

# ISO 15782-1:2009-10 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>2</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>4</b>	<b>Symbols and abbreviations .....</b>	<b>8</b>
<b>5</b>	<b>Public key infrastructure .....</b>	<b>8</b>
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
<b>6</b>	<b>Certification Authority systems .....</b>	<b>10</b>
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
<b>7</b>	<b>Data elements and relationships .....</b>	<b>30</b>
<b>8</b>	<b>Public key certificate and Certificate Revocation List extensions .....</b>	<b>30</b>
<b>Annex A (normative) Certification Authority audit journal contents and use .....</b>		<b>31</b>
<b>Annex B (informative) Alternative trust models .....</b>		<b>34</b>
<b>Annex C (informative) Suggested requirements for the acceptance of certificate request data .....</b>		<b>40</b>
<b>Annex D (informative) Multiple algorithm certificate validation example .....</b>		<b>42</b>
<b>Annex E (informative) Certification Authority techniques for disaster recovery .....</b>		<b>44</b>
<b>Annex F (informative) Distribution of certificates and Certificate Revocation Lists .....</b>		<b>47</b>
<b>Bibliography .....</b>		<b>48</b>