

Integrating the Healthcare Enterprise

5



**IHE IT Infrastructure (ITI)
Technical Framework Supplement
Document Digital Signature**

10

2009-2010

15

**Trial Implementation Supplement
August 10, 2009**

Table of Contents

20	1.1	Overview of Technical Framework.....	4
	1.2	Overview of Volume 3.....	4
	1.3	Audience.....	5
	1.4	Relationship to Standards.....	5
	1.5	Relationship to Real-world Architectures.....	5
25	1.6	Comments.....	6
	1.7	Copyright Permission.....	6
	5.3	Document Digital Signature Content Profile.....	9
	5.3.1	Overview.....	9
	5.3.2	Related Document content profiles.....	9
30	5.3.3	Context for Document Digital Signature.....	9
	5.3.4	References.....	11
	5.3.5	Digital Signature Document content profile Use Cases.....	12
	5.3.6	XDS Signature Document Content.....	14
	5.3.7	Source Mappings.....	17
35	5.3.8	DSG Creation Processing.....	22
	5.3.9	Processing by XDS Document Consumer.....	23
	5.3.10	Configuration.....	24

1 Foreword

40 Integrating the Healthcare Enterprise (IHE) is an initiative designed to stimulate the integration
of the information systems that support modern healthcare institutions. Its fundamental objective
is to ensure that in the care of patients all required information for medical decisions is both
correct and available to healthcare professionals. The IHE initiative is both a process and a
forum for encouraging integration efforts. It defines a technical framework for the
45 implementation of established messaging standards to achieve specific clinical goals. It includes
a rigorous testing process for the implementation of this framework. And it organizes
educational sessions and exhibits at major meetings of medical professionals to demonstrate the
benefits of this framework and encourage its adoption by industry and users.

The approach employed in the IHE initiative is not to define new integration standards, but rather
50 to support the use of existing standards, HL7, ASTM, ISO, DICOM, IETF, W3C, and others, as
appropriate in their respective domains in an integrated manner, defining configuration choices
when necessary. IHE maintain formal relationships with several standards bodies including
HL7, DICOM and refers recommendations to them when clarifications or extensions to existing
standards are necessary.

55 This initiative has numerous sponsors and supporting organizations in different medical specialty
domains and geographical regions. In North America the primary sponsors are the Healthcare
Information and Management Systems Society (HIMSS) and the Radiological Society of North
America (RSNA). IHE Canada has also been formed. IHE Europe (IHE-EUR) is supported by a
large coalition of organizations including the European Association of Radiology (EAR) and
60 European Congress of Radiologists (ECR), the Coordination Committee of the Radiological and
Electromedical Industries (COCIR), Deutsche Röntgengesellschaft (DRG), the EuroPACS
Association, Groupement pour la Modernisation du Système d'Information Hospitalier
(GMSIH), Société Française de Radiologie (SFR), Società Italiana di Radiologia Medica
(SIRM), the European Institute for health Records (EuroRec), and the European Society of
65 Cardiology (ESC). In Japan IHE-J is sponsored by the Ministry of Economy, Trade, and
Industry (METI); the Ministry of Health, Labor, and Welfare; and MEDIS-DC; cooperating
organizations include the Japan Industries Association of Radiological Systems (JIRA), the
Japan Association of Healthcare Information Systems Industry (JAHIS), Japan Radiological
Society (JRS), Japan Society of Radiological Technology (JSRT), and the Japan Association of
70 Medical Informatics (JAMI). Other organizations representing healthcare professionals are
invited to join in the expansion of the IHE process across disciplinary and geographic
boundaries.

The IHE Technical Frameworks for the various domains (IT Infrastructure, Cardiology,
Laboratory, Radiology, Patient Care Coordination, etc.) defines specific implementations of
75 established standards to achieve integration goals that promote appropriate sharing of medical
information to support optimal patient care. It is expanded annually, after a period of public
review, and maintained regularly through the identification and correction of errata. The current
version for these Technical Frameworks may be found at <http://www.ihe.net/>.

80 The IHE Technical Framework identifies a subset of the functional components of the healthcare
enterprise, called IHE Actors, and specifies their interactions in terms of a set of coordinated,

standards-based transactions. It describes this body of transactions in progressively greater depth. The volume I provides a high-level view of IHE functionality, showing the transactions organized into functional units called Integration Profiles that highlight their capacity to address specific clinical needs. The subsequent volumes provide detailed technical descriptions of each IHE transaction.

This IHE IT Infrastructure Technical Framework Supplement is re-issued for Trial Implementation through May 2010.

Comments and change proposals arising from Trial Implementation may be submitted to <http://forums.rsna.org> under the forum:

“Integrating the Healthcare Enterprise”

Select the sub-forum:

“IHE IT Infrastructure 2009-2010 Supplement for Trial Implementation”

The IHE IT Infrastructure Technical Committee will address these comments resulting from implementation Connectathon testing, and demonstrations such as HIMSS 2010.

1 Introduction

100 Integrating the Healthcare Enterprise (IHE) is an initiative designed to stimulate the integration of the information systems that support modern healthcare institutions. Its fundamental objective is to ensure that in the care of patients all required information for medical decisions is both correct and available to healthcare professionals. The Healthcare Information and Management Systems Society (HIMSS), the Radiological Society of North America (RSNA) are the current sponsors of this initiative. Other organizations representing healthcare professionals are invited to join with them.

105 The IHE initiative is both a process and a forum for encouraging integration efforts. It defines a technical framework for the implementation of established information exchange standards to achieve specific clinical goals. It includes a rigorous testing process for the implementation of this framework. And it organizes educational sessions and exhibits at major meetings of medical professionals to demonstrate the benefits of this framework and encourage its adoption by
110 industry and users.

The approach employed in the IHE initiative is not to define new integration standards, but rather to support the use of existing standards— HL7, IETF, ASTM, DICOM, ISO, OASIS, W3C, and potentially others, as appropriate in their respective domains—in an integrated manner, defining configuration choices when necessary. When clarifications or extensions to existing standards
115 are necessary, IHE refers recommendations to the relevant standards bodies.

1.1 Overview of Technical Framework

This document, part of the IHE Technical Framework, defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of medical information to support optimal patient care. It is expanded annually, after a period of public
120 review, and maintained regularly through the identification and correction of errata. The latest version of the document is always available via the Internet at www.ihe.net.

The IHE Technical Framework defines a subset of the functional components of the healthcare enterprise, called IHE Actors, and specifies their interactions in terms of a set of coordinated, standards-based transactions. It defines this body of transactions in progressively greater depth.
125 Volume I provides a high-level view of IHE functionality, showing the transactions organized into functional units called Integration Profiles that highlight their capacity to address specific clinical needs.

1.2 Overview of Volume 3

130 Section 2 presents the conventions used in this volume to define the document content implemented under IHE.

Section 3 provides an overview of the concepts in this Volume to define the content components of documents shared in a distributed healthcare environment.

135 Section 4 defines document content profiles in detail, specifying the metadata mappings for managing these documents, the standards employed, the information structures exchanged, and in some cases, implementation options for the content profile.

The appendices following the main body of this volume provide specific specification elements that may be reused as well as clarification of technical details. The final section of the volume is a glossary of terms and acronyms used in the IHE Technical Framework, including those from relevant standards.

140 **1.3 Audience**

The intended audience of this document is:

- Technical staff of vendors planning to participate in the IHE initiative
- IT departments of healthcare institutions
- Experts involved in standards development
- 145 • Anyone interested in the technical aspects of integrating healthcare information systems

1.4 Relationship to Standards

150 The IHE Technical Framework identifies functional components of a distributed healthcare environment solely from the point of view of their interactions in the healthcare enterprise. At its current level of development, it defines a coordinated set of transactions based on an expanding number of standards.

In some cases, IHE recommends selection of specific options supported by these standards; however, IHE does not introduce technical choices that contradict conformance to these standards. If errors in or extensions to existing standards are identified, IHE’s policy is to submit those to the appropriate standards bodies for resolution within their conformance and standards evolution strategy. IHE is therefore an implementation framework, not a standard. Referencing IHE as a standard and claiming conformance to IHE are both inappropriate. Conformance claims must be made in direct reference to specific standards. Conformance statements may, however, state that the products they describe are “implemented in accordance with the IHE Technical Framework”.

155

160

IHE encourages implementers to ensure that products implemented in accordance with the IHE Technical Framework also meet the full requirements of the standards underlying IHE, allowing the products to interact, although possibly at a lower level of integration, with products that have been implemented in compliance with the standards but that may not meet the IHE requirements.

165 **1.5 Relationship to Real-world Architectures**

The actors, transactions and document content described in the IHE Technical Framework are abstractions of the real-world healthcare information system environment. While some of the transactions are traditionally performed by specific product categories (EMR, Clinical Systems, etc.), the IHE Technical Framework intentionally avoids associating functions or actors with such product categories. For each actor, the IHE Technical Framework defines only those

170

functions associated with integrating information systems. The IHE definition of an actor should therefore not be taken as the complete definition of any product that might implement it, nor should the framework itself be taken as the complete definition of a healthcare information system architecture.

- 175 The reason for defining actors, transactions and document content is to provide a basis for defining the interactions among functional components of the healthcare information system environment. In situations where a single physical product implements multiple functions, only the interfaces between the product and external functions in the environment are considered to be significant by the IHE initiative. Therefore, the IHE initiative takes no position on the relative merits of an integrated environment based on a single, all-encompassing information system versus one based on multiple systems that together achieve the same end.
- 180

1.6 Comments

The IHE sponsors welcome comments on this document and the IHE initiative. They should be directed to the discussion server at <http://forums.rsna.org> or to:

- 185 Lisa Spellman
Senior Director Informatics
230 East Ohio St., Suite 500
Chicago, IL USA 60611-3270
Email: ihe@himss.org

190 1.7 Copyright Permission

No material in this volume is quoted from sources that require copyright permissions.

2 Conventions

195 This document has adopted the following conventions for representing the framework concepts and specifying how the standards upon which the IHE Technical Framework is based should be applied.

Italics

Used for filenames, URL, email addresses or new terms.

3 Role of this Volume in the Technical Framework

The IHE Technical Framework is based on actors that interact through transactions.

200 Actors are information systems or components of information systems that produce, manage, or act on information associated with operational activities in the enterprise.

Transactions are interactions between actors that transfer the required information through standards-based messages.

205 The Document Content Profiles specified in this ITI TF-3 provide the information content for documents that are shared using some of the transactions specified in ITI TF- 2a and 2b. In turn, implementation of the transactions described in the ITI-TF- 2a and 2b support the specification of Integration Profiles defined in ITI TF-1 as well as in other IHE domain’s Volume 1.

The role and implementation of the document content specified in this volume require an understanding of the transactions and the integration

210

EDITOR: Add the following section to ITI TF-1:2.1 Table 2-1 Integration Profiles Dependencies

Document Digital Signature (DSG)	None	None	-
----------------------------------	------	------	---

215

Volume 3

EDITOR: Add section 5.3

5.3 Document Digital Signature Content Profile

220 The Document Digital Signature (DSG) content profile specifies the use of digital signatures for documents that are shared between organizations.

5.3.1 Overview

225 Electronic documents are being increasingly relied upon in healthcare. Signatures have been a part of the electronic documentation process in health care and have traditionally been indicators of accountability. Reliable exchange of data between disparate systems requires a standard that implements non-repudiation to prevent document creators from denying authorship and rejecting responsibility.

230 This new XDS (Cross-Enterprise Document Sharing) document content profile is constrained to XDS. The document content profile can be used as a reference; however, its specifications are used in other contexts. Systems that do not use XDS can still work with their own methodologies, but those methods will not be covered in the document content profile portion of this supplement.

235 Other IHE clinical domains are encouraged to utilize the digital signature document described in the following document content profile to sign their clinical and administrative documents and use their defined message transfer or use of XDS. For example, Patient Care Coordination could create a patient care workflow that relies on signature or the sharing of patient consent documents.

240 An informative document associated with this supplement may be found on www.ihe.net (Resource Tab). It offers an how-to guide that expands on the issues of using digital signatures within the healthcare domain. It provides examples of how the DSG document content profile can be applied.

5.3.2 Related Document content profiles

This is an infrastructure document content profile that does not include specific workflow (ie: e-prescription and patient referrals). This document provides an infrastructure which may be further managed by their relative domains to ensure cohesiveness.

245 5.3.3 Context for Document Digital Signature

The infrastructure to do the signing, verification, and identity management exists and is not defined in this document content profile. The specific Private Key Infrastructure (PKI) is not

identified by this profile. Whichever infrastructure is selected shall adhere to ISO TS-17090 standards for PKI in healthcare.

250 The scope of this supplement is currently limited to by-reference signatures, where the signature is a reference to the whole document. This document content profile can be used by domains wanting to implement e-referral and e-prescription using signatures by-reference in XDS.

Other forms of signatures such as embedded signatures and partial XML signatures are out of scope for this document content profile. Eg: DICOM, PDF, Digitally signed report.

255 An XDS Repository is not responsible to validate any signature documents it stores. Only Document Sources and Document Consumer Actors are responsible to produce and process document content.

The following text from the XDS profile is supplied here for ease of reference. It will be removed when this document content profile is incorporated in the IHE IT Infrastructure Technical Framework.

260

This property is clearly stated in the IHE XDS Integration Profile, ITI TF-1: 10:

- *“As XDS is document content neutral, any type of clinical information without regard to content and representation is supported.*
- *“A document repository is responsible for storing documents in a transparent, secure, reliable and persistent manner and responding to document retrieval requests”*

265

In ITI TF-1:10.1.2.1 Provider and Register Transaction, it is stated: "A Document Source Actor initiates the Provide and Register Document Set Transaction. For each document in the submitted set, the Document Source Actor provides both the documents as an opaque octet stream and the corresponding metadata to the Document Repository. The Document Repository is responsible to persistently store these documents, and to register them in the Document Registry using the Register Documents transaction by forwarding the document metadata received from the Document Source Actor."

270

In ITI TF-1:10.4.2 XDS Document Concept, it is stated: "When submitted for sharing, an XDS Document is provided to the Document Repository Actor as an octet stream. When retrieved through the Retrieve Document transaction, it shall be unchanged from the octet stream that was submitted.....When submitted for sharing; an XDS Document is provided to the Document Repository Actor as an octet stream. When retrieved through the Retrieve Document transaction, it shall be unchanged from the octet stream that was submitted.

275

In Appendix K, it is stated:

“Furthermore:

- 1. When submitted for sharing, an XDS Document shall be provided to the Document Repository Actor as an octet stream with an associated MIME type.*
- 2. When retrieved through the Retrieve Document transaction, an XDS Document shall be unchanged from the octet stream that was submitted (full fidelity repository).”*

285

Appendix K.3, bullet 2, states that: "The XDS Repositories are not expected to perform any processing or translations on document content. Processing and translation are the responsibility of a Source EHR-CR or Consumer EHR-CR. The analysis, cross-document

290 *combination and presentation of document content is outside the scope of the XDS
Integration Profile and its actors."*

5.3.4 References

- [ASTM-E1985] E1985-98 -- Standard guide for user authentication and authorization
http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1985.htm?E+mystore
- 295 [ASTM-E2212] ASTM E2212 – Standard Practice for Healthcare Certificate Policy
http://www.astm.org/cgi-bin/SoftCart.exe/STORE/filtrexx40.cgi?U+mystore+odvl4256+-L+ASTM:E2212+/usr6/htdocs/astm.org/DATABASE.CART/REDLINE_PAGES/E2212.htm
- 300 [ASTM-E1762-05] ASTM E1762-05 – Standard Guide for the Authentication of Health Care Information
http://www.astm.org/cgi-bin/SoftCart.exe/STORE/filtrexx40.cgi?U+mystore+odvl4256+-L+ASTM:E1762+/usr6/htdocs/astm.org/DATABASE.CART/REDLINE_PAGES/E1762.htm
- 305 [ASTM-E2084] ASTM E2084 – Standard Specification for the Authentication of Healthcare Information using Digital Signatures
http://www.astm.org/cgi-bin/SoftCart.exe/STORE/filtrexx40.cgi?U+mystore+odvl4256+-L+ASTM:E2084+/usr6/htdocs/astm.org/DATABASE.CART/REDLINE_PAGES/E2084.htm
- 310 [ISO17090 (1,2,3)] ISO/TS 17090 – Health Informatics Digital Signatures for Healthcare
<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35489&CS1=35&ICS2=240&ICS3=80>
- [ISO 21091] ISO/TS 21091- Health Informatics – Directory Services for Security, Communications, and Identification of Professionals and Patients
<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35647&copelist=PROGRAMME>
- 315 [IETF RFC3280] IETF/RFC 3280 regarding [X.509](#)v3 PKIX Private Key Infrastructure RFC3280
<http://www.faqs.org/rfcs/rfc3280.html>
- [IETF RFC2633] IETF/RFC 2633 regarding S/MIME <http://www.imc.org/rfc2633>
- [DICOM 41] DICOM Supplement 41 ftp://medical.nema.org/medical/dicom/final/sup41_ft.pdf
- 320 [DICOM 86] DICOM Supplement 86
ftp://medical.nema.org/medical/dicom/supps/sup86_lb.pdf
- [NCPDP] NCPDP prescription data coding, content, formatting and taxonomy <http://www.ncpdp.org>
- [HL7 CDA] HL7 CDA
http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=infostand_hl7doc_arch_e#cda
- 325 [CEN ENV13607] Process flow guidance from CEN Pre-Standard ENV13607 - Health informatics
<http://www.centc251.org>
- [WS-I] WS-I Basic Security Profile Version 1.0, working draft <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

[ETSI TS 201 733] ETSI TS 201 733 Sections C.3.1 and C.3.2; Electronic Signatures and Infrastructures and (ESI)Electronic Signature Formats

330 http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=8179&curlItemNr=1&totalNrItems=1&optDisplay=10&qSORT=REFNB&qETSI_NUMBER=201+733&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&butExpertSearch=Search&includeNonActiveTB=FALSE&qREPORT_TYPE=SUMMARY

[ETSI TS 101 903] ETSI TS 101 903: XML Advanced Electronic Signatures XAdES

335 <http://www.w3.org/TR/XAdES/>

5.3.5 Digital Signature Document content profile Use Cases

The following use cases are resolved with Digital Signature:

5.3.5.1 Attesting a document as true copy

340 The purpose of this use case is to verify that the document being used is the same as the original document and has not been modified by error or intent. This is called establishing *document integrity*. It is also important to ascertain the identity of the signer, and the reason for the signature.

For example, if it needs to be confirmed that a document is a true copy of a source medical document the digital signature is checked. If the signature is verified, then the document is a true copy. If the signature is not verified, then the document has been modified and cannot be trusted.

5.3.5.2 Attesting clinical information content

When a physician has verified that a report is complete and correct, verification will be attested through the use of a signature.

350 If there is ever a need to verify this attestation, the digital signature provides a mechanism to perform the verification.

For example, a clinician who needs to rely on a document which was created by another clinician, may use a signature to ascertain that the version that they are using has been verified.

5.3.5.3 Attesting to a diagnostic report

355 When a doctor verifies and signs a diagnostic report, the digital signature can simultaneously sign the source data that was used to prepare the diagnostic report. For example, the digital signature for a mammography diagnostic report may sign:

- α. The examination procedure notes
- β. The DICOM Mammography images that were read by the radiologist, and
- γ. The verified diagnostic report.

360 This signature indicates more than that the diagnostic report is complete and correct. It also indicates the data that was examined and can detect whether that data is subsequently modified or damaged. Further, it indicates the extent of the data used. If there are also later reports in the XDS registry, e.g., a later lab report, the digital signature indicates that this later information was not used at the time that the report was signed.

365 **5.3.5.4 Attesting to a whole submission set**

When a doctor releases a set of documents for cross enterprise distribution, she can use a digitally signed manifest to indicate the complete grouping of documents:

- a. she is authorizing their release, and
- b. this is the full set of documents in this release:
 - 370 i. the medical documents, and
 - ii. their associated digital signatures at the time of release
 - iii. nothing more than the specified documents

The digital signature document does not mean that she is verifying the clinical content of the documents that is handled by other digital signatures that should be included in the set of
375 documents released.

The recipient organizations can use this digital signature to:

- identify the person who selected and authorized the release,
- obtain the complete list of documents released,
- verify that the released documents have not changed, and
- 380 • identify the associated XDS submission set.

5.3.5.5 Translation

When an original document must be translated (for the purposes of digital signature, translations and transformations will be handled the same way), the original signature cannot be used to
385 validate the translated document. There must be an additional signature generated by the translation. This additional signature signs:

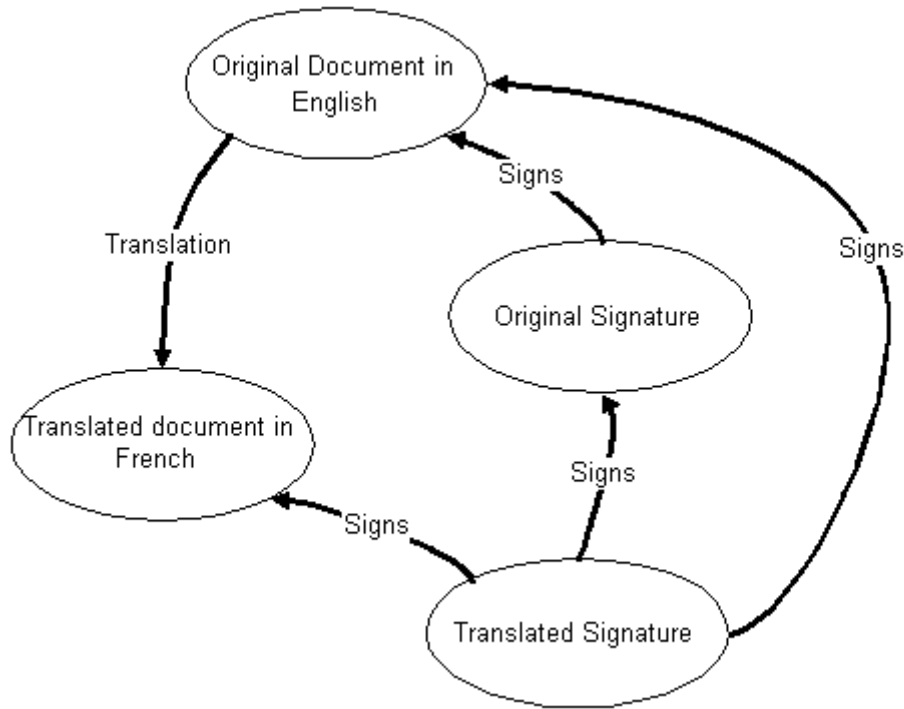
- The original document being translated,
- The resulting translation, and
- The original signature.

This can be used to verify that the translator had the original document, that the original
390 document was signed, and that the translator has attested to the validity of the translation.

Then all four objects must be provided to the user of the translated document:

- The translated document, which will be used
- The translator's signature which will be used to:
 - Verify the translated document
 - 395 ○ Confirm the original document
 - Confirm the original signature
- The original document, and

- The original signature



400

Figure 5.3.5-1 Entity for translation signatures

5.3.6 XDS Signature Document Content

5.3.6.1 Content Standards

405 XDS document content shall conform to XAdES schema for signatures, with extensions and restrictions defined in the following table. We are not changing any optionality, prohibiting use of options, or mandating options. Issues such as long term archival management of certificates are out of scope of this profile.

5.3.6.2 Constraints on Content Standards

Table 5.3.6-1: XDS Signature Document Content

Item	Format	Req.	Definition
Signature element, Id attribute	OID	R	Unique identifier for the XDS Signature document (uniqueID) for the signature document
CanonicalizationMethod element, Algorithm attribute	URI	R	constant value: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
SignatureMethod element, Algorithm attribute	URI	R	constant value: http://www.w3.org/2000/09/xmldsig#rsa-sha1
DigestMethod element, Algorithm attribute	URI	R	constant value: http://www.w3.org/2000/09/xmldsig#sha1
Reference element, URI attribute	text	R	constant value: #IHEManifest

Item	Format	Req.	Definition
Reference element, Type attribute	URI	R	constant value: http://www.w3.org/2000/09/xmlsig#Manifest
KeyInfo element	complex	R	Public key information for validating signatures.
X509Certificate element	base64	R ¹	The actual X.509v3 certificate of the signers, with the public key. This is required for archival validation.
QualifyingProperties element	complex	R	XaDES data for signature time and certificate validity data
SigningTime element	datetime	R	Time that signature was created
SigningCertificate element	complex	R	X.509 identifier of the signing certificates and identifiers for the issuing authorities and parent authorities up to the root authority
Signature Policy Identifier element	complex	R	If there is not a specific signing policy to refer to in the schema, then devices that comply with this profile comply with 'IHEITIDigitalSignatureContentProfile.'
SignatureProperties element	complex	R	Contains the extended properties for the signature
Signature Property element, ID="purposeOfSignature"	text	R	The coded value for the purpose of the signature, defined in ASTM E-1762-05
Manifest element	complex	R	A list of one or more document reference URIs and digest values to which the signature applies.
Manifest element, Id attribute	text	R	constant value: 'IHEManifest'
Reference element, URI attribute	any URI	R	For XDS documents where the uniqueID is an OID. urn:oid:XDSDocumentEntry.uniqueId e.g. "urn:oid:1.2.850.2345.3245.345" For other documents, any valid urn. Note: For DICOM objects the Unique ID is the SOP Instance UID. For CDA documents that have only an OID, the Unique ID is the OID. For other documents, an OID or other standard URN is required.
Transform element, algorithm attribute	any URI	R	For XML objects, use this constant value: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments For DICOM objects, specify the transfer syntax that was used for the hash. All other objects will not have a transfer element and are to be treated as binary BLOBs.

¹ Inclusion of the X.509 certificate enables archival validation of XDS documents in cases such as when the signing certificate expires after time of signing, making the public key no longer available by reference.

5.3.6.3 Mapping Example

410 The following example illustrates what the signature document content will look like:

```

410 <Signature Id="signatureOID" xmlns=http://www.w3.org/2000/09/xmldsig#
      xmlns:xad="xmlns="http://uri.etsi.org/01903/v1.1.1#">
      <SignedInfo>
      <CanonicalizationMethod
415   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="#IHEManifest"
        Type="http://www.w3.org/2000/09/xmldsig#Manifest">
420   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>base64ManifestDigestValue</DigestValue>
      </Reference>
      </SignedInfo>
      <SignatureValue>base64SignatureValue</SignatureValue>
      <KeyInfo>
425   <X509Data>
      <X509Certificate>base64X509certificate</X509Certificate>
      </X509Data>
      </KeyInfo>
      <Object>
430   <xad:QualifyingProperties>
      <xad:SignedProperties>
      <xad:SignedSignatureProperties>
      <xad:SigningTime> yyyymmddhhmmss</SigningTime>
      <xad:SigningCertificate>
435   <xad:Cert> <!-- identifier of signing certificate -->
      <xad:CertDigest>
      <xad:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <xad:DigestValue>base64 digest value</DigestValue>
      </CertDigest>
440   <xad:IssuerSerial>
      <xad:X509IssuerName>X.509 distinguished name of certificate</X509IssuerName>
      <xad:X509SerialNumber>certificate serial number</X509SerialNumber>
      </IssuerSerial>
      </Cert>
445   <xad:Cert> <!-- identifier of signing certificate's parent -->
      <xad:CertDigest>
      <xad:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <xad:DigestValue>base64 digest value</DigestValue>
      </CertDigest>
450   <xad:IssuerSerial>
      <xad:X509IssuerName>X.509 distinguished name of parent's certificate</X509IssuerName>
      <xad:X509SerialNumber>certificate serial number </X509SerialNumber>
      </IssuerSerial>
      </Cert>
455   </SigningCertificate>
      <xad:SignaturePolicyIdentifier>id</SignaturePolicyIdentifier>
      </SignedSignatureProperties>
      </SignedProperties>
      </QualifyingProperties>
460   <SignatureProperties>
      <SignatureProperty Id="purposeOfSignature" target="signatureOID" >

```

```

    code</SignatureProperty>
  </SignatureProperties>
  <Manifest Id="IHEManifest">
465   <Reference URI="urn:oid:1.2.840.97869786987.434536543"> <!-- document A-->
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <DigestValue>base64DigestValue</DigestValue>
     </Reference>
470   <Reference URI="urn:oid:1.2.840.87621394876.123764912764"> <!--XML document B-->
     <Transforms>
       <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
     </Transforms>
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <DigestValue>base64DigestValue</DigestValue> </Reference>
475   <Reference URI="urn :oid :1.2.3.4.5.6.7.8.9"> <!--DICOM document (or object) C-->
     <Transforms>
       <Transform Algorithm="urn:oid:1.2.840.10008.1.2.1"/>
     </Transforms>
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
480     <DigestValue>base64DigestValue</DigestValue>
     </DigestMethod>
     </Reference>
     </Manifest>
  </Object>
485 </Signature>

```

Figure 5.3.6-1 XML Example Signature

5.3.7 Source Mappings

Digital Signatures are stored by an XDS document source as documents in the Repository. They are represented by XDSDocumentEntry objects in the Registry. The table below defines how digital signature fields and signed document content information are used to populate attributes of XDSDocumentEntry objects.

5.3.7.1 Signature Metadata

This section defines the source for all required attributes and as many optional attributes as makes sense for implementors' applications. The columns of the following tables are:

- 495 • XDSDocumentEntryAttribute – name of an XDS attribute
- Optional? -- required status of the XDS attribute, one of R, R2, or O (optional)
- Source Type – one of the following values:
 - SA – Source Document Attribute
 - SAT – Source Document Attribute with Transformation
 - 500 FM – Fixed (constant) for all source documents, value set by this Mapping
 - FAD – Fixed (constant) for all source documents, value configured by Affinity Domain
 - LAD – Value taken from list configured into Affinity Domain

DS – Supplied by document source

n/a – not applicable (only to be used for R2 or O attributes)

505

- Source/Value – the use of this column is determined by the value of Source Type as follows:

Source Type	Use of Source/Value entry
SA	Name/identification of source attribute
SAT	Name/identification of source attribute
FM	Value
FAD	None
LAD	None
DS	Source if information in Document Source Actor
n/a	None

Any attribute labeled with a Source Type of SAT must have its transformation documented in the next section: Attribute Transforms.

Table 5.3..7-1: XDS Document Entry Attribute

XSDocumentEntryAttribute	Optional?	Constrained?	Extended Discussion (section number)?	Source Type	Source/ Value
authorInstitution	R2	No			
authorPerson	R2	No	Need doc. for transform	SAT	X.509v3 Certificate “Subject” . Represents the human and/or machine that signed the document in association with and on behalf of the signatureInstitution. The document signer may be the patient. Author is multivalued. The author field is the list of digital signature signers in this case. Note: for Asian names, one person may consume multiple slots. E.g., one for the kanji name and one for the phonetic name. The ID field will be the same when a single multi-part name is encoded as multiple Author fields.. <i>See the PWP Profile section ITI TF-1:2.3.2.4.5.2.3.1 for further information on name encoding and searching.</i>
authorRole	R2	no			
authorSpecialty	R2	no			

XSDDocumentEntryAttribute	Optional?	Constrained?	Extended Discussion (section number)?	Source Type	Source/ Value
classCode	R	yes		FM	Coding scheme= URN code value = <i>urn:oid:1.3.6.1.4.1.19376.1.2.1.1.1</i> Code value display name = "Digital Signature" note: The code value OID will be supplied as a change proposal
confidentialityCode	R	no		DS	An affinity domain policy should define how this code is related to the confidentiality codes of the signed documents.
creationTime	R	no	section number (should point to transform definition)	SAT	creationTime shall be the signature time. XML to HL-7 time format conversion required. Note: The XDS profile and various security standards require that these times be true time. The IHE Consistent Time profile provides that service.
entryUUID	R	no		N/A or DS	Supplied by Registry or Document Source
eventCodeList	R	no	need transformation	SAT	signaturePurpose One code shall contain the signature purpose. The signaturePurpose code shall be selected from ASTM 1762 when applicable. The affinity domain may define other purpose codes for signatures. Note: The eventCodeList may also contain other event codes that are unrelated to signature purpose. The ASTM codes are shown below in Table 4.7-2
formatCode	R	yes		LAD	Coding scheme = "URN" Code value = <i>"http://www.w3.org/2000/09/xmlsig#"</i> Code value display name = "Default Signature Style" Transform, stylesheet, or other formatting specification for displaying the digital signature. Code value will be provided by change proposal.
hash	R	no		N/A	This is NOT the digest of the signed document. This is a simple document hash for XDS repository integrity, not related to the hash used to calculate the signature itself.

XSDDocumentEntryAttribute	Optional?	Constrained?	Extended Discussion (section number)?	Source Type	Source/ Value
healthcareFacilityTypeCode	R	no		LAD	
languageCode	R	yes		FM	‘art’ Main language of the signature content shall be ‘art’ as in “artificial”.
legalAuthenticator	O	yes		N/A	Shall not be used because the body of the Digital Signature Document contains the full details
mimeType	R	yes		FM	text/xml
patientID	R	no		DS	
practiceSettingCode	R	no		LAD	
serviceStartTime	R	no	section number (should point to transform definition)	SAT	serviceStartTime shall be the signature time. XML to HL-7 time format conversion required. Note: The XDS profile and various security standards require that these times be true time. The IHE Consistent Time profile provides that service. Transform will be provided by change proposal.
serviceStopTime	R	no	section number (should point to transform definition)	SAT	serviceStopTime shall be the signature time. XML to HL-7 time format conversion required. Note: The XDS profile and various security standards require that these times be true time. The IHE Consistent Time profile provides that service. Transform will be provided by change proposal.
sourcePatientID	R	no		DS	
sourcePatientInfo	R	no		DS	
Title	R	no		SA	Display name of the purpose of the signature. Shall be equivalent to display name from the signaturePurpose above.
typeCode	R	no		LAD	Coding schema = “ASTM” Code value = “E1762” Code value display name = ”Full Document”
uniqueID	R	no		SA	<uniqueID Schema Section>

510

Table 5.3.7-2: Digital Signature Purposes

Code	Coding Scheme	Definition
1.2.840.10065.1.12.1.1	1.2.840.10065.1.12	Author ID
1.2.840.10065.1.12.1.2	1.2.840.10065.1.12	Co-Author ID
1.2.840.10065.1.12.1.3	1.2.840.10065.1.12	Co-participated
1.2.840.10065.1.12.1.4	1.2.840.10065.1.12	Transcriptionist
1.2.840.10065.1.12.1.5	1.2.840.10065.1.12	Verification
1.2.840.10065.1.12.1.6	1.2.840.10065.1.12	Validation
1.2.840.10065.1.12.1.7	1.2.840.10065.1.12	Consent
1.2.840.10065.1.12.1.8	1.2.840.10065.1.12	Witness
1.2.840.10065.1.12.1.9	1.2.840.10065.1.12	Event-Witness
1.2.840.10065.1.12.1.10	1.2.840.10065.1.12	Identity-Witness
1.2.840.10065.1.12.1.11	1.2.840.10065.1.12	Consent-Witness
1.2.840.10065.1.12.1.12	1.2.840.10065.1.12	Interpreter
1.2.840.10065.1.12.1.13	1.2.840.10065.1.12	Review
1.2.840.10065.1.12.1.14	1.2.840.10065.1.12	Source
1.2.840.10065.1.12.1.15	1.2.840.10065.1.12	Addendum
1.2.840.10065.1.12.1.16	1.2.840.10065.1.12	Administrative
1.2.840.10065.1.12.1.17	1.2.840.10065.1.12	Time Stamp

5.3.7.2 XDSSubmissionSet Metadata

515 This document content profile makes no changes to the structure of XDS Submission Sets. A Signature Document signs the content of one or more XDS Documents, including a whole Submission Set. However, metadata in Registry Document entries and Registry Submission Set entries for signed documents are not signed. In particular any patient Id merge in the XDS Document Registry will not invalidate signatures as the documents will not be changed when such merge are performed. While they may be replaced, they would not invalidate old signatures, and may call for a new signature.

520

5.3.7.3 XDSFolder Metadata

This document content profile makes no changes to the structure of XDS Folders.

5.3.7.4 Use of XDS Folders

This document content profile makes no changes to the structure of XDS Folders.

525 **5.3.8 DSG Creation Processing**

This section describes suggested processing needed by the Actor that would be creating and registering a Document Digital Signature document.

5.3.8.1 Signature of a one or more XDS Documents

A signed document (XDSDocumentEntry) is posted to the XDS Repository/Registry by:

- 530 1. Submitting a document along with its metadata (XDSDocumentEntry) to a repository/registry.
2. Create a DSG document that is compliant to this DSG Profile, containing references to each document using XDSDocument.UniqueId, and containing the appropriate document hash value.
- 535 3. Submitting a digital signature document along with its metadata (XDSDocumentEntry) to a repository/registry. This may be included in the same submission set that carried the document being signed but it is not required.
4. Submit an Association object connecting the digital signature XDSDocumentEntry object to the XDSDocumentEntry object it signs. This associationType is defined specifically for XDS Signature Documents.
- 540 5. Specifically, the Association object attributes are:
 - a. *sourceObject*: points to the digital signature XDSDocumentEntry object
 - b. *associationType*: Signs
 - c. *targetObject*: points to the XDSDocumentEntry object being signed
- 545 6. Other requirements on composing a registry submission may be specified in a separate Document Content Profile.

5.3.8.2 Signature of a whole XDS Submission Set

550 The use case "Attesting to a whole Submission Set" from section 4.5.4, enables the signing of a collection of documents and the XDS Submission Set. The following steps are performed by the Document Source actor in addition to the above steps to form such a 'Signed' Submission Set.

When a XDS Document Source Actor assembles a Submission Set to be signed it shall:

1. Create a Document Digital Signature per this DSG profile that includes:
 - a. A Reference to the submission set using the XDSSubmissionSet.UniqueId assigned by the XDS Document Source Actor.
 - 555 i. The digital hash of this entry shall be 0 (zero).
 - b. References to each of the documents in the Submission Set using their document.UniqueId.
 - ii. New documents will have their document.UniqueId assigned by the XDS Document Source

- 560 iii. The document.UniqueId for documents that had previously been submitted to the XDS, potentially by a different XDS Document Source, may be discovered by using the XDS Query Transaction.
- iv. Each document entry in the DSG document shall have a proper hash.
- 565 2. Assemble the submission set with all documents referenced in the DSG document and the DSG document.
3. The Submission Set shall be registered with the XDS Registry using the normal XDS Provide/Register Transaction with the additional processing shown in ITI TF-3: 4.8.1 above.

570 Note The XDSDocument.UniqueId values and the document hash values need to be available to the Document Source Actor at the time the Document Digital Signature document is created. This may be accomplished through the use of the XDS Query transaction.

5.3.9 Processing by XDS Document Consumer

5.3.9.1 Query Processing

575 The following sections describe how common queries can be performed in an affinity domain where document digital signatures are used.

5.3.9.1.1 Search for signatures, given a document

580 The signatures that apply to a specific document can be found by querying the XDS Registry to obtain the “signs” association linkages to that specific document. The documents at the other end of those linkages can then be checked to find the ones with a classCode of “Digital Signature”. Those are the signatures that apply to the specific document.

5.3.9.1.2 Search for documents, given a signature

585 The signature document itself contains a manifest that lists the document IDs for all of the signed documents. It might also contain a submission set ID for a submission set. The documents can be obtained through either the XDS system or an affinity domain mechanism based on the document IDs. (It is possible that authorization or other limits may prevent retrieval of some of these documents.)

5.3.9.1.3 Search for signatures

590 The signature documents all contain a classCode for digital signature. This can be used to query for digital signatures in a time range, for specific patient, etc. The signature purpose codes can be used to limit these signatures. For example, a query may choose to eliminate data integrity signatures and search only for clinician signatures.

5.3.9.1.4 Ignore signature documents in query

 The document classCode can also be used to suppress reporting of signatures in queries that are intended to retrieve only source documents. In an environment with extensive use of data

595 integrity, creation, verification, and other signatures there may be several signature documents
for each source document. If signature documents are not suppressed then a query for clinical
documents may also have distracting extra results returned for signatures.

5.3.9.2 Signature Verification

Signature verification is not a single concept. There are several kinds of verification:

- 600 a. Verify the integrity of the signature itself
- b. Verify a), plus that it is a valid signature
- c. Verify b), plus that specific documents are also unmodified and are the documents that were
signed. (This may be impossible if access to the documents is denied.)
- 605 d. Verify b), plus that there is a submission set reference in the manifest and that the documents
listed in the manifest are the complete list of documents in the submission set on the XDS
Registry.
- e. Verify b), plus that all of the documents are available and unmodified.
- f. Verify d), plus that all of the documents are available and unmodified.

610 The decision on what degree of verification is needed is determined by the application and use
case. This IHE content profile does not specify what level needs to be implemented.

5.3.10 Configuration

5.3.10.1 PKI Configuration

615 A PKI must exist and be configured. The definition and configuration of PKI is outside the scope
of this document content profile. However it is provided, it shall manage certificates in a manner
than conforms to the ISO/TS-17090 standard.

5.3.10.2 Affinity Domain Configuration

620 The local affinity domain must ensure that all documents referenced by the digital signature are
accessible by XDS or by an affinity domain specified means. Document accessibility must be
maintained for at least the duration of time that the signature is required to be maintained
according to affinity domain specified policy.

Glossary

- **Accountability**—the property that ensures that the actions of an entity may be traced uniquely to the entity
- 625 • **Attestation** – Attestation is a personal assertion of the truth of the statement to which you are attesting.
- 630 • **Digital Signature** - A useful legal equivalent to facsimile signature that may be generated for a variety of entities, including human and machine sources. Based on digital certificates attributable to well-known healthcare oriented certificate authorities; incorporating cryptographically secure techniques for signature generation and validation. An actor uses a private key to generate a digital signature by encrypting the hash value. By recalculating the hash digest value, and using the actor's certificate's public key to decrypt the electronic signature, it is possible to attest to the actor's signing ceremony and to the integrity of the signed record.
- 635 • **Hash** - A value uniquely calculated by using a well-known one way algorithm to create a digest of all the data constituting an electronic record.
- **Integrity** – The property of the data has not been altered, or destroyed in an unauthorized manner.
- 640 • **Non-repudiation** – This service provides proof of the integrity and origin of data which can be verified by any party.
- **Private Key** - a key in an asymmetric cryptographic algorithm; the possession of this key is restricted, usually to one entity.
- **Public key** - a key in an asymmetric algorithm that is publicly available
- **Signature ceremony** – an instance of an entity creating a digital signature document.
- 645 • **Signature purpose** - an indication of the reason an entity signs a document. This may be explicitly included as part of the signed information and can be used when determining accountability for various actions concerning the document. Examples include: author, transcriptionist/recorder, and witness.
- **Signature time** - the date and time of a signature ceremony.