
**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*





COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 Healthcare context terms	1
3.2 Security services terms	3
3.3 Public key infrastructure related terms	6
4 Abbreviations	9
5 Healthcare context	9
5.1 Certificate holders and relying parties in healthcare	9
5.2 Examples of actors	10
5.2.1 Regulated health professional	10
5.2.2 Non-regulated health professional	10
5.2.3 Patient/consumer	10
5.2.4 Sponsored healthcare provider	10
5.2.5 Supporting organization employee	10
5.2.6 Healthcare organization	10
5.2.7 Supporting organization	11
5.2.8 Devices	11
5.2.9 Applications	11
5.3 Applicability of digital certificates to healthcare	11
6 Requirements for security services in healthcare applications	12
6.1 Healthcare characteristics	12
6.2 Digital certificate technical requirements in healthcare	12
6.2.1 General	12
6.2.2 Authentication	13
6.2.3 Integrity	13
6.2.4 Confidentiality	13
6.2.5 Digital signature	13
6.2.6 Authorization	13
6.2.7 Access control	13
6.3 Healthcare-specific needs and the separation of authentication from data encipherment	14
6.4 Health industry security management framework for digital certificates	14
6.5 Policy requirements for digital certificate issuance and use in healthcare	14
7 Public key cryptography	14
7.1 Symmetric vs. asymmetric cryptography	14
7.2 Digital certificates	15
7.3 Digital signatures	15
7.4 Protecting the private key	16
8 Deploying digital certificates	17
8.1 Necessary components	17
8.1.1 General	17
8.1.2 CP	17
8.1.3 CPS	17
8.1.4 CA	17
8.1.5 RA	17
8.2 Establishing identity using qualified certificates	18
8.3 Establishing speciality and roles using identity certificates	18
8.4 Using attribute certificates for authorization and access control	19