

~~ELECTRONIC CIPHER GENERATION METHOD, APPARATUS AND DEVICE, AND ELECTRONIC CIPHER AUTHENTICATION SYSTEM~~

FIELD

5 The present disclosure relates to an information security field, and more particularly relates to an electronic password generating method, an electronic password generating device, an electronic password generating apparatus and an electronic password authentication system.

BACKGROUND

10 In recent years, with the rapid development of Internet and financial informatization, online banking is commonly appreciated by users and the banking industry for its convenience, efficiency and other advantages. In order to overcome the security defects of authentication based on fixed password, most banks and various large e-commerce web sites use dynamic password tokens or dynamic password cards to enhance the security of network authentication.

15 A dynamic password technology, also known as one time password (OTP for short) technology, is characterized in that a user inputs an electronic password according to a digit displayed on a dynamic password token provided by a service provider. Based on different ways to generate passwords, the dynamic password technology may be classified into a time-based dynamic password technology and a challenge/response-based dynamic password technology.

20 When the time-based dynamic password technology is used, an electronic password generating device and a server are synchronic in time, and store the same secret key seed. The electronic password generating device and the server generate one electronic password using the secret key seed at intervals (e.g., 60 seconds). When the user authentication needs to be performed, a user obtains a current electronic password on a display screen of the electronic password
25 generating device and then inputs the electronic password at a transaction terminal, and the transaction terminal sends the electronic password, a username, a static password and other information to the server for authentication.

 When the challenge/response-based dynamic password technology is used, an electronic password generating device and a server store the same secret key seed. When the user
30 authentication needs to be performed, the server generates a challenge code for a user, and the user obtains the challenge code and then inputs the challenge code to the electronic password

What is claimed is:

1. An electronic password generating method, comprising steps of:

prompting a user to input a challenge code by a prompting information, wherein the
5 prompting information is an information containing a meaning represented by the challenge code
to be input;

receiving the challenge code input by the user; and

generating a dynamic electronic password according to the input challenge code and a current
time parameter.

10 2. The method according to claim 1, wherein the prompting information at least comprises a
first prompting information and a second prompting information.

3. The method according to claim 2, wherein prompting the user to input the challenge code
by the prompting information comprises:

15 prompting the user to input a first information of the challenge code by the first prompting
information; and

prompting the user to input a second information of the challenge code by the second
prompting information.

20 4. The method according to claim 2 or 3, wherein the first prompting information is an
information prompting the user to input a transaction account, and the second prompting
information is an information prompting the user to input a transaction amount.

5. The method according to claim 1, wherein the challenge code at least comprises a first
information of the challenge code and a second information of the challenge code.

6. The method according to claim 5, wherein receiving the challenge code input by the user
comprises:

25 sequentially receiving the first information of the challenge code and the second information
of the challenge code which are input by the user.

7. The method according to claim 5 or 6, wherein the first information of the challenge code
is a transaction account, and the second information of the challenge code is a transaction amount.

30 8. The method according to any one of claims 1-7, before prompting the user to input the
challenge code by the prompting information, further comprising:

prompting the user to input a power-on password;

validating whether the power-on password input by the user is correct; and

if the power-on password input by the user is correct, prompting the user to input the challenge code by the prompting information.

9. An electronic password generating apparatus, comprising:

5 a prompting device configured for prompting a user to input a challenge code by a prompting information, wherein the prompting information is an information containing a meaning represented by the challenge code to be input;

an input device configured for inputting the challenge code; and

10 a processing chip configured for receiving the challenge code, and generating an electronic password according to the challenge code and a current time parameter.

10. The apparatus according to claim 9, wherein the prompting device comprises a display device and/or a sounding device, the display device is configured for displaying the prompting information in a form of a text, and the sounding device is configured for outputting the prompting information in a form of a voice.

15 11. The apparatus according to claim 9, wherein the input device comprises a button and/or a touch screen.

12. The apparatus according to claim 9, wherein the prompting information at least comprises a first prompting information and a second prompting information.

20 13. The apparatus according to any one of claims 9-12, wherein the prompting device is particularly configured for:

prompting the user to input a first information of the challenge code by the first prompting information; and

prompting the user to input a second information of the challenge code by the second prompting information.

25 14. The apparatus according to any one of claims 9-13, wherein the first prompting information is an information prompting the user to input a transaction account, and the second prompting information is an information prompting the user to input a transaction amount.

15. The apparatus according to claim 9, wherein the challenge code at least comprises a first information of the challenge code and a second information of the challenge code.

30 16. The apparatus according to claim 15, wherein the processing chip is particularly configured for:

sequentially receiving the first information of the challenge code and the second information of the challenge code which are input by the user.

17. The apparatus according to claim 15 or 16, wherein the first information of the challenge code is a transaction account, and the second information of the challenge code is a transaction amount.

18. The apparatus according to claim 9, wherein the input device is further configured for inputting a power-on password.

19. The apparatus according to claim 18, wherein the processing chip is further configured for validating whether the power-on password is correct; if the power-on password is correct, indicating for the prompting device to prompt the user to input the challenge code by the prompting information.

20. An electronic password authentication system, comprising:
an electronic password generating apparatus according to any one of claims 9-19; and
a transaction system configured for generating an electronic password at the transaction system according to the challenge code and the current time parameter, receiving the electronic password at the electronic password generating apparatus, and comparing the electronic password at the electronic password generating apparatus with the electronic password at the transaction system to complete the authentication.

**ELECTRONIC PASSWORD GENERATING METHOD, ELECTRONIC PASSWORD
GENERATING APPARATUS, AND ELECTRONIC PASSWORD AUTHENTICATION
SYSTEM**

FIELD

5 The present disclosure relates to an information security field, and more particularly relates to an electronic password generating method, an electronic password generating device, an electronic password generating apparatus and an electronic password authentication system.

BACKGROUND

10 In recent years, with the rapid development of Internet and financial informatization, online banking is commonly appreciated by users and the banking industry for its convenience, efficiency and other advantages. In order to overcome the security defects of authentication based on fixed password, most banks and various large e-commerce web sites use dynamic password tokens or dynamic password cards to enhance the security of network authentication.

15 A dynamic password technology, also known as one time password (OTP for short) technology, is characterized in that a user inputs an electronic password according to a digit displayed on a dynamic password token provided by a service provider. Based on different ways to generate passwords, the dynamic password technology may be classified into a time-based dynamic password technology and a challenge/response-based dynamic password technology.

20 When the time-based dynamic password technology is used, an electronic password generating device and a server are synchronic in time, and store the same secret key seed. The electronic password generating device and the server generate one electronic password using the secret key seed at intervals (e.g., 60 seconds). When the user authentication needs to be performed, a user obtains a current electronic password on a display screen of the electronic password
25 generating device and then inputs the electronic password at a transaction terminal, and the transaction terminal sends the electronic password, a username, a static password and other information to the server for authentication.

30 When the challenge/response-based dynamic password technology is used, an electronic password generating device and a server store the same secret key seed. When the user authentication needs to be performed, the server generates a challenge code for a user, and the user obtains the challenge code and then inputs the challenge code to the electronic password

What is claimed is:

1. An electronic password generating method, comprising steps of:

prompting a user to input a challenge code by a prompting information, wherein the
5 prompting information is an information containing a meaning represented by the challenge code
to be input;

receiving the challenge code input by the user; and

generating a dynamic electronic password according to the input challenge code and a current
time parameter,

10 wherein the prompting information at least comprises a first prompting information and a
second prompting information.

2. The method according to claim 1, wherein prompting the user to input the challenge code
by the prompting information comprises:

prompting the user to input a first information of the challenge code by the first prompting
15 information; and

prompting the user to input a second information of the challenge code by the second
prompting information.

3. The method according to claim 1 or 2, wherein the first prompting information is an
information prompting the user to input a transaction account, and the second prompting
20 information is an information prompting the user to input a transaction amount.

4. The method according to claim 1, wherein the challenge code at least comprises a first
information of the challenge code and a second information of the challenge code.

5. The method according to claim 4, wherein receiving the challenge code input by the user
comprises:

25 sequentially receiving the first information of the challenge code and the second information
of the challenge code which are input by the user.

6. The method according to claim 4 or 5, wherein the first information of the challenge code
is a transaction account, and the second information of the challenge code is a transaction amount.

7. The method according to any one of claims 1-6, before prompting the user to input the
30 challenge code by the prompting information, further comprising:

prompting the user to input a power-on password;

validating whether the power-on password input by the user is correct; and

if the power-on password input by the user is correct, prompting the user to input the challenge code by the prompting information.

8. An electronic password generating apparatus, comprising:

5 a prompting device configured for prompting a user to input a challenge code by a prompting information, wherein the prompting information is an information containing a meaning represented by the challenge code to be input;

an input device configured for inputting the challenge code; and

10 a processing chip configured for receiving the challenge code, and generating an electronic password according to the challenge code and a current time parameter,

wherein the prompting information at least comprises a first prompting information and a second prompting information.

15 9. The apparatus according to claim 8, wherein the prompting device comprises a display device and/or a sounding device, the display device is configured for displaying the prompting information in a form of a text, and the sounding device is configured for outputting the prompting information in a form of a voice.

10. The apparatus according to claim 8, wherein the input device comprises a button and/or a touch screen.

20 11. The apparatus according to any one of claims 8-10, wherein the prompting device is particularly configured for:

prompting the user to input a first information of the challenge code by the first prompting information; and

prompting the user to input a second information of the challenge code by the second prompting information.

25 12. The apparatus according to any one of claims 8-11, wherein the first prompting information is an information prompting the user to input a transaction account, and the second prompting information is an information prompting the user to input a transaction amount.

13. The apparatus according to claim 8, wherein the challenge code at least comprises a first information of the challenge code and a second information of the challenge code.

30 14. The apparatus according to claim 13, wherein the processing chip is particularly configured for:

sequentially receiving the first information of the challenge code and the second information of the challenge code which are input by the user.

15. The apparatus according to claim 13 or 14, wherein the first information of the challenge code is a transaction account, and the second information of the challenge code is a transaction amount.

16. The apparatus according to claim 8, wherein the input device is further configured for inputting a power-on password.

17. The apparatus according to claim 16, wherein the processing chip is further configured for validating whether the power-on password is correct; if the power-on password is correct, indicating for the prompting device to prompt the user to input the challenge code by the prompting information.

18. An electronic password authentication system, comprising:
an electronic password generating apparatus according to any one of claims 8-17; and
a transaction system configured for generating an electronic password at the transaction system according to the challenge code and the current time parameter, receiving the electronic password at the electronic password generating apparatus, and comparing the electronic password at the electronic password generating apparatus with the electronic password at the transaction system to complete the authentication.