Content

Title：	Regulations on Required Information for Certification Practice Statements Ch
Date：	2004.07.07
Legislative：	1.Promulgated on July 07 , 2004
Content：	Chapter 1　General Principles Article 1 These Regulations are enacted pursuant to Paragraph 2, Article 11 of the Electronic Signatures Act. Article 2 These Regulations make use of the following defined terms: 1. “Assurance” means a basis that the trusted entity has complied with certain security requirements. 2. “Assurance level” means a certain level in a relative assurance tier. 3. “Certificate policy (CP)” means a named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. 4. “Object identifier (OID)” means a unique alphanumeric/numeric identifier registered under the International Standard Organization registration standard, and which could be used to identify the uniquely corresponding CP; where the CP is modified, the OID is not changed accordingly. 5. “Subscriber” means a subject named or identified in a certificate that holds the private key which corresponds to the public key listed in the certificate. 6. “Relying party” means a recipient of a certificate who acts in reliance on that certificate. 7. “Repository” means a system for storing and retrieving certificates or other information relevant to certificates. 8. “Certificate revocation list (CRL)” means a list of revoked certificates digitally signed by a certification service provider. 9. “Activation data” means data values other than keys, thArticleArticlet are required to operate cryptographic modules and that need to be protected. Article 3 A certification service provider shall specify the following significant particulars in the first page of the certification practice statement (CPS): 1.The approval number issued by the competent authority 2.Types of certificate 3.Assurance levels of certificates 4.Applicability and restrictions on certificate usage 5.Limitations of liability, and allocation of liability within the application period for certificate revocation 6.Whether the certificate services are audited by a third party or have been granted any seal Article 4 A certification service provider shall specify the supported CPs, provide the OIDs of the CPs, and specify other significant documents supporting the CPS. Article 5 A certification service provider shall specify the identity or types of entity that fill the roles of participants operating and maintaining the certification service. In the event that an entity participates in the certification service by outsourcing, the certification service provider shall also specify the name and qualification of the entity. Article 6

A certification service provider shall specify the telephone number, mailing address and electronic mail address of a contact person to subscribers or relying parties to report the loss of private key and to consult matters of the CPS.

Article 7

A certification service provider shall specify the following subscriber obligations:

1.Ensuring accuracy of representations in certificate application

2.Safely generating and guarding the private key where the private key is generated by the subscriber

3.Complying with the restrictions on private key and certificate usage

4.Notifying the matters of private key compromise or loss

Article 8

A certification service provider shall specify the following replying party obligations:

1.Taking responsibilities to verify digital signatures

2.Placing reliance on the certificate within the purposes of certificate usage

3.Inspecting the certificate status

4.Acknowledging the liability provisions on certification service providers

Article 9

A certification service provider shall specify the following particulars in respect of the publication of information and the operation and maintenance of repositories:

1.The methods it publishes information such as certificates, certificate status, CPS and CP

2.When information must be published and the frequency of publication

3.Access control on repositories

Article 10

A certification service provider shall specify a notification mechanism in the case of CPS modification.

Article 11

A certification service provider shall specify the following particulars in respect of financial responsibility:

1.Amount of insurance coverage provided for liability for potential and actual damages

2.Whether the operation of the certification service provider is covered by insurance

3.Whether financial audit of the certification service provider is implemented by a third party

Article 12

A certification service provider shall specify the dispute resolution procedures and governing and applicable laws to resolve disputes arising out of the certification service or certificate usage.

Article 13

A certification service provider shall specify whether subscribers can request for refund. If applicable, it shall also specify the procedures for refund.

Article 14

A certification service provider shall specify the following particulars in respect of compliance audit or other assessment:

1.Frequency of compliance audit or other assessment

2.The qualifications of the personnel performing the audit or other assessment

3.Assurance of the independence of the personnel performing the audit or other assessment

4.The scope of the compliance audit or other assessment

5.Actions taken as a result of deficiencies found during the compliance audit or other assessment

6.The parts and methods to disclose the reports of compliance audit or other assessment

Article 15

A certification service provider shall specify the types of personal information of subscribers to be protected and methods to keep the information confidential:

1.Types of information to be kept confidential

2.Relevant particulars concerning personal information protection
Chapter 2　Identification and Authentication
Article 16
A certification service provider shall specify the rules of naming it adopts.
Article 17
A certification service provider shall specify the methods to prove the applicant’s possession of private key that corresponds to the registered public key.
Article 18
A certification service provider shall specify the identification and authentication requirements and procedures for applicants.
Article 19
A certification service provider shall specify a secure identification and authentication procedure for a revocation or suspension request.
Chapter 3　Operational Requirements
Article 20
A certification service provider shall specify the procedures to process applications for various certificates.
Article 21
A certification service provider shall specify conduct of subscribers constituting acceptance of the certificate in respect of certificate issuance, renewal, and modification.
Article 22
A certification service provider that provides certificate suspension service shall specify the following particulars:
1.Circumstances under which a certificate may be suspended upon request
2.Circumstances under which a certificate may be suspended by certification service provider
3.Who can request the suspension of a certificate
4.Procedures to request certificate suspension
5.How long the suspension may last
6.The time within which certification service provider must process the suspension request
7.Procedures to restore certificate usage
Article 23
A certification service provider shall specify the following particulars in respect of certificate revocation:
1.Circumstances under which a certificate may be revoked upon request
2.Circumstances under which a certificate shall be revoked by certification service provider
3.Who can request the revocation of the certificate
4.Procedures used for certificate revocation request
5.The time within which certification service provider must process the revocation request
6.Issuance frequency of a CRL made by the certification service provider
7.On-line revocation/status checking availability
Chapter 4　Non-Technical Security Controls
Article 24
A certification service provider shall specify the physical, procedural, and personnel security controls it adopts.
Article 25
A certification service provider shall specify the following particulars in respect of archival records:
1.Types of records that are archived, which shall include all data information necessary for certificate verification
2.Retention period for an archive
3.Protection of an archive
4.Archive backup procedures
5.Requirements for time-stamping of records
6.Management frequency of archived record
Article 26
A certification service provider shall specify the following procedures for key changeover:
1.For certificate verification, the procedures of certifying the new public key with the old public key

2.The methods to provide a new public key
Article 27
A certification service provider shall specify the plan relating to the recovery procedures in the event of compromise or disaster.
Article 28
A certification service provider shall specify the following procedures for termination of any certification service:
1.Procedures for notification and publication
2.Arrangements for the currently valid certificates
3.The transfer of archival records or the retention period
Chapter 5　Technical Security Controls
Article 29
A certification service provider shall specify the following particulars in respect of key pair generation and installation:
1.Who generates the public, private key pair of subscribers
2.Where the private key is not generated by the subscriber, how is it provided securely to the subscriber
3.How is the certification service provider's public key provided securely to subscribers or relying parties
4.Key sizes
5.Key parameters generation and the parameter quality checking
6.Keys usage purposes
Article 30
A certification service provider shall specify the following particulars in respect of private key protection:
1.Whether cryptographic module meets certain standards
2.Whether the private key is under n out of m multi-person control
3.Whether the private key is escrowed, backed up, archived, or transferred and stored in a cryptographic module; if applicable, what methods and procedures are
4.Methods of activating, deactivating, and destroying the private key
Article 31
A certification service provider shall specify the operational period of the certificates, whether the public key is archived, and the usage periods for the key pair.
Article 32
A certification service provider shall specify the protection mechanism of activation data.
Article 33
A certification service provider shall specify measures for software system and network security controls.
Chapter 6　Certificate Profile
Article 34
A certification service provider shall specify the following particulars in respect of certificate profile:
1.Version numbers
2.Certificate extensions
3.Algorithm object identifiers
4.Name forms
5.Name constraints
6.CP OIDs
7.Usage of policy constraints extension
8.Processing semantics for the critical CP extension
Article 35
A certification service provider shall specify the following particulars in respect of CRL profile:
1.Version numbers
2.CRL and CRL entry extensions
Article 36
These Regulations shall come into force from the date of their promulgation.