

ISO 17090-1:2013-05 (E)

Health informatics - Public key infrastructure - Part 1: Overview of digital certificate services

Contents	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 Healthcare context terms	1
3.2 Security services terms	3
3.3 Public key infrastructure related terms	6
4 Abbreviations	9
5 Healthcare context	9
5.1 Certificate holders and relying parties in healthcare	9
5.2 Examples of actors	10
5.3 Applicability of digital certificates to healthcare	11
6 Requirements for security services in healthcare applications	12
6.1 Healthcare characteristics	12
6.2 Digital certificate technical requirements in healthcare	13
6.3 Healthcare-specific needs and the separation of authentication from data encipherment	14
6.4 Health industry security management framework for digital certificates	14
6.5 Policy requirements for digital certificate issuance and use in healthcare	14
7 Public key cryptography	15
7.1 Symmetric vs. asymmetric cryptography	15
7.2 Digital certificates	15
7.3 Digital signatures	15
7.4 Protecting the private key	16
8 Deploying digital certificates	17
8.1 Necessary components	17
8.2 Establishing identity using qualified certificates	18
8.3 Establishing speciality and roles using identity certificates	18
8.4 Using attribute certificates for authorisation and access control	19
9 Interoperability requirements	20
9.1 Overview	20
9.2 Options for deploying healthcare digital certificates across jurisdictions	20
9.3 Option usage	22
Annex A (informative) Scenarios for the use of digital certificates in healthcare	23
Bibliography	38