ISO 21188:2006-05 (E)

Public key infrastructure for financial services - Practices and policy framework

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Abbreviated terms 8

5 Public key infrastructure (PKI) 9
5.1 General 9
5.2 What is PKI? 9
5.3 Business requirement impact on PKI environment 10
5.4 Functional perspectives 14
5.5 Business perspectives 19
5.6 Certificate policy (CP) 21
5.7 Certification practice statement (CPS) 23
5.8 Relationship between certificate policy and certification practice statement 24
5.9 Agreements 25
5.10 Time-stamping 26

6 Certificate policy and certification practice statement requirements 27
6.1 Certificate policy (CP) 27
6.2 Certification practice statement (CPS) 29

7 Certification authority control objectives 29
7.1 General 29
7.2 CA environmental control objectives 30
7.3 CA key life cycle management control objectives 32
7.4 Subject key life cycle management control objectives 33
7.5 Certificate life cycle management control objectives 34
7.6 CA certificate life cycle management controls 36

8 Certification authority control procedures 36
8.1 General 36
8.2 CA environmental controls 36
8.3 CA key life cycle management controls 51
8.4 Subject key life cycle management controls 55
8.5 Certificate life cycle management controls 60
8.6 CA certificate life cycle management controls 67

Annex A (informative) Management by certificate policy 69

Annex B (informative) Elements of a certification practice statement 78

Annex C (informative) Object identifiers (OID) 94

Annex D (informative) CA key generation ceremony 96

Annex E (informative) Mapping of RFC 2527 to RFC 3647 100

Bibliography 106