Digital Imaging and Communications in Medicine (DICOM)

Supplement 86: Digital Signatures in Structured Reports

Prepared by:

DICOM Standards Committee, Working Group 14 - Security

1300 N. 17th Street, Suite 1847

Rosslyn, Virginia 22209 USA

VERSION: Final Text, 2005/06/14 (amended 2005/08/01 to add data element tags)

Table of Contents

Foreword

This document is a Supplement to the DICOM Standard. It modifies PS 3.3, 3.6, 3.15, 3.16, and 3.17 of the published DICOM Standard. The additions outlined in this supplement are intended to address issues discovered during demonstrations of Digital Signatures in SR.

This Supplement includes additions to the Digital Signature mechanism introduced in Supplement 41. These additions provide support for including Digital Signatures in Structured Reports, and for collecting references to a set of related objects into a Key Object Selection Document with Digital Signatures.

Digital Signatures as defined in current DICOM profiles require the use of X.509 certificates and an appropriate key distribution mechanism. The key distribution mechanism has not been included in the scope of DICOM. There are several other standards development organizations (e.g. ISO TC 215 WG 4) that are considering Public Key Infrastructures (PKI) for use in healthcare. Even in the absence of a PKI, a site can create its own internal mechanism for key distribution.

Scope and Field of Application

This Supplement describes how Digital Signatures would be used within the context of a DICOM Structured Report. This supplement adds

— a code sequence attribute to the Digital Signatures Macro that can be used to identify the purpose of a Digital Signature (e.g. author, verifier, etc.),

— a mechanism for securely referencing a digitally signed object,

— a mechanism for securely referencing an object that is not digitally signed,

— a Digital Signature profile that describes the use of Digital Signatures in a Structured Report,

— a modification of the Key Object Selection Document Template, which can be used to collect secure references to a related set of DICOM composite objects.

The use of the mechanisms and profiles in this Supplement is intended to allow the reader of a structured report to determine

— if the report has been altered since its creation,

— if evidence referenced by the report has not been altered since the report creator utilized it,

— the identities of the parties that signed the report, thus minimizing the chance of a fictitious report being created.

Additions to PS 3.17

Add the following annex to PS 3.17

Annex X Digital Signatures in Structured Reports Use Cases (Informative)

The scenarios in which Digital Signatures would be used in DICOM Structured Reports include, but are not limited to the following.

Case 1: Human Signed Report and Automatically Signed Evidence.

a. The archive, after receiving an MPPS complete and determining that it has the complete set of objects created during an acquisition procedure step, creates a signed Key Object Selection Document Instance with secure references to all of the DICOM composite objects that constitute the exam. The Document would include a Digital Signature according to the Basic SR Digital Signatures Secure Use Profile with the Digital Signature Purpose Code Sequence (0400,0401) of (14,ASTM-sigpurpose,"Source Signature"). It would set the Key Object Selection Document Title of that Instance to (113035,DCM, "Signed Complete Acquisition Content"). Note that the objects that are referenced in the MPPS may or may not have Digital Signatures. By creating the Key Object Selection Document Instance, the archive can in effect add the equivalent of Digital Signatures to the set of objects.

b. A post-processing system generates additional evidence objects, such as measurements or CAD reports, referring to objects in the exam. This post-processing system may or may not include Digital Signatures in the evidence objects, and may or may not be included as secure references in a signed Key Object Selection Document.

c. Working at a reporting station, a report author gathers evidences from a variety of sources, including those referenced by the Key Object Selection Document Instance and the additional evidence objects generated by the post-processing system, and incorporates his or her own observations and conclusions into one or more reports.

d. It is desired that all evidence references from a DICOM SR be secure. The application creating the SR may either:

   1. create secure references by copying a verified Digital Signature from the referenced object or by generating a MAC code directly from the referenced object,

   2. make a secure reference to a signed Key Object Selection Document that in turn securely references the SOP Instances, or

   3. copy the secure reference information from a trusted Key Object Selection Document to avoid the overhead of recalculating the MAC codes or revalidating the reference Digital Signatures.

e. When the author completes a DICOM SR, the system, using the author’s X.509 Digital Signature Certificate generates a Digital Signature with the Digital Signature Purpose Code Sequence (0400,0401) of (1,ASTM-sigpurpose,”Author Signature“) for the report.

f. The author’s supervisor reviews the DICOM SR. If the supervisor approves of the report, the system sets the Verification Flag to “VERIFIED” and adds a Digital Signature with the Digital Signature Purpose Code Sequence (0400,0401) of (5,ASTM-sigpurpose,”Verification Signature“) or (6,ASTM-sigpurpose,”Validation Signature“) using the supervisor’s X.509 certificate.

g. At some later time, someone who is reading the DICOM SR SOP Instance wishes to verify its authenticity. The system would verify that the Author Signature, as well as any Verification or Validation Signature present are intact (i.e., that the signed data has not been altered based on the recorded Digital Signatures, and that the X.509 Certificates were valid at the time that the report was created).

h. If the report reader wishes to inspect DICOM source materials referenced in a DICOM SR, the system can insure that the materials have not been altered since the report was written by verifying the Referenced Digital Signatures or the Referenced SOP Instance MAC that the report creator generated from the referenced materials.

Case 2: Cross Enterprise Document Exchange

a. An application sends by any means a set of DICOM composite objects to an entity outside of the institutional environment (e.g. for review by a third party).

b. The application creates a signed Key Object Selection Document Instance with a Key Object Selection Document Title of (113031,DCM, “Signed Manifest”) referencing the set of DICOM Data Objects that it sent outside the institutional environment, and sends that SR to the external entity as a shipping manifest.

c. The external entity may utilize the Key Object Selection SR SOP Instance to confirm that it received all of the referenced objects intact (i.e., without alterations). Because the signed Key Object Selection Instance must use secure references, it can verify that the objects have not been modified.

Additions to PS 3.3

Add the following entries to the Digital Signatures Sequence in Table C.12-5 Digital Signatures Macro.

Table C.12-5
Digital Signatures Macro

Attribute Name	Tag	Type	Attribute Description
Digital Signatures Sequence	(FFFA,FFFA)	3	
…			
>Digital Signature Purpose Code	**(0400,0401)**	**3**	**The purpose of this Digital Signature.**

Sequence			
>>Include 'Code Sequence Macro' Table 8.8-1			*Baseline Context ID is 7007*

114 **Add the following entries to the Referenced SOP Sequence in Table C.17-3 SOP Instance Reference Macro.**

116 **Table C.17-3**
SOP Instance Reference Macro

Attribute Name	Tag	Type	Attribute Description
Study Instance UID	(0020,000D)	1	Unique identifier for the Study
Referenced Series Sequence	(0008,1115)	1	Sequence of Repeating Items where each Item includes the Attributes of a Series containing referenced Composite Object(s). One or more Items may be included in this sequence
>Series Instance UID	(0020,000E)	1	Unique identifier of a Series that is part of this Study and contains the referenced Composite Object(s).
>Retrieve AE Title	(0008,0054)	3	Title of the DICOM Application Entity where the Composite Object(s) may be retrieved on the network.
>Storage Media File-Set ID	(0088,0130)	3	The user or implementation specific human readable identifier that identifies the Storage Media on which the Composite Object (s) reside.
>Storage Media File-Set UID	(0088,0140)	3	Uniquely identifies the Storage Media on which the Composite Object (s) reside.
>Referenced SOP Sequence	(0008,1199)	1	References to Composite Object SOP Class/SOP Instance pairs that are part of the Study defined by Study Instance UID and the Series defined by Series Instance UID (0020,000E). One or more Items may be included in this sequence
>>Referenced SOP Class UID	(0008,1150)	1	Uniquely identifies the referenced SOP Class.
>>Referenced SOP Instance UID	(0008,1155)	1	Uniquely identifies the referenced SOP Instance.
>>Referenced Digital Signature Sequence	**(0400,0402)**	**3**	**Sequence of references to Digital Signatures in the referenced SOP Instance. Zero or more Items may be present.** **Note: The Attributes in this sequence can be used to detect if the referenced SOP Instance has been altered.**

>>>Digital Signature UID	(0400,0100)	1	The Unique Identifier of a Digital Signature held in the referenced SOP Instance.
>>>Signature	(0400,0120)	1	The Signature Value identified by the Digital Signature UID within the Referenced SOP Instance UID.
>>Referenced SOP Instance MAC Sequence	(0400,0403)	3	A MAC Calculation from data in the referenced SOP Instance that can be used as a data integrity check. Note: This Attribute may be used in place of the Referenced Digital Signature Sequence Attribute (0400,0402), particularly if the SOP Instance does not have appropriate Digital Signatures that can be referenced.
>>>MAC Calculation Transfer Syntax UID	(0400,0010)	1	The Transfer Syntax UID used to encode the values of the Data Elements included in the MAC calculation. When computing the MAC, only Transfer Syntaxes that explicitly include the VR and use Little Endian encoding shall be used. Notes: 1. Certain Transfer Syntaxes, particularly those that are used with compressed data, allow the fragmentation of the pixel data to change. If such fragmentation changes, Digital Signatures generated with such Transfer Syntaxes could become invalid. 2. This does not constrain the transfer syntax used to transmit the object.
>>>MAC Algorithm	(0400,0015)	1	The algorithm used in generating the MAC. Defined Terms: RIPEMD160 MD5 SHA1 Note: Digital Signature Security Profiles (see PS 3.15) may require the use of a restricted subset of these terms.
>>>Data Elements Signed	(0400,0020)	1	A list of Data Element Tags in the order they appear at the top level of the referenced SOP Instance that identify the Data Elements used in creating the MAC. See Section C.12.1.1.3.1.1.
>>>MAC	(0400,0404)	1	The MAC generated as described in Section 12.2.1.1, but unencrypted and without inclusion of fields from the Digital Signatures Sequence. See Section C.12.1.1.3.1.2.

2 Additions to PS 3.6

Add the following Attribute definitions to PS 3.6

Tag	**Name**	**VR**	**VM**
(0400,0401)	**Digital Signature Purpose Code Sequence**	**SQ**	**1**
(0400,0402)	**Referenced Digital Signature Sequence**	**SQ**	**1**
(0400,0403)	**Referenced SOP Instance MAC Sequence**	**SQ**	**1**
(0400,0404)	**MAC**	**OB**	**1**

3 Additions to PS 3.15

Add the following Secure Use Profiles to PS 3.15

A.Y BASIC SR DIGITAL SIGNATURES SECURE USE PROFILE

Any implementation that claims conformance to this Security Profile shall obey the following rules when creating a Structured Report or Key Object Selection Document that includes Digital Signatures:

a. When the implementation signs a Structured Report or Key Object Selection Document SOP Instance the Digital Signatures shall be created in accordance with the Structured Report RSA Digital Signature Profile.

b. In every signed Structured Report or Key Object Selection Document SOP Instance created, all referenced SOP Instances listed in the Referenced SOP Sequence Items of the Current Requested Procedure Evidence Sequence (0040,A375) and Pertinent Other Evidence Sequence (0040,A385) shall include either a Referenced Digital Signature Sequence or a Referenced SOP Instance MAC Sequence. The references may include both.

The implementation claiming conformance shall outline in its conformance statement the conditions under which it will either sign or not sign a Structured Report or Key Object Selection Document.

Add the following Digital Signature Profile to PS 3.15

C.X STRUCTURED REPORT RSA DIGITAL SIGNATURE PROFILE

This profile defines a mechanism for adding Digital Signatures to Structured Reports or Key Object Selection Documents where there is no more than one Verifying Observer. Instances that follow this Digital Signature Profile shall include at least one Digital Signature at the top level of the Data Set.

All Digital Signatures that follow this profile shall include a Digital Signature Purpose Code Sequence Attribute (0400,0401).

As a minimum, an implementation shall include the following attributes in generating the Digital Signature required by this profile:

a. the SOP Class UID
b. the Study and Series Instance UIDs
c. all attributes of the General Equipment Module that are present
d. the Current Requested Procedure Evidence Sequence
e. the Pertinent Other Evidence Sequence
f. the Predecessor Documents Sequence
g. the Observation DateTime
h. all attributes of the SR Document Content Module that are present

If the Verification Flag is set to “VERIFIED” (and the SOP Instance UID can no longer change) at least one of the Digital Signatures profile shall have the purpose of (5,ASTM-sigpurpose,”Verification Signature“) and shall also include the following Attributes in addition to the above attributes:

i. the SOP Instance UID
j. the Verification Flag
k. the Verifying Observer Sequence
l. the Verification DateTime

Notes: The system may also add a Creator RSA Digital Signature, which could cover other attributes that the machine can verify.

All occurrences of Referenced SOP Instance MAC Sequence (0400,0403) shall have the Value of MAC Algorithm (0400,0015) set to either "RIPEMD160", “MD5”, or “SHA1”.

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile. The Application Entity shall determine the identity of the signatories and obtain their certificate through an application-specific procedure such as a login mechanism or a smart card. The conformance statement shall specify how the application identifies signatories and obtains certificates.

Note: Structured Report RSA Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Creator RSA Digital Signature, may be used to corroborate the timestamp of a Structured Report RSA Digital Signature.

3 Additions to PS 3.16

Add the following references to Section 2 in PS 3.16

2 Normative references

…

ASTM E 1762-04 **Standard Guide for Electronic Authentication of Health Care Information, ASTM International**

ASTM E 2084-00 **Standard Specification for Authentication of Healthcare Information Using Digital Signatures, ASTM International**

Make the following changes to Table 8-1 in PS 3.16

Table 8-1 Coding Schemes

Coding Scheme Designator	Coding Scheme UID	Description
ACR		ACR Index for Radiological Diagnosis Revised, 3rd Edition 1986
AS4		American Society for Testing & Materials and CPT4 (see Appendix A of ASTM E1238 and its codes revisions).
ASTM-sigpurpose	**1.2.840.10065.1.12**	**ASTM E 2084 Signature Purpose codes (see Annex A1 of ASTM E 2084), ASTM Subcommittee E 31.20 Data and System Security for Health Information**
…		

Make the following changes to TID 2010 in PS 3.16

TID 2010 KEY OBJECT SELECTION

The Key Object Selection template is intended for flagging one or more significant images, waveforms, or other composite SOP Instances. Key Object Selection contains:

- coded document title stating the reason for significance of the referenced objects in the Key Object Selection,
- optional free form text comment in an explicitly identified language, and
- optional identification of the observer (device or person) which created the Key Object Selection.

Notes: 1. For instance, when this template is used to identify images rejected for quality reasons, the device or person performing the quality assessment is identified in observation context items (invoked through TID 1002). The reason for rejection can be included both as a code used as a concept modifier for the document title, and as text description.

2. The order of object references may be significant, e.g., when the title concept is "For Conference".

3. Instances referenced in a Key Object Selection Document may be securely referenced by Digital Signature or MAC mechanisms within the SR Document General Module (See PS 3.3).

The Template can only be instantiated at the root node and cannot be included in other templates. The Template is not extensible; that is, no other content items may be added to this template, or the templates that are included, recursively.

TID 2010
KEY OBJECT SELECTION
Type: Non-Extensible

	NL	Rel with Parent	VT	Concept Name	VM	Req Type	Condition	Value Set Constraint
1			CONTAINER	DCID(7010) Key Object Selection Document Titles	1	M		Root node
2	>	HAS CONCEPT MOD	CODE	EV (113011, DCM, "Document Title Modifier")	1-n	U		
3	>	HAS CONCEPT MOD	CODE	EV (113011, DCM, "Document Title Modifier")	1	UC	IF Row 1 Concept Name = (113001, DCM, "Rejected for Quality Reasons") or (113010, DCM," Quality Issue")	DCID (7011)
4	>	HAS CONCEPT MOD	CODE	EV (113011, DCM, "Document Title Modifier")	1	MC	IF Row 1 Concept Name = (113013, DCM, "Best In Set")	DCID (7012)
5	>	HAS CONCEPT MOD	INCLUDE	DTID(1204) Language of Content Item and Descendants	1	U		
6	>	HAS OBS CONTEXT	INCLUDE	DTID(1002) Observer Context	1	U		
7	>	CONTAINS	TEXT	EV(113012, DCM, ”Key Object Description”)	1	U		
8	>	CONTAINS	IMAGE	Purpose of Reference shall not be present	1-n	MC	At least one of Rows ~~7, 8, and 9~~ **8, 9, and 10** shall be present	
9	>	CONTAINS	WAVEFORM	Purpose of Reference shall not be present	1-n	MC	At least one of Rows ~~7, 8, and 9~~**8, 9, and 10** shall be present	
10	>	CONTAINS	COMPOSITE	Purpose of Reference shall not be present	1-n	MC	At least one of Rows ~~7, 8, and 9~~**8, 9, and 10** shall be	~~**Shall not reference another Key Object**~~

							present	~~**Selection Document**~~

Add the following rows to Defined Context Group 7010 in PS 3.16

CID 7010 Key Object Selection Document Title

Context ID 7010
Key Object Selection Document Title
Type: Extensible Version: 20020904

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	113000	Of Interest
DCM	113001	Rejected for Quality Reasons
DCM	113002	For Referring Provider
DCM	113003	For Surgery
DCM	113004	For Teaching
DCM	113005	For Conference
DCM	113006	For Therapy
DCM	113007	For Patient
DCM	113008	For Peer Review
DCM	113009	For Research
DCM	113010	Quality Issue
DCM	113013	Best In Set
DCM	113018	For Printing
DCM	**113030**	**Manifest**
DCM	**113031**	**Signed Manifest**
DCM	**113032**	**Complete Study Content**
DCM	**113033**	**Signed Complete Study Content**
DCM	**113034**	**Complete Acquisition Content**
DCM	**113035**	**Signed Complete Acquisition Content**

Add the following Defined Context Groups to PS 3.16

CID 7007 Signature Purpose

Context Group ID 7007 comprises the signature purposes codes of ASTM E 2084-00. The Coding Scheme Designator (0008,0102) shall be “ASTM-sigpurpose”. The ASTM document defines the signature purpose codes as OIDs. For the purposes of this Coding Scheme only the leaf digit is used as the Code Value (0008,0100).

Note: ASTM E 1762 provides the full definitions for the signature purpose OIDs defined by E 2084. The recommended Code Meanings (0008,0104) are the titles of the definitions for the leaves of the OIDs. For example, the OID 1.2.840.10065.1.12.1 corresponds to the leaf “id-purpose-author”, whose meaning could be encoded as “Author Signature” and whose code value is 1.

Add the following definitions to Annex D of PS 3.16

DICOM Code Definitions (Coding Scheme Designator “DCM” Coding Scheme Version “01”)

Code Value	Code Meaning	Definition	Notes
113030	Manifest	A list of objects that have been exported out of one organizational domain into another domain. Typically, the first domain has no direct control over what the second domain will do with the objects.	
113031	Signed Manifest	A signed list of objects that have been exported out of one organizational domain into another domain, referenced securely with either Digital Signatures or MACs. Typically, the first domain has no direct control over what the second domain will do with the objects.	
113032	Complete Study Content	The list of objects that constitute a study at the time that the list was created.	
113033	Signed Complete Study Content	The signed list of objects that constitute a study at the time that the list was created, referenced securely with either Digital Signatures or MACs.	
113034	Complete Acquisition	The list of objects that were	

	Content	**generated in a single procedure step.**	
113035	**Signed Complete Acquisition Content**	**The signed list of objects that were generated in a single procedure step, referenced securely with either Digital Signatures or MACs.**	