FAQs for Two-factor Authentication

Two-factor Authentication

1. **What is two-factor authentication?**
   
   Two-factor authentication is an authentication scheme that increases online security by relying on a combination of two different factors, something you know (e.g. user ID and password) and something you have (e.g. digital certificate or mobile phone SIM card) in the verification of a user’s identity.

2. **Why is two-factor authentication needed for internet banking transactions?**
   
   Although they may be able to illegally obtain your user ID or password, fraudsters cannot steal something you have in your physical possession, such as a digital certificate or mobile phone, over the internet.

3. **When do you need to use a one-time password or digital certificate?**
   
   Effective from 23rd April, 2018, you will need to use a one-time password to access all investment services through Cyberbanking or Mobile Banking (including Stock Trading, Linked Deposits, Cyberfund Centre, eIPOs, and FX/Precious Metal Margin Trading).

   You currently need to use either a one-time password or digital certificate when conducting any of the following designated transactions:
   
   - Fund transfers to non-registered BEA accounts in Hong Kong or China
   - Fund transfers to non-registered accounts at other local banks through CHATS or Electronic Clearing
   - Bill payments to merchants, except when the receiving merchant falls under the "Government or Statutory Organisation", "Utilities", "Education: Primary or Secondary School", or "Education: Post-secondary or Specialised Institution" categories
   - Setting up scheduled instructions or templates for the above-mentioned transactions
   - Any new transaction types as prescribed by BEA from time to time

4. **After I have used two-factor authentication to create my templates, do I need to use two-factor authentication again when I perform transactions using the authenticated template?**
   
   You do not need to use one-time password/digital certificate to complete the transaction unless you change the deposit account or bill account number for the transaction.

5. **Do I need to use one-time password/digital certificate to authenticate my templates created before 23 June 2005?**
   
   No. All templates, which have been created before 23 June 2005, will not be affected by the two-factor authentication arrangement.

6. **Do I need to go to a BEA branch to register for one-time password or digital certificate?**
   
   This is not necessary. You can register for a one-time password or digital certificate by directly accessing Cyberbanking internet service.
7. Can I register for both a one-time password and a digital certificate?

Yes. In fact, we strongly recommend that you register for both.

8. Why do investment services (Stock Trading, Linked Deposits, Cyberfund Centre, elPOs, and FX/Precious Metal Margin Trading) require “Two-factor Authentication” in Cyberbanking and Mobile Banking?

To enhance the protection of your investment accounts, effective from 23rd April, 2018, you will be required to activate a two-factor authentication security procedure, which consists of an SMS-based one-time password (“OTP”), in order to access all Cyberbanking and Mobile Banking investment services.

9. How will the “Two-factor Authentication” function in Cyberbanking change after 23rd April, 2018?

The “One-time password for Stock Trading only” option under the “Two-factor Authentication” function of Cyberbanking will be discontinued after 23rd April, 2018. You will be able to use a “One-time password (via SMS)” instead.

After the effective date, you can register for the “One-time password (via SMS)” option under the “Two-factor Authentication” function.

10. Do I need to register for the “One-time password (via SMS)” under “Two-factor Authentication” for investment services again if I have already registered before 23rd April, 2018?

If you have registered for the “Two-factor Authentication” service before 23rd April, 2018, you will not need to register for the “One-time password (via SMS)” under “Two-factor Authentication” again, and can use this service directly.

11. Do I need to activate “Two-factor Authentication” for every investment service in Cyberbanking?

Once you have activated “Two-factor Authentication” for one investment service, it will not be required for other investment services as long as you are still logged in to Cyberbanking.

However, you will be requested to recomplete “Two-factor Authentication” if you try to log in to Cyberbanking again after logging out.
However, Stock and FX/Precious Metal Margin Trading services under Mobile Banking are independent functions which require their individual "Two-factor Authentication".
12. **What is a one-time password?**

A one-time password is an SMS-based password generated by a bank and sent to your registered mobile phone number as an additional form of identity authentication. A one-time password enables you to perform designated transactions and access investment services through the Cyberbanking service. Each password is used only once for a designated transaction and expires after 100 seconds.

13. **How do I use a one-time password?**

When you perform a designated transaction or access investment services through the Cyberbanking service, a one-time password will be sent to your registered mobile phone. You must input the password on the web page to complete your transaction.

14. **What is the use of “BEA Authentication Message”?**

The “BEA Authentication Message” will appear on your mobile phone to identify the sender (BEA) of SMS Communications in future.

15. **Why am I unable to successfully register for a one-time password?**

When you register for a one-time password, the mobile phone number that you use must be the same as the one you have registered with BEA. If not, please approach any BEA branch to have your record updated and then try again.

16. **What should I do if I receive an SMS containing a one-time password on my mobile phone but am not performing any internet banking transactions?**

Please contact the Cyberbanking Customer Services Hotline on 2211 1345 immediately.

17. **Is there any charge for using one-time password in Cyberbanking?**

It is free of charges at the time being. On the other hand, your mobile network operator may charge you for SMS usage fee for accessing the services. Details please refer to your mobile network operator.

18. **Do I need to enroll the service for receiving SMS messages with telecommunication companies in order to receive SMS messages?**

Customer does not need to apply for the SMS with your telecommunication company as all mobile phones are capable of receiving SMS.
19. Can I register an overseas mobile phone number for using the service?

You can register an overseas mobile phone number for using the service. Mobile phone numbers of the following countries would support the service currently:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td></td>
<td>Asia</td>
<td></td>
</tr>
<tr>
<td>USA, Canada</td>
<td>1</td>
<td>Malaysia</td>
<td>60</td>
</tr>
<tr>
<td>Europe</td>
<td></td>
<td>Philippines</td>
<td>63</td>
</tr>
<tr>
<td>Russia</td>
<td>7</td>
<td>Singapore</td>
<td>65</td>
</tr>
<tr>
<td>Greece</td>
<td>30</td>
<td>Japan</td>
<td>81</td>
</tr>
<tr>
<td>Netherlands</td>
<td>31</td>
<td>South Korea</td>
<td>82</td>
</tr>
<tr>
<td>Belgium</td>
<td>32</td>
<td>Vietnam</td>
<td>84</td>
</tr>
<tr>
<td>France</td>
<td>33</td>
<td>China</td>
<td>86</td>
</tr>
<tr>
<td>Spain</td>
<td>34</td>
<td>India</td>
<td>91</td>
</tr>
<tr>
<td>Hungary</td>
<td>36</td>
<td>Hong Kong</td>
<td>852</td>
</tr>
<tr>
<td>Italy</td>
<td>39</td>
<td>Macau</td>
<td>853</td>
</tr>
<tr>
<td>Switzerland</td>
<td>41</td>
<td>Taiwan</td>
<td>886</td>
</tr>
<tr>
<td>Austria</td>
<td>43</td>
<td>Israel</td>
<td>972</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>44</td>
<td>Oceania</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>45</td>
<td>Australia</td>
<td>61</td>
</tr>
<tr>
<td>Sweden</td>
<td>46</td>
<td>New Zealand</td>
<td>64</td>
</tr>
<tr>
<td>Norway</td>
<td>47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td>48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>351</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>352</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>353</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td>358</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>420</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remarks: Not all the mobile phone numbers from the above-mentioned countries can receive an international SMS messages. Prior to the service registration, please confirm with your mobile network operator whether your mobile phone number/service plan can receive an international SMS.

20. Can I register a pre-paid SIM card mobile phone number for using the service?

You cannot register a pre-paid SIM card mobile phone number for using the service.
21. **What is a digital certificate?**

A digital certificate is a form of electronic identification that helps establish your identity online. A digital certificate enables you to perform designated transactions through Cyberbanking internet service. It can be stored in a Hong Kong Smart ID card or USB Token.

22. **How do you use a digital certificate when making an internet banking transaction?**

When you perform a designated transaction through Cyberbanking internet service, you need to insert your Hong Kong Smart ID card/USB token storing your digital certificate into a smart card reader/USB drive and type the e-Cert PIN/USB token PIN to complete the transaction. After the transaction is completed, please remove the Hong Kong Smart ID card/USB token from the device immediately.

23. **Why I need digital certificate?**

Digital certificate provides:

- **Confidentiality:** the information contained in the message is kept confidential and only the sender and the intended recipient will be able to read and understand it;
- **Authenticity:** proof of identity of the parties to an electronic transaction;
- **Integrity:** assurance that the contents of a message have not been tampered with or modified;
- **Non-repudiation:** proof of agreement to the terms of the transaction and prevention of denial of commitment.

24. **Which kind of digital certificates are accepted by Cyberbanking?**

You can use any one of the following 1024-bit digital certificates for Cyberbanking:

- Hongkong Post e-Cert (Personal) for Smart ID Card
- Hongkong Post e-Cert (Personal)
- Digi-Sign Personal ID-Cert Class 1

25. **Is there any charge for using digital certificate in Cyberbanking?**

It is free of charges at the time being.

26. **How can I register my digital certificate in Cyberbanking?**

First of all, you shall log in to Cyberbanking and register your digital certificate under “Two-factor Authentication” option of “Settings” function. Then, you can use your registered digital certificate to conduct designated transactions in Cyberbanking.

27. **Can I use my digital certificate to log in to Cyberbanking?**

If you want to use digital certificate for login, please log in to Cyberbanking and register/update your digital certificate by selecting the “Login to Cyberbanking with digital certificate” option. Afterwards, you can use digital certificates to log in to Cyberbanking and confirm designated transactions prescribed by BEA.
28. If I have a joint account, do I need to register all account holders’ digital certificates in Cyberbanking?

Each account holder shall register his/her digital certificate one by one in Cyberbanking. After the first account holder is registered his/her digital certificate, the other account holder can then register his/her digital certificate.

29. If my registered digital certificate will be expired soon, what should I do?

You should renew your digital certificate with your Certification Authority one month before the expiry date of your digital certificate. Then, you should log in to Cyberbanking and update it with your renewed digital certificate under “Two-factor Authentication” option of “Settings” function.

30. If my registered digital certificate is expired, what should I do?

You should visit any of BEA branches in person to cancel the use of digital certificate in your Cyberbanking account.

31. What certificate storage devices can I use to log in to Cyberbanking?

You can choose one of the following devices:
- Smart ID Card
- USB Token

32. What do I need to install if I want to use Smart ID Card for Cyberbanking?

You should install the “e-Cert Control Manager” software provided by Hongkong Post before you use Smart ID Card in Cyberbanking if you are using Windows 98/NT/ME, you are also required to install a Microsoft Management Console in your PC. For details and download the softwares, please visit Hongkong Post website [http://www.hongkongpost.gov.hk/](http://www.hongkongpost.gov.hk/).

(Notes: “e-Cert Control Manager” software is not yet supported Windows Vista.)

33. Why the browser screen will be erased when I drag the e-Cert PIN input box for input Smart ID Card PIN?

You should not drag the box and enter your Smart ID Card PIN into the box directly to complete the transaction.

34. What should I do if I input wrong Smart ID Card PIN for 5 times?

Your Smart ID Card might be blocked. You are advised to visit Hongkong Post in person to unblock the Smart ID Card.

35. Why I can conduct another designated transactions again without entering Smart ID Card PIN just after successful execution of a designated transaction for less than 1 minute?

This is a default setting of “Password Timeout” in e-Cert Control Manager. The system will request you to input Smart ID Card PIN after 1 minute.