INTERNATIONAL STANDARD

ISO 17090-3

Second edition
2021-03

Health informatics — Public key infrastructure —

Part 3: Policy management of certification authority

Informatique de santé — Infrastructure de clé publique —
Partie 3: Gestion politique d'autorité de certification

Reference number
ISO 17090-3:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviations **1**
5 Requirements for digital certificate policy management in a healthcare context **2**
5.1 General 2
5.2 Need for a high level of assurance 2
5.3 Need for a high level of infrastructure availability 2
5.4 Need for a high level of trust 2
5.5 Need for Internet compatibility 3
5.6 Need to facilitate evaluation and comparison of CPs 3
6 Structure of healthcare CPs and healthcare CPSs **3**
6.1 General requirements for CPs 3
6.2 General requirements for CPSs 4
6.3 Relationship between a CP and a CPS 4
6.4 Applicability 4
7 Minimum requirements for a healthcare CP **5**
7.1 General requirements 5
7.2 Publication and repository responsibilities 5
7.2.1 Repositories 5
7.2.2 Publication of certification information 5
7.2.3 Frequency of publication 5
7.2.4 Access controls on repositories 5
7.3 Identification and authentication 6
7.3.1 Initial registration 6
7.3.2 Initial identity validation 7
7.3.3 Identification and authentication for re-keying requests 8
7.3.4 Identification and authentication for revocation request 8
7.4 Certificate life-cycle operational requirements 9
7.4.1 Certificate application 9
7.4.2 Certificate application processing 10
7.4.3 Certificate issuance 10
7.4.4 Certificate acceptance 11
7.4.5 Key pair and certificate usage 11
7.4.6 Certificate renewal 12
7.4.7 Certificate re-key 13
7.4.8 Certificate modification 13
7.4.9 Certificate revocation and suspension 14
7.4.10 Certificate status services 17
7.4.11 End of subscription 18
7.4.12 Private key escrow 18
7.5 Physical controls 18
7.5.1 General 18
7.5.2 Physical controls 18
7.5.3 Procedural controls 18
7.5.4 Personnel controls 18
7.5.5 Security audit logging procedures 18
7.5.6 Record archive 18
7.5.7 Key changeover 19
7.5.8 Compromise and disaster recovery 19