CLAIMS

1. An IC card comprising:

a storage unit configured to store a first password;

a generation unit configured to generate a second password that is a password for authenticating a card user, based on the first password stored in the storage unit in advance, a predetermined parameter and a predetermined algorithm; and

an authentication unit configured to compare a third password acquired from an external apparatus and the second password, and to determine validity of the card user based on a result of the comparison,

wherein the generation unit is configured to store, in the storage unit, the second password generated if the authentication unit determines that the card user is valid.

2. The IC card according to claim 1,

wherein the predetermined algorithm includes a calculation involving the first password and the predetermined parameter, and

the generation unit is configured to generate the second password by performing the calculation on the first password and the predetermined parameter.

3. The IC card according to claim 2,

wherein the storage unit stores the predetermined parameter in advance, and

the IC card further comprises a change unit configured to change the predetermined parameter stored in the storage unit in response to a request to change the predetermined parameter, if the authentication unit has determined that the card user is valid.

4. The IC card according to claim 1,

wherein the storage unit stores an initial value of the second password, and

the IC card further comprises an initialization processing unit configured to change the first password stored in the storage unit to the initial value of the second

password in response to a request to initialize the second password, if the authentication unit has determined that the card user is valid.

5. The IC card according to any one of claims 1 to 3,

wherein the storage unit stores an initial value of the second password and counter information indicating the number of times the second password has been generated,

the authentication unit executes:

first authentication processing for comparing the third password and the second password, and determining the validity of the card user based on a result of the comparison; and

second authentication processing for comparing a fourth password acquired from the external apparatus and the initial value of the second password, and determining the validity of the card user based on a result of the comparison,

if the authentication unit has determined from the first authentication processing that the card user is valid, the generation unit generates the second password, and updates the counter information stored in the storage unit, and

the IC card further comprises a counter information processing unit configured to output the counter information to the external apparatus, if the authentication unit has determined from the second authentication processing that the card user is valid.

6. The IC card according to claim 5 comprising:

an initialization processing unit configured to change the first password stored in the storage unit to the initial value of the second password, and initialize the counter information stored in the storage unit, in response to a request to initialize the second password, if the authentication unit has determined from the first authentication processing that the card user is valid.

7. The IC card according to claim 2 or 3,

wherein the storage unit stores an initial value of the second password as the first password, and stores counter information indicating the number of times the second password has been generated,

the authentication unit is configured to execute:

first authentication processing for comparing the third password and the second password, and determining the validity of the card user based on a result of the comparison; and

second authentication processing for comparing a fourth password acquired from the external apparatus and the initial value of the second password, and determining the validity of the card user based on a result of the comparison, and

the generation unit is configured to generate the second password based on the initial value of the second password, the predetermined parameter, the calculation and the counter information stored in the storage unit, and if it is determined from the first authentication processing performed by the authentication unit that the card user is valid, updates the counter information stored in the storage unit.

8. The IC card according to claim 7 comprising:

a counter information processing unit configured to output the counter information to the external apparatus, if it has been determined from the second authentication processing performed by the authentication unit that the card user is valid; and

an initialization processing unit configured to initialize the counter information stored in the storage unit in response to a request to initialize the counter information, if it is determined from the first authentication processing performed by the authentication unit that the card user is valid.

9. The IC card according to claim 1,

wherein the predetermined parameter includes supply information supplied from the external apparatus,

the predetermined algorithm includes replacement processing for replacing a value at a predetermined position of the first password with a predetermined replacement value generated based on the supply information, and

the generation unit generates the second password based on the replacement processing.

10. The IC card according to claim 9,

wherein the storage unit stores replacement processing information indicating at least one of the predetermined position, a type of the supply information and a method for generating the predetermined replacement value, and

the IC card further comprises a change unit configured to change the replacement processing information stored in the storage unit in response to a request to change the replacement processing information, if the authentication unit has determined that the card user is valid.

11. The IC card according to any one of claims 1 to 10,

wherein the storage unit stores selection information for selecting one of a plurality of predetermined algorithms of different types, and

the generation unit is configured to select one of the plurality of predetermined algorithms based on the selection information stored in the storage unit, and to generate the second password based on the selected predetermined algorithm.

12. An IC module comprising:

a storage unit configured to store a first password;

a generation unit configured to generate a second password that is a password for authenticating a card user, based on a first password stored in a storage unit in advance, a predetermined parameter and a predetermined algorithm; and

an authentication unit configured to compare a third password acquired from an external apparatus and the second password, and to determine validity of the card user based on a result of the comparison,

wherein the generation unit is configured to store, in the storage unit, the second password generated if the authentication unit determines that the card user is valid.

13. An IC card system comprising;

the IC card according to any one of claims 1 to 8; and

an authentication center apparatus that is connected to the IC card via the external apparatus,

wherein the authentication center apparatus has:

a center storage unit that stores card identification information for identifying the IC card, the first password and the predetermined parameter in association with each other;

a center generation unit configured to generate the second password based on the first password, the predetermined parameter stored in the center storage unit and the predetermined algorithm,

a center authentication unit configured to compare the third password acquired from the card user via the external apparatus and the second password, and to determine the validity of the card user based on a result of the comparison; and

a synchronization processing unit configured to change the first password and the predetermined parameter stored in the center storage unit to the first password and the predetermined parameter stored in the IC card if the first password and the predetermined parameter stored in the IC card do not match the first password and the predetermined parameter stored in the center storage unit in association with the card identification information corresponding to the IC card.