

ISO/IEC 27099:2022-07 (E)

Information technology - Public key infrastructure - Practices and policy framework

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	8
5	Public key infrastructure (PKI) general concepts	8
5.1	General	8
5.2	What is PKI?	9
5.2.1	General	9
5.2.2	Public key infrastructure process flow	10
5.3	Use of PKI Service components within example business flows	10
5.3.1	General	10
5.3.2	Illustration of certificate application in a contractual PKI environment	10
5.4	Certification authority (CA)	13
5.5	Business perspectives	14
5.5.1	General	14
5.5.2	Business risks	14
5.5.3	Applicability	14
5.5.4	Legal issues	14
5.5.5	Regulatory issues	14
5.5.6	Business usage issues	15
5.5.7	Interoperability issues	15
5.6	Certificate policy (CP)	16
5.6.1	General	16
5.6.2	Policy Authority and certificate policy usage	16
5.6.3	Certificate policies within a hierarchy of trust	17
5.6.4	Certificate status	18
5.7	Certification practice statement (CPS)	19
5.7.1	General	19
5.7.2	CPS creation	19
5.7.3	Purpose	19
5.7.4	Level of specificity	19
5.7.5	Approach	19
5.7.6	Audience and access	20
5.8	Agreements	20
5.9	Time-stamping	20
5.10	Trust models	21
5.10.1	Trust model considerations	21
5.10.2	Wildcard certificate considerations	24
5.10.3	Relying party considerations	24
5.11	Component services	25
5.12	PKI hierarchies and independently managed CAs	27
5.13	Root CA	27
5.13.1	General	27
5.13.2	CA relationships and PKI hierarchies	27

6	Certificate policy (CP), certification practice statement (CPS) and their relationship to information security management system (ISMS)	28
6.1	General	28
6.2	Certificate policy (CP) guidance	28
6.3	Certification practice statement (CPS) guidance	30
7	Certification authority objectives and controls	30
7.1	General	30
7.2	Certification practice statement and certificate policy management	31
7.2.1	Certificate policy management	31
7.2.2	CPS and CA management	32
7.2.3	Subscriber and relying party agreements	33
7.3	Information security	34
7.4	Asset classification and management	35
7.5	Human resources security	36
7.6	Physical and environmental security	37
7.7	Operations security	39
7.8	Access control	40
7.9	System acquisition development and maintenance	42
7.10	Business continuity management	42
7.11	Monitoring, conformance and compliance	44
7.12	Audit journal security assurance	44
7.13	CA key life cycle management controls	49
7.13.1	CA key generation	49
7.13.2	CA key storage, back-up, and recovery	50
7.13.3	CA public key distribution	52
7.13.4	CA key usage	52
7.13.5	CA key archival and destruction	53
7.13.6	CA key compromise	53
7.14	Subject key life cycle management controls	54
7.14.1	CA-provided subject key generation services (if supported)	54
7.14.2	CA-provided subject key storage and recovery services (if supported)	55
7.14.3	Hardware token life cycle management if outsourced to an external service (if supported)	56
7.14.4	Subject key management, if supported	58
7.15	Certificate life cycle management controls	59
7.15.1	Subject registration	59
7.15.2	Certificate renewal (if supported)	60
7.15.3	Certificate rekey	61
7.15.4	Certificate issuance	62
7.15.5	Certificate distribution	62
7.15.6	Certificate revocation	63
7.15.7	Certificate suspension (if supported)	63
7.15.8	Revocation status information service	65
7.15.9	Controlled CA termination	66
7.16	Root CA controls	67
7.16.1	Physical and environmental security	67
7.16.2	Operations security	67
7.16.3	Access control	68
7.16.4	Root CA key generation	68
7.16.5	Generation of root CA keys script requirements	69
7.16.6	Root CA public key distribution	69
7.16.7	Root CA key compromise	69
7.17	CA certificate life cycle management controls - subordinate CA certificate	70
	Annex A (informative) Management by certificate policy	71
	Annex B (informative) CA key generation ceremony	78
	Annex C (informative) Certification authority audit journal contents and use	82

Annex D (informative) Certificate and PKI roles 85
Annex E (informative) Changes to ISO 21188:2018 to produce ISO/IEC 27099 91
Bibliography 93