Examples of acceptable authentication methods to reduce and mitigate hacking risks associated with phishing attacks

(A) Passkey

1. Passkeys[1] are a password-less authentication method that internet brokers and VASPs may adopt to strengthen client login security.

2. Passkey authentication is based on public-key cryptography. When a passkey is created, the passkey is stored in the client's device, hardware security key[2] or passkey manager[3], while the corresponding public key is stored and used by the internet brokers and VASPs for verifying client logins. This design reduces the risks associated with stolen client passwords, intercepted OTPs, and other credential-based account takeover attacks.

3. Furthermore, passkeys are designed to be phishing resistant, as they are linked to the genuine website or application for which they were created and can only be used in connection with that specific website or application. If a client is redirected to a fraudulent website, his/her passkey could not be used to authenticate that site, thereby preventing unauthorised account access through phishing attacks.

Expected standards for passkey implementation

Internet brokers and VASPs may implement passkey solutions provided by third-party providers or develop their own passkey solutions. In both cases, the solutions should be subject to appropriate certification, ie, FIDO certification.

Internet brokers and VASPs should:

(a) ensure that passkey registration and setup are subject to strong identity verification. Any additional passkeys for the same client's internet trading account should only be created after authentication and authorisation using an existing registered passkey or other robust verification controls.

Illustrative scenarios on the passkey set up procedures for different types of clients are set out below:

---

1 For further information on passkeys and FIDO authentication, please refer to the materials published by the FIDO Alliance at https://fidoalliance.org/passkeys/.

2 Passkeys can be stored in hardware security keys, which are physical devices, such as Universal Serial Bus (USB), Near Field Communication (NFC), or Bluetooth-enabled security keys, where the passkey is stored directly on the device itself and does not synchronise across devices. They use FIDO2/WebAuthn protocols to retain the cryptographic credentials on the hardware itself, thereby reducing the risk of remote interception and providing stronger protection against phishing and credential theft.

3 Passkeys can be stored in passkey managers tied to the user's account in a platform ecosystem such as Apple, Google, or Microsoft. These passkeys can be synchronised and used across trusted devices within the same ecosystem, such as Apple iCloud Keychain, Google Password Manager, and Microsoft Password Manager. This arrangement allows users to sign in across multiple devices while continuing to benefit from stronger protection against phishing.

(i) *New clients*: The client accesses the internet trading services through the mobile application, desktop application, or trading website. During onboarding or first-time setup of the account through the trading application/website and after the client has successfully completed the firm's required identity verification steps, the trading application/website prompts the client to create a passkey linked to his/her internet trading account.

(ii) *Existing clients with a bound device*: The client logs in the mobile application or desktop application that supports passkey authentication through a bound device. After completing the existing login process, the client is prompted to create a passkey linked to the client's internet trading account.

(iii) *Existing clients without a bound device during the 12-month implementation period*: The client logs in the mobile application, desktop application, or trading website using the existing authentication process, such as client ID, password, SMS OTP. The client is then prompted to create a passkey linked to the client's internet trading account and to bind the device (where applicable).

(iv) *Existing clients without a bound devices after the 12-month implementation period*: The client should use robust verification methods, such as personal identity verification and biometric data verification (see examples under paragraph 7 below) or visit the internet broker's or VASP's office in person to create the passkey;

(b) establish and implement comprehensive policies, procedures and controls to properly manage the revocation and recovery of passkeys where the bound device, hardware security key or passkey manager is lost, compromised, replaced or no longer accessible;

(c) provide clear guidance to clients on the steps to take if a bound device, hardware security key or passkey manager is lost or compromised, and require appropriate client identity verification before allowing any creation, revocation or recovery of passkeys; and

(d) implement appropriate controls to mitigate risks associated with synchronised software-based passkeys across multiple client devices and ensure that passkey synchronisation cannot be abused to facilitate unauthorised access.

(B) Device binding

4. Device binding creates a secure association between the internet broker or VASP's internet trading platform and the client's device based on securely enrolled device attributes. This approach enables the internet broker or VASP to verify that any login request originates from a device previously registered to the client's account. This reduces reliance on credentials alone and helps mitigate unauthorised account access from unregistered devices.

5. However, when device binding is conducted using weak verification methods, such as user login credentials and OTP-based authentication, it becomes vulnerable to

unauthorised device registration stemming from phishing attacks. As such, internet brokers and VASPs should use robust verification method for device binding to reduce the risk of account takeover and unauthorised device registration.

Expected standards for robust verification methods for device binding

Internet brokers and VASPs should:

(a) implement robust verification methods for registering and linking clients' internet trading account to their devices. Such methods should incorporate phishing-resistant authentication methods and/or additional verification controls to confirm that the device belongs to the legitimate client before it is registered for system login or trading; and

(b) provide clear guidance to clients on the steps to take if a bound device is lost, including how to de-register the lost bound device and how to bind a replacement device. For example:

- To prevent unauthorised access, the client should first de-register the lost bound device either (i) by contacting the customer service hotline and completing the required identity verification; or (ii) through self-service device management portals on the internet trading platform, provided that the client can login using another previously bound device or other authentication methods; and

- After the lost bound device has been de-registered, the client may bind a replacement device using robust verification methods.

6. After the 12-month implementation period, clients can only bind their devices using robust verification methods. Examples of robust verification methods for device binding are set out below:

Example 1 – Passkey authentication

Clients, who have registered a passkey for their internet trading accounts, may use cross-device passkey authentication to securely log in the mobile application, desktop application, or trading website using the unbound device. After logging in, the client will be prompted with the option to bind his/her device. If he/she chooses to do so, the device will be bound.

Example 2 – Biometric data verification against internal records

As part of the account opening procedures, the client is required to provide his/her biometrics data, specifically facial data. This information is collected and verified through a liveness detection process[4] and securely stored in the internet broker's or VASP's database ("Database").

[4] During this process, the clients is required to take a selfie and will be prompted to perform specific actions, such as blinking their eyes and turning their heads, to ensure the biometric data is being captured from a live person and to prevent the use of deep-fakes.

When the client wishes to bind a new device to his/her internet trading account, the client is required to first login to the mobile/desktop application on the new device using his/her login credentials (ie, username and password).

- The mobile/desktop application on the new device will then prompt the client to take selfie and complete the liveness checks.
- The mobile/desktop application collects this information and verify it against the information stored in the Database, which is independent of the device's native biometric authentication functions.
- If the data collected matches the data stored in the Database, the new device will be bound.

Example 3 – Personal identity document verification

When the client wishes to bind a new device to his/her internet trading account, the client is required to first login to the mobile/desktop trading application on the new device using his/her login credentials (ie, username and password).

- The mobile/desktop trading application on the new device will then prompt the client to capture images of his/her identity document (for example, Hong Kong identity card) from different angles to verify authenticity of the document.
- The mobile/desktop trading application will extract the unique identity number from the document by utilising Optical Character Recognition technology, and cross-check it with the identity record previously collected during the account opening process and stored in the Database.
- The client will be prompted to take a selfie, which will be matched against the photo on the identity document, thereby preventing authentication using stolen documents.
- If the data of the identity document matches the data stored in the Database, the new device will be bound.

Example 4 – Physical verification

When a client wishes to bind a new device to his/her internet trading account, the client may visit the internet broker's or VASP's office in person for identity verification. This process would generally require the client to present valid identity documents that match the internet broker's or VASP's internal records, together with the device intended for binding, and, where appropriate, other additional supporting proof of identity.