CLAIMS

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

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

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

sending, by the resource requester and to the resource provider, encrypted verification information comprising verification information encrypted using a server terminal private key;

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

receiving, by the resource provider and from the resource requester, the encrypted verification information;

decrypting, by the resource provider, the encrypted authorization information 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;

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

operating, by the resource provider, resources according to the authorization information and the verification 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:

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.

3. The method of claim 1, wherein the authorization information comprises at least identity information of an authorized user and time stamp information of authorization.

4. The method of claim 1, further comprising:

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

processing, by the resource provider, the encrypted user public key by using the 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.

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

6. The method of claim 1, further comprising:

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

7. The method of claim 1, 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.

8. The method of claim 1, further comprising:

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

issuing the verification information for verifying authorization information.

9. The method of claim 8, 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.

10. The method of claim 9, further comprising:

verifying the permission of the resource requester when resource operation-based

authorization information is received.

11. 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 10.