CLAIMS

1. A privacy data access method, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; and the method is executed by the SDK, and the method comprises:

obtaining a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

2. The method according to claim 1, wherein the request further comprises identification information corresponding to the target user and authorization authentication information; and before the obtaining access configuration information from the first application, the method further comprises:

sending, to the first application, an authentication request that carries the identification information corresponding to the target user and the authorization authentication information, to perform identity authentication by using the first application; and

when the identity authentication succeeds, performing the operation of obtaining the access configuration information from the first application.

3. The method according to claim 1, wherein the data access comprises data writing; the request further comprises first data to be written; the first data is plaintext data generated inside the TEE system; and the access configuration information further comprises a privacy-related field in data and an encryption key held by the TEE system; and

the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

encrypting, by using the encryption key, a privacy-related field in the first data to obtain second data; and

writing, according to the storage address of the digital asset corresponding to the target user, the second data into the digital asset corresponding to the target user in the external storage device of the TEE system.

4. The method according to claim 1, wherein the data access comprises data reading; the access configuration information further comprises a privacy-related field in data and a decryption key; and the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

obtaining to-be-read third data from the external storage device of the TEE system according to the storage address of the digital asset corresponding to the target user;

decrypting, by using the decryption key, a privacy-related field in the third data to obtain fourth data for internal use in the TEE system; and

returning the fourth data to the second application.

5. The method according to claim 4, wherein if the third data is data that is generated by a target user outside the TEE system and encrypted with a private key of the target user, the decryption key comprises a public key of the target user; or if the to-be-read third data is data that is generated inside the TEE system and encrypted, the decryption key comprises a decryption key held by the TEE system.

6. The method according to claim 1, wherein the obtaining a data access request from the second application comprises: intercepting, by using AspectJ, the data access request sent by the second application.

7. The method according to claim 1, wherein the privacy data comprises risk control data, and the second application comprises a risk control service application; and the data reading comprises history data query, and the data writing comprises exception event data update.

8. A risk control privacy data analysis method, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the method comprises:

receiving, by the risk control analysis application, indication information used to indicate privacy data analysis, wherein the indication information comprises identification information

corresponding to a target user and an analysis type;

sending, by the risk control analysis application, a query request based on the indication information, wherein the query request comprises the identification information;

receiving, by the SDK, the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

obtaining, by the SDK, to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

9. The method according to claim 8, wherein the enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type comprises:

decrypting at least a part of fields of the to-be-analyzed data to obtain target data;

returning the target data to the risk control analysis application; and

performing, by the risk control analysis application, an analysis operation on the target data according to the analysis type, to obtain an analysis result.

10. A TEE-based computer system, where a plurality of TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; the system comprises a memory, a processor, and a computer program stored in the memory and running on the processor, and the SDK implements the following steps when executing the program by using the processor:

obtaining a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

11. The system according to claim 10, wherein the request further comprises identification information corresponding to the target user and authorization authentication information; and before the obtaining access configuration information from the first application, the following steps are further executed:

sending, to the first application, an authentication request that carries the identification information corresponding to the target user and the authorization authentication information, to perform identity authentication by using the first application; and

when the identity authentication succeeds, performing the operation of obtaining the access configuration information from the first application.

12. The system according to claim 10, wherein the data access comprises data writing; the request further comprises first data to be written; the first data is plaintext data generated inside the TEE system; and the access configuration information further comprises a privacy-related field in data and an encryption key held by the TEE system; and

the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

encrypting, by using the encryption key, a privacy-related field in the first data to obtain second data; and

writing, according to the storage address of the digital asset corresponding to the target user, the second data into the digital asset corresponding to the target user in the external storage device of the TEE system.

13. The system according to claim 10, wherein the data access comprises data reading; the access configuration information further comprises a privacy-related field in data and a decryption key; and the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

obtaining to-be-read third data from the external storage device of the TEE system according to the storage address of the digital asset corresponding to the target user;

decrypting, by using the decryption key, a privacy-related field in the third data to obtain fourth data for internal use in the TEE system; and

returning the fourth data to the second application.

14. The system according to claim 13, wherein if the third data is data that is generated by a target user outside the TEE system and encrypted with a private key of the target user, the

decryption key comprises a public key of the target user; or if the to-be-read third data is data that is generated inside the TEE system and encrypted, the decryption key comprises a decryption key held by the TEE system.

15. The system according to claim 10, wherein the obtaining a data access request from the second application comprises: intercepting, by using AspectJ, the data access request sent by the second application.

16. The system according to claim 10, wherein the privacy data comprises risk control data, and the second application comprises a risk control service application; and the data reading comprises history data query, and the data writing comprises exception event data update.

17. A TEE-based computer system, wherein a plurality of TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the system comprises a memory, a processor, and a computer program stored in the memory and running on the processor, wherein when executing the program by using the processor, the risk control analysis application implements the following steps: receiving indication information used to indicate privacy data analysis, wherein the indication information comprises identification information corresponding to a target user and an analysis type; and sending a query request based on the indication information, wherein the query request comprises the identification information;

wherein when executing the program by using the processor, the SDK implements the following steps: receiving the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and obtaining to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

18. A privacy data access apparatus, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; and the apparatus is deployed in the SDK, and the apparatus comprises:

a first obtaining module, configured to obtain a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

a second obtaining module, configured to obtain, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

an access module, configured to perform privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

19. A risk control privacy data analysis apparatus, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the apparatus comprises:

a receiving module, configured to indicate the risk control analysis application to receive indication information used to indicate privacy data analysis, wherein the indication information comprises identification information corresponding to a target user and an analysis type;

a sending module, configured to indicate the risk control analysis application to send a query request based on the indication information, wherein the query request comprises the identification information;

an obtaining module, configured to indicate the SDK to receive the query request, and obtain, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

an analysis module, configured to indicate the SDK to obtain to-be-analyzed data from the external storage device of the TEE system, and enable, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

20. A computer-readable nonvolatile storage medium, wherein the storage medium stores a computer program, and when the computer program is performed by a processor, the method according to any one of claims 1 to 9 is implemented.