SECURE OFFLINE RESOURCE OPERATIONS

CLAIM OF PRIORITY

[0001] This application claims priority to Chinese Application No. 201611175289.6, filed on December 19, 2016, and U.S. Application No. 15/845,422, filed on December 18, 2017, which are incorporated by reference is its entirety.

BACKGROUND

[0002] Resources owned by a user can be digitally stored on a resource server. Normally, when the user performs a resource operation (such as, depositing or withdrawing an amount of a resource to or from the resource server), the resource server needs to be online to complete the resource operation.

SUMMARY

[0003] The present disclosure describes secure offline resource operations.

[0003a] In one aspect, the present disclosure refers to a method for resource operation in an offline state. The method includes: sending, by a resource requester and to a resource provider, authorization information based on a resource operation; receiving, by the resource provider and from the resource requester, the authorization information associated with the resource operation; and operating, by the resource provider and as resource operation-based authorization information, resources according to the authorization information by allocating a gate passage right to the resource requester by operation of a physical gate. In another aspect, the present disclosure refers to a system for resource operation in an offline state. The system includes a plurality of modules configured to perform the aforementioned method.

[0004] In an implementation, information associated with a resource operation is transmitted by a resource requester to a resource provider. The resource operation is associated with a resource stored on a resource server. The information associated with the resource operation is received by the resource provider from the resource requester. The resource operation is performed, by the resource provider, based on the received information from the resource requester instead of information from the resource server.

[0005] Implementations of the described subject matter, including the previously described implementation, can be implemented using a computer-implemented method; a non-transitory, computer-readable medium storing computer-readable instructions to perform the computer-implemented method; and a computer-implemented system comprising one or more computer memory devices interoperably coupled with one or more computers and having tangible, non-transitory, machine-readable media storing instructions that, when executed by the one or more computers, perform the computer-implemented method/the computer-readable instructions stored on the non-transitory, computer-readable medium.

[0006] The subject matter described in this specification can be implemented in particular implementations, so as to realize one or more of the following advantages. First, the described approach can be used to enable offline resource operations. For example, a user wants to perform an offline resource operation using a user device

CLAIMS

1. A method for resource operation in an offline state, the method comprising:

sending, by a resource requester and to a resource provider, authorization information based on a resource operation;

receiving, by the resource provider and from the resource requester, the authorization information associated with the resource operation; and

operating, by the resource provider and as resource operation-based authorization information, resources according to the authorization information by allocating a gate passage right to the resource requester by operation of a physical gate.

2. The method of claim 1, further comprising:

encrypting, by the resource requester, the resource operation-based authorization information by using a user private key as encrypted authorization information; and

decrypting, by the resource provider, the encrypted authorization information by using a user public key to obtain the authorization information, wherein the user private key and the user public key are a pair of asymmetrical and mutually matched keys.

3. The method of claim 2, further comprising:

generating the user private key and the user public key;

sending the user private key to the resource requester; and

sending the user public key to the resource provider.

4. The method of claim 2, wherein the authorization information comprises at least identity information of an authorized user and time stamp information of authorization.

5. The method of claim 2, further comprising:

sending, by the resource requester, the encrypted authorization information and a user public key encrypted by using a server terminal private key as an encrypted user public key to the resource provider; and

processing, by the resource provider, the encrypted user public key by using a server

terminal public key to generate the user public key, wherein the server terminal private key and the server terminal public key are a pair of asymmetrical and mutually matched keys.

6. The method of claim 5, wherein the authorization information comprises at least identity information of an authorized user and time stamp information at a time of authorization.

7. The method of claim 5, further comprising:

sending, by the resource requester, verification information encrypted by using the server terminal private key as encrypted verification information for the authorization information to the resource provider;

receiving, by the resource provider, the encrypted verification information;

decrypting, by the resource provider, the encrypted verification information by using the server terminal public key to generate the verification information; and

operating, by the resource provider, the resources according to the verification information.

8. The method of claim 7, further comprising:

performing coding integration on the authorization information and the verification information to map into a pattern.

9. The method of claim 7, further comprising:

generating the server terminal private key and the server terminal public key;

generating the user private key and the user public key;

sending the user private key, the user public key and the encrypted verification information to the resource requester; and

sending the server terminal public key to the resource provider.

10. The method of claim 7, further comprising:

verifying permission of the resource requester to generate the verification information; and

issuing the verification information for verifying authorization information.

11. The method of claim 10, wherein generating the verification information comprises:

generating information indicating success in verification when an account balance or a credit balance of the resource requester is no less than a preset amount.

12. The method of claim 11, further comprising:

verifying the permission of the resource requester when resource operation-based authorization information is received.

13. A system for resource operation in an offline state, the system comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.