**Verify Identity**

Introduction

Electronic transaction (e-transaction) means convenience as well as efficiency to many people. To ensure e-transaction is conducted in a reliable and trustworthy manner, the information system concerned would perform an authentication process beforehand in order to:

- establish confidence in user identities presented electronically;
- ensure that the credentials are valid for the transaction concerned; and
- ensure that the credentials presented have not expired, been revoked or withdrawn.

Depending on the potential risk and the trust level required, the information system would verify one or more of the following pieces of information to confirm user identity:

1. what the user knows (e.g. password);
2. what the user has (e.g. an ID card or token); and/or
3. what the user is or does (e.g. fingerprint or voice recognition).

The authentication system generally involves two major processes: registration and authentication. Registration process consists of two parts: registration and revocation.

1. Registration
    i. Registration: a process, may be one-off, to enable your use of online services;
    ii. Revocation: a process to be performed when the service is no longer required.
2. Authentication: a process to be performed each time when transaction is conducted.

Registration

Depending on the potential risk and the trust level required, service providers would require users to adopt different means for registration, such as:

1. Users should submit in person their proofs of identity for verification;
2. Users should submit written application with their signature appended or together with their proofs of identity; or
3. Users should register and submit their personal information (such as email address or mobile phone number) through electronic means.

Users may be required to read and accept certain terms of use before the completion of registration.

Upon successful registration, service providers would create a service account for the users or let the users register via their existing account. Service providers may also provide users with some credentials for subsequent transactions, which may include:

- a user name and initial password (or personal identification number "PIN"); or
- a security token, which displays numbers to be used as part of a password.

Tips on Registration

- You may provide only the required information for registration;
- You may abandon the registration if you don't want to provide certain personal information or accept certain terms of use;
- You should change the initial password or PIN as soon as possible;
- You should keep good custody of the password, PIN or token so as to prevent it from being stolen by others.

Authentication

Before an e-transaction is conducted, the information system providing the service would verify user identity by asking them to provide their user name and one or more credentials, such as:

- password or PIN;
- one-time password displayed on a security token; and/or
- digital certificate.

Transactions with more stringent authentication requirements would adopt multi-factor authentication. The more factors used in authentication, the better the likelihood of confirming the user identity. Users may consider if the credentials required by the transaction are good enough for verifying identity. They may also need to be aware of the potential risks involved if the credentials are improperly used.

Tips on Authentication

- Ensure the authenticity of the website before conducting transaction;
- Keep record of the transaction, such as writing down the transaction reference number, date of transaction, etc. or keeping the printed copy of the transaction record;
- Log out the system after completing the transaction;
- Change the password or PIN regularly;

- Keep safe custody of PIN or security device;
- Check the account transaction summary and account login record regularly.

Revocation

You may need to suspend or revoke your registered service in the following circumstances:

- Your account is suspected of being used by others;
- Your token is lost. The one who finds it might use it to impersonate you;
- You no longer use the service.

Tips on Revocation

To minimise your liability or loss, you are advised to:

- Request the service provider to revoke the account as soon as possible if the service is no longer required;
- Report to the service provider as soon as possible :
  - when there is change in identity information, e.g. mobile phone number for receiving the one-time password (OTP) through SMS;
  - when security token is lost; or
  - when unusual transaction or activity record is detected.

General Tips

To ensure e-transaction is conducted in a secure manner, electronic service should adopt one-factor or multiple-factor authentication to verify user identity. Throughout the authentication process, a user should:

- Be cautious in providing personal or sensitive information and accepting the terms of use during e-service registration;
- Ensure the credentials (such as password or security token) are properly kept to prevent them from being stolen for impersonation;
- Ensure the authenticity of the website before logging in to conduct e-transaction, and log out the system after completing the transaction; and
- Remember to revoke inactive account to prevent unauthorised use.

Conclusion

**Verify Identity, Transact Confidently**