networked device, such as a computer, a telephone or mail. When using a computer or telephone, the information holder is prompted to give input on the validity terms of the virtual identifier, e.g. the time period in which the virtual identifier can be used to get information, and how many times the virtual identifier can be used to get information from an information source or a processing entity. The processing entity can also allow the user to select a default validity setting. The processing entity stores the input and creates a virtual identifier for the information holder. The processing entity may issue the virtual identifier to the information holder or give it directly to a specified third party.

Virtual Identifier Creation Process:

An example of a virtual identifier is a string that comprises the information holder’s user id, the code name of the information source, e.g. a credit card issuing company’s code name. The processing entity could also create a random string using a random number generator algorithm and append it to the first string and makes sure that the final string is not a string that is already being used by the information holder. The processing entity then links the virtual identifier to the static information, such as a credit card number. The processing entity also links the validity attributes which specify the time period during which the identifier is valid, how many times the identifier can be used to get information and other constraints to the identifier. The validity attributes could also be included in the virtual identifier string. The links could be established through database tables. Also a time period is specified for an identifier during which the identifier can be used by different entities, such as a non-information-destination to give input, such as reporting a no payment from the information holder, to the information source, and to conduct tracking, auto-drafting or auto-billing.

Using a Virtual Identifier by an Information Holder:

An information holder discloses a virtual identifier to third parties during the processes where the information holder’s sensitive information is involved.

Using a Virtual Identifier by a Non-Information-Destination Entity:

A non-information-destination entity passes the virtual identifier along with other information to the processing entity, an information-destination entity or a non-information-destination entity.

Processing a Virtual Identifier by a Processing Entity:

A processing entity processes transactions that contain virtual identifiers. A processing entity determines the purpose of a transaction request, such as getting information, giving input to an information source, tracking, automatic drafting or automatic billing. It maps a virtual identifier to the static identity information through a data management mechanism, such as a database system. It checks if a virtual identifier is valid for the type of the request. If it is valid for getting information, the processing entity gets the requested information and transfers it to the entity that needs the information. If it is valid for reporting to the information source, the processing entity sends the report data to the information source.

Communication Processes:

Communications between different entities are done through devices connected to networks including private networks and public networks such as the Internet, telephones and mail services. Virtual private network techniques
and wireless devices can be used. Cryptographic techniques and secure links could be used for secure communication.

[0044] While several embodiments of the invention have been shown and described herein, it will be obvious to those skilled in the art that various changes and modifications can be made therein without departing from the scope of the invention as defined by the Claims.

I claim:

1. A method of protecting a static identifier of an information holder, comprising:
   a) receiving a request for one or a plurality of virtual identifiers by a processing entity computer system;
   b) creating one or a plurality of virtual identifiers by said processing entity computer system with each of said one or a plurality of virtual identifiers uniquely identifies said information holder;
   c) linking said one or a plurality of virtual identifiers to said static identifier by said processing entity computer system;
   d) issuing said one or a plurality of virtual identifiers to said information holder;
   e) receiving a message comprising a request for service with a virtual identifier by said processing entity computer system from a first device of a requesting party, said requesting party being a party that received said virtual identifier from said information holder or from a non-information-destination and submitted said request for service to said processing entity computer system;
   f) processing said request for service from said requesting party by said processing entity computer system;
   g) transmitting the result of step f) to said first device of said requesting party or a second device of said requesting party;

  whereby the creation and issuance of the virtual identifiers are independent of those of the static identifier since the format of the virtual identifier is independent of that of the static identifier.

2. The method as recited in claim 1 further comprising:
   a) receiving said static identifier of said information holder from a device of said information holder by said processing entity computer system;
   b) transmitting said static identifier to a data management system.

3. The method as recited in claim 2 wherein the step of receiving said static identifier from a device of said information holder is conducted through a public network.

4. The method as recited in claim 3 wherein said public network is the Internet.

5. The method as recited in claim 2 wherein step e) is conducted through a public network.

6. The method as recited in claim 5 wherein said public network is the Internet.

7. The method as recited in claim 5, further comprising: validating said virtual identifier by said processing entity computer system.

8. The method as recited in claim 7, further comprising: identifying by said processing entity computer system said static identifier of said information holder using said virtual identifier.

9. The method as recited in claim 8 wherein step f) is conducted through transmitting a message comprising a request for sensitive information of said information holder with said static identifier to an information source and receiving the requested sensitive information from said information source.

10. The method as recited in claim 8 wherein the result of step f) comprises said static identifier.

11. The method as recited in claim 8 further comprising: updating said virtual identifier’s validity status by said processing entity computer system.

12. The method as recited in claim 11 wherein said static identifier is a social security number.

13. The method as recited in claim 9 wherein said virtual identifier is valid for one-time or multiple-time for requesting said sensitive information.

14. The method as recited in claim 8 wherein said virtual identifier comprises validity attributes.

15. A system of protecting a static identifier of an information holder, comprising:
   a) a data management system to store and retrieve data;
   b) a processing entity to receive a request for one or a plurality of virtual identifiers, to create one or a plurality of virtual identifiers with each of said one or a plurality of virtual identifiers uniquely identifies said information holder, to link said one or a plurality of virtual identifiers to said static identifier, to issue said one or a plurality of virtual identifiers to said information holder, to receive a message comprising a request for service with a virtual identifier from a first device of a requesting party, said requesting party being a party that received said virtual identifier from said information holder or from a non-information-destination and submitted said request for service to said processing entity computer system, to process said request for service from said requesting party, to transmit the result of the above processing to said first device of said requesting party or a second device of said requesting party, said processing entity residing in a computer system; and
   c) wherein said processing entity sends data to and gets data from said data management system.

16. The system as recited in claim 15 wherein said processing entity receives said message comprising a request for service through a public network.

17. The system as recited in claim 16 wherein said public network is the Internet.

18. The system as recited in claim 15 wherein said data management system comprises a database system.

19. The system as recited in claim 15 wherein said processing entity processes said request for service through transmitting a message comprising a request for obtaining sensitive information of said information holder to an information source.

20. The system as recited in claim 19 wherein said virtual identifier is limited to be valid for one-time or multiple-time.