THE GOVERNMENT	THE SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness
No. 69/2024/ND-CP	*Hanoi, June 25, 2024*

DECREE

Providing electronic identification and authentication[1]

Pursuant to the June 19, 2015 Law on Organization of the Government; and the November 22, 2019 Law Amending and Supplementing a Number of Articles of the Law on Organization of the Government and the Law on Organization of Local Administration;

Pursuant to the November 19, 2015 Law on Cyberinformation Security;

Pursuant to the June 12, 2018 Law on Cyber Security;

Pursuant to the June 22, 2023 Law on E-Transactions;

Pursuant to the November 27, 2023 Law on Identity;

Pursuant to the June 17, 2020 Investment Law, which has a number of articles amended and supplemented under Law No. 72/2020/QH14, Law No. 03/2022/QH15, Law No. 05/2022/QH15, Law No. 08/2022/QH15, Law No. 09/2022/QH15, Law No. 20/2023/QH15, and Law No. 26/2023/QH15;

At the proposal of the Minister of Public Security;

The Government promulgates the Decree providing electronic identification and authentication.

Chapter I

GENERAL PROVISIONS

Article 1. Scope of regulation

This Decree provides in detail electronic identity; grant, management and use of electronic identification accounts; updating and storage of information in the electronic identification and authentication system; conditions and order for connection to the electronic identification and authentication system; electronic authentication services; order and procedures for grant, locking and unlocking of

[1] Công Báo Nos 847-848 (23/7/2024)

electronic identity cards; and responsibilities of related agencies, organizations and individuals with regard to electronic identification and authentication and electronic identity.

Article 2. Subjects of application

This Decree applies to Vietnamese agencies, organizations and citizens; foreign organizations and individuals residing and operating in Vietnam's territory that directly participate or are engaged in electronic identification and authentication activities and electronic identity.

Article 3. Interpretation of terms

In this Decree, the terms below shall be construed as follows:

1. Electronic identity means information of an agency, organization or individual in the electronic identification and authentication system that enables the identification of that only agency, organization or individual in the electronic environment.

2. Electronic identity subject means an identified agency, organization or individual that is attached to its/his/her electronic identity.

3. Electronic identification means the activities of registering, cross-checking, creating and attaching an electronic identity to an electronic identity subject.

4. Electronic identification and authentication management agency is the Police Department for Administrative Management of Social Order under the Ministry of Public Security.

5. Electronic identification account means a set of login name and password or other means of authentication that are created by the electronic identification and authentication management agency and used to log in and use the features, utilities, and applications of the electronic identification and authentication system and the connected and shared information systems in accordance with law.

6. Electronic authentication means the activities of authenticating, confirming, affirming, certifying and providing electronic identities, electronic identification accounts or other information in the National Population Database, Identity Database, and National Immigration Database via the electronic identification and authentication system and electronic identification and authentication platform.

7. Authentication factor means a means of authentication used to confirm and affirm electronic identity subjects before logging in and exploiting information in the electronic identification and authentication system.

8. Means of authentication means a number of methods that enable users to carry out electronic authentication: password, secret code, barcode, terminal device, one-time-password device or software, cryptographic device or software, identity card, citizen identity card, passport, face photo, fingerprint, voice, and iris, or other tools and methods used for the purpose of electronic authentication.

9. Electronic authentication service provider means a public service unit or an enterprise of the People's Public Security forces that meets the conditions for dealing in and providing electronic authentication services specified in this Decree.

10. Electronic identification website means a utility created and developed by the Ministry of Public Security from the electronic identification and authentication system to conduct electronic identification and authentication activities in settlement of administrative procedures, public administrative services and other transactions in the electronic environment; and to develop features, utilities and applications to serve agencies, organizations and individuals.

11. Electronic identification and authentication platform means an information system serving the exchange of information between the electronic identification and authentication system and information systems of state agencies, political organizations, socio-political organizations, electronic authentication service providers and other organizations and individuals.

Article 4. Principles of electronic identification and authentication

1. To comply with the Constitution and law, and ensure lawful rights and interests of agencies, organizations and individuals.

2. To ensure accuracy, publicity and transparency in management, and convenience for agencies, organizations and individuals.

3. To ensure security and safety for equipment and confidentiality of data when conducting electronic identification and authentication.

4. Agencies, organizations and individuals permitted to exploit and use electronic identities shall keep their electronic identification account information confidential and comply with the law on personal data protection.

5. Any violation of the law on electronic identification and authentication must be detected and promptly handled in accordance with law.

6. To ensure compliance with treaties to which Vietnam is a contracting party.

7. Electronic identification accounts may not be used for activities or transactions that are contrary to law, infringe upon security, national defense, national interests, public interests, or lawful rights and interests of organizations and individuals.

8. All agencies, organizations and individuals may not illegally interfere in the operation of the electronic identification and authentication system.

Chapter II

ELECTRONIC IDENTITIES, ELECTRONIC IDENTIFICATION, ELECTRONIC IDENTIFICATION ACCOUNTS, AND ELECTRONIC AUTHENTICATION

Article 5. Electronic identities of foreigners

1. The electronic identity of a foreigner comprises:

a/ Identification number;

b/ Surname, middle name and given name;

c/ Date of birth;

d/ Gender;

dd/ Nationality;

e/ Serial number, code, date of issuance, and place of issuance of passport or international travel document;

g/ Face photo;

h/ Fingerprints.

2. Foreigner identification number is a unique sequence of natural numbers established by the electronic identification and authentication system to manage the electronic identity of a foreigner.

Article 6. Electronic identities of agencies and organizations

1. Information on the electronic identity of an agency/organization comprises:

a/ Identification number;

b/ Name(s), including Vietnamese name, abbreviated name (if any) and foreign-language name (if any);

c/ Date of establishment;

d/ Head office address;

dd/ Tax identification number (if any);

e/ Enterprise identification number (if any);

g/ Electronic identification code (if any);

h/ Surname, middle name and given name, and personal identification number (or foreigner identification number) of the legal representative or head of the agency/organization who carries out the procedures for grant of an electronic identification account for the agency/organization.

2. Agency/organization identification number is a unique sequence of natural numbers established by the electronic identification and authentication system to manage the electronic identity of an agency/organization.

Article 7. Classification of, and subjects entitled to be granted, electronic identification accounts

Vietnamese agencies, organizations and citizens and foreign organizations and individuals residing in Vietnam's territory shall be granted electronic identification accounts, specifically as follows:

1. Vietnamese citizens who are aged full 14 years or older and have been granted citizen identity cards or identity cards which remain valid shall be granted level-1 electronic identification accounts or level-2 electronic identification accounts.

Vietnamese citizens who are aged between full 6 years and under 14 years and have been granted identity cards shall be granted level-1 electronic identification accounts or level-2 electronic identification accounts when needed. Vietnamese citizens who are aged under 6 years and have been granted identity cards shall be granted level-1 electronic identification accounts when needed.

2. Foreigners who are aged full 6 years or older and have been granted permanent residence cards or temporary residence cards in Vietnam shall be granted level-1 electronic identification accounts or level-2 electronic identification accounts when needed. Foreigners who are aged under 6 years and have been granted permanent residence cards or temporary residence cards in Vietnam shall be granted level-1 electronic identification accounts when needed.

3. Agencies and organizations established or registered to operate in Vietnam shall be granted electronic identification accounts regardless of account level.

Article 8. Updating of information to the electronic identification and authentication system

1. Changes of personal information in the National Population Database, Electronic Civil Status Database, Identity Database, National Immigration Database, and other national databases and specialized databases related to electronic identity and information already integrated to electronic identification accounts shall be automatically updated to the electronic identification and authentication system.

2. Information of agencies and organizations in the National Enterprise Registration Database and other national databases and specialized databases related to electronic identity shall be automatically updated to the electronic identification and authentication system in order to create identification numbers and electronic identification accounts of agencies and organizations serving electronic identification and authentication activities.

Article 9. Use of electronic identification accounts and other electronic transaction accounts created by agencies, organizations, and individuals

1. Level-1 electronic identification accounts of Vietnamese citizens and foreigners shall be used for access to, and exploitation and use of, electronic identity information and some features, utilities, and applications of the electronic identification and authentication system and connected and shared information systems in accordance with law.

2. Level-2 electronic identification accounts of Vietnamese citizens shall be used for access to, and exploitation and use of electronic identity cards and information other than the information already integrated to electronic identity cards that is shared, integrated and updated from national databases and specialized databases, and all features, utilities, and applications of the electronic identification and authentication system and connected and shared information systems in accordance with law.

3. Level-2 electronic identification accounts of foreigners and electronic identification accounts of agencies and organizations shall be used for access to, and exploitation and use of, electronic identity information and other information that is shared, integrated and updated from national databases and specialized databases, and all features, utilities, and applications of the electronic identification and authentication system and connected and shared information systems in accordance with law.

4. Electronic identity subjects may use their electronic identification accounts to login to, authenticate and use features and utilities on the National Identification Application, the electronic identification website at dinhdanhdientu.gov.vn or vneid.gov.vn or other utilities on applications and software of other agencies, organizations, and individuals that have been connected to the electronic identification and authentication system.

5. Electronic identification accounts shall be used to carry out administrative procedures and public administrative services in the electronic environment and other activities at the demand of electronic identity subjects.

6. Electronic identity information and information integrated to electronic identity cards and electronic identification accounts have evidentiary value like information provided or papers and documents used and presented that contain such information in carrying out administrative procedures, public services, and other transactions and activities.

7. Agencies, organizations and individuals may create electronic transaction accounts in accordance with the law on e-transactions to serve their transactions and activities and shall authenticate and assure the accuracy of the accounts they create, decide on the level and validity of their accounts at each level. Agencies, organizations and individuals may only use information provided by account holders to create electronic transaction accounts with the latter's consent.

Article 10. Procedures for grant of electronic identification accounts to Vietnamese citizens

1. Grant of a level-1 electronic identification account

a/ The citizen uses a digital device to download and install the National Identification Application;

b/ The citizen uses the National Identification Application to enter information on his/her personal identification number, his/her own mobile phone number, and his/her email address (if any); declares information according to the instructions on the National Identification Application; takes face image using the digital device and sends a request for grant of an electronic identification account to the electronic identification and authentication management agency;

c/ The electronic identification and authentication management agency checks and authenticates information of the citizen and notifies the account registration result via the National Identification Application or via the citizen's mobile phone number or email address;

d/ In case the citizen is a person aged under 14 years, person under guardianship or represented person, the guardian or representative of such person shall use his/her own mobile phone number and level-2 electronic identification account to declare and register for grant of a level-1 electronic identification account to such person via the National Identification Application.

2. Grant of a level-2 electronic identification account

a/ The citizen comes to a commune-level Public Security office or identity management agency, regardless of his/her place of residence, presents his/her valid citizen identity card or identity card, and carries out procedures for grant of a level-2 electronic identification account;

b/ The citizen fills in the request for grant of electronic identity account, using Form TK01 provided in the Appendix to this Decree, clearly stating information on his/her own mobile phone number and email address (if any) and other information requested to be integrated to the electronic identity card (if he/she so wishes), to the receiving officer;

c/ The receiving officer enters information provided by the citizen into the electronic identification and authentication system for authentication; and authenticates the face photo and fingerprints of the citizen against those stored in the Identity Database;

d/ The electronic identification and authentication management agency checks and authenticates information of the citizen requesting the grant of a level-2 electronic identification account and notifies the citizen of the result of the registration for grant of a level-2 electronic identification account via the National Identification Application or the citizen's mobile phone number or email address;

dd/ In case the citizen is a person aged under 14 years, person under guardianship or represented person, he/she shall, together with his/her guardian or representative, come to a commune-level public security office or the agency performing procedures for grant of identity cards to carry out procedures for grant of a level-2 electronic identification account;

Guardians or representatives of Vietnamese citizens aged under 14 years, persons under guardianship, and represented persons shall use their own mobile phone numbers to declare and register for grant of level-2 electronic identification accounts for such persons.

3. Citizens who have not yet been granted citizen identity cards or identity cards shall file a request for grant of electronic identification accounts when carrying out procedures for grant of identity cards and follow the order and procedures specified in Clauses 1 and 2 of this Article.

Article 11. Order and procedures for grant of electronic identification accounts to foreigners

1. Grant of a level-1 electronic identification account

a/ The foreigner uses a digital device to download and install the National Identification Application;

b/ The foreigner uses the National Identification Application to enter information on the serial number of his/her passport or international travel document and email address or mobile phone number with subscriber information already registered (if any); declares information according to the instructions on the National Identification Application; takes face photo using the digital device and sends a request for grant of an electronic identification account to the electronic identification and authentication management agency via the National Identification Application;

c/ The electronic identification and authentication management agency notifies the account registration result via the National Identification Application or the foreigner's mobile phone number or email address;

d/ In case the foreigner is a person aged under 14 years, a person under guardianship, or a represented person, the guardian or representative of such person uses his/her own mobile phone number and level-2 electronic identification account to declare and register for grant of a level-1 electronic identification account for such person via the National Identification Application.

2. Grant of a level-2 electronic identification account

a/ The foreigner comes to the Immigration Management Agency under the Ministry of Public Security or a provincial-level Public Security agency and presents his/her valid passport or international travel document to carry out procedures for grant of a level-2 electronic identification account;

b/ The foreigner fills in the request for grant of an electronic identification account, using Form TK01 provided in the Appendix to this Decree, providing information on his/her mobile phone number and email address (if any) and other information requested to be integrated into the National Identification Application, to the receiving officer;

c/ The receiving officer enters the information provided by the foreigner into the electronic identification and authentication system; takes the face photo and fingerprints of the foreigner for verification against those stored in the National Immigration Database;

d/ The immigration management agency sends a request for grant of an electronic identification account to the electronic identification and authentication management agency;

dd/ The electronic identification and authentication management agency notifies the account registration result via the National Identification Application or the foreigner's mobile phone number or email address;

e/ The foreigner who is a person aged under 14 years, person under guardianship and represented person shall, together with his/her guardian or representative, come to the immigration management agency under the Ministry of Public Security or the provincial-level Public Security agency to carry out procedures for grant of a level-2 electronic identification account;

Guardians or representatives of foreigners who are aged between full 6 years and under 14 years, persons under guardianship or represented persons shall use their own mobile phone numbers to declare and register for grant of level-2 electronic identification accounts for such foreigners.

Article 12. Procedures for grant of electronic identification accounts for agencies and organizations

1. A legal representative or the head of an agency/organization, or the person authorized by the legal representative or head shall use his/her level-2 electronic identification account to login to the National Identification Application, provide information as instructed by the Application and send a request for grant of an electronic identification account for the agency/organization after obtaining the consent of all other legal representatives of the agency/organization (if any).

In case of hand-delivery of a dossier, the legal representative or head of the agency/organization or authorized person shall fill in the request for grant of electronic identification account for agency/organization, using Form TK02 provided in the Appendix to this Decree, and submit the dossier at the electronic identification and authentication agency or an identity management agency that is convenient for him/her.

2. The electronic identification and authentication management agency shall check and authenticate information about the agency/organization in the National Enterprise Registration Database and other national databases and specialized databases.

In case the information about the agency/organization is not yet available in the National Enterprise Registration Database and other national databases and specialized databases, the electronic identification and authentication management agency shall verify information about the agency/organization.

3. The electronic identification and authentication management agency shall notify the result of registration for grant of an electronic identification account to the legal representative or head of the agency/organization who carries out the procedures for grant of an electronic identification account via the National Identification Application or his/her mobile phone number or email address.

In case the agency/organization is disqualified for grant of an electronic identification account, the electronic identification and authentication management agency shall notify thereof in writing, via text message or via the electronic identification account of the person who carries out the procedures for grant of an electronic identification account.

Article 13. Time limits for processing requests for grant of electronic identification accounts

After receiving a complete and valid dossier as specified in this Decree, the electronic identification and authentication management agency shall grant electronic identification accounts within the following time limits:

1. For Vietnamese citizens who already have a citizen identity card or identity card and such card remains valid:

a/ One working day, for cases of granting level-1 electronic identification accounts;

b/ Three working days, for cases of granting level-2 electronic identification accounts.

2. Seven working days, for Vietnamese citizens who have a citizen identity card but such card has expired or who have no identity card.

3. For foreigners:

a/ One working day, for cases of granting level-1 electronic identification accounts;

b/ Three working days, for cases of granting of level-2 electronic identification account and the information about the requester's face photo and fingerprints is available in the National Immigration Database;

c/ Seven working days, for cases of granting level-2 electronic identification accounts but the information about the requester's face photo and fingerprints is not yet available in the National Immigration Database.

4. For organizations:

a/ Three working days, in case the information about the requesting organization, that needs to be verified, is available in national databases or specialized databases;

b/ Fifteen days, in case the information about the requesting organization, that needs to be verified, is not yet available in national databases or specialized databases.

Article 14. Activation and use of electronic identification accounts

1. Electronic identity subjects that are individuals, agencies or organizations shall activate their electronic identification accounts on the National Identification Application within 7 days after receiving a notice of grant of electronic identification accounts. Past 7 days, if their electronic identification accounts are not activated, the electronic identity subjects shall contact the electronic identification and authentication management agency through the hotline for receiving and solving inquiries about electronic identification and authentication to activate the electronic identification accounts.

2. The use of electronic identification accounts by persons aged under 14 years, persons under guardianship, and represented persons must be consented and confirmed by their guardians or representatives via the National Identification Application. Guardians and representatives shall use electronic identification accounts of persons aged under 14 years, persons under guardianship, and represented persons to conduct transactions and other activities for the latter's rights and interests.

3. The use of electronic identification accounts and electronic authentication services is legally valid to affirm and prove that the electronic identity subjects have performed and approved the transactions in question.

4. The electronic identification and authentication management agency shall connect, share, and authenticate data for electronic identity subjects to use their electronic identification accounts in other countries according to treaties to which Vietnam is a signatory.

Article 15. Order and procedures for locking and unlocking electronic identification accounts

1. Locking and unlocking electronic identification accounts of Vietnamese citizens

The electronic identification and authentication system shall automatically lock/unlock the electronic identification account of a citizen when the citizen's

electronic identity card is locked/unlocked or when his/her citizen identity card or identity card expires.

2. Locking electronic identification accounts of foreigners and organizations

a/ The electronic identification and authentication system shall automatically record, check, authenticate and lock the electronic identification account of a foreigner in case the foreigner requests locking his/her electronic identification account; the foreigner violates the agreement on use of the National Identification Application; the foreigner's passport or international travel document expires; the foreigner's period of residence in Vietnam expires; or the foreigner dies. The recording shall be conducted based on the foreigner's declaration on the National Identification Application or the updating of information specified in Article 8 of this Decree;

b/ The electronic identification and authentication system shall automatically record, check, authenticate and lock the electronic identification account of an organization in case the organization requests locking its electronic identification account; the organization violates the agreement on use of the National Identification Application; or the organization is dissolved, goes bankrupt, or suspends or terminates operation in accordance with law. The recording shall be conducted based on the organization's declaration on the National Identification Application or the updating of information specified in Article 8 of this Decree;

c/ Proceeding-conducting agencies and other competent agencies shall send requests for locking/unlocking electronic identification account or electronic identity card, made according to Form TK03 provided in the Appendix to this Decree, to the commune-level Public Security agency or the identity management agency under the nearest provincial- or district-level Public Security agency for processing;

d/ Within 1 working day after receiving a request for locking/unlocking electronic identification account or electronic identity card from a proceeding-conducting agency or another competent agency, the commune-level Public Security agency or the provincial- or district-level Public Security agency's identity management agency shall consider and forward the request to the head of the Ministry of Public Security's identity management agency for consideration and approval via the electronic identification and authentication system;

dd/ Within 2 working days after receiving the proposal of the commune-level Public Security agency or the provincial- or district-level Public Security agency's identity management agency, the head of the Ministry of Public Security's identity management agency shall consider and approve the request for locking electronic

identification account in the case specified in Clause 2 of this Article and notify such to the requesting agency and the subject whose account is locked. In case of refusal to lock the electronic identification account, he/she shall issue a written reply, clearly stating the reason.

3. Unlocking electronic identification accounts

a/ The electronic identification and authentication system shall automatically unlock electronic identification accounts when the grounds for locking these electronic identification accounts no longer exist;

b/ Proceeding-conducting agencies and other competent agencies shall send requests for locking/unlocking electronic identification account or electronic identity card to the commune-level Public Security agency or identity management agency of the nearest provincial- or district-level Public Security agency for processing;

c/ Within 1 working day after receiving a request for locking/unlocking electronic identification account or electronic identity from a proceeding-conducting agency or another competent agency, the commune-level Public Security office or provincial- or district-level Public Security agency's identity management agency shall consider and forward the request to the head of the Ministry of Public Security's identity management agency for consideration and approval via the electronic identification and authentication system;

d/ Within 2 working days after receiving the proposal from the commune-level Public Security office or provincial- or district-level Public Security agency's identity management agency, the head of the Ministry of Public Security's identity management agency shall consider and approve the request for unlocking electronic identification account in the case specified in Clause 2 of this Article and notify such to the requesting agency and the subject whose account is unlocked. In case of refusal to unlock the electronic identification account, he/she shall issue a written reply, clearly stating the reason.

Article 16. Competence to grant, lock and unlock electronic identification accounts for Vietnamese citizens, foreigners, and agencies and organizations

The Director of the Police Department for Administrative Management of Social Order under the Ministry of Public Security is competent to grant, lock, and unlock electronic identification accounts for Vietnamese citizens, foreigners, and agencies and organizations.

Article 17. Storage of information in the electronic identification and authentication system

1. All information about electronic identities and other information integrated into electronic identification accounts shall be stored eternally in the electronic identification and authentication system.

2. Information on login history of electronic identification accounts shall be stored in the electronic identification and authentication system for a period of at least 5 years from the time of login. Account holders are allowed to exploit information on login history of their electronic identification accounts; the agency managing the electronic identification and authentication system is allowed to exploit information on account login history to serve state management work; other cases must comply with law.

Article 18. Conditions and procedures for connection to the electronic identification and authentication system

1. State agencies, political organizations, socio-political organizations, and public service providers that wish to have the information systems under their management connected to the electronic identification and authentication system must ensure that the information systems under their management at least meet the security requirements applicable to level-3 information systems as prescribed by the law on level-based assurance of security for information systems.

2. The connection and sharing of information specified in Clause 1 of this Article shall be carried out on the basis of a written agreement between the electronic identification and authentication management agency and agencies/organizations managing databases or information systems to be connected, which must clearly state the scope and purpose of the connection.

3. Within 30 days after reaching a written agreement as specified in Clause 2 of this Article, the electronic identification and authentication management agency shall conduct an appraisal and physical inspection of the database or information system of the agency/organization requesting the connection; in case the agency/organization's database or information system has been connected to the National Population Database, the time limit for consideration and grant of permission for the connection is 7 working days.

In case of permitting the connection, the electronic identification and authentication management agency shall notify in writing thereof to the connection-requesting agency or organization and carry out the connection according to the written agreement. In case of refusal to permit the connection, such agency shall issue a written reply, clearly stating the reason.

4. Agencies and organizations other than those specified in Clause 1 of this Article may have their information systems connected to the electronic

identification and authentication system through an electronic authentication service provider.

5. Electronic authentication service providers that are connected to the electronic identification and authentication system to provide electronic authentication services shall not be required to carry out the procedures specified in this Article.

Article 19. Electronic authentication

1. Electronic authentication of electronic identities and electronic identification accounts shall be performed via the electronic identification and authentication system and electronic identification and authentication platform in accordance with this Decree.

2. State agencies, political organizations, socio-political organizations, and organizations providing public services may request electronic authentication by having their information systems connected to, and sharing information with, the electronic identification and authentication system or having their information systems connected to, and sharing information with, national databases or specialized databases containing the information subject to electronic authentication.

3. Organizations and individuals other than those specified in Clause 2 of this Article may request electronic authentication by using the services provided by electronic authentication service providers; the performance of electronic authentication of electronic identities and electronic identification accounts at the request of the organizations and individuals specified in this Clause must be consented by electronic identity subjects through making confirmation on the National Identification Application, SMS via phone numbers of these subjects or other forms of confirmation as prescribed.

4. Organizations and individuals may not provide or share electronic authentication results with/to other organizations and individuals, unless otherwise prescribed by the law on personal data protection; electronic authentication results are not valid to serve as authentication factor in other transactions.

Article 20. Levels of authentication of electronic identification accounts

1. The electronic identification and authentication system shall perform authentication of electronic identification accounts at the following levels:

a/ Level 1: Authentication of electronic identification accounts based on one authentication factor specified in Clause 7, Article 3 and the corresponding means

of authentication specified in Clause 8, Article 3 of this Decree, without biometric information.

b/ Level 2: Authentication of electronic identification accounts based on two different authentication factors specified in Clause 7, Article 3 and the corresponding means of authentication specified in Clause 8, Article 3 of this Decree, without biometric information.

c/ Level 3: Authentication of electronic identification accounts based on two or more different authentication factors specified in Clause 7, Article 3 and the corresponding means of authentication specified in Clause 8, Article 3 of this Decree, including one biometric information item.

d/ Level 4: Authentication of electronic identification accounts based on authentication factors, including at least 1 biometric factor (face photo, fingerprint, voice, iris), at least 1 factor owned by the electronic identity subject (identity card, digital device, software) and 1 factor known to the electronic identity subject (password; secret code; 2D barcode).

2. For other electronic transaction accounts created by agencies, organizations and individuals by themselves, it is suggested to refer to the provisions of Clause 1 of this Article to classify and identify the level of authentication in correspondence to each operation and process of these agencies, organizations or individuals or comply with the provisions of specialized laws and instructions of competent state management agencies in each field.

Article 21. Methods of electronic authentication in performing transactions through the electronic identification and authentication system

1. Electronic authentication for online transactions shall be performed through authentication means appropriate to the level of authentication requested by the organizations providing these online services.

2. For cases of authentication of account information at the place of transaction, the authentication shall be performed through the authentication solution provided in the National Identification Application.

Chapter III

ELECTRONIC AUTHENTICATION SERVICES

Article 22. Electronic authentication services

1. Electronic authentication services constitute a conditional business line.

2. Electronic authentication service providers must satisfy the conditions specified in Article 23 of this Decree and be granted a certificate of eligibility for dealing in electronic authentication services by the Ministry of Public Security.

3. Electronic authentication service providers shall post the list of electronic authentication products and services they provide on the electronic identification website.

Article 23. Conditions for provision of electronic authentication services

1. Conditions on an organization/enterprise

Being a public service unit or an enterprise of the People's Public Security forces.

2. Conditions on personnel

a/ The head of the organization or the legal representative of the enterprise must be a Vietnamese citizen and permanently residing in Vietnam;

b/ The organization or enterprise must have personnel possessing a university or higher degree in information security or information technology or electronics and telecommunications, who shall be responsible for provision of services, system administration, system operation, and assurance of system's information security.

3. Conditions on physical facilities, technical equipment, service provision management process and security and order assurance plan

Organizations and enterprises requesting grant of a certificate of eligibility for dealing in electronic authentication services must have a scheme on service provision activities, including the following contents: plan and process for provision of electronic authentication services, covering descriptions of the information technology system; descriptions of the technical plan on technological solutions; plan on storage and assurance of integrity of data, and assurance of information security of the service provision system; plan on protection of personal data and data of organizations; plan on assurance of security and order; plan on fire prevention and fighting, disaster preparedness and assurance of stable and uninterrupted operation of electronic authentication services; the organizations'/enterprises' technical equipment must be located in Vietnam and inspected in terms of information security in accordance with law.

4. Electronic authentication service providers may entrust other organizations to perform a number of activities including: providing counseling, introducing, and answering inquiries about electronic authentication services; seeking partners, negotiating, and reaching agreement on contents related to activities and utilities

for the provision of authentication services; and supporting and taking care of customers using the services, and other trade promotion activities in accordance with law. Entrusted activities must comply with law.

Article 24. Dossiers and procedures for grant of certificates of eligibility for dealing in electronic authentication services

1. A dossier of application for a certificate of eligibility for dealing in electronic authentication services must comprise:

a/ An application for a certificate of eligibility for dealing in electronic authentication services, made according to Form XT01 provided in the Appendix to this Decree;

b/ The scheme, documents and papers proving the applicant's satisfaction of the conditions specified in Clauses 2 and 3, Article 23 of this Decree.

2. Procedures and time limit for settlement:

a/ An organization/enterprise shall hand-deliver or send by post 1 dossier specified in Clause 1 of this Article to the Ministry of Public Security or submit it online via the National Public Service Portal or the Public Service Portal of the Ministry of Public Security;

b/ In case the dossier is incomplete or invalid, within 3 working days after receiving it, the Ministry of Public Security shall notify thereof in writing for the organization/enterprise to supplement the dossier;

c/ Within 3 working days after receiving a valid dossier, the Ministry of Public Security shall send a consultation request to related ministries and ministerial-level agencies to seek the latter's opinions;

d/ Within 10 days after receiving the consultation request from the Ministry of Public Security, the consulted ministries and ministerial-level agencies shall check, appraise and give their written replies to the Ministry of Public Security;

dd/ Within 30 days after receiving a complete and valid dossier, the Ministry of Public Security shall conduct an appraisal and physical inspection at the organization/enterprise and grant a certificate of eligibility for dealing in electronic authentication services, made according to Form XT03 provided in the Appendix to this Decree, if the organization/enterprise is qualified; in case of refusal to grant a certificate, it shall issue a written reply, clearly stating the reason.

Article 25. Re-grant and change of certificates of eligibility for dealing in electronic authentication services

1. The contents of an organization's/enterprise's certificate of eligibility for dealing in electronic authentication services may be changed in case the organization/enterprise changes the information about its legal representative, head office address, transaction name, or the plan or process appraised by the Ministry of Public Security under Clause 3, Article 23 of this Decree.

2. The organization/enterprise shall submit 1 dossier of request for change of the contents of its certificate of eligibility for dealing in electronic authentication services specified at Point a, Clause 2, Article 24 of this Decree to the Ministry of Public Security. The dossier must comprise:

a/ A declaration requesting renewal or change of a certificate of eligibility for dealing in electronic authentication services, made according to Form XT02 provided in the Appendix to this Decree;

b/ Legally valid documents and papers proving the change of information specified in Clause 1 of this Article.

3. In case the organization/enterprise changes the information about its legal representative, head office address or transaction name, within 10 days after receiving a complete and valid dossier, the Ministry of Public Security shall conduct an appraisal and issue a certificate of eligibility for dealing in electronic authentication services with changed information, if the organization/enterprise is qualified; in case of refusal of the change, it shall issue a written reply, clearly stating the reason.

4. In case the organization/enterprise changes the information about the plan or operation process for provision of electronic authentication services as specified in Clause 3, Article 23 of this Decree, within 30 days after receiving a complete and valid dossier, the Ministry of Public Security shall conduct an appraisal, consult related ministries and ministerial-level agencies, conduct a physical inspection and issue a certificate of eligibility for dealing in electronic authentication services with changed information, if the organization/enterprise is qualified; in case of refusal of the change, it shall issue a written reply, clearly stating the reason.

5. A certificate of eligibility for dealing in electronic authentication services shall be re-granted in case it is lost or damaged to an extent that makes it unusable. The order and procedures for re-grant of a certificate of certificate of eligibility for dealing in electronic authentication services are as follows:

a/ The requesting organization/enterprise shall submit 1 dossier of request for re-grant of a certificate of eligibility for dealing in electronic authentication services specified at Point a, Clause 2, Article 24 of this Decree to the Ministry of

Public Security. The dossier must comprise: a declaration form requesting re-grant or change of a certificate of eligibility for dealing in electronic authentication services; the scheme and documents and papers proving the requester's satisfaction of the conditions specified in Clauses 2 and 3, Article 23 of this Decree;

b/ Within 3 working days after receiving a valid dossier, the Ministry of Public Security shall consider and re-grant the certificate of eligibility for dealing in electronic authentication services to the organization providing electronic authentication services; in case of refusal to re-grant the certificate, it shall issue a written reply, clearly stating the reason.

Article 26. Revocation of certificates of eligibility for dealing in electronic authentication services

1. An electronic authentication service provider shall have its certificate of eligibility for dealing in electronic authentication services revoked in the following cases:

a/ Failing to operate continuously for 6 months or more;

b/ Being dissolved or bankrupt in accordance with law;

c/ Failing to remedy violations of regulations on personal data protection, information security, and cyber security at the request of a competent state agency.

2. The Ministry of Public Security shall issue a decision on revocation of a certificate of eligibility for dealing in electronic authentication services, made according to Form XT04 provided in the Appendix to this Decree.

3. Electronic authentication service providers whose certificates of eligibility for dealing in electronic authentication services are revoked shall be responsible for ensuring the lawful rights and interests of electronic identity subjects and related parties in accordance with law.

Article 27. Expenses for grant and use of electronic identification accounts and use of electronic authentication services

1. Electronic identity subjects being agencies, organizations, Vietnamese citizens, and foreigners shall not be required to pay expenses for registration for grant of electronic identification accounts created by the electronic identification and authentication system and expenses for use of their own electronic identification accounts in electronic transactions.

2. Organizations and individuals exploiting electronic authentication services shall pay expenses to electronic authentication service providers in accordance with the law on price.

3. State agencies, political organizations, and socio-political organizations shall not be required to pay expenses when using electronic authentication services.

Chapter IV

ELECTRONIC IDENTITY CARDS

Article 28. Issuance of electronic identity cards

1. An electronic identity card shall be expressed in the form of a feature or utility of the National Identification Application by login to a citizen's electronic identification account.

2. Electronic identity cards shall be issued along with the issuance of level-2 electronic identification accounts to Vietnamese citizens according to the order and procedures specified in Article 10 of this Decree.

3. The use of electronic identity cards by login to citizens' level-2 electronic identification accounts shall be as valid as use of valid citizen identity cards or identity cards when carrying out administrative procedures, using public services, and conducting other transactions or activities.

4. Electronic identity cards shall be eternally stored in the electronic identification and authentication system. Historical information about use of electronic identity cards shall be stored in the electronic identification and authentication system for 5 years from the time of use.

5. The Minister of Public Security shall specify forms of expression of electronic identity cards in the National Identification Application.

Article 29. Order and procedures for locking electronic identity cards

1. The electronic identification and authentication system shall automatically record, check, authenticate, and lock electronic identity cards in the cases specified at Points b, c and d, Clause 1, Article 34 of the Law on Identity. The recording shall be conducted through updating of information to the electronic identification and authentication system as specified in Article 8 of this Decree.

2. Persons who have been issued electronic identity cards shall file requests for locking electronic identity cards in person at the commune-level Public Security agency or the identity management agency of the nearest provincial- or district-level Public Security agency or via the National Identification Application;

such a request shall be made according to Form TK03 provided in the Appendix to this Decree. The identity management agency shall record, check, authenticate, and lock the electronic identity cards immediately after receiving citizens' requests on the electronic identification and authentication system.

3. Proceeding-conducting agencies and other competent agencies shall send requests for locking electronic identity cards to the commune-level Public Security agency or the identity management agency of the nearest provincial- or district-level Public Security agency for processing.

4. Within 1 working day after a commune-level Public Security agency or provincial- or district-level Public Security agency's identity management agency receives a request for locking electronic identity card from a proceeding-conducting agency or another competent agency, it shall consider and forward the request to the head of the identity management agency of the Ministry of Public Security for consideration and approval via the electronic identification and authentication system.

5. Within 2 working days after receiving a request for locking electronic identity card from a commune-level Public Security agency or provincial- or district-level Public Security agency's identity management agency, the head of the identity management agency of the Ministry of Public Security shall consider and approve the request as specified in Clause 2, this Article and notify thereof to the requesting agency and the citizen. In case of refusal to lock the electronic identity card, he/she shall reply in writing, clearly stating the reason.

Article 30. Order and procedures for unlocking electronic identity cards

1. The electronic identification and authentication system shall automatically review, check and unlock electronic identity cards when the grounds for locking of the electronic identity cards no longer exist.

2. Persons whose electronic identity cards are locked shall file requests for unlocking electronic identity cards at the commune-level Public Security agency or the identity management agency of the nearest provincial- or district-level Public Security agency or via the National Identification Application; such a request shall be made according to Form TK03 provided in the Appendix to this Decree. The identity management agency shall record, check, authenticate, and unlock the electronic identity cards immediately after receiving citizens' requests for unlocking electronic identity cards via the electronic identification and authentication system.

3. Proceeding-conducting agencies and other competent agencies shall send requests for unlocking electronic identity cards to the commune-level Public

Security agency or the identity management agency of the nearest provincial- or district-level Public Security agency for processing.

4. Within 1 working day after a commune-level Public Security agency or provincial- or district-level Public Security agency's identity management agency receives a request for unlocking electronic identity card from a proceeding-conducting agency or another competent agency, it shall consider and forward the request to the head of the identity management agency of the Ministry of Public Security for consideration and approval through the electronic identification and authentication system.

5. Within 2 working days after receiving a request for unlocking electronic identity card from a commune-level Public Security agency or provincial- or district-level Public Security agency's identity management agency, the head of the identity management agency of the Ministry of Public Security shall consider and approve the request as specified in Clause 2, this Article, and notify thereof to the requesting agency and the citizen. In case of refusal to unlock the electronic identity card, he/she shall reply in writing, clearly stating the reason.

Chapter V

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS

Article 31. Responsibilities of electronic identity subjects

1. To protect electronic identity information.

2. To ensure the safety of authentication factors.

3. To immediately notify electronic authentication service providers when losing control of means of authentication or detecting unauthorized use of their own electronic identity, or having other reasons that are likely to cause unsafety in the use of the services.

Article 32. Responsibilities of electronic authentication service users

1. To abide by technical regulations on electronic identification and authentication.

2. To manage and ensure confidentiality of information on electronic identification accounts, and ensure safety in the use of electronic identification accounts.

3. To take responsibility for the transactions they have performed and comply with regulations of related parties regarding electronic transactions.

Article 33. Responsibilities of electronic authentication service providers and agencies, organizations and individuals creating accounts by themselves

1. Responsibilities of electronic authentication service providers

a/ To provide electronic authentication services to organizations and individuals on the basis of agreement in the form of service provision contract;

b/ To manage operations of organizations entrusted to provide electronic authentication products and services as specified in Clause 4, Article 23 of this Decree;

c/ To ensure that communication channels operate and services are provided around the clock;

d/ To comply with the laws on cyberinformation security, cyber security and e-transactions; standards and technical regulations in the field of electronic authentication, information confidentiality, ensuring the accuracy of authentication; to issue electronic authentication procedures with the approval of the electronic identification and authentication management agency;

dd/ To comply with plans and procedures for provision of electronic authentication services appraised by the Ministry of Public Security;

e/ To send reports on electronic authentication operations, made according to Form XT05 provided in the Appendix to this Decree, to the electronic identification and authentication management agency on a biannual or an annual basis or at the request of the electronic identification and authentication management agency.

2. Responsibilities of agencies, organizations and individuals that create accounts by themselves for their own activities:

a/ To take responsibility for the accuracy of the accounts they create;

b/ To protect personal data they collect and manage in accordance with law;

c/ To obtain the consent of data subjects in all activities related to data management, exploitation and use;

d/ To delete data they collect and manage at the request of data subjects, unless otherwise provided for by law.

Article 34. Responsibilities of the Ministry of Public Security

1. To build, manage, protect, and operate the electronic identification and authentication system and the electronic identification and authentication

platform, to apply electronic identification account solutions in state management, administrative reform, and disaster and epidemic prevention and control.

2. To perform the state management of electronic identification and authentication. To provide unified regulations on the principle and numerical structure of foreigner identification number and agency/organization identification number.

3. To assume the prime responsibility for, and coordinate with ministries and ministerial-level agencies in, connecting national databases and specialized databases serving electronic identification and authentication.

4. To assume the prime responsibility for, and coordinate with the Ministry of Information and Communications, Ministry of Planning and Investment, Ministry of Justice, Ministry of National Defense, Government Office, and related ministries and ministerial-level agencies in, inspecting and examining electronic identification and authentication activities.

5. To connect and integrate the electronic identification and authentication system with/into the electronic identification exchange platform of the National Public Service Portal to serve the checking of accounts, settlement of administrative procedures, and provision of online public services in accordance with law.

6. To assume the prime responsibility for, and coordinate with the Ministry of Information and Communications, Ministry of National Defense and Government Cipher Committee in, ensuring information safety and confidentiality for the electronic identification and authentication system.

7. To assume the prime responsibility for, and coordinate and reach agreement with ministries, ministerial-level agencies, government-attached agencies, the Government Cipher Committee, and provincial-level People's Committees in, specifying plans on data connection, sharing and exploitation serving the use of electronic identities, electronic identification accounts and electronic identity cards; to ensure information confidentiality, safety and security, and comply with the performance of administrative procedures in a face-to-face manner and in the electronic environment.

8. To assume the prime responsibility for, and coordinate and reach agreement with ministries, ministerial-level agencies, government-attached agencies, Government Cipher Committee, and provincial-level People's Committees in, specifying plans on connection, sharing and exploitation of data for use of electronic identities, electronic identification accounts, and electronic identity cards provided and created by the electronic identification and

authentication system; to ensure information confidentiality, safety and security, and conformity with the performance of administrative procedures in a face-to-face manner and in the electronic environment.

9. To assume the prime responsibility for, and coordinate with the Ministry of Justice, Ministry of Planning and Investment, and Ministry of National Defense in ensuring the connection, sharing, and updating of information in the National Population Database, National Immigration Database, Civil Status Database, and National Enterprise Registration Database to serve electronic identification and authentication.

10. To ensure that communication channels operate and services are provided around the clock.

Article 35. Responsibility of the Ministry of Information and Communications

To coordinate with the Ministry of Public Security and Ministry of National Defense in ensuring information safety and confidentiality for the electronic identification and authentication system.

Article 36. Responsibilities of the Ministry of Planning and Investment

1. To assume the prime responsibility for, and coordinate and reach agreement with the Ministry of Public Security and related ministries and sectors in, specifying plans on connection and sharing of information of agencies and organizations in the National Enterprise Registration Database with the electronic identification and authentication system to create identification numbers and electronic identification accounts for agencies and organizations to serve electronic identification and authentication activities; to ensure information safety and security.

2. To coordinate with the Ministry of Public Security in issuing and managing electronic identification accounts for organizations and enterprises within the ambit of its functions and tasks.

3. To ensure the use of electronic identities and electronic identification accounts for performance of administrative procedures and public administrative services in electronic environment within the ambit of its management as specified by law.

Article 37. Responsibilities of the Ministry of National Defense

1. To guide agencies, units, enterprises and individuals under its management to conduct electronic identification and authentication in accordance with regulations on protection of state secrets in the field of national defense.

2. To coordinate and reach agreement with the Ministry of Public Security in specifying plans on connection and sharing for use of electronic identities, electronic identification accounts, and electronic identity cards provided and established by the electronic identification and authentication system.

3. To coordinate with the Ministry of Public Security in ensuring information security and cyber security for the electronic identification and authentication system.

Article 38. Responsibilities of the Government Cipher Committee

1. To guide the application of standards and technical regulations on civil cryptography and use of digital signature authentication services exclusive for official duties in electronic identification and authentication activities.

2. To assume the prime responsibility for, and coordinate with the Ministry of Public Security in, assessing cryptographic safety for electronic authentication service users.

3. To coordinate with the Ministry of Public Security in ensuring information safety and confidentiality in use of cryptographic products for the electronic identification and authentication system and use of electronic identities, electronic identification accounts, and electronic identity cards in provision of digital signature services exclusive for official duties.

Article 39. Responsibilities of ministries, ministerial-level agencies, government-attached agencies and provincial-level People's Committees

1. To ensure the use of electronic identities, electronic identification accounts and electronic identity cards for performance of administrative procedures and public administrative services in the electronic environment.

2. To coordinate and reach agreement with the Ministry of Public Security in specifying plans for data connection and sharing for use of electronic identities, electronic identification accounts and electronic identity cards provided and created by the electronic identification and authentication system; to ensure information safety and security.

3. To ensure stable and uninterrupted operation of national databases and specialized databases for authentication at the request of specialized database management agencies, state agencies, political organizations, socio-political organizations, and other organizations assigned to provide public services.

Chapter VI

IMPLEMENTATION PROVISIONS

Article 40. Effect

1. This Decree takes effect on July 1, 2024.

2. The Government's Decree No. 59/2022/ND-CP of September 5, 2022, on electronic identification and authentication, ceases to be effective on the effective date of this Decree.

3. Accounts created and granted to individuals by the National Public Service Portal and ministerial- and provincial-level information systems for settlement of administrative procedures may be used through June 30, 2024.

4. Accounts created and granted to agencies and organizations by the National Public Service Portal and ministerial- and provincial-level information systems for settlement of administrative procedures may be used through June 30, 2025.

5. Electronic identification accounts and certificates of eligibility for provision of e-authentication services granted under Decree No. 59/2022/ND-CP of September 5, 2022, on electronic identification and authentication, remain valid through their expiry date as specified by law.

6. For citizens who have been granted level-2 electronic identification accounts before the effective date of this Decree, the identity management agency of the Ministry of Public Security shall create electronic identity cards for them and display such electronic identity cards through the National Identification Application from July 1, 2024.

7. To amend and supplement Clause 1, Article 7 of Decree No. 45/2020/ND-CP of April 8, 2020, on performance of administrative procedures in the electronic environment, as follows:

"1. Organizations and individuals shall carry out administrative procedures on the National Public Service Portal and ministerial- and provincial-level information systems for settlement of administrative procedures, using electronic identification accounts granted by the electronic identification and authentication system and already connected and integrated to the National Public Service Portal and ministerial- and provincial-level information systems for settlement of administrative procedures".

8. To amend and supplement Point a, Clause 1, Article 21a of Decree No. 107/2021/ND-CP of December 6, 2021, amending and supplementing a number of

articles of the Government's Decree No. 61/2018/ND-CP of April 23, 2018, on the implementation of the single-window and inter-agency single-window mechanisms in settlement of administrative procedures, as follows:

"a/ Examining and authenticating electronic identification accounts of the individual/organization through his/her personal identification number, for Vietnamese citizens, or serial number of his/her passport (or international travel document), for foreigners, or its code, for organizations, in ministerial- and provincial-level information systems for settlement of administrative procedures by connecting and sharing data with the electronic identification and authentication system. In case the individual/organization has not yet been granted an electronic identification account, the dossier-receiving officer at the single-window section shall guide him/her/it to create, or create a level-1 electronic identity account for him/her/it. In case the individual/organization authorizes another person to carry out administrative procedures, the electronic identification account is identified as the electronic identification account of the authorizer."

Article 41. Implementation responsibility

1. The Ministry of Public Security shall guide, examine and urge the implementation of this Decree.

2. In the course of implementation of this Decree, the Ministry of Public Security shall coordinate with the Ministry of Information and Communications in summarizing and settling problems according to their state management functions, and in case of necessity, report thereon to the Prime Minister for consideration and settlement.

3. Ministers, heads of ministerial-level agencies, heads of government-attached agencies, and chairpersons of provincial-level People's Committees shall implement this Decree.-

On behalf of the Government
For the Prime Minister
Deputy Prime Minister
TRAN LUU QUANG

** The Appendix to this Decree is not translated.*