ISO 17090-3:2021 (E)

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

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviations

5 Requirements for digital certificate policy management in a healthcare context

5.1 General
5.2 Need for a high level of assurance
5.3 Need for a high level of infrastructure availability
5.4 Need for a high level of trust
5.5 Need for Internet compatibility
5.6 Need to facilitate evaluation and comparison of CPs

6 Structure of healthcare CPs and healthcare CPSs

6.1 General requirements for CPs
6.2 General requirements for CPSs
6.3 Relationship between a CP and a CPS
6.4 Applicability

7 Minimum requirements for a healthcare CP

7.1 General requirements
7.2 Publication and repository responsibilities
7.2.1 Repositories
7.2.2 Publication of certification information
7.2.3 Frequency of publication
7.2.4 Access controls on repositories
7.3 Identification and authentication
7.3.1 Initial registration
7.3.1.1 Types of name
7.3.1.2 Need for names to be meaningful
7.3.1.3 Anonymity or pseudonymity
7.3.1.4 Rules for interpreting various name forms
7.3.1.5 Uniqueness of names
7.3.1.6 Recognition, authentication and role of trademarks
7.3.2 Initial identity validation
7.3.2.1 Method to prove possession of private key
7.3.2.2 Authentication of identity of organizations
7.3.2.3 Authentication of identity of individuals
7.3.2.4 Non-verified subscriber information
7.3.2.5 Validation of authority
7.3.2.6 Criteria for interoperation
7.3.3 Identification and authentication for re-keying requests
7.3.3.1 Identification and authentication for routine re-key
7.3.3.1.1 CA routine re-keying
7.3.3.1.2 RA routine re-keying
7.3.3.1.3 Certificate holder routine re-keying

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

7.4.10.3 Operational features
7.4.11 End of subscription
7.4.12 Private key escrow
7.5 Physical controls
7.5.1 General
7.5.2 Physical controls
7.5.3 Procedural controls
7.5.4 Personnel controls
7.5.5 Security audit logging procedures
7.5.6 Record archive
7.5.6.1 General
7.5.6.2 Types of record archived
7.5.6.3 Retention period for archive
7.5.7 Key changeover
7.5.8 Compromise and disaster recovery
7.5.9 CA termination
7.6 Technical security controls
7.6.1 Key pair generation and installation
7.6.1.1 Key pair generation
7.6.1.2 Private key delivery to certificate holder
7.6.1.3 Public key delivery to certificate issuer
7.6.1.4 CA public key delivery to relying parties
7.6.1.5 Key sizes
7.6.1.6 Public key parameter generation and quality checking
7.6.1.7 Key usage purposes in accordance with the X.509 v3 key usage field
7.6.2 Private key protection
7.6.2.1 General
7.6.2.2 Cryptographic module standards and controls
7.6.2.3 Private key (n out of m) multi-person control
7.6.2.4 Private key escrow
7.6.2.5 Private key backup
7.6.2.6 Private key archive
7.6.2.7 Private key transfer into or from a cryptographic module
7.6.2.8 Private key storage on cryptographic module
7.6.2.9 Method of activating private key
7.6.2.10 Method of deactivating private key
7.6.2.11 Method of destroying private key
7.6.2.12 Cryptograhic Module Rating
7.6.3 Other aspects of key management
7.6.3.1 Public key archive
7.6.3.2 Certificate operational periods and key pair usage periods
7.6.3.3 Restrictions on CA's private key use
7.6.4 Activation data
7.6.5 Computer security controls
7.6.6 Life-cycle technical controls
7.6.7 Network security controls
7.6.8 Time stamping
7.7 Certificate, CRL and OCSP profiles
7.8 Compliance audit
7.8.1 General
7.8.2 Frequency of CA compliance audit
7.8.3 Identity/qualifications of auditor
7.8.4 Auditor's relationship to audited party
7.8.5 Topics covered by audit
7.8.6 Actions taken as a result of deficiency
7.8.6.1 General
7.8.6.2 Critical failure category
7.8.6.3 Major failure category
7.8.6.4 Partial failure category
7.8.6.5 Minor failure category
7.8.7 Communication of audit results
7.9 Other business and legal matters
7.9.1 Fees
7.9.2 Financial responsibility

7.9.3 Confidentiality of business information
7.9.4 Privacy of personal information
7.9.4.1 Privacy plan
7.9.4.2 Information treated as private
7.9.4.3 Information not deemed private
7.9.4.4 Responsibility to protect confidential information
7.9.4.5 Notice and consent to use private information
7.9.4.6 Disclosure pursuant to judicial or administrative process
7.9.4.7 Other information release circumstances — Disclosure upon certificate holder's request

7.9.5 Intellectual property rights
7.9.6 Representations and warranties
7.9.6.1 General
7.9.6.2 CA representations and warranties
7.9.6.3 RA representations and warranties
7.9.6.4 Certificate holder representations and warranties
7.9.6.5 Relying party representations and warranties
7.9.7 Disclaimers of warranties
7.9.8 Limitations of liability
7.9.8.1 Limitations of CA liability
7.9.8.2 Limitations of RA liability
7.9.8.3 Limitations of certificate holder liability
7.9.9 Indemnities
7.9.10 Term and termination
7.9.11 Individual notices and communication with participants
7.9.12 Amendments
7.9.12.1 Procedure for amendment
7.9.12.2 Notification mechanism and period
7.9.12.3 Circumstance under which OID must be changed
7.9.13 Dispute resolution procedures
7.9.14 Governing law
7.9.15 Compliance with applicable law
7.9.16 Miscellaneous provisions
7.9.16.1 Entire agreement
7.9.16.2 Assignment
7.9.16.3 Severability
7.9.16.4 Enforcement

8 Model PKI disclosure statement

8.1 Introduction
8.2 Structure of PKI disclosure statement

Page count: 34