ISO 15782-1:2009-10 (E)

Certificate management for financial services - Part 1: Public key certificates

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Symbols and abbreviations 8

5 Public key infrastructure 8
5.1 Overview 8
5.2 Public key management infrastructure process flow 9
5.3 Certification Authority (CA) 9
5.4 Registration Authority (RA) 10
5.5 End entities 10

6 Certification Authority systems 10
6.1 General 10
6.2 Responsibilities in CA systems 12
6.3 Certificate life cycle requirements 15
6.4 Security quality assurance and audit requirements 29
6.5 Business continuity planning 30

7 Data elements and relationships 30

8 Public key certificate and Certificate Revocation List extensions 30

Annex A (normative) Certification Authority audit journal contents and use 31

Annex B (informative) Alternative trust models 34

Annex C (informative) Suggested requirements for the acceptance of certificate request data 40

Annex D (informative) Multiple algorithm certificate validation example 42

Annex E (informative) Certification Authority techniques for disaster recovery 44

Annex F (informative) Distribution of certificates and Certificate Revocation Lists 47

Bibliography 48