ISO 21188:2018 (E)

Public key infrastructure for financial services — Practices and policy framework

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Public key infrastructure (PKI)

5.1 General
5.2 What is PKI?
5.2.1 General
5.2.2 Public key infrastructure process flow
5.3 Business requirement impact on PKI environment
5.3.1 General
5.3.2 Illustration of certificate application in a closed environment
5.3.3 Illustration of certificate application in a contractual PKI environment
5.3.4 Illustration of certificate application in an open environment
5.4 Certification authority (CA)
5.5 Business perspectives
5.5.1 General
5.5.2 Business risks
5.5.3 Applicability
5.5.4 Legal issues
5.5.5 Regulatory issues
5.5.6 Business usage issues
5.5.7 Interoperability issues
5.5.8 Audit journal requirements
5.5.8.1 General
5.5.8.2 Security quality assurance
5.6 Certificate policy (CP)
5.6.1 General
5.6.2 Certificate policy usage
5.6.3 Certificate policies within a hierarchy of trust
5.6.4 Certificate status
5.7 Certification practice statement (CPS)
5.7.1 General
5.7.2 Authority
5.7.3 Purpose
5.7.4 Level of specificity
5.7.5 Approach
5.7.6 Audience and access
5.8 Agreements
5.9 Time-stamping
5.10 Trust models
5.10.1 Trust model considerations
5.10.2 Wildcard considerations
5.10.3 Relying party considerations
5.10.3.1 General

5.10.3.2 Certificate validation
5.10.3.3 Certificate revocation or suspension

6 Certificate policy and certification practice statement requirements

6.1 Certificate policy (CP)
6.2 Certification practice statement (CPS)

7 Certification authority control procedures

7.1 General
7.2 CA environmental controls
7.2.1 Certification practice statement and certificate policy management
7.2.2 Security management
7.2.3 Asset classification and management
7.2.4 Personnel security
7.2.5 Physical and environmental security
7.2.6 Operations management
7.2.7 System access management
7.2.8 Systems development and maintenance
7.2.9 Business continuity management
7.2.10 Monitoring and compliance
7.2.11 Audit logging
7.3 CA key life cycle management controls
7.3.1 CA key generation
7.3.2 CA key storage, back-up and recovery
7.3.3 CA public key distribution
7.3.4 CA key usage
7.3.5 CA key archival and destruction
7.3.6 CA key compromise
7.4 Subject key life cycle management controls
7.4.1 CA-provided subject key generation services (if supported)
7.4.2 CA-provided subject key storage and recovery services (if supported)
7.4.3 Integrated circuit card (ICC) life cycle management (if supported)
7.4.4 Requirements for subject key management
7.5 Certificate life cycle management controls
7.5.1 Subject registration
7.5.2 Certificate renewal (if supported)
7.5.3 Certificate rekey
7.5.4 Certificate issuance
7.5.5 Certificate distribution
7.5.6 Certificate revocation
7.5.7 Certificate suspension (if supported)
7.5.8 Certificate validation services
7.6 Controlled CA termination
7.7 CA certificate life cycle management controls – subordinate CA certificate

Annex A (informative) Management by certificate policy

A.1 Introduction and purpose of certificate policies
A.2 Definition of a certificate policy
A.3 Establishing policies in certificates
A.4 Certificate applicability under a named certificate policy
A.5 Cross-certification, certificate chains, policy mapping and certificate policies
A.5.1 Cross-certification
A.5.2 Certificate chains
A.5.3 Certificate policy mapping
A.5.4 Policy constraints
A.6 Types of certificate
A.7 Certificate classes and naming
A.8 Certificate policy provisions
A.8.1 General
A.8.2 Interpretation
A.8.3 Obligations
A.8.4 Enforcement
A.8.5 Liability
A.8.6 Operational requirements

A.9 Certificate policy management

Annex B (informative) Elements of a certification practice statement

B.1 General
B.2 Introduction
B.2.1 General
B.2.2 Overview
B.2.3 Identification
B.2.4 Community and applicability
B.2.5 Contact details
B.3 General provisions
B.3.1 General
B.3.2 Obligations
B.3.3 Liability
B.3.4 Interpretation and enforcement
B.3.5 Publication and repositories
B.3.6 Compliance audit
B.3.7 Confidentiality
B.4 Identification and authentication
B.4.1 General
B.4.2 Initial registration
B.4.3 Routine rekey
B.4.4 Rekey after revocation — no key compromise
B.4.5 Revocation request
B.4.6 Suspension request
B.5 Operational requirements
B.5.1 General
B.5.2 Certificate application
B.5.3 Certificate issuance
B.5.4 Certificate acceptance
B.5.5 Certificate suspension, revocation and status management
B.5.6 Security audit procedures
B.5.7 Records archival
B.5.8 Key changeover
B.5.9 Compromise and disaster recovery
B.5.10 CA termination
B.6 Physical, procedural and personnel security controls
B.6.1 General
B.6.2 Physical security controls
B.6.3 Procedural controls
B.6.4 Personnel security controls
B.7 Technical security controls
B.7.1 General
B.7.2 Key pair generation and installation
B.7.3 Private key protection
B.7.4 Other aspects of key pair management
B.7.5 Activation data
B.7.6 Computer security controls
B.7.7 Life cycle security controls
B.7.8 Network security controls
B.7.9 Cryptographic mechanism engineering controls
B.8 Certificate and CRL profiles
B.8.1 General
B.8.2 Certificate profile
B.8.3 CRL profile
B.8.4 OCSP profile
B.9 Practices administration
B.9.1 General
B.9.2 Change procedures
B.9.3 Publication and notification procedures
B.9.4 CP compliance

Annex C (informative) Object identifiers (OID)

C.1 Why have an OID?

C.2 What is an OID?
C.3 Registration of OIDs
C.4 Why do you need an OID and how should they be managed?

Annex D (informative) CA key generation ceremony

D.1 General
D.2 Roles and responsibilities
D.2.1 General
D.2.2 Operating system administrator
D.2.3 CA application administrator
D.2.4 Cryptographic materials custodian
D.2.5 Key shareholders
D.2.6 Master of ceremonies
D.2.7 Policy authority
D.2.8 Independent observer
D.3 CA key generation ceremony script
D.4 CA key generation ceremony procedures

Annex E (informative) Mapping of RFC 2527 to RFC 3647

Annex F (normative) Certification authority audit journal contents and use

F.1 CA and RA audit journal contents and protection
F.1.1 General
F.1.2 Elements to be included in all journal entries
F.1.3 Certificate application information to be journalized by an RA or CA
F.1.4 Events to be journalized
F.1.5 Security-sensitive events to be journalized
F.1.6 Messages and data to be journalized
F.1.7 Audit journal backup
F.1.8 Audit journal use

Annex G (informative) Alternative trust models

G.1 Introduction
G.2 Hierarchical trust model
G.3 Non-hierarchical trust model
G.4 Hybrid trust model
G.5 Certificate trust levels
G.6 Short-term certificate (STC)
G.7 Long-term certificate (LTC)
G.8 Monitoring considerations
G.8.1 General
G.8.2 Overview
G.8.3 Policy authority (PA)
G.8.4 Certificate authority (CA)
G.8.5 Registration authority (RA)
G.8.6 Subject
G.8.7 Relying party (RP)
G.8.8 Subject cryptographic mechanism provider (SCMP)

Page count: 108