Guidelines for Conducting Digital Identity Authentication by Financial Services Enterprises

1. These Guidelines have been adopted for the purposes of providing the public with convenient, fast, and secure digital financial services and assisting financial service enterprises in using a suitable digital identity authentication mechanism to reduce potential risks.

   The term "financial service enterprises" in these Guidelines refers to financial service enterprises as defined in Article 2, Paragraph 2 of the Organic Act Governing the Establishment of the Financial Supervisory Commission.

2. In carrying out digital identity authentication, financial service enterprises shall observe the Personal Data Protection Act and regulations governing anti-money laundering and counter-terrorism financing, internal control and audit systems of respective financial service industry, relevant regulations and self-regulatory rules for electronic business and financial information security management, relevant rules of financial industry self-regulatory organizations as well as these Guidelines.

   These Guidelines apply to the digital identity authentication operation of financial service enterprises involving natural persons.

3. The term "digital identity authentication" used in these Guidelines refers to the process of utilizing proper technologies in the digital financial environment to authenticate that customers are who they claim to be.

   The digital identity authentication mechanism contains three phases – identity enrollment, credential management, and identity authentication. When a customer first uses a digital financial service, the financial service enterprise, through "identity enrollment" and

“credential management” operations, verifies and confirms whether the identity information provided by the customer is correlated to the customer, and binds, issues, and activates a credential. Subsequently each time the customer uses a digital financial service, the service enterprise will, through the “identity authentication” operation, confirm the customer’s identity based on the credential provided by the customer and the identity authentication protocol (see Figure 1).

The actors in the digital identity authentication mechanism are as follows:

(1) Customer: The target of identity authentication.

(2) Registration authority: The entity in charge of identity enrollment-related operations (including applications, identity proofing and identity information verification, registrations, and record-keeping).

(3) Credential service provider: The entity in charge of managing the credential lifecycle and maintaining correlation between credentials and identity information. “Credential” refers to a dataset that can be used as evidence to the identity or rights claimed by customers. It also includes media that store credentials, such as IC ATM cards, securities broker’s order placement certificates, and futures broker’s order placement certificates.

(4) Relying party: An entity that relies on and uses the output from an identity authentication mechanism.

(5) Verifier: An entity that provides identity verification services.

(6) Trusted third party: An entity that provides digital identity authentication services other than services provided by the registration authority, credential service provider, and verifier and is trusted by the aforementioned actors.

For the purpose of digital identity authentication, a financial service

enterprise, by its organizational structure and operating procedures, can act concurrently as the registration authority, credential service provider, trusted party, and verifier.

4. The three phases of the digital identity authentication mechanism specified in Point 3, Paragraph 2 contain the following operating procedures in principle:
   (1) Identity enrollment:
      A. Identity proofing: The customer provides their identity information (e.g. name, ID Card, national health insurance card (NHI Card), credit card, biometrics, cell phone number, email address, natural person certificate, digital signature certificate, IC ATM card, online banking password, electronic payment account password, or e-passport) for the registration authority to verify such information. Where necessary, the registration authority may enlist the service of a trusted third party to provide information so as to ensure the truthfulness, validity, and accuracy of the customer's identity information.
      B. Registration and record-keeping: The registration authority will send the identity information that has passed identity proofing to the credential service provider for it to carry out credential production and other subsequent operations. The registration authority will record and preserve the collected data and files, information on the identity proofing process, information on the decision made (application accepted/rejected, or request for supplemental information), and other related information.
   (2) Credential management:
      A. Binding and issuance: After producing a credential, the credential service provider will establish links among the

customer, the identity information, and the credential and carry out the binding operation before issuing the credential to the customer.

B. Activation and storage: After receiving the credential, the customer should activate it according to the operating procedure of the credential service provider, and safekeep the credential to prevent it from unauthorized use.

C. Suspension, revocation and/or replacement: The credential service provider will take proper actions, such as suspension, revocation, renewal, or replacement of a credential based on its usage and the customer's status.

(3) Identity authentication:

A. Authentication of correlation between customer and credential: The customer requests digital financial service from the relying party and presents their credential. The relying party requests identity authentication service from the verifier. The verifier, based on the existing identity authentication protocol of the credential service provider and the credential presented by customer, verifies whether the customer does own and hold the previously bound credential.

B. Send the authentication result and perform record-keeping: After confirming that the customer does own and hold the credential, the verifier, based on the relationship between the credential and identity information registered in the database, sends the authentication result to the relying party and retains relevant authentication records.

Under the preceding paragraph, the roles of each actor and operating procedures in each phase are illustrated in Figure 2 through Figure 5.

5. When a financial service enterprise conducts digital identity authentication, its “risk level of application scenarios” and “assurance level of authentication mechanism” should match each other based on the risk-based principles, and the risk level and the assurance level should be assessed based on the following operations; the same shall apply when a financial service enterprise uses the identity authentication mechanism of another financial service enterprise to provide digital financial services:
   (1) Assessment of “service scenario risk level” for digital identity authentication: A financial service enterprise should instruct its business units to assess risks associated with the identity authentication mechanism when it plans the service scenarios for its digital financial services, determine the risk levels, and produce a “Service Scenario Risk Assessment Report for Digital Identity Authentication.” A risk assessment may cover risks affecting a company’s customers, operations, finances, reputation, and compliance performance when the identity authentication mechanism used for a particular service scenario fails to work.
   (2) Assessment of digital identity “authentication assurance level”: A financial service enterprise should, based on the needs of its service scenarios, carry out assurance level assessment for the digital identity authentication mechanism it might adopt, evaluate each of the three phases – identity enrollment, credential management, and identity authentication —come up with an overall assurance level, and produce a “Digital Identity Authentication Assurance Level Assessment Report.”
   (3) Matching the “service scenario risk level” and the “authentication assurance level”: After completing the “Service Scenario Risk Assessment Report for Digital Identity Authentication” and the

"Digital Identity Authentication Assurance Level Assessment Report," and taking into consideration other factors (e.g. company size, costs, market, complexity, and regulatory compliance), the financial service enterprise should select the appropriate identity authentication mechanism for the "service scenario risk level" based on the "authentication assurance level" needed.

Where the governing regulations, a particular industry's self-regulatory rules, or the applicable rules of financial industry self-regulatory organizations have stipulated the requirements for customer's digital identity authentication, the financial service enterprise may be exempted from performing the assessments under the preceding paragraph; where the governing rules and regulations do not stipulate new digital financial service scenarios or new digital identity authentication methods, the financial service enterprise shall conduct assessments according to the preceding paragraph, and in addition, shall inquire with the competent authority about whether to apply for a new business trial prior to offering the digital financial services.

6. Potential risks associated with the failure of the identity authentication mechanism used for the service scenario contemplated under Point 5, Paragraph 1, Subparagraph 1 include:
   (1) Inconvenience or distress to customers.
   (2) Damage to the reputation of customers and the financial service enterprise.
   (3) Financial loss or agency liability of customers and the financial service enterprise.
   (4) Harm to the financial service enterprise, related programs, or public interests.
   (5) Unauthorized release of sensitive information.

(6) Violation of relevant regulations by the financial service enterprise.

A financial services enterprise should assess the risk level of each of the aforementioned subparagraphs and categorize them into different levels such as low, medium, high, and very high.

7. The digital identity authentication assurance level under Point 5, Paragraph 1, Subparagraph 2 is the degree of confidence in the result of verifying a customer's asserted identity using a specific digital identity authentication mechanism.

A financial service enterprise may, based on the nature of its business, distinguish the aforementioned assurance level into different levels. In the example of four levels, the meanings of each level are as follows:

(1) Level of assurance 1 (LoA1): Little or almost no confidence in customer's asserted identity as verified using a specific digital identity authentication mechanism; or LoA1 may be employed only when the risk arising from identity authentication failure is low.

(2) Level of assurance 2 (LoA2): Moderate confidence in customer's asserted identity as verified using a specific digital identity authentication mechanism; or at least LoA2 should be employed when the risk arising from identity authentication failure is medium.

(3) Level of assurance 3 (LoA3): High confidence in customer's asserted identity as verified using a specific digital identity authentication mechanism; or at least LoA3 should be employed when the risk arising from identity authentication failure is high.

(4) Level of assurance 4 (LoA4): Very high confidence in customer's asserted identity as verified using a specific digital identity authentication mechanism; or LoA4 should be employed when the risk arising from identity authentication failure is very high.

8. For digital identity authentication, a financial service enterprise should establish a risk management mechanism and include it in its internal control and audit system to effectively protect customer interests and prevent fraud and malpractice.

   The aforementioned risk management mechanism should contain at least the following particulars:

   (1) Periodically evaluate the operating procedures for the three phases of the digital identity authentication mechanism as well as the potential risks, threats, and weaknesses that may be encountered while a financial service system is being used by users (customers, employees, and third-party outsourced service providers), evaluate whether the identity verification technologies and management mechanisms are adequate, and to make improvements.

   (2) Employ appropriate measures to prevent, monitor, and manage information and communication security risks, including protective measures to prevent tampering, identity theft, and data misuse, and establish operating procedures for investigating and handling confirmed or alleged digital identity fraud cases.

   (3) If digital identity authentication involves other organizations, delineate related risks and responsibilities, and if necessary and feasible, enter into an agreement with such organizations that specifies the rights and obligations of the parties concerned.

   (4) Establish internal standard operating procedures for handling customer complaints, disputes, and remediation, including the reporting, handling, and remedial measures for situations such as identity authentication failure and unauthorized transactions so as to prevent harm to customers' rights to use digital financial services, and prevent the worsening of problems that may affect

the financial service enterprise's normal operation.

(5) Provide education and training to employees conducting digital identity authentication, which should at least include identity authentication-related regulations, technologies, operating procedures, risk identification, and response measures, and should also cover the protection of customer interests.

(6) Establish a business continuity and disaster recovery plan to increase the reliability of the digital identity authentication mechanism.

9. A financial service enterprise should heed the following matters relating to customer rights and interests when conducting digital identity authentication:

(1) Whether a customer enrolls in the digital identity authentication mechanism of the financial service enterprise should be left to the decision of the customer. The financial service enterprise should offer multiple channels to make it convenient for customers to complete the identity authentication procedure either in person at a physical business premises or remotely via a mobile device or the Internet.

(2) With regard to personal information obtained, inform the customer that they may withdraw or modify their expressed consent to the manner of data collection, processing, and utilization.

(3) Provide promotional materials to educate customers about security awareness and periodically update the content of such materials to reflect changes in external risks. The promotional materials should at least contain information on how customers can protect their own digital identity, personal data, and credential, how they can be sure the communication channel for financial service (e.g. official website) is legitimate, control measures for

risk mitigation (e.g. the reasons why multi-factor authentication is used and online transaction limits are set), common external threats (e.g. social engineering, phishing), and legal and other rights and protections customers may have in case of unauthorized transactions.

10. Financial industry trade associations and financial industry self-regulatory organizations may establish operating procedures and assessment operations for digital identity authentication in reference to these Guidelines and give individual financial service enterprises the flexibility to establish their own internal rules.