
**Health informatics — Public key
infrastructure —**

Part 1:
Overview of digital certificate services

Informatique de santé — Infrastructure de clé publique —

Partie 1: Vue d'ensemble des services de certificat numérique



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.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic 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.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
3.1 Healthcare context terms	2
3.2 Security services terms	3
3.3 Public key infrastructure related terms	6
4 Abbreviations	9
5 Healthcare context.....	10
5.1 Certificate holders and relying parties in healthcare.....	10
5.2 Examples of actors	10
5.3 Applicability of digital certificates to healthcare.....	12
6 Requirements for security services in healthcare applications	12
6.1 Healthcare characteristics	12
6.2 Digital certificate technical requirements in healthcare	13
6.3 Separation of authentication from encipherment	14
6.4 Health industry security management framework for digital certificates.....	15
6.5 Policy requirements for digital certificate issuance and use in healthcare	15
7 Public key cryptography	15
7.1 Symmetric vs asymmetric cryptography	15
7.2 Digital certificates	16
7.3 Digital signatures.....	16
7.4 Protecting the private key.....	16
8 Deploying digital certificates.....	17
8.1 Necessary components	17
8.2 Establishing identity using qualified certificates	18
8.3 Establishing speciality and roles using identity certificates	19
8.4 Using attribute certificates for authorization and access control	20
9 Interoperability requirements	20
9.1 Overview	20
9.2 Options for deploying healthcare digital certificates across jurisdictions	21
9.3 Option usage	22
Annex A (informative) Scenarios for the use of digital certificates in healthcare	23
Bibliography	35