# Regulations Governing the Security of Electronic Stored Value Cards

( 2018.03.31 Amended )

Article 1 These Regulations are enacted pursuant to Paragraph 2, Article 4 of the Act Governing Issuance of Electronic Stored Value Cards.

Article 2 Issuers shall establish security measures in accordance with the security requirements and design set forth in these Regulations to ensure the security of the electronic stored value cards so as to protect the interests of consumers.

Article 3 The term "security requirements and design" mentioned in the preceding paragraph means the following:

1. For card transactions, an issuer shall implement the requirements set forth in these Regulations for the confidentiality, integrity, authentication and non-repeatability of transaction information in accordance with the level of card applications.

2. For card management, an issuer shall take measures to protect its transaction system and the transaction systems of its contracted merchants and recharge institutions from the threat of unauthorized access or intrusion, and attack, and to effectively uphold the integrity and confidentiality of the transaction system, protect its operational security and maintain high level of availability.

3. For terminal equipment and user environment, an issuer shall implement security control and strengthen the security of terminal equipment to protect it from illegal transaction or tampering.

4. For the issuance of electronic stored value cards, an issuer shall choose proper type of card based on the level of applications.

Article 4 The terms as used in this Act shall have the following meanings:

1. "Recharge institution" means a certain institution that provides the card recharge services on behalf of an issuer at its request.

2. "Online transaction" means a transaction that can be carried out through real-time connection with a contracted merchant, a recharge institution or directly with the issuer and record the balance of the electronic stored value card and the transactions on the end of the issuer in any type of network, which includes instant message transmission between a contracted merchant and the issuer, between a recharge institution and the issuer, and between a recharge institution or a contracted merchant and its terminal equipment.

3. The term "type of network" referred to in the preceding subparagraph includes:

(1) "Dedicated network" means using an electronic equipment or communication equipment to carry out message transmission via connection by means of dial-up, leased line or virtual private network (VPN).

(2) "Internet" means using an electronic equipment or communication equipment to carry out message transmission through an Internet service provider.

(3) "Mobile network" means using an electronic equipment or communication equipment to carry out message transmission through a telecommunication service provider.

4. "Off-line transaction" means a transaction that can be carried out at the terminal equipment and record the balance of the electronic stored value card and the transactions on the end of the electronic stored value card in any kind of interface without real-time connection with the issuer.

5. The term "kinds of interface" referred to in the preceding subparagraph includes:

(1) Contact interface: Using magnetic, optical or electronic type of stored value card to carry out message transmission with the terminal equipment by means of direct contact.

(2) Contactless interface: Using an electronic stored value card produced with radio frequency, infrared or other wireless communication technology to carry out message transmission with the terminal equipment without direct contact.

(3) Network and other offline manners: Using an electronic stored value card to carry out message transmission with a remote contracted merchant or recharge institution via a network, communication equipment or other means without connecting instantly with the issuer for authorization.

6. Types of transaction:

(1) "Online purchase transaction" means when a purchase transaction takes place, the authentication of the transaction is carried out by transmitting the related information to the issuer for processing through connection, and record the balance of the electronic stored value card and the transactions on the end of the issuer.

(2) "Offline purchase transaction" means when a purchase transaction takes place, the authentication of the transaction does not require the transmission of related information to the issuer for processing through connection, and record the balance of the electronic stored value card and the transactions on the end of the electronic stored value card.

(3) "Online recharge transactions" means when a recharge transaction takes place, the authorization of the transaction is carried out by transmitting the related information to the issuer

for processing through connection, and record the balance of the electronic stored value card and the transactions on the end of the issuer.

(4) "Offline recharge transaction" means when a recharge transaction takes place, the authorization of recharge does not require the transmission of related information to the issuer for processing through connection, and record the balance of the electronic stored value card and the transactions on the end of the electronic stored value card.

(5) "Fund transfer transaction" means when the funds in a registered electronic stored value card with value storage function are transferred to an electronic payment account of the same cardholder, relevant message on the authorization of fund transfer must be sent to the issuer for processing via connection, and record the balance of the electronic stored value card and the transactions on the end of the electronic stored value card or the issuer.

(6) "Clearing and settlement transaction" includes the transmission of batch accounting information between a contracted merchant or recharge institution and its terminal equipment, the batch accounting information between a contracted merchant or recharge institution and the issuer, and offline recharge amount authorization request between a recharge institution and the issuer.

7. Commonly used cryptographic algorithms include the following:

(1) "Symmetric encryption/ decryption algorithm" means Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES).

(2) "Asymmetric encryption/ decryption algorithm" means

Rivest, Shamir and Adleman Encryption Algorithm (RSA) and Elliptic Curve Cryptography (ECC).

(3) "Hash function" means Secure Hash Algorithm (SHA).

8. One-time password (OTP) is generated using a one-time password generator, short message or other means. OTP is randomly generated and can be used only once.

9. IC Card" means the card or the equipment with IC chip functions.

10. Magnetic stripe card" means the card or the equipment with magnetic stripe functions.

Article 5 For all kind of electronic stored value card transactions, an issuer shall classify the card's application level in accordance with these Regulations in consideration of the nature of product or service and transaction amount.

Products or services are classified into two types by nature:

1. Type 1: To pay charges and fees, taxes, fines, or other expenses imposed by government, and to pay service fees of public utilities (as defined in Article 2 of Act for the Supervision of Privately Run Public Utilities), telecommunication service charges, tuition and miscellaneous fees, medical expenses, public transportation (as defined in Article 2 of the Act of Encouraging Public Transportation Development and gondola, taxi and public bicycle and public motor vehicles) and parking fees, donated funds collected through donations in accordance with the Charity Donations Destined For Social Welfare Funds Implementation Regulations, other types of services approved by the Competent Authority that support government policy and are offered for public interest, to pay charges and fees, taxes and fines which contracted merchants is entrusted by governments at all levels to collect, and for service fees which contracted

merchants is entrusted by Public Utilities to collect.

2. Type 2: To pay for all kinds of products or services.

Transaction amount are classified into two types：

1. Small-sum transaction: The electronic stored value card can be used to pay only for purchase transactions under NT$1,000.

2. Unlimited-sum transaction: The electronic stored value card is not limited to paying small-sum transactions.

The nature of product or service and transaction amount mentioned in the two preceding paragraphs are classified into two application level:

1. Level 1: For payment of small-sum transactions or the type 1 of products or services transactions.

2. Level 2: For the type 2 of products or services and the payment of unlimited-sum transactions.

Article 6 For card transactions, an issuer shall ensure that the electronic stored value cards it issues meet the following security requirements:

1. Online purchase transaction

(1) Confidentiality: For transactions processed via Internet/mobile network connection, the security design shall meet A requirements.

(2) Integrity: For transactions processed via dedicated network connection, the security design shall meet B1 requirements; for transactions processed via Internet/mobile network connection, the security design shall meet B2 requirements.

(3) Authentication: For Level 1 transactions, the security design shall meet C1 or C3 requirements; for Level 2 transactions, the security design shall meet C2 requirements.

(4) Non-repeatability: The security design shall meet F requirements.

2. Off-line purchase transaction

(1) Confidentiality: For transactions processed via network/other offline means interface, the security design shall meet A requirements.

(2) Integrity: For Level 1 transactions processed via contact/contactless interface, the security design shall meet B1 requirements; For Level 2 transactions processed via contact/contactless interface, the security design shall meet B2 requirements; For transactions processed via network/other offline means interface, the security design shall meet B2 requirements.

(3) Authentication of stored value card: For Level 1 transactions processed via contact/contactless interface, the security design shall meet D1 requirements; For Level 2 transactions processed via contact/contactless interface, the security design shall meet D2 requirements; For transactions processed via network/other offline means interface, the security design shall meet D2 requirements.

(4) Authentication of terminal: For Level 1 transactions processed via contact/contactless interface, the security design shall meet E1 requirements; For Level 2 transactions processed via contact/contactless interface, the security design shall meet E2 requirements; For transactions processed via network/other offline means interface, the security design shall meet E2 requirements.

(5) Non-repeatability: The security design shall meet F requirements.

3. Online recharge transaction

(1) Confidentiality: For transactions processed via Internet/mobile network connection, the security design shall

meet A requirements.

(2) Integrity: For transactions processed via dedicated network connection, the security design shall meet B1 requirements; for transactions processed via Internet/mobile network connection, the security design shall meet B2 requirements.

(3) Authentication of issuer: For Level 1 transactions processed via dedicated network connection, the security design shall meet E1 requirements; For Level 2 transactions processed via dedicated network connection, the security design shall meet E2 requirements; for transactions processed via Internet/mobile network connection, the security design shall meet E2 requirements.

(4) Non-repeatability: The security design shall meet F requirements.

4. Off-line recharge transaction

(1) Confidentiality: For transactions processed via network/other offline means interface, the security design shall meet A requirements.

(2) Integrity: For Level 1 transactions processed via contact/contactless interface, the security design shall meet B1 requirements; For Level 2 transactions processed via contact/contactless interface, the security design shall meet B3 requirements; For transactions processed via network/other offline means interface, the security design shall meet B3 requirements.

(3) Authentication of terminal: For Level 1 transactions processed via contact/contactless interface, the security design shall meet E1 requirements; For Level 2 transactions processed via contact/contactless interface, the security design shall meet E2 requirements; For transactions processed via

network/other offline means interface, the security design shall meet E2 requirements.

(4) Non-repeatability: The security design shall meet F requirements.

5. Fund transfer transaction

(1) Confidentiality: For transactions processed via Internet/mobile network connection, the security design shall meet A requirements.

(2) Integrity: For transactions processed via dedicated network connection, the security design shall meet B1 requirements; for transactions processed via Internet/mobile network connection, the security design shall meet B2 requirements.

(3) Authentication: For Level 1 transactions, the security design shall meet C1 or C3 requirements; for Level 2 transactions, the security design shall meet C2 requirements.

(4) Non-repeatability: The security design shall meet F requirements.

6. Clearing and Accounting transaction

(1) Confidentiality: For transactions processed via Internet/mobile network connection, the security design shall meet A requirements.

(2) Integrity: For transactions processed via dedicated network connection, the security design shall meet B1 requirements; for transactions processed via Internet/mobile network connection, the security design shall meet B2 requirements.

(3) Authentication of message: For transactions processed via Internet/mobile network connection, the security design shall meet C2 requirements.

(4) Non-repeatability: The security design shall meet F requirements.

7. Where the transaction information in Subparagraphs 1 ~ 6 above contains personal data as defined in the Personal Data Protection Act, the issuer shall adopt symmetric or asymmetric cryptographic system to encrypt such personal data to ensure their confidentiality and prevent unauthorized access. The level of cryptographic strength of the cryptographic system shall not be lower than that required for confidentiality (A requirements) set out in Subparagraph 1 of Article 7 herein.

Article 7 The security design for confidentiality, integrity, authentication, and non-repeatability of transactions mentioned in the preceding articles shall meet the following requirements:

1. Confidentiality requirements A: Employ the following symmetric or asymmetric cryptographic system to encrypt the full text of message to prevent unauthorized access to the plaintext of message:

(1) The symmetric cryptographic system shall adopt 3DES 112 bits, AES 128bits or other cryptographic algorithms and keys offering the same or higher level of security strength.

(2) The asymmetric cryptographic system shall adopt RSA 1024 bits, ECC 256 bits or other cryptographic algorithms and keys offering the same or higher level of security strength. Starting from January 1, 2017, newly issued electronic stored value cards to which this paragraph applies shall adopt RSA algorithm with key size of at least 1024 bits.

2. Integrity

(1) Protective measures B1: Employ one of the check sum technologies below to prevent malicious alteration of message:

a. Longitudinal Redundancy Check (LRC).

b. Cyclic Redundancy Check (CRC).

c. Hashing algorithm to generate a message digest.

(2) Protective measures B2: Employ encryption/decryption technology that can prevent malicious alteration of message, using, for example, Message Authentication Code (MAC) for symmetric system or Digital Signature for asymmetric system.

a. The symmetric cryptographic system shall adopt a symmetric cryptographic algorithm specified in Item (1), Subparagraph 1 of this article.

b. The asymmetric cryptographic system shall adopt an asymmetric cryptographic algorithm specified in Item (2), Subparagraph 1 of this article.

(3) Protective measures B3: Besides the security requirements set forth for B2, the amount of recharge in the recharge transaction message must be included in the computing of message integrity.

3. Authentication

(1) Protective measures C1: To ensure the accuracy of cardholder, any of the following methods can be used for authentication of cardholder; if any of methods 1 ~ 3 below is used, the issuer shall also use symmetric or asymmetric cryptographic system for authentication to ensure the validity of electronic stored value card and prevent the use of illegal electronic stored value card.

a. Smart card with cryptographic operation capability.

b. Memory IC card + fixed password.

c. Magnetic strip card + magnetic card password.

d. User ID + one-time password(e.g. OTP sent via short message).

e. User ID + Information agreed between the cardholder and the issuer, which is not known to any third party (e.g. fixed password, pattern lock or gesture lock).

f. User ID+ A physical device in the possession of cardholder (e.g. password generator, password card, IC card, computer, mobile device, and hardware cryptopattern module): The issuer should verify that such equipment is the physical equipment held by the cardholder as agreed between the cardholder and the issuer.

g. User ID+ Biometric Characteristics of the Cardholder (e.g. fingerprints, face, iris, voice, palm print, veins, and signature): The issuer shall directly or indirectly verify such biometric characteristics, and adjust the false acceptance rate of biometric characteristics based on its risk tolerance in order to effectively authenticate the cardholder's identity, and shall allow additional kinds of biometrics if necessary. Indirect verification will be processed on the cardholder's device (such as a mobile device). The issuer will only read the verification result, and shall allow additional source verification if necessary. If indirect verification is adopted, the effectiveness of the cardholder ID verification mechanism shall be assessed in advance.

(2) Protective measures C2: Employ chip-based electronic stored value card or terminal security module with authentication function to ensure the accuracy of message source, using, for example, Message Authentication Code (MAC) for symmetric system or Digital Signature for asymmetric system.

a. The symmetric cryptographic system shall adopt a symmetric cryptographic algorithm specified in Item (1), Subparagraph 1 of this article.

b. The asymmetric cryptographic system shall adopt an asymmetric cryptographic algorithm specified in Item (2), Subparagraph 1 of this article.

c. Adopt the two or more verification mechanisms provided in e to g in the foregoing item and agree with the cardholder upon the notification method of the transaction in advance (e.g. text message, push notification, etc.)

(3) Protective measures C3: The issuer should employ information inquiry (e.g. card number, expiration date and verification number) to ensure the validity of electronic stored value card, and prevent the use of illegal electronic stored value card and shall refund the transaction amount within fourteen (14) days for unauthorized transactions where the cardholder needs not assume loss incurred from reported the card loss. However the cardholder should cooperate and assist in subsequent investigation conducted by the issuer.

(4) Protective measures D1: Employ symmetric or asymmetric cryptographic system to authenticate the electronic stored value card from the terminal equipment to prevent the use of fraudulent electronic stored value card.

(5) Protective measures D2: Employ symmetric or asymmetric cryptographic system to authenticate the electronic stored value card from the terminal equipment to prevent the use of fraudulent electronic stored value card.

a. The symmetric cryptographic system shall adopt a symmetric cryptographic algorithm specified in Item (1), Subparagraph 1 of this article.

b. The asymmetric cryptographic system shall adopt an asymmetric cryptographic algorithm specified in Item (2), Subparagraph 1 of this article.

(6) Protective measures E1: Employ symmetric or asymmetric cryptographic system to verify the legality of terminal equipment or issuer from the electronic stored value card to

prevent unauthorized terminal equipment from processing transactions.

(7) Protective measures E2: Employ symmetric or asymmetric cryptographic system to verify the legality of terminal equipment or issuer from the electronic stored value card to prevent unauthorized terminal equipment from processing transactions.

a. The symmetric cryptographic system shall adopt a symmetric cryptographic algorithm specified in Item (1), Subparagraph 1 of this article.

b. The asymmetric cryptographic system shall adopt an asymmetric cryptographic algorithm specified in Item (2), Subparagraph 1 of this article.

4. Non-repeatability F requirements: Use the mechanism of sequence number, date and time, time series or cryptographic challenge-response protocol to prevent using the message of an earlier successful transaction to complete another transaction.

Article 8 For card management, an issuer shall adopt the following protective measures and related security requirements:

1. Establishing Security strategies

(1) Establish computer resources access control mechanism and security protection measures.

(2) The transactions must be traceable.

(3) Monitor illegal transactions.

(4) Sound key management..

2. Enhancing system security

(1) Enhance the security and availability of the computer systems.

(2) Enhance the security and availability of the application systems.

3. Drafting operations management rules.

Article 9 Security design to address the security requirements for an issuer with respect to card management as provided in the preceding article shall meet the following criteria:

1. Establishing computer resources access control mechanism and security protection measures to prevent unauthorized access to system resources and minimize the possibility of illegal entry by implementing the following measures and controls:

(1) Establish the hardware or software security systems, such as firewall, security software and detection software.

(2) Control the frequency of incorrect password entries.

(3) Encrypt the password file of computer system.

(4) Save the transaction log and audit trail.

(5) Design an access control, such as using password or ID card.

(6) Implement login time control.

(7) Use VPN for remote access.

(8) Tiered management of system resources based on their significance and sensitivity.

(9) Enforce the change of preset passwords for application software and network operating systems.

(10) Ensure personal data protection when the system provides all kinds of service functions.

2. Transactions must be traceable. The transaction log shall contain the following information and be saved in the mainframe of the issuer for future reference:

(1) User ID or card number.

(2) Transaction amount.

(3) The ID of terminal equipment.

(4) Transaction sequence number or transaction date and time.

3. The issuer shall monitor illegal transactions.

4. Key management shall give the following security considerations:

(1) Ensure the quality of keys (prevent the use of weak keys).

(2) Ensure that the leak of key content will not occur during the use, storage, transfer or destruction of key.

(3) Store keys in hardware security module that is FIPS 140-2 Level 3 compliant or higher, and are subject to expressed key export restrictions.

(4) Make duplicate of keys to ensure their usability.

(5) Implement proper access control procedure for the upgrade or disposal of key storage equipment or medium to ensure that leakage of keys will not occur.

5. Enhance the security and availability of the computer systems, including:

(1) Prepare backup mainframe, server, communication equipment, networks, and peripheral equipment.

(2) Install virus detection software to scan the network nodes and servers periodically, and periodically update the virus definitions.

(3) Install the patches or hotfixes of systems if necessary.

(4) Establish an intrusion detection mechanism for extranet and periodically update attribute code.

(5) Establish an online control mechanism and restrict connection to non-business related websites.

(6) Arrange email-related social engineering drill every year for system operations/ maintenance personnel.

(7) Conduct vulnerability scan every quarter and take incremental improvement actions based on the risk level.

(8) Conduct code scanning or black box testing for changed programs every half a year and take incremental improvement

actions based on the risk level.

(9) Put servers, network equipment and other operations equipment centrally in the machine room with three lines of defense established, including perimeter access control, internal space surveillance and equipment cabinet access control to ensure the physical security of operations equipment.

6. Enhance the security and availability of application systems:

(1) The security design for Internet application system shall meet the following requirements:

a. The device PIN shall not be transmitted over the Internet and sensitive data shall be end-to-end encrypted during transmission over the Internet.

b. There shall be session control and website session timeout mechanism in place. If the cardholder does not take any action within ten minutes, the system shall discontinue the session or take other protective measures. However, if the cardholder uses a physical device in the possession of the cardholder specified in Item (1).(f), Subparagraph 3 of Article 7 to carry out transactions, the timeout may be extended to thirty minutes.

c. The system shall be able to identify external networks, the sources of transaction data sent therefrom, and the accuracy of transaction data.

d. The system should be able to identify the consistency between cardholder input and payment instruction received.

e. When the cardholder undergoes identity verification and transaction, the system shall use one time random number or timestamp to prevent resend attack.

f. When the cardholder undergoes identity verification and transaction and it is necessary to use random number function for operation, the system shall use secure random number

function to generate the random number needed.

g. When the cardholder changes his agreement to the online transaction, two or more identity verification must be carried out first in accordance with any transaction security design provided in Item (1).(e)~(g), Subparagraph 3 of Article 7 herein.

h. The system shall be designed with masking function for the display of personal data.

i. The system shall be designed with access control, protective and surveillance measures for personal datafiles and database.

j. A counterfeit and money laundering detection system should be established with risk analysis modules and indicators set up for instant alert and suitable actions when irregular transaction activities occur. The risk analysis modules and indicators should be examined and revised regularly.

(2) The security design for cardholder-end applications shall meet the following requirements:

a. The issuer shall use digital certificate recognized by the operating system for code signing.

b. At the time of executing a transaction, the system shall first verify the authenticity of website.

c. The issuer shall avoid storing sensitive data, and if necessary, adopt relevant protective mechanism, such as encryption or scrambling, safekeep the encryption keys and take effective precautions against data theft.

(3) The security design for the applications provided for mobile devices shall meet the following requirements:

a. Check that the authority required for the application on the mobile device shall be comparable to the service to be provided before release. The initial release or any change of authority shall be approved by the legal compliance or the risk control

departments in order to have a comprehensive evaluation complying with the obligation to inform under the Personal Information Protection Act.

b. The issuer should provide the name, version and download site of application for mobile devices on its website.

c. When the mobile device application is opened, if the system detects that the mobile device could have been hacked, the system should remind the cardholder to beware the risk.

d. A reminder suggesting the installation of anti-virus software shall be placed in a noticeable manner (such as on the download page of the mobile app).

e. When the system adopts certificate authority for encrypted data transmission, the mobile device application should establish a list of trusted certificate authorities and authenticate the entire certificate chain and the validity of certificates issued.

f. Before using NFC to transmit payment transaction data, the transaction should be confirmed manually by cardholder.

g. The design of the mobile app shall conform to the relevant self-disciplinary regulations specified by the Banks Association of the ROC (hereinafter referred to as the "Bankers Association") with respect to mobile applications.

(4) The issuer shall conduct penetration testing regularly for its Internet service systems or applications and take incremental improvement actions based on the risk level.

(5) The design of the barcode technology shall conform to relevant self-disciplinary regulations specified by the Bankers Association with respect to the security of the application of the barcode.

7. Draft operations management rules. The internal accountability system and approval procedure of the issuer,

contracted merchants and recharge institutions and attribution of responsibility between them and the cardholders shall include:

(1) Security policy, standard, procedure or guidelines, including the equipment specifications.

(2) Descriptions of security mechanisms and security procedures.

(3) Key management measure or rules.

(4) Security instructions for cardholders and a complete contract.

Article 10 Regarding the terminal equipment and user environment, an issuer shall adopt the following protective measures:

1. Establishing security strategies

(1) Maintain the physical integrity of the terminal equipment and user environment.

(2) Ensure the transaction security of the terminal equipment.

(3) Establish an effective or real-time blacklist management mechanism.

(4) Reduce the probability of accidental trigger of transaction for contactless electronic stored value cards.

(5) Terminal equipment for off-line recharge transactions should be equipped with security module.

(6) Adopt necessary measures to reduce the incidence of fake card transactions if Level 1 electronic stored value card is used for off-line recharge/purchase transactions at a contracted merchant providing Type 2 products or services.

2. Implement measures to enhance system availability.

3. Draft operations management rules, which should be implemented in internal environment management as well.

Article 11 Security design to address the security requirements for an issuer with respect to terminal equipment and user environment as

provided in the preceding article shall meet the following criteria:

1. Maintain the physical integrity of terminal equipment and user environment. It shall adopt the following security designs:

(1) Check periodically the quantity of terminal and relevant devices:

a. Make sure each original facility is environment properly numbered.

b. Check the onsite facilities and devices to see if they are consistent with the original state.

c. Create a checklist, conduct review regularly and follow up.

(2) Sign a non-disclosure agreement with the terminal equipment supplier, and ask the supplier to create a list of terminal equipment installation and maintenance personnel, and automatically notify the issuer whenever the list is updated.

(3) Make sure the installation and maintenance personnel of terminal equipment supplier show identification document when they work onsite. Besides the installation and maintenance operations, the terminal equipment supplier shall readily support the issuer's needs to inspect whether terminal equipment is being tampered with or has a skimmer installed.

(4) The issuer shall from time to time dispatch personnel to inspect the terminal equipment installed at the contracted merchants or recharge institutions to see whether the equipment is being unjustly tampered with and check whether its software is being altered without authorization.

2. Ensure the transaction security of terminal equipment. It shall comply with the following rules:

(1) For information contained in the electronic stored value card, except for account number, card number, expiration date,

transaction sequence number, and other data necessary for verifying whether a transaction occurs, no other data may be stored in the terminal equipment.

(2) To ensure the validity of terminal equipment, each piece of terminal equipment shall have a unique ID number.

(3) For Level 2 transactions, the security module of terminal equipment should be individualized (that is, the keys for each terminal equipment are different).

3. To effectively prevent transactions using invalid electronic stored value cards, an issuer should establish a blacklist management mechanism. The blacklist for online transactions shall be authenticated in real-time, and the blacklist for off-line transactions shall be updated at least daily.

4. The issuer shall effectively prevent contracted merchants from making unwarranted payment deductions and the terminal equipment should implement the following design to minimize the probability of accidental trigger when the cardholder of a contactless electronic stored value card has no intention to make a transaction:

(1) The sensing distance is kept below 10 cm (inclusive).

(2) A transaction is prompted by sound, light signal or graphic image.

5. Terminal equipment for off-line recharge transactions should be equipped with security module and the following designs for recharge transaction:

(1) Recharge transactions are individually authorized.

(2) The amount per recharge is limited.

(3) The cumulative recharge amount is limited (e.g. daily limit). If the limit is reached, request for authorization of additional amount from the issuer can be made through the terminal

equipment.

(4)The security modules should be properly managed, e.g. implementing the production, issuance, and delivery process, production operation control, and security control of security modules.

6. When an electronic stored value card of application Level 1 is used for transactions at a contracted merchant providing Type 2 products or services, the issuer shall demand that the contracted merchant installs surveillance equipment and keeps recording all the time during the business hours, or takes other necessary measures to minimize fake card transactions if the authentication of the blacklist is not returned to the issuer for real-time authentication.

7. If the terminal equipment is a personal electronic or communication device held by the cardholder (e.g. an IC card reader, mobile device simulating the function of electronic stored value card reader mode, etc.), then subparagraph 1, item 2 and 3, subparagraph 2, and subparagraph 5 shall not be applied.

8. System availability should be managed and controlled, e.g. Spare device, network redundancy, redundant circuitry, uninterruptible power supply (UPS) or other methods which can ensure to enhance availability of system.

9. Draft terminal equipment management rules, including description of equipment specifications and security mechanism, description of security procedures, principles for the security module control operation, blacklist management mechanism, and measures for contract signing with contracted merchants and recharge institutions, and their management.

Article 12　An issuer shall choose the proper types of electronic stored value

card based on the intended application level:

1. An electronic stored value card must be one of the following types to be applicable for application level 1:

(1) Smart card with cryptographic operation capability.

(2) Memory IC card + fixed password.

(3) Magnetic strip card + fixed password.

2. An electronic stored value card that is a security-certified IC card to be applicable for application level 2.

The term "security certified" means that as confirmed by the competent authority, the security level has passed the third-party evaluation of an institution recognized by the National Communication Commission of Executive Yuan or the Common Criteria Recognition Arrangement (CCRA) as meeting or on a par with any of the following criteria:

1. ISO/IEC15408 Common Criteria v2.3 EAL4+ (augmented by AVA_VLA.4 and ADV_IMP.2)

2. ISO/IEC15408 Common Criteria v3.1 EAL4+ (augmented by AVA_VAN.5).

3. CNS 15408 EAL4+(augmented by AVA_VLA.4 and ADV_IMP.2).

4. Other evaluation criteria accepted by the competent authority.

Article 13 An issuer shall adopt the following protective measures for the electronic stored value cards it issues:

1. Establishing security strategies

(1) Verify the validity of electronic stored value card.

(2) Incorporate specific security design if user ID + fixed password are adopted.

(3) Personal data stored in the electronic stored value cards must be protected.

2. Drafting operations management rules, which should be Draft

the electronic stored value card delivery control process.

Article 14 The security design to address the security requirements for an issuer with respect to electronic stored value cards it issues as provided in the preceding article shall meet the following criteria:

1. The electronic stored value card must have an independent and unique ID or the function of authentication to ensure its validity.

2. Electronic stored value card that adopts user ID + fixed password shall have the following security designs:

(1) If the user ID uses only explicit data (such as uniform business number, ID card number, mobile phone number, email address, and credit card number) for identification, a cardholder code should be used for additional identification, which may not use any explicit data mentioned above.

(2) The password shall comprise of no less than six characters.

(3) The password shall not be identical to the user ID or the cardholder code.

(4) The password should not be made up of identical alphanumeric characters, continuous English alphabets or numbers, with the exception of default password.

(5) The password is suggested the use of combination of alphanumeric characters, and preferably contain upper case and lower case English alphabets or symbols.

(6) When wrong password is inputted five consecutive times, access to e-payment platform should be restricted and the cardholder must reapply for the setting of password.

(7) Changed password shall not be the same as the previously set password.

(8) If the password has not changed for more than one year, the

issuer should take proper actions.

(9) If the issuer issues a default password at the time the cardholder registers, the cardholder shall be required to change the default password when he/she logs in the first time.

3. Personal data stored in the electronic stored value cards must be protected: If personal data are stored in electronic stored value cards, access control or cardholder verification mechanism shall be implemented to restrict access.

4. Draft the electronic stored value card delivery control process: The issuer should properly manage the life cycle of electronic stored value cards, should draft electronic stored value card production, issuance, and delivery control processes, implement control of card production outsource operation, and implement physical security control of electronic stored value cards.

Article 15 An issuer shall file quarterly reports on the amount of irregular transactions with the Competent Authority, and submit an improvement plan with the Competent Authority if the cumulative amount (of irregular transactions) for the year exceeds one percent (1%) of its paid-in capital.

Article 16 An issuing transaction shall file statistical data on card transactions by the nature of products or services and transaction amount as provided in Article 5 herein with the Competent Authority or an institution designated by the Competent Authority every quarter.

Article 17 An issuer shall engage an accountant to audit its status of compliance with these Regulations, and submit the audit report to the Competent Authority for reference in two (2) months after the end of each fiscal year.

Article 18 These Regulations are in force from the date of promulgation.