

ISO 17090-1:2021 (E)

Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services

Contents

| | |
|-------|---|
| | Foreword |
| | Introduction |
| 1 | Scope |
| 2 | Normative references |
| 3 | Terms and definitions |
| 3.1 | Healthcare context terms |
| 3.2 | Security services terms |
| 3.3 | Public key infrastructure related terms |
| 4 | Abbreviations |
| 5 | Healthcare context |
| 5.1 | Certificate holders and relying parties in healthcare |
| 5.2 | Examples of actors |
| 5.2.1 | Regulated health professional |
| 5.2.2 | Non-regulated health professional |
| 5.2.3 | Patient/consumer |
| 5.2.4 | Sponsored healthcare provider |
| 5.2.5 | Supporting organization employee |
| 5.2.6 | Healthcare organization |
| 5.2.7 | Supporting organization |
| 5.2.8 | Devices |
| 5.2.9 | Applications |
| 5.3 | Applicability of digital certificates to healthcare |
| 6 | Requirements for security services in healthcare applications |
| 6.1 | Healthcare characteristics |
| 6.2 | Digital certificate technical requirements in healthcare |
| 6.2.1 | General |
| 6.2.2 | Authentication |
| 6.2.3 | Integrity |
| 6.2.4 | Confidentiality |
| 6.2.5 | Digital signature |
| 6.2.6 | Authorization |
| 6.2.7 | Access control |
| 6.3 | Healthcare-specific needs and the separation of authentication from data encipherment |
| 6.4 | Health industry security management framework for digital certificates |
| 6.5 | Policy requirements for digital certificate issuance and use in healthcare |
| 7 | Public key cryptography |
| 7.1 | Symmetric vs. asymmetric cryptography |
| 7.2 | Digital certificates |
| 7.3 | Digital signatures |
| 7.4 | Protecting the private key |
| 8 | Deploying digital certificates |
| 8.1 | Necessary components |
| 8.1.1 | General |
| 8.1.2 | CP |

| | |
|----------------|--|
| 8.1.3 | CPS |
| 8.1.4 | CA |
| 8.1.5 | RA |
| 8.2 | Establishing identity using qualified certificates |
| 8.3 | Establishing speciality and roles using identity certificates |
| 8.4 | Using attribute certificates for authorization and access control |
| 9 | Interoperability requirements |
| 9.1 | Overview |
| 9.2 | Options for deploying healthcare digital certificates across jurisdictions |
| 9.2.1 | General |
| 9.2.2 | Option 1 — Single hierarchy of CAs |
| 9.2.3 | Option 2 — Relying party management of trust |
| 9.2.4 | Option 3 — Cross-recognition |
| 9.2.5 | Option 4 — Cross-certification |
| 9.2.6 | Option 5 — Bridge CA |
| 9.3 | Option usage |
| Annex A | (informative) Scenarios for the use of digital certificates in healthcare |
| A.1 | Introduction |
| A.2 | Scenario explanation |
| A.3 | Services exemplified in healthcare scenarios |
| A.4 | Scenario descriptions |
| A.4.1 | Emergency department access to records |
| A.4.2 | Temporary services (emergency aid) |
| A.4.3 | Member enrolment |
| A.4.4 | Tele-imaging |
| A.4.5 | Automated results reporting to the physician |
| A.4.6 | Results reporting with practitioner messaging |
| A.4.7 | Patient-physician treatment discussion |
| A.4.8 | Patient care registry summary |
| A.4.9 | Patient-pharmacist question |
| A.4.10 | Patient-physician messaging, unstructured to specific clinician |
| A.4.11 | Remote access to a clinical information system |
| A.4.12 | Emergency access |
| A.4.13 | Remote transcription |
| A.4.14 | Electronic prescription |
| A.4.15 | Authentication of physician orders |
| A.4.16 | Potential uses of digital signatures in healthcare |