|  | **Standard type** | **Standard notation** | **The full name of the standard** | **Regulations apply** |
| --- | --- | --- | --- | --- |
| **1** | **Standard cryptography and digital signature** | | | |
| 1.1 | Asymmetric cryptography and digital signature | PKCS #1 | RSA Cryptography Standard | - Apply one of two standards:  - For RSA standards:  + Version 2.1  + Apply the             RSAES-OAEP schema for encryption and RSASSA-PSS for signing.  - For ECDSA standard: The minimum key length is 256 bits. |
| ANSI X9.62-2005 | Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) |
| 1.2 | Symmetric code | TCVN 7816: 2007  (FIPS PUB 197) | Information technology - Cryptographic techniques - AES data encryption algorithm | Apply one of the two standards |
| NIST 800-67 | Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher |
| 1.3 | Safe hash function | FIPS PUB 180-4 | Secure Hash Standard | Apply one of six hash functions: SHA-224,                       SHA-256, SHA-384, SHA-512, SHA-512/224,  SHA-512/256 |
| **2** | **Standard information and data** | | | |
| 2.1 | Format of digital certificate and revocation list of digital certificates | RFC 5280 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |  |
| 2.2 | Syntax of cryptographic message | PKCS #7 | Cryptographic Message Syntax Standard | Version 1.5 |
| 2.3 | Syntax of private key information | PKCS #8 | Private-Key Information Syntax Standard | Version 1.2 |
| 2.4 | Syntax requires authentication | PCKS #10 | Certification Request Syntax Standard | Version 1.7 |
| 2.5 | Interfaces with cryptographic cards | PKCS #11 | Cryptographic token interface standard | Version 2.20 |
| 2.6 | Syntax of exchanging personal information | PKCS #12 | Personal Information Exchange Syntax Standard | Version 1.0 |
| **3** | **Policy standards and regulations for digital signature authentication** | | | |
|  | Certification framework and deed policy | RFC 3647 | Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework |  |
| **4** | **Standard protocol for storing and retrieving digital certificates** | | | |
| 4.1 | Directory Access Protocol Schema | RFC 2587 | Internet X.509 Public Key Infrastructure LDAPv2 Schema | Apply one of the two standards |
| RFC 4523 | Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates |
| 4.2 | Directory access protocol | RFC 2251 | Lightweight Directory Access Protocol (v3) | Application of RFC 2251 standard or set of four standards:                          RFC 4510, RFC 4511, RFC 4512, RFC 4513 |
| 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 |
| **5** | **Standard check status of digital certificates** | | | |
| 5.1 | The protocol for transmitting and receiving digital certificates and the list of digital certificates is revoked | RFC 2585 | Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP | Apply one or both FTP and HTTP protocols |
| 5.2 | Protocol for checking the status of digital certificates online | RFC 2560 | X.509 Internet Public Key Infrastructure - On-line Certificate status protocol |  |
| **6. Standard system of devices for managing secret keys, digital certificates and creating digital signatures according to the mobile digital signature model (Mobile PKI)** | | | | |
| 6.1 | Security requirements for SIM cards | FIPS PUB 140-2 | Security Requirements for Cryptographic Modules | - Apply one of two standards.  - For FIPS PUB 140-2 standard: Minimum level 2 requirement (level 2)  - For ISO / IEC 15408 standard: Minimum requirement of level 4 (level 4) |
| Common Criteria (ISO/IEC 15408) | Common Criteria for Information Technology Security Evaluation |
| 6.2 | Functional and professional requirements | ETSI TR 102 203 | Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements | Version V1.1.1 |
| 6.3 | Web service interface | ETSI TS 102 204 | Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface | Version V1.1.4 |
| 6.4 | Security frame | ETSI TR 102 206 | Mobile Commerce (M-COMM);  Mobile Signature Service;  Security Framework | Version V1.1.3 |
| 6.5 | Roaming specifications | ETSI TS 102 207 | Mobile Commerce (M-COMM);  Mobile Signature Service;  Specifications for Roaming in Mobile Signature Services | Version V1.1.3 |
| **7. Standard system of devices for managing secret keys, digital certificates and creating digital signatures according to the Remote Signing model** | | | | |
| 7.1 | Policy and security requirements for digital signature servers | ETSI TS 119 431-1 | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev | The whole standard of 2 parts is applied;  Version V1.1.1 (2018-12) |
| ETSI TS 119 431-2 | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation |
| 7.2 | Digital signature creation protocol | ETSI TS 119 432 | Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation | Version V1.1.1  (2019-03) |
| 7.3 | The signing application on the digital signing server | CEN EN 419 241-1 | Security Requirements for Trustworthy Systems Supporting Server Signing; |  |
| 7.4 | Required for the digital signing module | CEN EN 419 241-2 | Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing | Version V0.16 |
| 7.5 | Security requirements for HSM hardware security block | CEN IN 419 221-5 | Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services | Version V0.15  (2016-11) |