

CLAIMS:

1. A method comprising:
 - encrypting, by a client terminal, sensitive data by using a key in response to receipt of the sensitive data;
 - sending, by the client terminal, the encrypted sensitive data to a provider server through a first request;
 - obtaining, by the client terminal, a unique tag identifying the sensitive data from a third party server, the unique tag being further used for identifying the key;
 - sending, by the client terminal, the key and the unique tag to the provider server through a second request; and
 - sending three-party service data identified by the unique tag to the third party server so that the third party server generates a three-party service request that carries the unique tag and the three-party service data and sends the three-party service request to the provider server, wherein the client terminal, the provider server and the third party server are different from one another.
2. The method of claim 1, further comprising requesting the provider server to decrypt the sensitive data corresponding to the unique tag by using the key.
3. The method of claim 1, wherein the first request and the second request are different requests.
4. The method of claim 1, the unique tag includes a random code and a timestamp.
5. The method of claim 1, further comprising sending the key and the unique tag to the third party server so that the third party server obtains the unique tag and the key and wherein the three-party service request further carries the unique tag and the key.

6. The method of claim 1, wherein the key is a dynamic key generated for the sensitive data.

7. A method comprising:

acquiring, by a provider server, encrypted sensitive data sent by a client terminal through a first request, the encrypted sensitive data being obtained by the client terminal through encryption by using a key;

acquiring, by the provider server, a unique tag and the key sent by the client terminal through a second request, the unique tag is a unique tag identifying the sensitive data and the first request and the second request being different requests;

storing, by the provider server, the encrypted sensitive data and the unique tag as a key-value pair;

decrypting, by the provider server, the sensitive data corresponding to the unique tag by using the key;

receiving a three-party service request sent from a third party server, the three-party service request carrying the unique tag and three-party service data; and

performing processing on the three-party service data and the sensitive data corresponding to the unique tag, wherein:

the three-party service request further carries the key; and

acquiring the unique tag and the key sent by the client terminal through the second request comprises acquiring the unique tag, the key and the three-party service data from the received three-party service request, the three-party service request being sent by the third party server in response to receipt of the second request carrying the unique tag, the key and the three-party service data that is sent by the client terminal.

8. The method of claim 7, further comprising:

generating a unique tag of the sensitive data; and

returning the unique tag back to the client terminal.

9. The method of claim 8, wherein the unique tag includes a random code and a timestamp.

10. The method of claim 7, further comprising:
receiving the unique tag that is sent together with the encrypted sensitive data, the unique tag being generated for the sensitive data by the client terminal after receiving the sensitive data.

11. The method of claim 7, further comprising:
receiving the unique tag that is sent together with the encrypted sensitive data, the unique tag being generated by a third party server for the sensitive data.

12. A method comprising:
acquiring, at a third party server, a unique tag corresponding to sensitive data received by a client terminal; and
sending, by the third party server, a three-party service request that carries the unique tag and three-party service data to a provider server, to cause the provider server to process the three-party service data and the sensitive data, the unique tag being further used for identifying the three-party service data, wherein:
the sensitive data does not pass through the third party server to avoid a leakage of the sensitive data at the third party server,
the sensitive data is encrypted by the client terminal by using a key and sent to the provider server through a first request;
the key and the unique tag are sent to the provider server by the client terminal through a second request; and
the first request and the second request are different requests.

13. The method of claim 12, wherein the provider server decrypts the sensitive data corresponding to the unique tag by using the key.

14. The method of claim 12, wherein the third party server, the client terminal and the provider server are different from one another.