CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

retrieving, by an off-chain trusted execution environment (TEE~~),~~) on an off-chain privacy computing unit, a check-triggering instruction from a server, wherein

the check-triggering instruction ~~is configured to trigger~~triggers the off-chain TEE to perform a consistency check on basic data of a user to be identified~~;~~, wherein the basic data of the user comprises user identification information of the user, and

the off-chain TEE on the off-chain privacy computing unit is verified as trustworthy by a trusted institution that is an authoritative authentication server;

in response to the check-triggering instruction, retrieving, by the off-chain TEE, encrypted standard basic data of the user from ~~a~~the trusted institution;

decrypting the encrypted standard basic data of the user to obtain decrypted standard basic data;

retrieving, by the off-chain TEE, encrypted basic data of the user from a first institution;

retrieving, by the off-chain TEE, the basic data of the user by decrypting the encrypted basic data;

performing, by the off-chain TEE, the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data to obtain a check result, wherein the consistency check comprises know your customer (KYC) check; and

in response to receiving a check result acquisition request from a second institution, sending, from the off-chain TEE, the check result to ~~a~~the second institution.

2. The computer-implemented method of claim 1, comprising:

retrieving, by the off-chain TEE, the encrypted basic data based on the user identification information of the user from a cloud storage server, wherein the encrypted basic data is uploaded by the first institution to the cloud storage server.

3. The computer-implemented method of claim 2, wherein the user identification information comprises an account registered by the user at the first institution or assigned to

the user by the first institution in response to an operation initiated by the user at the first institution.

~~4. The computer-implemented method of claim 1, comprising:~~

~~decrypting the encrypted standard basic data of the user to obtain standard basic data.~~

~~4~~5. The computer-implemented method of claim 1~~4~~, wherein performing the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data comprises:

comparing the basic data of the user with the decrypted standard basic data; and

determining that the basic data is real data in response to the check result indicating that the basic data is the same as the decrypted standard basic data, or determining that the basic data is false data in response to the check result indicating that the basic data is not the same as the decrypted standard basic data.

~~5~~6. The computer-implemented method of claim 1, comprising:

receiving, by the off-chain TEE, the~~a~~ check result acquisition request from the second institution, wherein the check result acquisition request is configured to request the check result.

~~6~~7. The computer-implemented method of claim ~~5~~6, wherein the check result acquisition request comprises the user identification information of the user.

~~7~~8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

retrieving, by an off-chain trusted execution environment (TEE~~),~~) on an off-chain privacy computing unit, a check-triggering instruction from a server, wherein

the check-triggering instruction~~ is configured to~~ triggers the off-chain TEE to perform a consistency check on basic data of a user to be identified, wherein the basic data of the user comprises user identification information of the user, and~~;~~

the off-chain TEE on the off-chain privacy computing unit is verified as trustworthy by a trusted institution that is an authoritative authentication server;

in response to the check-triggering instruction, retrieving, by the off-chain TEE, encrypted standard basic data of the user from ~~a~~the trusted institution;

decrypting the encrypted standard basic data of the user to obtain decrypted standard basic data;

retrieving, by the off-chain TEE, encrypted basic data of the user from a first institution;

retrieving, by the off-chain TEE, the basic data of the user by decrypting the encrypted basic data;

performing, by the off-chain TEE, the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data to obtain a check result, wherein the consistency check comprises know your customer (KYC) check; and

in response to receiving a check result acquisition request from a second institution, sending, from the off-chain TEE, the check result to ~~a~~the second institution.

8~~9~~.~~——~~ The non-transitory, computer-readable medium of claim 7~~8~~, wherein the operations comprise:

retrieving, by the off-chain TEE, the encrypted basic data based on the user identification information of the user from a cloud storage server, wherein the encrypted basic data is uploaded by the first institution to the cloud storage server.

9~~10~~.~~——~~ The non-transitory, computer-readable medium of claim 8~~9~~, wherein the user identification information comprises an account registered by the user at the first institution or assigned to the user by the first institution in response to an operation initiated by the user at the first institution.

~~11.——The non-transitory, computer-readable medium of claim 8, wherein the operations comprise:~~

~~decrypting the encrypted standard basic data of the user to obtain standard basic data.~~

10~~2~~.~~—~~ The non-transitory, computer-readable medium of claim 7~~11~~, wherein performing the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data comprises:

comparing the basic data of the user with the decrypted standard basic data; and

determining that the basic data is real data in response to the check result indicating that the basic data is the same as the decrypted standard basic data, or determining that the basic data is false data in response to the check result indicating that the basic data is not the same as the decrypted standard basic data.

113.— The non-transitory, computer-readable medium of claim 78, wherein the operations comprise:

receiving, by the off-chain TEE, thea check result acquisition request from the second institution, wherein the check result acquisition request is configured to request the check result.

124.— The non-transitory, computer-readable medium of claim 113, wherein the check result acquisition request comprises the user identification information of the user.

135. —A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

retrieving, by an off-chain trusted execution environment (TEE),) on an off-chain privacy computing unit, a check-triggering instruction from a server, wherein

the check-triggering instruction is configured to triggers the off-chain TEE to perform a consistency check on basic data of a user to be identified, wherein the basic data of the user comprises user identification information of the user, and;

the off-chain TEE on the off-chain privacy computing unit is verified as trustworthy by a trusted institution that is an authoritative authentication server;

in response to the check-triggering instruction, retrieving, by the off-chain TEE, encrypted standard basic data of the user from athe trusted institution;

decrypting the encrypted standard basic data of the user to obtain decrypted standard basic data;

retrieving, by the off-chain TEE, encrypted basic data of the user from a first institution;

retrieving, by the off-chain TEE, the basic data of the user by decrypting the encrypted basic data;

performing, by the off-chain TEE, the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data to obtain a check result, wherein the consistency check comprises know your customer (KYC) check; and

in response to receiving a check result acquisition request from a second institution, sending, from the off-chain TEE, the check result to ~~a~~the second institution.

1~~4~~6.~~—~~ The computer-implemented system of claim 1~~3~~5, wherein the one or more operations comprise:

retrieving, by the off-chain TEE, the encrypted basic data based on the user identification information of the user from a cloud storage server, wherein the encrypted basic data is uploaded by the first institution to the cloud storage server.

1~~5~~7.~~—~~ The computer-implemented system of claim 1~~4~~6, wherein the user identification information comprises an account registered by the user at the first institution or assigned to the user by the first institution in response to an operation initiated by the user at the first institution.

~~18. The computer-implemented system of claim 15, wherein the one or more operations comprise:~~

~~decrypting the encrypted standard basic data of the user to obtain standard basic data.~~

1~~6~~9.~~———————~~ The computer-implemented system of claim 13~~18~~, wherein performing the consistency check on the basic data of the user based on the decrypted~~encrypted~~ standard basic data comprises:

comparing the basic data of the user with the decrypted standard basic data; and

determining that the basic data is real data in response to the check result indicating that the basic data is the same as the decrypted standard basic data, or determining that the basic data is false data in response to the check result indicating that the basic data is not the same as the decrypted standard basic data.

1720.— The computer-implemented system of claim 1315, wherein the one or more operations comprise:

receiving, by the off-chain TEE, thea check result acquisition request from the second institution, wherein the check result acquisition request is configured to request the check result.