|  |  |
| --- | --- |
| **MINISTRY OF INFORMATION AND COMMUNICATIONS**No. 6 /2015/TT-BTTTT | **SOCIALIST REPUBLIC OF VIET NAM****Independence – Freedom – Happiness***Ha Noi, March 23rd, 2015* |

**Circular**

**Defininga list of mandatory standards applicableto digital signature and digital signature authentication service**

*Pursuant to the Law on Electronic Transaction dated November 29th, 2005;*

*Pursuant to Decree No. 26/2007/NĐ*-*CP dated February 15th, 2007 by the Government detailing the implementation of the Law on Electronic Transaction regarding digital signature and digital signature authentication service, Decree No. 106/2011/NĐ*-*CP dated November 23rd, 2011 and Decree No.170/2013/NĐ*-*CP dated November 13th, 2013;*

*Pursuant to Decree No. 132/2013/ND-CP dated October 16th, 2013 by the Government defining functions, tasks, entitlements and organizational structure of the Ministry of Information and Communications;*

*In consideration of the proposal of General Director of Department of Science and Technology,*

*The Minister of Information and Communications hereby promulgates the Circular defining a list of mandatory standards applicable to digital signature and digital signature authentication service.*

**Article 1. Scope of regulation**

This Circular defines a list of mandatory standards applicable to digital signature and digital signature authentication service (Appendix enclosed).

**Article 2.** **Subject of application**

This Circular is applicable to:

1. Organizations providing the national digital signature authentication service;
2. Organizations providing the public digital signature authentication service;
3. Organizations providing the specialized digital signature authentication service granted a certificate of qualification for digital signature safety by the Ministry of Information and Communications;
4. Organizations providing the foreign digital signature authentication service granted a certificate of recognition by the Ministry of Information and Communications;

**Article 3.Organization of implementation**

1. According to every period, the Ministry of Information and Communications considers, revises, supplements the List of mandatory standards applicable to digital signature and digital signature authenticationservice defined at Article 1 of this Circular in line with the development of technology and the State managing policies.
2. Department of Science and Technology is responsible for presiding periodical check and updating the List of mandatory standards applicable to digital signature and digital signature authentication service defined at Article 1 of this Circular.
3. The National Electronic Authentication Centre is responsible for instructing the application of standards under the List of mandatory standards applicable to digital signature and digital signature authentication service defined at Article 1 of this Circular.

**Article 4.Provision of implementation**

1. This Circular comes into effect on September 15th, 2015.
2. Decision No.59/2008/QĐ-BTTTT on December 31st, 2008 of the Minister of Information and Communications promulgating the List of mandatory standards applicable to digital signature and digital signature authentication service expires as from the date of this effectiveness, except that the regulation on “Security Hash” at item 2.3 of the List of mandatory standards applicable to digital signature and digital signature authentication service enclosed to Decision No.59/2008/QĐ-BTTTT continues its effectiveness until March 31st, 2016.
3. In case of any difference between the regulation of this Circular and the regulation of Circular No.22/2013/TT-BTTTT on December 23rd, 2013 that promulgates a list of technical standards on information technology in the State agencies in the same standard relating to using digital signature and digital signature authentication service provided by organizations providing digital signature authentication servicein the State agencies, the regulation of this Circular will prevail.
4. Chief of Office, Director General of Department of Science and Technology,Director of National Electronic Authentication Centre, heads of agencies, units affiliated to the Ministry,organizations and individuals related are responsible for the implementation of this Circular.
5. In the performance, if having further queries, agencies, organizations, and individuals are advised to reflect to the Ministry of Information and Communications timely for review, settlement./.

|  |  |
| --- | --- |
| ***Recipients:**** Prime Minister, Deputy Prime Ministers;
* Office of the Party Central Committee;
* Office of the General Secretary;
* Office of the National Assembly;
* Office of the Government;
* National Commission for Application of Information Technology;
* Steering committee on Information Technology of the Party agency;
* Central Committee of Vietnam Fatherland Front;
* Central agency of organizations;
* Supreme people’s procuracy;
* Supreme people’s court;
* State Audit of Vietnam;
* Ministries and Ministerial-level agencies, Government agencies;
* People’s committees of provinces, cities under central authority;
* IT units of Ministries, Ministerial-level agencies, Government agencies;
* People’s committees and Departments of Information and Communications of provinces, cities under central authority;
* Organizations providing digital signature authentication service;
* Bureau of Legal Normative Documents Post-Review (Ministry of Justice);
* Gazette, Government Portal;
* Ministry of information and Communications:

+ Minister and Deputy Ministers;+ Agencies, units under Ministry;+ Ministry Portal;* Telecom enterprises;
* Achieves: filling, Science & Technology (5b).
 | **MINISTER***(Signed)***Nguyen Bac Son** |

**Appendix**

**list of mandatory standards applicable to digital signature and digital signature authentication service**

*(Enclosed to Circular No.6/2015/TT-BTTTT dated March 23rd,, 2015 of the Minister of Information and Communications)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Type of standard | Symbol of standard | Full name of standard | Applicable requirement |
| 1 | Security standard for HSM and cryptographic card  |
| 1.1 | Security Requirements for HSM hardware security block | FIPS PUB 140-2 | Security Requirements for Cryptographic Modules | - Minimum requirement (level 3) |
| 1.2 | Security Requirements for Token và Smart card | FIPS PUB 140-2 | Security Requirements for Cryptographic Modules | - Minimum requirement (level 2) |
| 2 | Cryptography Standard and digital signature |
| 2.1 | Non-symmetric cryptography and digital signature  | PKCS #1 | RSA Cryptography Standard | * Version 2.1
* Apply

rsAes-oaep schema for code and RSASSA-PSS for signature |
| 2.2 | Symmetric cryptography | TCVN7816:2007(FIPS PUB 197) | Information Technology - Cryptography Technique – AES data encryption algorithm  | Apply one of two standards  |
|  |  | NIST 800-67 | Recommendation for the Triple Data Encryption Algorithem (TDEA) Block Cipher |  |
| 2.3 | Secure Hash | FIPS PUB 180-4 | Secure Hash Standard | Apply one of six hashes:SHA-224,SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 |
| No. | Type of standard | Symbol of standard | Full name of standard | Applicable requirement |
| 3 | Data, information standard  |
| 3.1 | Digital certificate format and Revocation List | RFC 5280 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |  |
| 3.2 | Cryptographic Message Syntax | PKCS #7 | Cryptographic Message Syntax Standard | Version 1.5 |
| 3.3 | Private-Key Information Syntax | PKCS #8 | Private-Key Information Syntax Standard | Version 1.2 |
| 3.4 | Certification Request Syntax | PCKS #10 | Certification Request Syntax Standard | Version 1.7 |
| 3.5 | Exchange interface to Cryptographic cards  | PKCS #11 | Cryptographic token interface standard | Version 2.20 |
| 3.6 | Personal Information Exchange Syntax | PKCS #12 | Personal Information Exchange Syntax Standard | Version 1.0 |
| 4 | Policy standard and digital signature certification practices |
|  | Certificate Policy and Certification Practices Framework | RFC 3647 | Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework |  |
| 5 | Digital certificate access and storage protocol standard  |
| 5.1 | Directory Access Protocol Schema | RFC 2587 | Internet X.509 Public Key Infrastructure LDAPv2 Schema | Apply one of two standards |
| RFC 4523 | Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Type of standard | Symbol of standard | Full name of standard | Applicable requirement |
| 5.2 | Directory Access Protocol | RFC 2251 | Lightweight Directory Access Protocol (v3) | Apply RFC 2251 standard or a set of four standards:RFC 4510,RFC 4511,RFC 4512,RFC 450 |
| RFC 4510 | Lightweight Directory Access Protocol (LdAp): Technical Specification Road Map |
| RFC 4511 | Lightweight Directory Access Protocol (LDAP): The Protocol |
| RFC 4512 | Lightweight Directory Access Protocol (LDAP): Directory Information Models |
| RFC 4513 | Lightweight Directory Access Protocol (LdAp): Authentication Methods and Security Mechanisms |
| 6 | Digital certificate status standard  |
| 6.1 | Digital certificate transmitting-receiving protocol and Digital certificate Revocation List | RFC 2585 | Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP | Apply one of two protocols FTP và HTTP |
| 6.2 | On-line Certificate status protocol | RFC 2560 | X.509 Internet Public Key Infrastructure - On-line Certificate status protocol |  |
| 7 | TimeStamp service standard  |
| 7.1 | Time­Stamp Protocol | RFC 3161 | Internet X.509 Public Key Infrastructure - Time­Stamp Protocol (TSP) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Type of standard | Symbol of standard | Full name of standard | Applicable requirement |
| 7.2 | Time­Stamp service | TCVN 7818­1:2007 (ISO/IEC 18014­1:2002) | Information Technology - Cryptography Technique - Time­Stamp service - Part 1: General Frame | Apply a set of three standards:TCVN 7818­1:2007TCVN 7818­2:2007TCVN 7818­3:2010 |
| TCVN 7818­2:2007 (ISO/IEC 18014 - 2: 2002) | Information Technology - Cryptography Technique - Time­Stamp service - Part 2: Independent card creation regulations  |
| TCVN 7818­3:2010 (ISO/IEC 18014­3: 2009) | Information Technology - Cryptography Technique - Time­Stamp service - Part 3: Link card creation regulations |