TECHNICAL SPECIFICATION

ISO/TS 27790

First edition
2009-12-01

Health informatics — Document registry framework

Informatique de santé — Cadre d'enregistrement de document

Reference number
ISO/TS 27790:2009(E)

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.

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

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 27790 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

Development and implementation of electronic health records (EHR) are rapidly progressing around the world. An appropriate deployment of EHR will enhance various aspects of healthcare delivery in the future. EHR are thought to enable the provision of essential care information to providers at point-of-care through information and telecommunications technologies. This includes a broad spectrum of capabilities including acquisition, storage, presentation, and management of patient information (represented in different digital forms such as video, audio or data) and communication of this information between care facilities with the use of communications links.

Recent development of health information exchange where the patients' EHR are accessed securely whenever necessary (sharing EHR information at point-of-care and by the consumer citizen) requires that electronic health records of an individual, although they originate from various health-related subjects distributed over space and time, remain accessible irrespective of their centralized or distributed storage. The use of centralized registry systems pointing to such records can greatly facilitate the discovery of their locations to allow effective access to the appropriate and secured EHR.

This Technical Specification describes the principles and specification of interoperability needed to support a registry system for locating and accessing records grouped into documents. The supported documents may contain any type of person-centric health information, structured or not, depending on the standard used for their content. The clinical document architecture (CDA) is one such standard that is a likely companion to this Technical Specification. This Technical Specification does not address the security and privacy considerations in detail but refers to related work in this critical area. The specification is not intended to be prescriptive either from a methodological or a technological perspective but rather to provide a coherent inclusive description of principles and practices that could facilitate the formulation of policies and governance practices locally or nationally.

Health informatics — Document registry framework

1 Scope

This Technical Specification specifies a general-purpose document registry framework for transmitting, storing and utilizing documents in clinical and personalized health environments. It is quite broad in its applicability to realise the goal of sharing health-related documents spanning a broad spectrum of health domains such as healthcare specialities covering laboratory, cardiology, eye care, etc. and the many areas of personalized health.

This web services-based registry framework includes a document registry and associated repository to allow the sharing of any form of health documents including HL7 CDA (clinical document architecture). It specializes in health, W3C Web Services Standards, ISO 15000 (ebXML registry standards) and OASIS ebXML Registry Information Model 3.0 through the use of the IHE Cross-Enterprise Document Sharing (XDS) from the Integrating the Healthcare Enterprise (IHE) Information Technology Infrastructure (ITI) technical framework, quoting from the Cross-Enterprise Document Sharing (XDS) Profile:

“The Cross-Enterprise Document Sharing IHE Integration Profile facilitates the registration, distribution and access across health enterprises of patient and citizen electronic health records. Cross-Enterprise Document Sharing (XDS) is focused on providing a standards-based specification for managing the sharing of documents between all health enterprises, ranging from private physician offices to clinics to acute care in-patient facilities to personal heath record systems. The XDS IHE Integration Profile assumes that these enterprises belong to one or more affinity domains. An affinity domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and that share a common registry infrastructure.”

This Technical Specification also supports document registration and retrieval via the federation of documents’ registries (see IHE Cross-Community Access) in terms of individual users to reduce health information extrusion possibilities.

This Technical Specification supports the sharing of documents of any standardized content in the context of healthcare and well-being. It describes the means of locating and accessing documents among a diverse set of health organizations. It is designed for leverage of existing health informatics for structuring and semantically rich health information, if so desired. It does not require the development of new health informatics standards.

This Technical Specification also references a number of companion standards-based specifications that offer optional extensions to enhance the basic capabilities offered by IHE XDS, as listed below.

1) An XDS extension supporting the fragmentation of the content of the documents into two parts: a header fragment and a body fragment. This separation scheme enhances confidentiality because the gathering of both header and body and their relational information involves cracking into multiple repository servers. This has been developed as an IHE Korean Extension on the IHE XDS Profile.

NOTE 1 The incremental effectiveness achieved by header/body separation will have to be re-evaluated once the effectiveness of the security solutions to protect data at rest (e.g. encryption) has been finalized.

2) A series of security- and privacy-related IHE profiles, such as Patient Identification Cross-Referencing (PIX), Patient Demographics Query (PDQ), Basic Patient Privacy Consent (BPPC), and Cross-Enterprise User Assertion (XUA).

NOTE 2 The use of IHE Audit trail and Node Authentication (ATNA) as well as Consistent Time (CT) is required as part of IHE XDS. These Profiles are therefore not listed above.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

OASIS Standards/ISO/TS 15000 (all parts), *Electronic business eXtensible Markup Language (ebXML)*

ebXML RIM V 3.0, OASIS ebXML Registry Information Model

ebXML RS V 3.0, OASIS ebXML Registry Service Specification

IHE IT Infrastructure Framework

IHE ITI-TF-1 IHE IT Infrastructure Technical Framework V5.0:

- Cross-enterprise Document Sharing (XDS.b) Integration profile
- Audit Trail and Node Authentication (ATNA) Integration profile
- Consistent Time (CT) Integration profile

Extensible Markup Language (XML) 1.0 W3C Recommendation, http://www.w3c.org/TR/REC-xml

SOAP Version 1.2 specification, http://www.w3.org/TR/soap12-part1/, March 2004

SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/

WSDL 1.1 Note http://www.w3.org/TR/wsdl

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. Only key terms and definitions are provided in this clause.

3.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

3.2
accountability
property that ensures that the actions of an entity may be traced uniquely to that entity

3.3
actor
user of the system-of-interest interacting with the system in a particular usage context (role)

3.4
agent
device that provides data in a manager/agent communicating system

3.5
architecture
that set of design artefacts or descriptive representations that are relevant for describing an object such that it can be produced to requirements (quality) as well as maintained over the period of its useful life (change)

3.6
archival
relating to the storage of data over a prolonged period

3.7
attestation
process of certifying and recording legal responsibility for a particular unit of information

3.8
authentication
act of verifying the claimed identity of an entity

3.9
authorization
granting of rights, including the granting of access based on access rights

3.10
availability
⟨in computer science⟩ property of data or of resources being accessible and usable on demand by an authorized entity

3.11
class
description of a set of objects that share the same attributes, methods and associations

3.12
clinical process
steps that are involved in the delivery of healthcare services to a patient/consumer

3.13
clinician
healthcare professional who delivers healthcare services directly to a patient/consumer

3.14
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

3.15
consumer
person requiring, scheduled to receive, receiving or having received a healthcare service

3.16
controller
natural or legal person, public authority, agency or any other body that, alone or jointly with others, determines the purposes and means of the processing of personal data

3.17
data aggregation
process by which information is collected, manipulated and expressed in summary form

NOTE Data aggregation is primarily performed for reporting purposes, policy development, health service management, research, statistical analysis and population health studies.

3.18
data format
arrangement of data in a file or stream

3.19
data integrity
property that data have not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989, definition 3.3.21]

3.20
data object
collection of data that have a natural grouping and may be identified as a complete entity

3.21
data structure
manner in which application entities construct the data set information resulting from the use of an information object

3.22
data subject's consent
any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

3.23
data validation
process used to determine if data are accurate, complete or meet specified criteria

3.24
Electronic health record
EHR
repository of information regarding the health status of a subject of care, in computer processable form

[ISO/TR 20514:2005, definition 2.11]

3.24.1 electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by healthcare providers, which can be distributed over a number of sites or aggregated at a particular source

NOTE The information is organized primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is stored and transmitted securely [NEHRT:2000].

3.24.2 longitudinal collection of personal health information of a single individual, entered or accepted by healthcare providers, and stored electronically

NOTE The record may be made available at any time to providers, who have been authorized by the individual, as a tool in the provision of health care services. The individual has access to the record and can request changes to its contents. The transmission and storage of the record is under strict security [OHIH:2001].

3.24.3 collection of data and information gathered or generated to record clinical care rendered to an individual

[ASTM E1769:1995]

3.24.4 comprehensive, structured set of clinical, demographic, environmental, social, and financial data and information in electronic form, documenting the health care given to a single individual

[ASTM E1769:1995]

3.24.5 healthcare record in computer-readable format

NOTE Definitions 3.21 to 3.26 of ISO 13606-1:2008 provide further information.

3.24.6 electronic patient record that resides in a system designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge, and other aids

[IOM:1991]

3.24.7 virtual compilation of non-redundant health data about a person across a lifetime, including facts, observations, interpretations, plans, actions and outcomes

NOTE Health data include information on allergies, history of illness and injury, functional status, diagnostic studies, assessments, orders, consultation reports, treatment records, etc. Health data also include well-being data such as immunization history, behavioural data, environmental information, demographics, health insurance, administrative data for care delivery processes and legal data such as consents.

3.25
encounter
patient contact
contact between a clinician and patient

3.26
event
change in device status that is communicated by a notification reporting service

3.27
framework
logical structure for classifying and organizing complex information

3.28
generalization
taxonomic relationship between a more general element and a more specific element

3.29
healthcare professional
person who is authorized by a nationally recognized body to be qualified to perform certain health duties

3.30
host system
term used as an abstraction of a medical system to which measurement devices are attached

3.31
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

3.32
information model
structured specification of the information requirements of a project

3.33
information object
provision of an abstract data model applicable to the communication of vital signs information and related patient data

NOTE The attributes of an information object definition describe its properties. Each information object definition does not represent a specific instance of real-world data, but rather a class of data that share the same properties.

3.34
inheritance
mechanism by which more specific elements incorporate structure and behaviour of more general elements

3.35
instance
realization of an abstract concept or specification

EXAMPLES Object instance, application instance, information service element instance, VMD instance, class instance, operating instance.

3.36
integrity
property of data whose accuracy and consistency are preserved regardless of changes made

3.37
interaction
combination of the specific elements that are needed to support the functional requirements defined within the use case model

3.38
interchange format
representation of the data elements and the structure of the message containing those data elements while in transfer between systems

NOTE The interchange format consists of a data set of construction elements and a syntax. The representation is technology-specific.

3.39
interoperability
ability of two or more systems or components to exchange information and to use the information that has been exchanged

[IEEE Standard Computer Dictionary]

3.40
latency
⟨communications⟩ time delay between the sending of a signal from one device and its reception by another device

3.41
manager
device that receives data in a manager/agent communicating system

3.42
medical device
device, apparatus or system used for patient monitoring, patient treatment or therapy, which does not normally enter metabolic pathways

NOTE For the purposes of this document, the scope of medical devices is further limited to those patient-connected medical devices which provide support for electronic communications.

3.43
message element
unit of structure within a message type

3.44
message type
organization of message elements that is specified in a hierarchical message definition

3.45
model
abstraction used to express the relevant concepts and interdependencies of a project

3.46
object
instance of a class

3.47
object attributes
data that, together with methods, define an object

3.48
object class
descriptor used in association with a group of objects with similar properties (attributes), common behaviour (operations), common relationships to other objects and common semantics

3.49
object diagram
diagram showing connections between objects in a system

3.50
object method
procedure or process acting upon the attributes and states of an object class

3.51
object-oriented analysis
method of analysis where the problem domain is modelled in the form of objects and their interactions

3.52
operation
function or transformation that may be applied to or by objects in a class

NOTE Sometimes also called service.

3.53
participants
data exporters and data importers

3.54
patient
individual person who is a subject of care

3.55
personal health data
any personal data relevant to the health of an identified or identifiable natural person

3.56
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

3.57
processing of personal data
processing
any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use

3.58
processor
natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller

3.59
protocol
standard set of rules describing the transfer of data between devices, specifying the format of the data and the signals to start, control and end the transfer

3.60
record
collection of data

3.61
record entry
semantically indivisible clinical statement that may be structurally large or small, but which loses meaning if broken up

3.62
reference information model
single information model that covers the domain of activity being addressed by a standards developing organization using this methodology

3.63
registry
collection of all the official records relating to something, or the place where they are kept

3.64
repository
place where something is safely kept

3.65
scenario
statement of healthcare-relevant events defined as a sequence of interactions

3.66
security
combination of confidentiality, integrity and availability

3.67
semantic interoperability
ability for data shared by systems to be understood at the level of formally defined domain concepts

3.68
service
specific behaviour that a communication party in a specific role is responsible for exhibiting

3.69
specialization
definition of a concept or class subordinate to a general concept or class

3.70
standards developing organization
any organization one of whose functions is to create and/or publish standards

3.71
subject of care
one or more persons scheduled to receive, receiving, or having received a healthcare service

3.72
system
demarcated part of the perceivable universe, existing in time and space, that may be regarded as a set of elements and relationships between these elements

3.73
timestamp
attribute or field in data which denotes the time of data generation

3.74
vital sign
clinical information relating to one or more patients; measured by or derived from apparatus connected to the patient, or otherwise gathered from the patient

4 Abbreviated terms

—	ANSI	American National Standards Institute
—	B2B	Business to Business
—	CDA	Clinical Document Architecture
—	ebXML	Electronic Business Extensible Markup Language
—	ECG	Electrocardiogram
—	HL7	Health Level 7
—	IHE	Integrating the Healthcare Enterprise
—	MIME	Multipurpose Internet Mail Extension
—	MVC	Model-View-Controller
—	OASIS	Organization for the Advancement of Structured Information Standards
—	OMS	Object Management Service
—	PKI	Public Key Infrastructure
—	RCA	Registry Client Application
—	RIM	Reference Information Model
—	RS	Registry Service
—	SAML	Security Assertion Markup Language
—	SOAP	Simple Object Access Protocol
—	UDDI	Universal Description, Discovery and Integration
—	UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
—	XACML	Extensible Access Control Markup Language
—	XML	Extensible Markup Language

5 Document registry framework

5.1 General structure of the framework

The document registry framework includes a number of specification components organized as shown in Figure 1. These will be specified in 5.2 to 5.6.

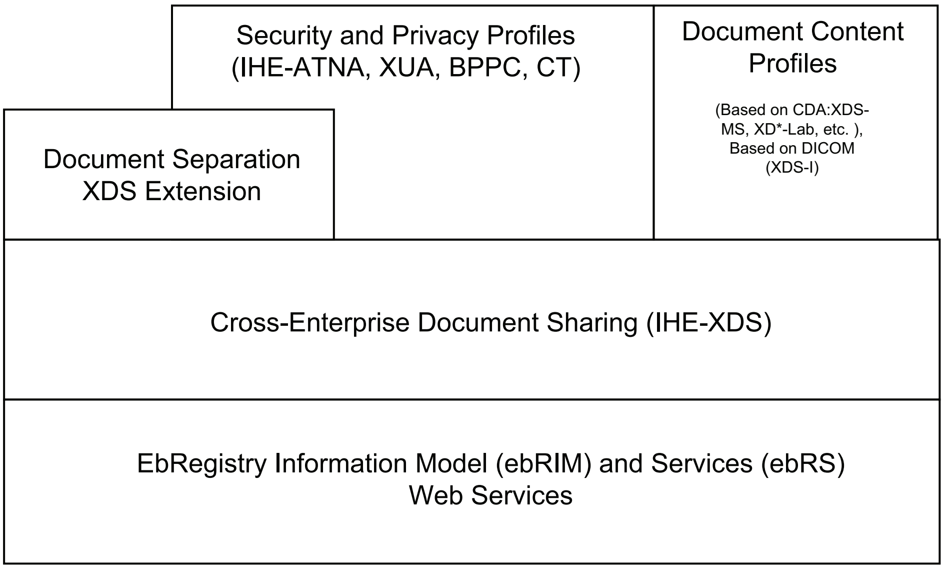
Security and Privacy Profiles
(IHE-ATNA, XUA, BPPC, CT)
Document Content Profiles
(Based on CDA:XDS-MS, XD*-Lab, etc.), Based on DICOM (XDS-I)
Document Separation XDS Extension
Cross-Enterprise Document Sharing (IHE-XDS)
EbRegistry Information Model (ebRIM) and Services (ebRS) Web Services

Figure 1 — General structure of the document registry framework

5.2 Information model (ebRIM) and services (ebRS) web services

These standards form the foundation upon which the document registry framework is established. In particular, they include web services with MTOM/XOP and ebRegistry Services that organize the registry metadata according to the ebRegistry Information Model (ebRIM).

The following references apply:

- ebXML RIM V 3.0, OASIS ebXML Registry Information Model;
- ebXML RS V 3.0, OASIS ebXML Registry Service Specification;
- Extensible Markup Language (XML) 1.0 W3C Recommendation, http://www.w3c.org/TR/REC-xml;
- SOAP Version 1.2 specification, http://www.w3.org/TR/soap12-part1/, March 2004;
- SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/;
- WSDL 1.1 Note http://www.w3.org/TR/wsdl.

5.3 Cross-enterprise document sharing (IHE-XDS)

This IHE Profile adapts the standards defined in 5.2 to the sharing of health documents using a registry and one or more repositories. In particular, it defines registry metadata specific to a person’s health documents. It remains sufficiently general to address documents encapsulating one or more electronic health records across healthcare specialties and well-being management.

XDS defines five actors that are functional abstractions of systems that cooperate in providing a document-sharing service based on a registry. These are depicted in Figure 2 and listed in Table 1.

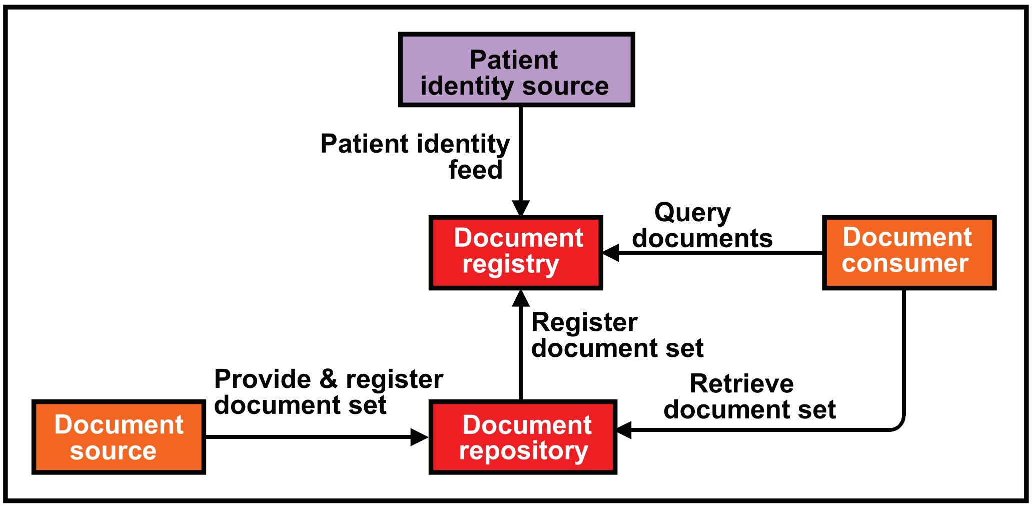

Figure 2 — XDS actors and transactions

Table 1 — Related actors and required operations

Actor	Required operation
Document source	Creates metadata related to one or more XDS documents that it sends to one or more document repositories and associated document registries.
Document repository	Stores XDS documents and forwards their metadata for the registration request to a document registry.
Document registry	Creates a DocumentEntry when it receives a registration request for an XDS document. This includes the link to the document repository where the document may be retrieved.
Document consumer	May query the document registry to search for relevant XDS documents based on the metadata of the DocumentEntry and may retrieve one or more of these from document repositories.
Patient identity source	Provides the authoritative source of person identifiers against which XDS document may be registered by document repositories and queried by document consumers.

The following references apply:

IHE ITI-TF-1 IHE IT Infrastructure Technical Framework:

— Cross-enterprise Document Sharing (XDS.b) integration profile;

— Audit Trail and Node Authentication (ATNA) integration profile;

— Consistent Time (CT) integration profile.

ISO/TR 28380-2 references the most current version of the IHE technical frameworks, which specifies the IHE profiles identified in this Technical Specification. These integration and content profiles are listed at: www.ihe.net/IT_Infrastructure_Profiles.

5.4 Document separation XDS extension

This option offers a means of achieving protection of privacy by separating the document content into two fragments and storing them in different repositories. This may be useful when a requirement for access to the content of clinical documents for research purposes exists, where researchers are prohibited from accessing privacy-sensitive data such as patient identities. This also allows distinct use of the header fragment (e.g. for administrative tasks) and the body fragment for non-patient-specific clinical activities such as research and population health.

In the separation of the document content in two fragments, the integrity and ability to digitally sign the document content shall be preserved (i.e. a digital signature applied to the whole document content before the fragments are created and placed under the registry and repositories management shall remain valid once the fragments have been reassembled).

NOTE When applied to CDA documents, the header/body split does not guarantee the absence of patient-identifiable information in the CDA body (e.g. physician free-form text notes), or that CDA header information is free from clinical descriptive information (service episode, facility, author specialty, etc.). An alternative might be to consider publication (with appropriate access controls) of different CDAs (with header and body) with different content subsets (e.g. for administrative use or for clinical research).

The following reference applies: Korean National Extension to IHE IT Infrastructure Technical Framework - CDA Document Separation - XDS Extension (see Annex A).

5.5 Patient identification, security and privacy profiles

Optional security and privacy profiles offer a means of achieving protection of privacy by supporting interoperability for conveying user assertions and managing/enforcing privacy consent.

The following references may apply:

IHE IT Infrastructure Technical Framework:

- Patient Identification Cross-Referencing (PIX) integration profile;
- Basic Patient Privacy Consent (BPPC) integration profile;
- Patient Demographics Query (PDQ) integration profile;
- Cross-Enterprise User Assertion (XUA) integration profile.

5.6 Document content profiles

Optional document content profiles offer a means of supporting interoperability at the document content level across a variety of types of clinical document.

The following references may apply:

IHE Patient Care Coordination Technical Framework:

- cross-enterprise sharing of medical summaries (XDS-MS) content profile;
- exchange of personal health records (XPHR) content profile;
- emergency department referral (EDR);
- pre-procedure history and physical (PPHP);
- emergency department encounter record (EDER);

- functional status assessment profile (FSA);
- antepartum record (APR);
- immunization content (IC);
- cross-enterprise sharing of imaging information (XDS-I).

IHE Laboratory Coordination Technical Framework:

- cross-enterprise sharing of laboratory reports (XD-Lab) content profile.

Annex A
(informative)

Korean National Extension to IHE IT Infrastructure Technical Framework CDA Document Separation - XDS Extension

A.1 Requirements for document sharing with document content separation

A.1.1 General

A requirement for access to clinical documents for research purposes exists, where researchers are prohibited from accessing privacy-sensitive data such as patient identities. One way to support it is to use two (separate) document repositories, one for document header information and the other for document bodies. The content of the header repository can be searched efficiently to determine the records of a particular set of patients relevant to the research, e.g. females within a certain age range. The corresponding set of data records is then retrieved from the document body repository. Examples include tissue banks and population-based research.

The effectiveness of this document content separation option is dependent on the specific use of CDA, and specifically on the type of information present in header and body. Projects implementing this option are advised to conduct a risk analysis specific to this document content to determine if such an option reduces risk to an acceptable level. In all cases, proper access control management will be needed to allow authorized users access to documents.

This IHE document is directly related to a number of documents, as shown in Figure A.1:

— it is referenced by the ISO/TS 27790 Document Registry Framework,

— it references the IHE Cross-Enterprise Document Sharing Integration Profile,

— it references ebRS, ebRIM (published also as part of ISO 15000) and underlying Web Services.

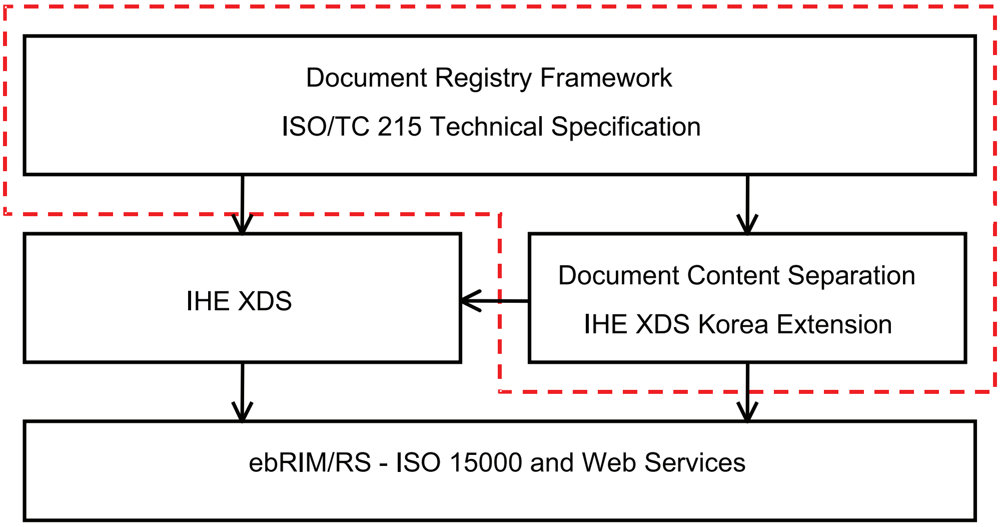
Document Registry Framework
ISO/TC 215 Technical Specification
IHE XDS
Document Content Separation
IHE XDS Korea Extension
ebRIM/RS - ISO 15000 and Web Services

Figure A.1 — Document content separation in document registry framework

The dotted line in Figure A.1 highlights that for the review of the ISO/TC 215 Committee Draft of the DRF Technical Specification, the Document Content Separation-IHE XDS Korea Extension (this annex) has been included as an informative annex. As the Technical Specification becomes finalized, this annex will be removed and IHE Korea/IHE International will publish this Extension as a separate document.

A.1.2 Document sharing: cross-enterprise document sharing (XDS)

The cross-enterprise document sharing (XDS) IHE Integration Profile facilitates the registration, distribution and access of patient electronic health records across health enterprises. XDS focuses on providing a standard-based specification for managing the sharing of documents between health care enterprises, ranging from a private physician's clinic to an acute care in-patient facility.

A.1.3 Document separation

A.1.3.1 General

Document separation supports the document registration and retrieval via the XDS access to repositories served by an XDS Document Registry in which a CDA document is fragmented and distributed on one or more XDS repositories so that the possibility of privacy violation can be reduced.

A.1.3.2 Header/body separation

CDA documents are persistent objects to be stored in permanent storage systems. They include very sensitive information such as the identities of patients and care providers, the diagnostic information on the diseases the patients suffer from, the treatments provided to the patients and so on. If such data are exposed, it may cause serious privacy violations and legal issues. Even worse, the exposed data can be maliciously used against the patients, e.g. blackmailing. Note that the header of a CDA document contains information about the identities of a patient and a care provider, and the body includes clinical data such as diagnoses and/or treatments. As such, an exposition of the information in the header in itself may cause a violation of privacy. While the information in the body alone is relatively anonymous and can be used for, say, research purposes, coupling both types of information poses a much greater threat to the patient's privacy. Therefore, this Korean National Extension to the IHE XDS Integration Profile specifies a scheme in which the body and header of a CDA document are separated and stored in two independent XDS repositories.

The first requirement is to enhance the confidentiality of CDA documents via the header/body separation scheme. The scheme enhances confidentiality because an illegal acquisition of a complete CDA document requires breaking into two XDS repository actors for the header and body, and an XDS document registry actor for the information that associates them, which is much harder and takes a longer amount of time than cracking into a single repository server when the separation scheme is not used.

NOTE 1 The security enhancement added by the header/body separation scheme will have to be re-evaluated once the effectiveness of the general security solutions (e.g. encryptions) to protect data has been finalized.

The second requirement is to allow discriminated accesses to the header fragment (e.g. for administrative tasks) and the body fragment (e.g. for patient-independent clinical research or public health).

NOTE 2 The header/body separation does not guarantee that there is no patient-identifiable information in the CDA body (e.g. free-form text notes by the physician), or that the CDA header is free from any descriptive clinical information (e.g. service episode, facility, author specialty, etc.). An alternative implementation guideline could be to consider fragmenting different content subsets for each CDA type.

A.2 Content separation specification

A.2.1 Provide and register documents by CDA separation

A.2.1.1 Overview

This extension relates directly to the fragmentation of the content of the document to be published into two parts: a header fragment and a body fragment. The registration of a CDA document flows from the Document Provider to the Document Source, to the Document Repository, and finally to the Document Registry. The retrieval of a CDA document, on the other hand, flows from the Document Consumer, to the Document Registry, to the Document Repositories and back to the Document Consumer.

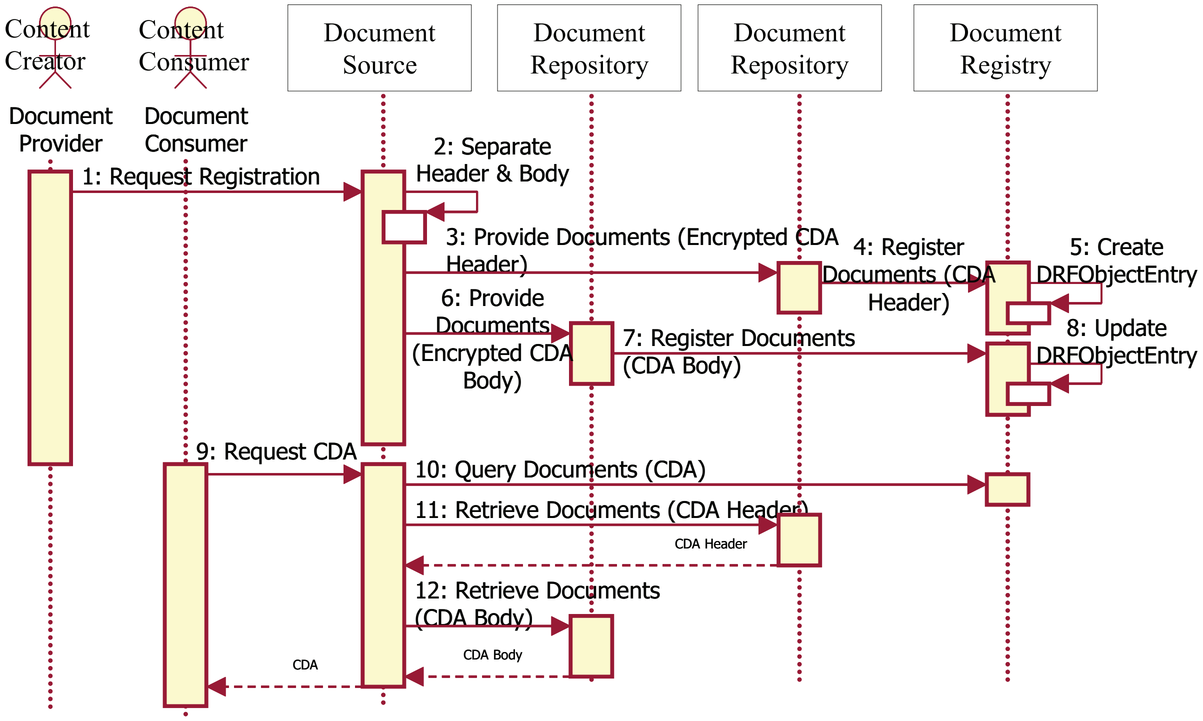
Content Creator
Content Consumer
Document Source
Document Repository
Document Repository
Document Registry
Document Provider
Document Consumer
1: Request Registration
2: Separate Header & Body
3: Provide Documents (Encrypted CDA Header)
4: Register Documents (CDA Header)
5: Create DRFObjectEntry
6: Provide Documents (Encrypted CDA Body)
7: Register Documents (CDA Body)
8: Update DRFObjectEntry
9: Request CDA
10: Query Documents (CDA)
11: Retrieve Documents (CDA Header)
CDA Header
12: Retrieve Documents (CDA Body)
CDA Body
CDA

Figure A.2 — Flow of registration and retrieval of a separated CDA header/body

A.2.1.2 Use case

The content creator can submit the separated header fragment document and body fragment document of CDA, which are to be stored in one or more Document Repositories. The Document Repository extracts meta-information, including the locations of the separated header and body, and registers them to the Document Registry. Figure A.3 shows this use case. A link arrow is used to represent the direction of flow between actors.

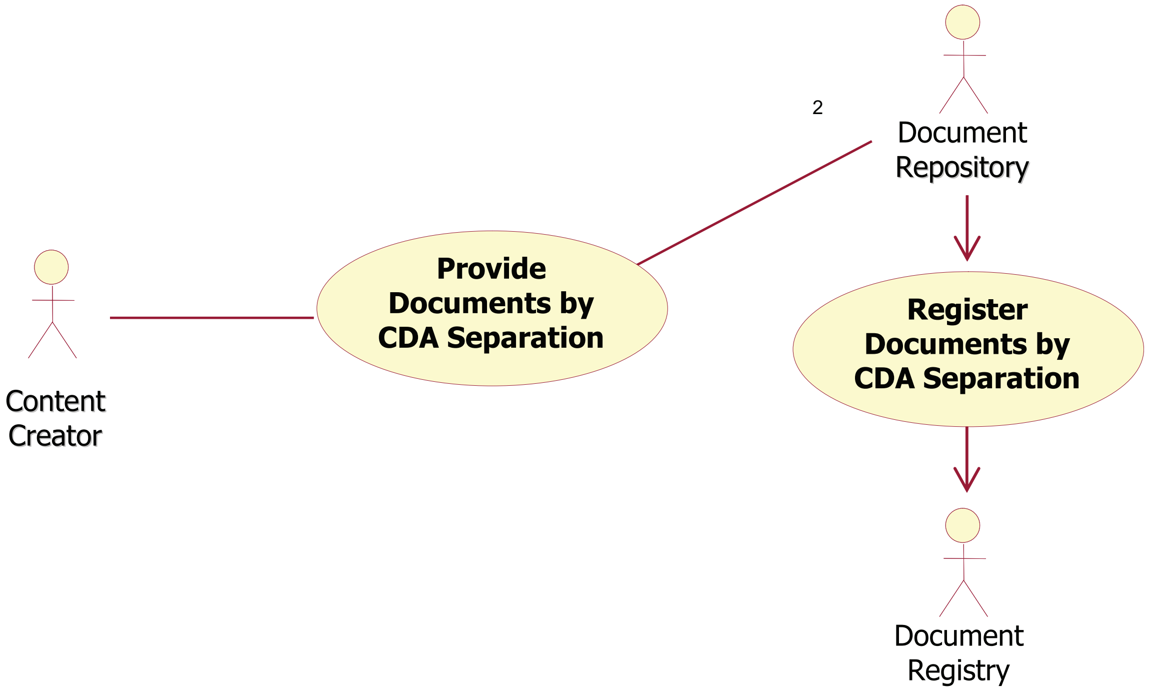
2
Document Repository
Provide Documents by CDA Separation
Register Documents by CDA Separation
Content Creator
Document Registry

Figure A.3 — Use case: provide and register documents by CDA fragment separation

Table A.1 — Related actors and required operations

Actor	Required operation
Document source	Divides a CDA document into the header and body fragments and creates metadata related to those fragments for their registration and sends them to one or more Document Repositories.
Document repository	Stores the fragments as XDS Documents and forwards the fragment metadata for the registration request to a Document Registry when the Document Source sends either a header or body fragment of a CDA document.
Document registry	Verifies whether a DocumentEntry for the corresponding header fragment exists when it receives a registration request for a body fragment.

A.2.1.3 Sequential operation

A.2.1.3.1 Overview

Figure A.4 describes the sequential operation for the storing and registration of separated CDA documents.

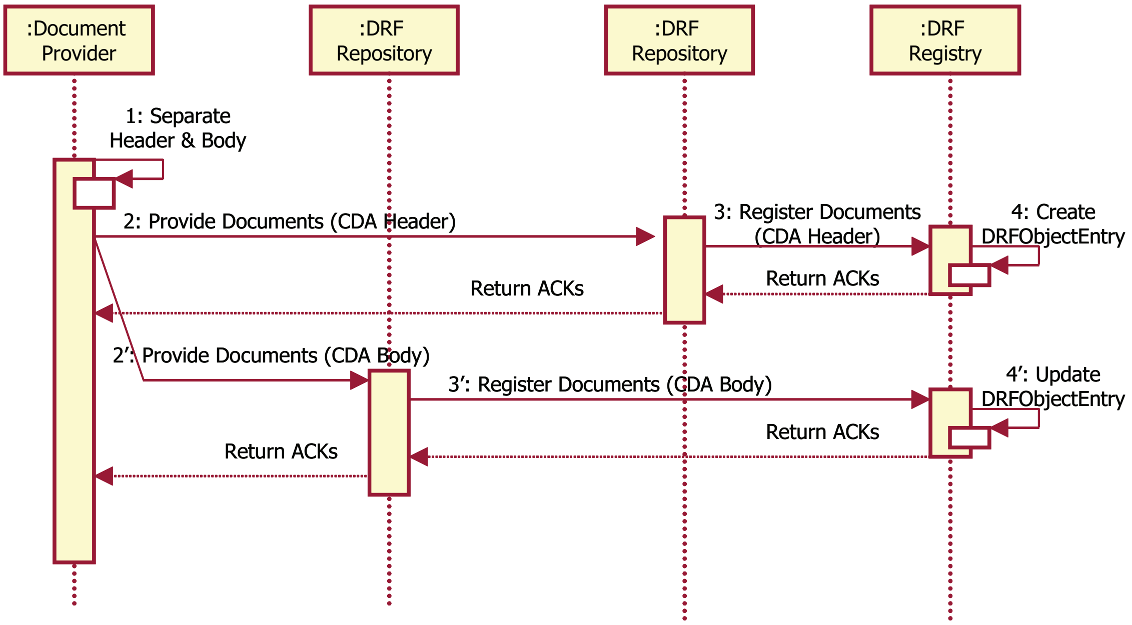
:Document Provider
:DRF Repository
:DRF Repository
:DRF Registry
1: Separate Header & Body
2: Provide Documents (CDA Header)
3: Register Documents (CDA Header)
4: Create DRFObjectEntry
Return ACKs
Return ACKs
2': Provide Documents (CDA Body)
3': Register Documents (CDA Body)
4': Update DRFObjectEntry
Return ACKs
Return ACKs

Figure A.4 — Sequence diagram: provide and register documents by CDA separation

A.2.1.3.2 Separate header and body

The Document Source separates the CDA document into the header and body fragments.

A.2.1.3.3 Provide and register documents (CDA header|CDA body)

The Document Provider provides the separated CDA header and body fragments to distributed Document Repositories. It also provides some metadata needed for the Document Entry creation in the Document Registry.

A.2.1.3.4 Register documents (CDA header|CDA body)

The Document Repository verifies the authenticity of the CDA header or body fragment. It also includes metadata (e.g. URI) for the Document Entry and requests registration to the Document Registry.

A.2.1.3.5 Create/update document entry in registry

The Document Registry performs a validation of the existence of CDA header and body fragments and creates or updates Documents Entries.

A.2.2 Query and retrieve content-separated CDA documents

A.2.2.1 Use case

The document consumer actor can issue a query to search for a CDA document via the Document Registry. The returned values from the query include the URIs pointing to the Document Respositories that store the header and body fragments of the document in question. Using these URIs, the Document Consumer retrieves the header and body from the corresponding DRF Repositories. Figure A.5 shows the use case for this requirement.

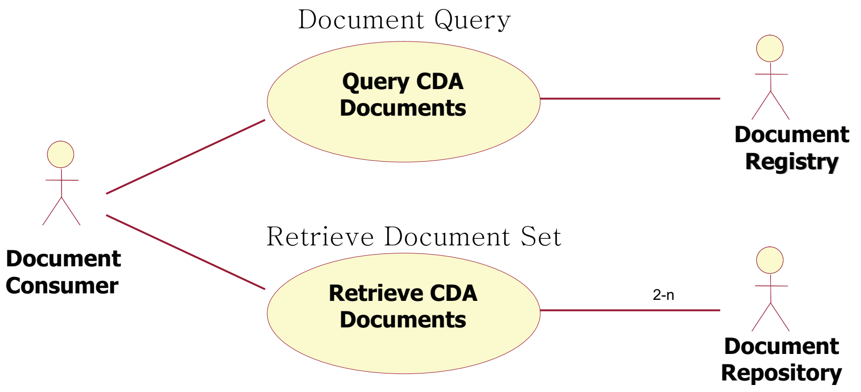

Figure A.5 — Use case: query and retrieve CDA documents

Table A.2 — Related actors and required operations

Actor	Required operation
Document consumer	Requests a query with search conditions to the Document Registry.
Document registry	Analyses a query from the Document Consumer, performs a search and returns the result.
Document repository	Accepts a document set retrieval request and returns a set of target header or body fragments.

A.2.2.2 Sequential operation

A.2.2.2.1 Overview

Figure A.6 describes the sequence of operations to process queries and retrieval requests on the separated CDA documents.

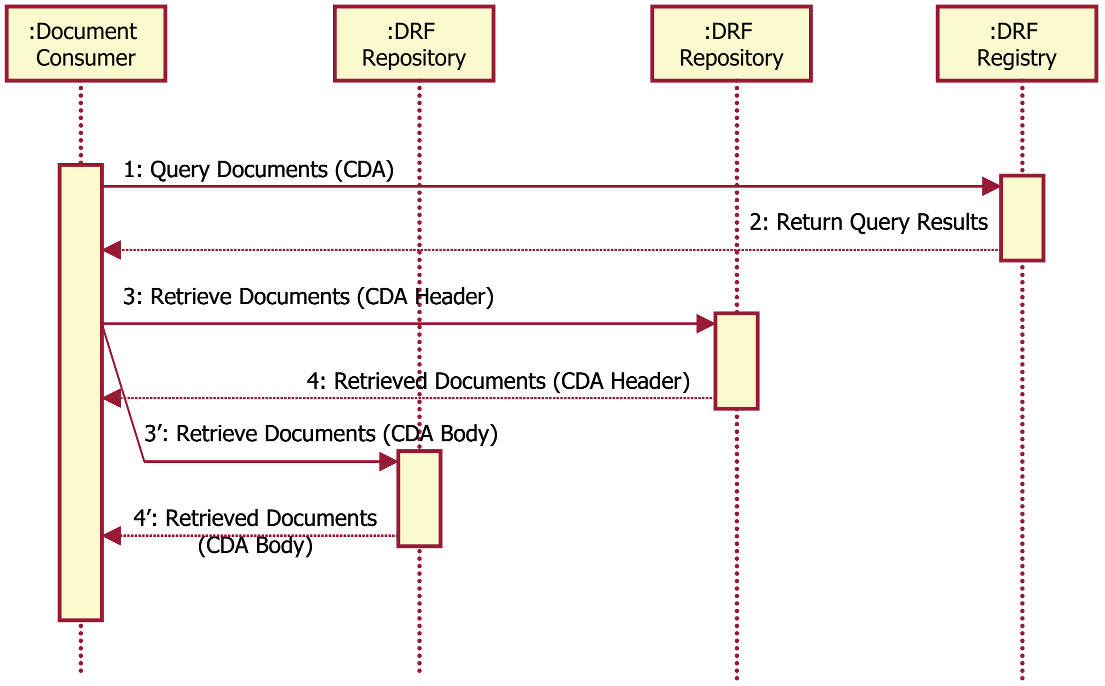
:Document Consumer
:DRF Repository
:DRF Repository
:DRF Registry
1: Query Documents (CDA)
2: Return Query Results
3: Retrieve Documents (CDA Header)
4: Retrieved Documents (CDA Header)
3’: Retrieve Documents (CDA Body)
4’: Retrieved Documents (CDA Body)

Figure A.6 — Sequence diagram: query and retrieve CDA documents

A.2.2.2.2 Query documents (CDA)

This is the query message that is transmitted to the Document Registry.

A.2.2.2.3 Return query results

The Document Registry returns the result of the query message. The result value is a list of DocumentEntries or a UUID list of searched documents (see XDS stored query).

A.2.2.2.4 Retrieve documents (CDA header|CDA body)

The Document Consumer retrieves either the header or body fragment from the corresponding Document Repository.

A.2.2.2.5 Return documents (CDA header|CDA body)

The requested Document Repository returns the retrieved document to the Document Consumer.

A.2.3 Document integrity

A.2.3.1 Overview

Figure A.7 illustrates the process to ensure document integrity with the CDA separation scheme.

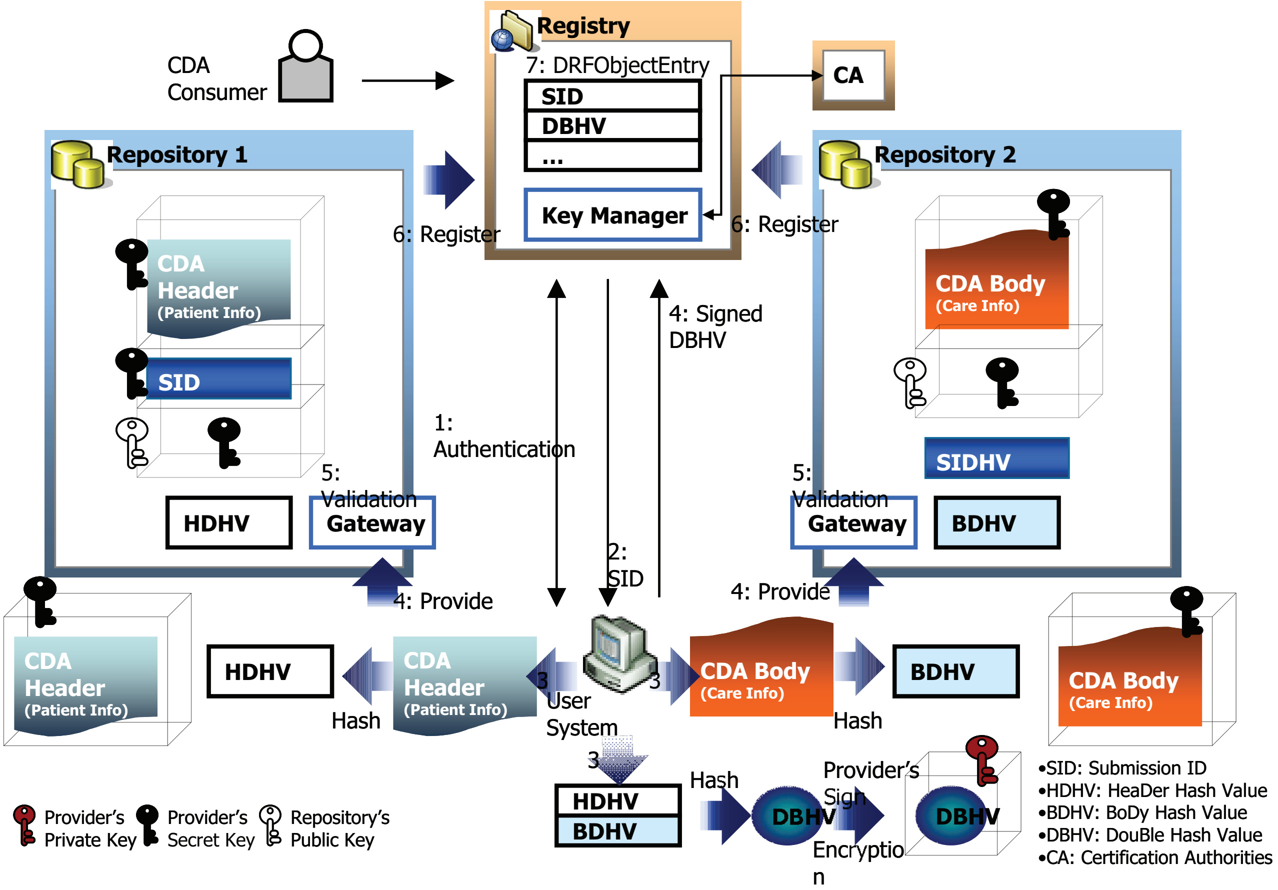

Figure A.7 — Key strategies for enhanced CDA registration in DRF

A.2.3.2 User authentication

The CDA provider is authenticated via the user system.

A.2.3.3 Publication of SID

The (DRF) Registry publishes SID (Submission ID) for the user system to allow submission of clinical documents. SID is a UUID for identifying a pair of CDA header and body fragments and is used to track the pair during the registration transaction.

A.2.3.4 CDA separation

The user system divides a CDA document into a pair of header and body fragments and then encrypts them. The HDHV (header hash value) and BDHV (body hash value) are the hash values of the header and body fragments, respectively. The DBHV (double hash value) is a hash value created with an aggregate of HDHV and BDHV. DBHV is used during the verification process, especially for integrity checking. DBHV is digitally signed with the CDA Provider’s private key. Separated header and body fragments are digitally signed with the CDA Provider’s secret key and enveloped. The secret key is encrypted with the repository’s public key and enveloped. SIDHV (SID hash value) is the hash value of SID, and created and digitally signed with the CDA Provider’s secret key and enveloped.

A.2.3.5 Providing CDA document to repository

Data prepared in the third step are sent to a repository. In Figure A.7, the header and body fragments are sent to Repository 1 and Repository 2, respectively. The final data provided to each repository and the registry is as follows:

— Repository 1: encrypted header text|encrypted SID|encrypted CDA Provider’s secret key|HDHV

— Repository 2: encrypted body text|SIDHV|encrypted CDA Provider’s secret key|BDHV

— Registry: digitally signed DBHV

NOTE The same SID is stored differently as an encrypted SID in Repository 1 and as a hash value (SIDHV) in Repository 2, so that the association between the header and body is protected.

A.2.3.6 Validation by repository

The gateway inside a repository verifies the integrity of data received from the user system. Each repository acquires the CDA Provider’s secret key using its own private key. The repositories decrypt the header and body with the CDA Provider’s secret key and then re-compute their hash values. The gateway compares the new hash values with the hash values received from the user system to verify the data integrity.

A.2.3.7 Registering CDA Document to Registry

A repository creates metadata for a received object (header or body) and registers it to the registry if the verification was successful.

A.2.3.8 Verification by Registry and Transaction Termination (Creating CDRObjectEntry)

The registry finishes a registration transaction using SID and SIDHV received from each repository and then creates a DRFObjectEntry. It verifies the integrity of data received from the repositories by comparing a signed DBHV received from the user system with a newly computed hash value from the aggregate of HDHV and BDHV.

A.2.4 Document life cycle

The life cycle of documents, such as replacement, addendum and depreciation, is beyond the scope of this option.

Bibliography

[1] ASTM E1769:1995[1], *Standard Guide for Properties of Electronic Health Records and Record Systems*

[2] Building and Using a Clinical Data Repository, available at: http://www.informatics-review.com/thoughts/cdr.html

[3] MCDONALD, C.J., *The barriers to electronic medical record systems and how to overcome them*, J. Am. Med. Inform. Assoc., **4**(3), pp. 213-221, 1997

[4] CDA Final Release 1, available at: http://www.hl7.org/Memonly/downloads/Standards_CDA/R1/HL7_CDA_R1_FINAL.zip

[5] Clinical Document Architecture, available at: http://www.hl7.org/Library/standards_non1.htm#CDA

[6] ebXML RIM V2.0, available at: http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebrim.pdf

[7] ebXML RS V2.0, available at: http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebrs.pdf

[8] ebXML Specification, available at: http://www.ebxml.org/specs/index.htm

[9] HL7 Standards, Inc. available at: http://www.hl7.org

[10] IHE IT Infrastructure Framework - Cross-Enterprise Document Sharing (XDS)

[11] IL KWANG KIM and IL KON KIM, *CDR (Clinical Document Repository) Framework for Electronic Health Record Sharing and Medical Information Network*, The 6th CJK Medical Informatics Conference, Nagoya, Japan, 2004

[12] J2EE V1.4 Documentation, available at: http://java.sun.com/j2ee/1.4/docs/index.html

[13] HEIMANN, K.U., *Discharge and referral data exchange using global standards - the SCIPHOX project in Germany*, J. Am. Med. Inform. Assoc., **70**, pp. 195-203, 2003

[14] Latest version of SOAP Version 1.2 specification, available at: http://www.w3.org/TR/soap12-part1/ March 2004

[15] MULLER, M.L., *Cross-institutional data exchange using the clinical document architecture (CDA)*, Int. J. Med. Inform., **74**, pp. 245-256, 2005

[16] Model-View-Controller, available at: http://java.sun.com/blueprints/patterns/MVC-detailed.html

[17] OASIS Standards and Other Approved Work, available at: http://www.oasis-open.org

[18] WAYLAND, R., *Clinical Data Repository Project*, University of Virginia, 1998, available at: http://www.itc.virginia.edu/virginia.edu/spring98/cdr/all.html

[19] SAML v2.0, OASIS Working Draft, March 15, 2005, available at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[1] Standard withdrawn in 2004.

[20] Service Oriented Architecture and Web Service, IBM, available at: http://www-306.ibm.com/software/solutions/webservices/documentation.html

[21] SOAP 1.1 Specification, available at: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[22] The 2nd Workshop Collection, Health and Medical Information Research Center, pp. 20-24, 6 April 2005

[23] UDDI Specification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec

[24] W3C Web Services Activity, available at: http://www.w3.org/2002/ws

[25] Web Services Architecture, W3C Working Group Note 11 February 2004, available at: http://www.w3.org/TR/ws-arch, Accessed March 2004

[26] XACML v2.0, OASIS Standard, February 1, 2005, available at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[27] XML Encryption Syntax and Processing W3C Recommendation 10 December 2002, available at: http://www.w3.org/TR/xmlenc-core

[28] XML Key Management Specification (XKMS) Version 2.0, W3C Editor's Draft 30th March 2005, available at: http://www.w3.org/2001/XKMS/

[29] XML Schema, W3C Recommendation May 2, 2001, available at: http://www.w3.org/XML, http://www.w3.org/2001/XMLSchema.html

[30] XML-Signature Syntax and Processing W3C Recommendation 12 February 2002, available at: http://www.w3.org/TR/xmldsig-core

[31] ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[32] ISO 13606-1, *Health informatics — Electronic health record communication — Part 1: Reference model*

[33] ISO 20514, *Health informatics — Electronic health record — Definition, scope and context*

[34] ISO 28380-2, *Health informatics — IHE global standards adoption — Part 2: Integration and content profiles*

ICS 35.240.80

Price based on 24 pages