

ISO 17090-2:2015-11 (E)

Health informatics - Public key infrastructure - Part 2: Certificate profile

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	1
5	Healthcare CPs	2
5.1	Certificate types required for healthcare	2
5.2	CA certificates	2
5.2.1	Root CA certificates	2
5.2.2	Subordinate CA certificates	2
5.3	Cross/Bridge certificates	3
5.4	End entity certificates	3
5.4.1	Individual identity certificates	3
5.4.2	Organization identity certificate	4
5.4.3	Device identity certificate	4
5.4.4	Application certificate	4
5.4.5	AC	4
5.4.6	Role certificates	5
6	General certificate requirements	6
6.1	Certificate compliance	6
6.2	Common fields for each certificate type	6
6.3	Specifications for common fields	7
6.3.1	General	7
6.3.2	Signature	8
6.3.3	Validity	8
6.3.4	Subject public key information	8
6.3.5	Issuer name field	9
6.3.6	The subject name field	10
6.4	Requirements for each healthcare certificate type	11
6.4.1	Issuer fields	11
6.4.2	Subject fields	11
7	Use of certificate extensions	14
7.1	General	14
7.2	General extensions	14
7.2.1	authorityKeyIdentifier	14
7.2.2	subjectKeyIdentifier	14
7.2.3	keyUsage	14
7.2.4	privateKeyUsagePeriod	14
7.2.5	certificatePolicies	14
7.2.6	subjectAltName	14
7.2.7	basicConstraints	15
7.2.8	CRLDistributionPoints	15
7.2.9	ExtKeyUsage	15

7.2.10	Authority information access	15
7.2.11	Subject information access	15
7.3	Special subject directory attributes	15
7.3.1	hcRole attribute	15
7.3.2	subjectDirectoryAttributes	17
7.4	Qualified certificate statements extension	17
7.5	Requirements for each health industry certificate type	17
7.5.1	Extension fields	17
Annex A (informative) Certificate profile examples		19
Bibliography		31