ISO 17090-3:2021 (E)

Health informatics — Public key infrastructure — Part 3: Policy management of certification authority

Contents

7.3.3.2 Re-key after revocation
7.3.3.2.1 CA re-key after revocation
7.3.3.2.2 RA re-key after revocation
7.3.3.2.3 Certificate holder re-key after revocation
7.3.4 Identification and authentication for revocation request
7.3.4.1 CA
7.3.4.2 RA
7.3.4.3 Certificate holder
7.4 Certificate life-cycle operational requirements
7.4.1 Certificate application
7.4.1.1 Who can submit a certificate application
7.4.1.2 Enrollment process and responsibilities
7.4.2 Certificate application processing
7.4.2.1 Performing identification and authentication functions
7.4.2.2 Approval or rejection of certificate applications
7.4.2.3 Time to process certificate applications
7.4.3 Certificate issuance
7.4.3.1 CA actions during certificate issuance
7.4.3.2 Notifications to certificate holders by the CA of issuance of the certificate
7.4.4 Certificate acceptance
7.4.4.1 Conduct constituting certificate acceptance
7.4.4.2 Publication of the certificate by the CA
7.4.4.3 Notification of certificate issuance by the CA to other entities
7.4.5 Key pair and certificate usage
7.4.5.1 Certificate holder private key and certificate usage
7.4.5.2 Relying party public key and certificate usage
7.4.6 Certificate renewal
7.4.6.1 Circumstances for certificate renewal
7.4.6.2 Who may request renewal
7.4.6.3 Processing certificate renewal requests
7.4.6.4 Notification to certificate holder of certificate renewal
7.4.6.5 Conduct constituting acceptance of a renewal certificate
7.4.6.6 Publication of the renewal certificate by the CA
7.4.6.7 Notification of certificate renewal by the CA to other entities
7.4.7 Certificate re-key
7.4.8 Certificate modification
7.4.8.1 Circumstances for certificate modification
7.4.8.2 Who may request certificate modification
7.4.8.3 Processing certificate modification requests
7.4.8.4 Notification to certificate holder of modified certificate issuance
7.4.8.5 Conduct constituting acceptance of a modified certificate
7.4.8.6 Publication of the modified certificate by the CA
7.4.8.7 Notification of modified certificate issuance by the CA to other entities
7.4.9 Certificate revocation and suspension
7.4.9.1 Circumstances for revocation
7.4.9.2 Who can request revocation
7.4.9.3 Procedure for revocation request
7.4.9.4 Revocation request grace period
7.4.9.5 Time within which a CA must process the revocation request
7.4.9.6 Revocation checking requirements for relying parties
7.4.9.7 CRL issuance frequency
7.4.9.8 Maximum latency for CRLs
7.4.9.9 On-line revocation/status checking availability
7.4.9.10 On-line revocation checking requirements
7.4.9.11 Other forms of revocation advertisements available
7.4.9.12 Special requirements regarding key compromise
7.4.9.13 Circumstances for suspension
7.4.9.14 Who can request suspension
7.4.9.15 Procedures for suspending certificates
7.4.9.16 Limits on suspension period
7.4.9.17 Notification of certificate suspension
7.4.10 Certificate status services
7.4.10.1 Operational characteristics
7.4.10.2 Service availability

Page count: 34