Electronic Authentication Animations –
Common Authentication Methods (Script)

Introduction

Joe has just learnt from Alan that there are three types of authentication factor and five common authentication methods for implementing an e-authentication system.

Joe now wants to know more about the real life example for each of the authentication methods. Alan then tells him more about the five common authentication methods:

- Password and PIN based authentication
- SMS based authentication
- Symmetric-key authentication
- Public-key authentication
- Biometric authentication

Password and PIN based authentication

Working principle: Using password or Personal Identification Number (PIN) to login is the most common knowledge-based (something you know) authentication method.

Real life example: Use of password to login HK public library system for book reservation.

SMS based authentication

Working principle: SMS is used as a delivery channel for a one-time password (OTP) generated by an information system. User receives a password through the message shown in the cell phone, and enters the password to complete the authentication.

Real life example: Use of SMS-based authentication in login of Internet banking system.

Symmetric-key authentication

Working principle: In symmetric key authentication, user shares a unique, secret key with an authentication server. The user may be required to send a randomly generated message (the challenge) encrypted by the secret key to the authentication server. If the server can match the received encrypted message (the response) using its shared secret key, the user is authenticated. A slight variation of this approach is the use of OTP tokens, which generate the OTP on user side for matching with that generated on server side.

Real life example: Use of OTP to login Internet banking system.

Public-key authentication

Working principle: Public-key cryptography provides an authentication method that uses a private and public key pair. A private key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others.

Real life example: Updating address of registered voters with the Registration and Electoral Office.

Biometric authentication

Working principle: Biometrics is a method by which a person's authentication information is generated by digitizing measurements （encoded value） of a physiological or behavioral characteristic. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

Real life example: Use of fingerprint in Passenger e-Channel of HK Immigration

Conclusion

There are different authentication methods, solutions and ways of implementation to meet business assurance level, user requirements and budget. The choice of one or more authentication methods can boost the confidence in conducting business.

Choose Among Different Authentication Methods

The comparison among the common authentication methods is available in the following link: http://www.e-authentication.gov.hk/en/professional/compare.htm

To learn more information on electronic authentication, please visit "e-Authentication" website at: http://www.e-authentication.gov.hk