# Regulations Governing the Security of Electronic Stored Value Cards

( 2015.04.30 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 cardholder using an electronic equipment or communication equipment to instantly connect directly with the issuer or via a contracted merchant or a recharge institution through any type of network to carry out a transaction, 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 with its terminal equipment.

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

(1) Dedicated network: Using an electronic equipment or communication equipment to carry out message transmission directly via dial-up, leased line or virtual private network (VPN) connection.

(2) Internet: Using an electronic equipment or communication equipment to carry out message transmission through an Internet service provider.
(3) Mobile network: Using an electronic equipment or communication equipment to carry out message transmission through a telecommunication service provider.
4. "Off-line transaction" means a cardholder of electronic stored value card carrying out transaction at the terminal equipment of a contracted merchant or recharge institution through all kinds of interface without connecting instantly 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 of a contracted merchant or recharge institution 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 of a contracted merchant or recharge institution 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.
(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.
(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.
(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.

(5) "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.

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

1. Nature of product or service

| Nature of Product or Service | Description |
|---|---|
| Type 1 | I. 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 parking fees, donated funds collected through donations in accordance with the Charity Donations Destined For Social Welfare Funds Implementation Regulations, or other types of services approved by the Competent Authority that support government policy and are offered for public interest.<br>II. 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. |
| Type 2 | To pay for all kinds of products or services. |

2. Transaction amount

| Transaction amount | Description |
|---|---|

| | |
|---|---|
| Small-sum transaction | The electronic stored value card can be used to pay only for purchase transactions under NT$1,000. |
| Unlimited- sum transaction | The electronic stored value card is not limited to paying small-sum transactions. |

3. Application level

| Nature of product or service | | Type 1 | Type 2 |
|---|---|---|---|
| Transaction Amount | Small-sum transaction | Level 1 | Level 1 |
| | Unlimited- sum transaction | Level 1 | Level 2 |

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

| Type of connection | Dedicated network | | Internet／mobile network | |
|---|---|---|---|---|
| Application level | Level 1 | Level 2 | Level 1 | Level 2 |
| Protective measure | | | | |
| Confidentiality | Not required | Not required | A | A |
| Integrity | B1 | B1 | B2 | B2 |
| Authentic- | Authenticat- | C1 | C2 | C1 | C2 |

| ation | ion of | | | | |
|---|---|---|---|---|---|
| | message or | | | | |
| | cardholder | | | | |
| Non-repeatability | | F | F | F | F |

2. Off-line purchase transaction

| Type of interface | Contact／contactless | | Network and other offline means | |
|---|---|---|---|---|
| Application level | Level | Level | Level | Level |
| Protective measure | 1 | 2 | 1 | 2 |
| Confidentiality | Not requi-red | Not requi-red | A | A |
| Integrity | B1 | B2 | B2 | B2 |

| | | | | | |
|---|---|---|---|---|---|
| Authentic-tion | Authenticat-ion of stored value card | D1 | D2 | D2 | D2 |
| | Authenticat-ion of terminal | E1 | E2 | E2 | E2 |
| Non-repeatability | | F | F | F | F |

3. Online recharge transaction

| Type of connection | Contact／contactless | | Internet／mobile network | |
|---|---|---|---|---|
| Application level / Protective measure | Level 1 | Level 2 | Level 1 | Level 2 |
| Confidentiality | Not requi- | Not requi- | A | A |

| | red | red | | |
|---|---|---|---|---|
| Integrity | B1 | B1 | B2 | B2 |
| Authentic-tion / Authenticat-ion of issuer* | E1 | E2 | E2 | E2 |
| Non-repeatability | F | F | F | F |

(*: Applicable to electronic stored value cards with authentication and value storage functions only)

4. Off-line recharge transaction

| Type of interface | Contact／contactless | | Network and other offline means | |
|---|---|---|---|---|
| Application level / Protective measure | level 1 | level 2 | level 1 | level 2 |
| Confidentiality | Not | Not | A | A |

| | | | | |
|---|---|---|---|---|
| | requi- | requi- | | |
| | red | red | | |
| Integrity | B1 | B3 | B3 | B3 |
| Authentic- Authenticat- | E1 | E2 | E2 | E2 |
| tion ion of | | | | |
| terminal | | | | |
| Non-repeatability | F | F | F | F |

5. Clearing and Accounting transaction

| Type of connection | Contact／ | | Network and | |
|---|---|---|---|---|
| | contactless | | other offline | |
| | | | means | |
| Application level | level | level | level | level |
| Protective measure | 1 | 2 | 1 | 2 |
| Confidentiality | Not | Not | A | A |

| | | | | | |
|---|---|---|---|---|---|
| | | requi- | requi- | | |
| | | red | red | | |
| Integrity | | B1 | B1 | B2 | B2 |
| Authentic- | Authenticat- | Not | Not | C2 | C2 |
| tion | ion of | requi- | requi- | | |
| | message | red | red | | |
| Non-repeatability | | F | F | F | F |

6. Where the transaction information in Subparagraphs 1 ~ 5 above contains personal data as defined in the Computer-Processed 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 set out in Article 7 (A) 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:

| Protective measure | Basic principles of security design |
|---|---|

| | | |
|---|---|---|
| Confidentiality | A | Employ symmetric or asymmetric cryptographic system to encrypt the full text of message to prevent unauthorized access to the plaintext of message:<br>1. The symmetric cryptographic system shall adopt one of the algorithms below:<br>(1) The Triple Data Encryption Algorithm (TDEA), Two Key Triple Data Encryption Algorithm (2TDEA) with 112 key bits, or Three Key Triple Data Encryption Algorithm (3TDEA) with 168 key bits published by the U.S. National Institute of Standards and Technology (NIST); or<br>(2) The NIST Advanced Encryption Standard (AES Algorithm) with |

| | | | key size of 128, 192, or 256 bits. |
|---|---|---|---|
| | | | 2. The asymmetric cryptographic system shall adopt one of the algorithms below: |
| | | | (1) The Rivest, Shamir, and Adleman Encryption Standard (RSA Algorithm) with key size of 1024 or 2048 bits; or |
| | | | (2) The Elliptic Curve Digital Signature Algorithm (ECDSA Algorithm) with 256 bits prime modulus (P-256). |
| Integrity | B1 | | Employ one of the check sum technologies below to prevent malicious alteration of message: |
| | | | 1. Longitudinal Redundancy Check (LRC). |
| | | | 2. Cyclic Redundancy Check (CRC). |

| | | |
|---|---|---|
| | | 3. Hashing algorithm to generate a message digest. |
| | 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.<br>1. The symmetric cryptographic system shall adopt one of the algorithms below:<br>(1) TDEA, 2TDEA with key size of 112 bits or 3TDEA with key size of 168 bits.<br>(2) AES Algorithm with key size of 128, 192, or 256 bits.<br>2. The asymmetric cryptographic system shall adopt one of the algorithms below: |

| | | | |
|---|---|---|---|
| | | | (1) RSA Algorithm with key size of 1024 or 2048 bits.<br>(2) ECDSA Algorithm with 256 bits prime modulus (P-256). |
| | | 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. |
| Authentication | Authentication of message or cardholder | C1 | To ensure the accuracy of cardholder, any of the following methods can be used for authentication of cardholder:<br>1. User ID + fixed password.<br>2. Magnetic card + magnetic card password.<br>3. User ID + one-time password: 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. |
| | | | | 4. Provide chip-based electronic stored value card with authentication function on the basis of cryptography. |
| | | | 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. |
| | | | | 1. The symmetric cryptographic |

| | | | |
|---|---|---|---|
| | | | system shall adopt one of the algorithms below:<br>(1) TDEA, 2TDEA with key size of 112 bits or 3TDEA with key size of 168 bits.<br>(2) AES Algorithm with key size of 128, 192, or 256 bits.<br>2. The asymmetric cryptographic system shall adopt one of the algorithms below:<br>(1) RSA Algorithm with key size of 1024 or 2048 bits.<br>(2) ECDSA Algorithm with 256 bits prime modulus (P-256). |
| | Authentication of stored value card | 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. |
| | | | D2 | Employ symmetric or asymmetric cryptographic system to authenticate the electronic stored value card with the terminal equipment to prevent the use of fraudulent electronic stored value card.<br>1. The symmetric cryptographic system shall adopt one of the algorithms below:<br>(1) TDEA, 2TDEA with key size of 112 bits or 3TDEA with key size of 168 bits.<br>(2) AES Algorithm with key size of 128, 192, or 256 bits.<br>2. The asymmetric cryptographic system shall adopt one of the algorithms below:<br>(1) RSA Algorithm with key size |

| | | | |
|---|---|---|---|
| | | | of 1024 or 2048 bits. |
| | | | (2) ECDSA Algorithm with 256 bits prime modulus (P-256). |
| | Authentication of terminal／issuer | 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. |
| | | 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. |

| | | | |
|---|---|---|---|
| | | | 1. The symmetric cryptographic system shall adopt one of the algorithms below:<br>(1) NIST TDEA, 2TDEA with key size of 112 bits or 3TDEA with key size of 168 bits.<br>(2) NIST AES Algorithm with key size of 128, 192, or 256 bits.<br>2. The asymmetric encryption/decryption system shall adopt one of the algorithms below:<br>(1) RSA Algorithm with key size of 1024 or 2048 bits.<br>(2) ECDSA Algorithm with 256 bits prime modulus (P-256). |
| Non-repeatability | F | 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:

| Protective measures | Security requirements |
|---|---|
| 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. Prevent small contracted merchants from making unwarranted payment deductions. |
| | 5. Sound key management. |

| | |
|---|---|
| Enhancing system security | Enhance the security and availability of the computer systems. |
| Drafting operations management rules | Draft 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:

| Security Requirements | Security Design |
|---|---|
| Establishing computer resources access control mechanism and security protection measures. | It shall be able to prevent unauthorized access to system resources and minimize the possibility of illegal entry by implementing the following measures and controls:<br>1. Establish the hardware or software security systems, such as firewall, security software and detection software.<br>2. Control the frequency of incorrect password entries.<br>3. Encrypt the password file of computer system.<br>4. Save the transaction log and audit trail.<br>5. Design an access control, such as using password or ID card.<br>6. Implement login time control.<br>7. Use VPN for remote access.<br>8. Tiered management of system resources based on their significance and sensitivity.<br>9. Enforce the change of preset passwords for application software and network operating systems.<br>10. Ensure personal data protection when the system provides all kinds of service functions. |
| The | The transaction log shall contain the following |

| | |
|---|---|
| transactions must be traceable | information and be saved in the mainframe of the issuer for future reference:<br>1. User ID or card number.<br>2. Transaction amount.<br>3. The ID of terminal equipment.<br>4. Transaction sequence number or transaction date and time. |
| Monitoring illegal transactions | The issuer shall monitor illegal transactions. |
| Prevent small contracted merchants from making unwarranted payment deductions | 1. A contracted merchant whose paid-in capital is below NT$80,000,000 and annual revenue is below NT$60,000,000 shall carry out transactions in accordance with any of the following manners:<br>(1) Card swiping or card insertion.<br>(2) Input of password.<br>(3) Any other system designs for cardholder to confirm a transaction.<br>(4) The sensing distance is kept below 4cm (inclusive).<br>2. Provisions set forth in the preceding item do not apply to the contracted merchant that meets any of the following conditions:<br>(1) Providing Type 1 products or services.<br>(2) The franchisee whose franchisor's paid-in capital is at least NT$80,000,000 or its the annual revenue is at least NT$60,000,000.<br>3. The issuer shall sign a tripartite merchant contract with the franchisor and the franchisee referred to in the preceding item jointly or respectively, and shall comply with the following provisions:<br>(1) The issuer shall establish an internal control system to prevent the franchisee from making unwarranted payment deductions.<br>(2) The issuer shall, in the tripartite contract or in the contract signed with the franchisor, require the franchisor to bear equal responsibility with respect to cardholders if an intentional act or negligence of its franchisee or the employees of the franchisee results in unwarranted payment deductions. |

| | |
|---|---|
| Sound key management | Key management shall give the following security considerations:<br>1. Ensure the quality of keys (prevent the use of weak keys).<br>2. Ensure that the leak of key content will not occur during the use, storage, transfer or destruction of key.<br>3. Make duplicate of keys to ensure their usability.<br>4. 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. |
| Enhance the security and availability of the computer systems | Offsite redundancy and failure prevention measures shall be established, including:<br>1. Prepare backup mainframe, server, communication equipment, networks, and peripheral equipment.<br>2. Install virus detection software to scan the network nodes and servers periodically.<br>3. Install the patches or hotfixes of systems if necessary.<br>4. Ensure the physical security of servers and network equipment. |
| 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:<br>1. Security policy, standard, procedure or guidelines, including the equipment specifications.<br>2. Descriptions of security mechanisms and security procedures.<br>3. Key management measure or rules.<br>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:

| Protective measures | Security requirements |
|---|---|
| Establishing security strategies | Maintain the physical integrity of the terminal equipment and user environment.<br>Ensure the transaction security of the terminal |

| | |
|---|---|
| | equipment.<br>Establish an effective or real-time blacklist management mechanism.<br>Reduce the probability of accidental trigger of transaction for contactless electronic stored value cards.<br>Design terminal security module for off-line recharge transactions.<br>Adopt necessary measures to reduce the incidence of fake card transactions if Level 1 electronic stored value card is used for off-line transactions at a contracted merchant providing Type 2 products or services.<br>Directions for the development of Internet application systems. |
| Enhancing the system availability | Implement measures to enhance system availability. |
| Drafting operations management rules | 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:

| Security requirements | Security design |
|---|---|
| Maintain the physical integrity of terminal equipment and user environment | It shall adopt the following security designs:<br>I. Check periodically the quantity of terminal and relevant devices:<br>1. Make sure each original facility is environment properly numbered.<br>2. Check the onsite facilities and devices to see if they are consistent with the original state.<br>3. Create a checklist, conduct review regularly and follow up.<br>II. 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. |

| | |
|---|---|
| | III. Make sure the 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.<br>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. |
| Ensure the transaction security of terminal equipment | The processing of transactions with terminal equipment shall comply with the following rules:<br>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.<br>2. To ensure the validity of terminal equipment, each piece of terminal equipment shall have a unique ID number.<br>3. For Level 2 transactions, the security module of terminal equipment should be individualized (that is, the keys for each terminal equipment are different). |
| Establish an effective or real-time blacklist management mechanism | 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 updated in real-time, and the blacklist for off-line transactions shall be updated at least daily. |
| Reduce the probability of accidental trigger of transaction for contactless electronic | 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:<br>1. The sensing distance is kept below 6 cm (inclusive); and<br>2. A transaction is prompted by sound, light signal or |

| | |
|---|---|
| stored value cards | graphic image. |
| Design terminal security module for off-line recharge transactions | Terminal equipment for off-line recharge transactions should be equipped with security module and the following designs for recharge transaction:<br>1. Recharge transactions are individually authorized.<br>2. The amount per recharge is limited.<br>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.<br>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. |
| Ought to adopt necessary measures to reduce the incidence of fake card transaction if Level 1 electronic stored value card is used for off-line transactions at a contracted merchant providing Type 2 products or services | If a Level 1 electronic stored value card is used for off-line 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. |
| Directions for the development of Internet application systems | If the electronic stored value card holders conduct transactions over the Internet using a browser, the network application system shall have the following designs:<br>1. The website shall adopt Secure Sockets Layer (SSL) mechanism or encrypt the transmissions in other manners with the level of cryptographic |

註解 [u1]: Top-up better?

| | |
|---|---|
| | strength not lower than that specified in Article 7 (A) on confidentiality.<br>2. The check code of terminal equipment for each transaction shall be generated dynamically and randomly, or protected by cryptographic operations.<br>3. The system should be designed with Graphic One Time Password (GOTP) with masking function or random buttons.<br>4. The system should have the design of dynamic page presentation or restricting selection by mouse click only to prevent the simulation of SendKey Control.<br>5. The system should have session control and timeout mechanism.<br>6. In the case of multi-page design, the system should verify the authenticity of the previous webpage.<br>7. The client-side component should verify the authenticity of website.<br>8. The client-side component should have anti-theft mechanism to verify the validity or authenticity of website.<br>9. The client-side component should have a CodeSign to ensure the integrity of the component.<br>10.The client-side component should have the implementation of exclusive mode when accessing card.<br>The client-side component should have the design that allows cardholders to confirm a transaction manually.<br>When the system is hacked, the issuer shall immediately shut down the network service to ensure the security of transactions. |
| Implement measures to enhance the system availability | System availability should be managed and controlled with the following measures:<br>1. Planning network redundancy or other methods which can ensure to enhance availability of system.<br>2. Planning redundant circuitry or uninterruptible power supply (UPS). |
| Draft | Draft terminal equipment management rules, |

| | |
|---|---|
| operations 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:

| Application level | Applicable types of electronic stored value card |
|---|---|
| Level 1 | The electronic stored value card must be one of the following types; electronic stored value cards with features in Point 3, 4, or 5 can be used for online transactions only:<br>1. Smart card with cryptographic operation capability.<br>2. Memory IC card + fixed password.<br>3. User ID + one-time password.<br>4. Magnetic strip card + fixed password.<br>5. User ID + fixed password. |

| | |
|---|---|
| Level 2 | The electronic stored value card must be one of the following types:<br>1. Smart card that meets the security requirements set forth in Article 6 herein and has had security certified.<br>2. User ID + security-certified one-time password generator (e.g. OTP Token) (transactions can be carried out online and on real-time basis only. |

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:

| Protective measures | Security requirements |
|---|---|
| Establishing security | 1. Verify the validity of |

| | |
|---|---|
| strategies | electronic stored value card.<br>2. Incorporate specific security design if user ID + fixed password are adopted.<br>3. Personal data stored in the electronic stored value cards must be protected. |
| Drafting operations management rules | 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:

| Security requirements | Security design |
|---|---|
| Verify the validity of electronic stored value card. | Ensure the validity of electronic stored value card by any of the following means:<br>1. The card has an independent and unique ID. |

| | |
|---|---|
| | 2. The card has the function of authentication. |
| Incorporate specific security design if user ID + fixed password are adopted | Electronic stored value card that adopts user ID + fixed password shall have the following security designs:<br>1. Security design for user ID:<br>(1) If the issuer uses the explicit data of customers (e.g. Uniform Business No., ID No., and account number) for user ID, a cardholder ID shall also be used for identification purpose.<br>(2) The user ID shall not have less than six digits.<br>(3) The user ID may not be identical English alphabets or numbers, or consecutive English alphabets or sequential |

| | | |
|---|---|---|
| | | numbers. |
| | | (4) If a customer did not change the password in one month (calendar days) after receiving the user ID, the customer may not use the same user ID for sign-in. |
| | | (5) A customer may log in with the password once at a time. |
| | | (6) The use of cardholder ID shall at least follow the rules below: |
| | | a. The cardholder ID may not be the explicit data of customer. |
| | | b. If wrong ID is entered five times, the issuer should take proper action. |
| | | c. The cardholder ID may not be identical to the user ID when first established; the same rule applies to change of cardholder |

| | |
|---|---|
| | ID. |
| | 2. Security design for password: |
| | (1) The password shall not be less than six digits. If it is used in combination with transaction password, the password shall not be less than four digits. |
| | (2) Suggest the use of combination of English alphabets and numerals for password, and preferably include upper case and lower case English alphabets or signs. |
| | (3) The password may not use identical English alphabets or numbers, or consecutive English alphabets or sequential numbers. |
| | (4) The password and user ID may not be identical. |
| | (5) The transaction may not |

| | |
|---|---|
| | continue if wrong password is entered five times consecutively. |
| | (6) The new password may not be identical to the one just used. |
| | (7) Make change of preset password compulsory during the first-time login. |
| 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. |
| Draft the electronic stored value card delivery control process | The issuer should properly manage the life cycle of electronic stored value cards, including:<br>1. Drafting electronic stored value card production, issuance, and delivery control processes. |

| | |
|---|---|
| | 2. Implementing control of card production outsource operation. |
| | 3. Implementing 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 Issuer that are currently issuing electronic stored value cards and have been approved to engage in electronic stored value card business and banks that are currently engaging in electronic stored value card business shall make adjustment within six (6) months after the promulgation and implementation of these Regulations if they do not comply with the provision of "prevent small contracted merchants from making unwarranted payment deductions" in Article 9 herein.

Article 19 These Regulations are in force from the date of promulgation.