

ISO/IEC 15945:2002-02 (E)

Information technology - Security techniques - Specification of TTP services to support the application of digital signatures

Contents

Page

Reference number INTERNATIONAL STANDARD 15945 First edition 2002-02-01 Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures Technologies de l'information -- Techniques de sécurité -- Spécifications des services TTP pour supporter l'application des signatures numériques PDF disclaimer This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area. Adobe is a trademark of Adobe Systems Incorporated. Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below. or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester. ISO copyright office Case postale 56 · CH-1211 Geneva 20 Tel. + 41 22 749 01 11 Fax + 41 22 749 09 47 E-mail copyright@iso.ch Web www.iso.ch CONTENTS 1 Scope 1

2	Normative references	1
2.1	Identical Recommendations	International Standards 2
2.2	Additional references	2
3	Definitions	3
4	Abbreviations	4
5	Descriptive classification of services	5
5.1	Certificate management services	5
5.2	Key management services	8
5.3	Other services	9
6	Minimal certificate and CRL profile	10
6.1	Minimal certificate profile	10
6.2	Minimal CRL profile	11
7	Certificate management messages	11
7.1	Overview of certificate management services and messages	12
7.2	Assumptions and restrictions for some of the services	15
8	Data structures for certificate management messages	19
8.1	Overall message	19
8.2	Common Data Structures	22
8.3	Data structures specific for Certificate Request Messages of type CertReq	24
8.4	Data structures specific for other messages	29
8.5	Transport protocols	32
8.6	Complete ASN.1 Module	32
9	Online Certificate Status Protocol	40
9.1	Protocol Overview	40

9.2	Functional Requirements	42
9.3	Detailed Protocol	43
9.4	ASN.1 Module for OCSP	47
Annex A - Interworking		50
Annex B - Algorithms		51
B.1	Hash Algorithms	51
B.2	Digital Signature Algorithms	51
Annex C - Bibliography		52