Integrating the Healthcare Enterprise

IHE IT Infrastructure
Technical Framework Supplement

Document Digital Signature
(DSG)

Trial Implementation

Date: September 9, 2016
Author: IHE ITI Technical Committee
Email: iti@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework V13.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on September 9, 2016 for trial implementation and may be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure Technical Framework. Comments are invited and may be submitted at http://www.ihe.net/ITI_Public_Comments.

This supplement describes changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume.

Amend Section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text **~~bold strikethrough~~**. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at: http://ihe.net.

Information about the IHE IT Infrastructure domain can be found at: http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at: http://ihe.net/Resources/Technical_Frameworks.

CONTENTS

Introduction to this Supplement

The changes to the IHE DSG Profile are significant should be considered a breaking-change from the original DSG supplement published in 2009. The DSG supplement has remained in "Trial Implementation" since 2009. Breaking changes during "Trial Implementation" are proper and should be expected.

The Document Digital Signature (DSG) Profile is a Document Content Profile that provides general purpose methods of digitally signing of documents for communication and persistence. This method can be used within a Document Sharing infrastructure (e.g., XDS, XCA, XDM, XDR, and MHD). There are three methods of digital signature provided: Enveloping, Detached, and SubmissionSet. An Enveloping Signature is a signature approach that encapsulates the signed content within the signature syntax. A Detached Signature is a signature approach that manages the signature as a manifest that points at independently managed content. The SubmissionSet Signature is a Detached Signature that covers a SubmissionSet. This supplement chooses the use of XML Digital Signature. Other types of signatures may be valid but are not part of this profile.

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.

This second revision of the DSG supplement addresses the following:

- Puts the profile into the current supplement template
- Puts the profile into the current Document Content format
- Adds Enveloping Signature, which is especially useful when Document Sharing is not used. For example: RFD based output.
- Adds details on how to use Detached Signature for a SubmissionSet Signature, which has been used in France.
- Update the signature standards: XAdES specifically that now includes profiles for Long-Term signatures

Open Issues and Questions

None

Closed Issues

DSG_2: HL7 CDA®[1] has produced an Enveloped Signature, DICOM®[2] has an enveloped signature, and so does PDF. An enveloped signature is a signature approach where the signature syntax is enveloped within the structure of the signed content. This has not been brought into this supplement due to scope of the original work item. This approach can be brought to IHE as a future work item that may be a CP or might need to be a Supplement work item. Care has been taken in this CP to assure that the signature block is self-standing and could thus be used in an enveloped signature.

DSG_1: Need new assigned numbers. DSG was never give a Volume 1 Section (assigned 37), and DSG was previously given Volume 3 Section 5.3 but that is the same number used by DEN (assigned 5.5).

DSG_3: The original DSG forced the signature algorithms to SHA1. This is likely not the choice we would make today. Should we upgrade our algorithm? If so, should we provide a historic option? Or is the creation algorithm not critical, as the algorithm identification is included in the signature? Meaning that it is clear to the consumer which algorithm was used, we will assure that consumers must support sha1 and sha2. Should also note that a new algorithm to replace SHA is in development so future will change.

DSG_4: ITI has uses of Document Creator and Document Consumer that presumes these are abstract actors for creating/consuming Document content, where Document content is a generic concept defined in Document Sharing. However the current PCC technical framework has defined these actors specific to Document Content that is CDA centric. Thus there are 'options' that are inappropriate for Document Content profiles that are not CDA centric. ITI has many of these including BPPC, XDW, DEN, and DSG. I will follow the same documentation model as other ITI profiles, ignoring these options. However ITI really needs to have their own abstract definition of actors that do more of a binding to the Document Sharing concepts.

DSG_5 and **DSG_6**: Enveloping signature as included here is for use cases that don't use Document Sharing so this supplement does not give guidance on how to create the Document Sharing metadata (e.g., XDS). The metadata would need to describe the XML-Signature format is Enveloping the signed document, while also describing the signed document in a way that doesn't confuse a Document Consumer. Future efforts could propose solutions.

DSG_7: Detached signature uses XAdES mechanism for pointing at the signed document(s). This requires a URI, so we use only the Document Unique ID, and don't carry the homeCommunityId. Where the document is within the local domain, the homeCommunityId is not necessary.

DSG_8: There is no example signature included as XAdES includes examples.

[1] HL7 and CDA are registered trademarks of Health Level Seven International.

[2] DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

DSG_9: The use of the new XAdES brings in new standards. Thus is a breaking change from the original DSG.

DSG_10: XAdES now includes a mechanism for purpose of signature; they refer to this as "CommitmentTypeIndication". The DSG Profile proposes that the ASTM signature purpose vocabulary be used as it includes healthcare signature needs.

DSG_12: Comments integrated from CP-ITI-412.

DSG_16: There is use in France of a SubmissionSet signature. This is the DSG Detached Signature containing the references and hashes of all the documents that would be in a SubmissionSet, and a reference to the SubmissionSet unique ID with a zero hash value. This DSG Document is included in the SubmissionSet. This was added as another option.

DSG_11: The PCC committee is revising the definition of Content Creator and Content Consumer actors to make it easier to use with non-CDA based Content Profiles. After Public Comment on the PCC change, the DSG Profile will be updated to align with the new Content Creator and Content Consumer.

DSG_14: The classCode defined here is from the original revision of DSG. Due to its use in the original DSG, there is strong interest in maintaining this code.

DSG_15: The typeCode defined here is from the original revision of DSG. Due to its use in the original DSG, there is strong interest in maintaining this code.

DSG_17: There was comment on review that XAdES-X-L is too onerous as the inclusion of the CRL is 'tremendously increased document size'. So the commenter requests that we NOT use the new XAdES-X-L, but rather simple XAdES. We choose XAdES-X-L as it fits our use-cases. We allow local policy to support other configurations.

General Introduction

Update the following Appendices to the General Introduction as indicated below. Note that these are not appendices to Volume 1.

Appendix A - Actor Summary Definitions

No new actors defined.

Appendix B - Transaction Summary Definitions

No new transactions defined.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

Glossary Term	Definition
Detached Signature	A Digital Signature approach that includes only references to the signed content (aka manifest) within the signature syntax. The signature is over content external to the Signature element, and can be identified via a URI or transform. Consequently, the signature is "detached" from the content it signs. This definition typically applies to separate data objects, but it also includes the instance where the Signature and data object reside within the same XML document but are sibling elements. [W3C XMLDSIG]
Digital Signature	Formally speaking, a value generated from the application of a private key to a message via a cryptographic algorithm such that it has the properties of integrity, message authentication and/or signer authentication. (However, we sometimes use the term signature generically such that it encompasses Authentication Code values as well, but we are careful to make the distinction when the property of signer authentication is relevant to the exposition.) A signature may be (non-exclusively) described as detached, enveloping, or enveloped. [W3C XMLDSIG]
Enveloping Signature	A Digital Signature approach that encapsulates the signed content within the signature syntax. The signature is over content found within an Object element of the signature itself. The Object (or its content) is identified via a Reference (via a URI fragment identifier or transform). [W3C XMLDSIG]

Glossary Term	Definition
Hash	A value uniquely calculated by using a 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. "The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." [SEC] A simple checksum can provide integrity from incidental changes in the data; message authentication is similar but also protects against an active attack to alter the data whereby a change in the checksum is introduced so as to match the change in the data. [W3C XMLDSIG]
Long Term Signature	A signature that is intended to be valid for months or years later.
Non-repudiation	The assurance that someone cannot deny something, such as the receipt of a message or the authenticity of a statement or contract. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
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 purpose	An indication of the reason that an entity signed a document. This may be explicitly included as part of the signature information and can be used when determining accountability for various actions concerning the document. Examples include attesting to: authorship, correct transcription, and witness of specific event. Also known as a “Commitment Type Indication”
Signature time	The date and time that a signature was created.

Volume 1 – Profiles

Copyright Licenses

NA

Domain-specific additions

NA

Add Section 37

37 Document Digital Signature (DSG) Profile

The Document Digital Signature (DSG) Profile is a Document Content Profile that defines general purpose methods of digitally signing of documents for communication and persistence. Among other uses, these methods can be used within an IHE Document Sharing infrastructure (e.g., XDS, XCA, XDM, XDR, and MHD). There are three methods of digital signature defined here: Enveloping, Detached (manifest), and SubmissionSet.

- An Enveloping Signature is a Digital Signature Document that contains both the signature block and the content that is signed. Access to the contained content is through removing the Enveloping - Digital Signature. Among other uses, this method should not be used with Document Sharing infrastructure.
- A Detached Signature is a Digital Signature Document that contains a manifest that points at independently managed content. Detached signatures leave the signed document or documents in the original form. Among other uses, this method is recommended for use with a Document Sharing infrastructure to support Digital Signatures, as this method does not modify the original Document Content. This method uses the Document Sharing "SIGNS" relationship provide linkage.
- A SubmissionSet Signature is a Detached Signature Document that attests to the content in a SubmissionSet by: containing a manifest of all the other Documents included in the SubmissionSet, and a reference to the SubmissionSet. The Document Sharing "SIGNS" relationship may be used but is not required.

Ink-on-paper signatures have been a part of the documentation process in health care and have traditionally been indicators of accountability. Reliable exchange and storage of electronic data between disparate systems requires a standard that implements equivalent non-repudiation to prevent document creators from denying authorship and rejecting responsibility.

37.1 Actors/Transactions

This section defines the actors, transactions, and/or content modules in this profile. General definitions of actors are given in the Technical Frameworks General Introduction Appendix A at http://ihe.net/Technical_Frameworks/.

Figure 37.1-1 shows the actors directly involved in the DSG Profile and the direction that the content is exchanged.

This profile defines only the capability for Document Digital Signature. This profile does not include transport, workflow, or other content profiles. The grouping of the content module described in this profile to specific actors is described in more detail in the "Required Actor Groupings" section below.

Figure 37.1-1: DSG Actor Diagram

Table 37.1-1 lists the content module(s) defined in the DSG Profile. To claim support with this profile, an actor shall support all required content modules (labeled "R") and may support optional content modules (labeled "O").

Table 37.1-1: DSG Profile - Actors and Content Modules

Actors	Content Modules	Optionality	Reference
Content Creator	Document Digital Signature	R	ITI TF-3: 5.5
Content Consumer	Document Digital Signature	R	ITI TF-3: 5.5

37.1.1 Actor Descriptions and Actor Profile Requirements

Most requirements are documented in Content Modules (Volume 3). This section documents any additional requirements on profile's actors.

A Content Creator that conforms to this profile shall have the capability to create a digital signature document conforming to the Document Digital Signature content module using the signature option(s) chosen.

A Content Consumer that conforms to this profile shall have the capability to verify signatures using the signature option(s) chosen.

37.2 DSG Actor Options

Table 37.2-1 lists the option(s) defined in the DSG Profile.

Table 37.2-1: DSG Profile - Options

Actors	Option	Reference
Content Creator	Detached Signature (Note 1)	Section 37.2.1
	SubmissionSet Signature (Note 1)	Section 37.2.1.1
	Enveloping Signature (Note 1)	Section 37.2.2
Content Consumer	Detached Signature (Note 1)	Section 37.2.1
	SubmissionSet Signature (Note 1)	Section 37.2.1.1
	Enveloping Signature (Note 1)	Section 37.2.2

Note 1: Content Creator Actors and Content Consumer Actors shall support at least one option.

37.2.1 Detached Signature Option

Content Creators that support the Detached Signature Option shall have the capability to create a Detached Signature document that is composed of the Signature block as specified in ITI TF-3: 5.5.2 and 5.5.3, and a manifest of references to the signed documents. The signature document does not include the content of the documents that are signed. The Detached Signature Option supports the signing of multiple documents with one signature document.

The digital signature document, when published using Document Sharing profiles (e.g., XDS, XDR, XDM, XCA, etc.), shall conform to the Document Sharing metadata rules identified in ITI TF-3: 5.5.6.

Content Consumers that support the Detached Signature Option shall have the capability to perform signature verification specified in ITI TF-3: 5.5.5 for documents signed with a Detached Signature.

37.2.1.1 SubmissionSet Signature Option

The SubmissionSet Signature Option is a variant on the Detached Signature Option.

The Content Creator shall have the ability to create a Detached Signature document that includes reference to all the documents included in the SubmissionSet, except for the Detached Signature document itself; and a reference to the SubmissionSet unique ID. This Detached Signature document is included in the SubmissionSet.

The SubmissionSet Signature Option requires the use of a Document Sharing Profile.

Content Consumers that support the SubmissionSet Signature Option shall have the capability to perform signature verification specified in ITI TF-3: 5.5.5 for all the documents contained within the Detached Signature.

37.2.2 Enveloping Signature Option

Content Creators that support the Enveloping Signature Option shall have the capability to create an Enveloping Signature document that is composed of the signature block as specified in ITI TF-3: 5.5.2 and 5.5.4, and the document that is signed. The Enveloping Signature Option only supports one document per signature document.

No guidance is given for use of Document Sharing with Enveloping Signatures. This is due to the fact that one document contains both signature and content; so it is unclear what the metadata should represent. XDS Affinity Domain or other Policy Domain may provide the guidance.

Content Consumers that support the Enveloping Signature Option shall have the capability to perform signature verification specified in ITI TF-3: 5.5.5 for documents signed with an Enveloping Signature.

37.3 DSG Required Actor Groupings

There are two actors in this profile, the Content Creator and the Content Consumer. Content is created by a Content Creator and is to be consumed by a Content Consumer. The sharing or

transmission of content from one actor to the other is not specifically addressed by this profile. This communication may be achieved by the Document Sharing profiles, or by other means.

When Digital Signature documents are stored using a Document Sharing profile, such as XDS, the metadata rules are defined in ITI TF-3: 5.5.6.

Content Creator and Content Consumer shall be grouped with CT Time Client Actor as Digital Signatures require a reliable date and time.

Content Creator and Content Consumer should be grouped with ATNA Secure Node or Secure Application to record an Audit Message when a signature is created or validated.

Table 37.3-1: DSG - Required Actor Groupings

DSG Actor	Actor to be grouped with	Reference	Content Bindings Reference
Content Creator	CT Time Client	ITI TF-1: 7.1	--
Content Creator with the SubmissionSet Signature Option	XDS.b Document Source	ITI TF-1: 10.1 (Note 1)	--
	XDR Document Source	ITI TF-1: 15.1 (Note 1)	--
	XDM Portable Media Creator	ITI TF-1: 16.1 (Note 1)	--
Content Consumer	CT Time Client	ITI TF-1: 7.1	--
Content Consumer with the SubmissionSet Signature Option	XDS.b Document Consumer	ITI TF-1: 10.1 (Note 1)	--
	XDR Document Recipient	ITI TF-1: 15.1 (Note 1)	--
	XDM Portable Media Importer	ITI TF-1: 16.1 (Note 1)	--

Note 1: One or more of the Document Sharing infrastructure groupings must be supported.

37.4 Document Digital Signatures Profile Overview

The purpose of digital signatures in healthcare can vary greatly and it is important to understand the distinct use cases. A Digital Signature is a standards-based method to assure content integrity, authenticity, and authentication of the identity of the signer. The identity of the signer is assured through use of Private Key and Public Key management. Management of Private Key and Public Keys are not addressed by this profile.

37.4.1 Verify Document Integrity

One purpose of use of a Digital Signature is to verify that the document being used is the same as the document that was signed and has not been modified by error or intent. This is called establishing document integrity. Document signatures may be used to establish document integrity; that is, to verify that the current document is the same as the signed document, and it

has not been modified by error or intent. Document signatures may also be used to ascertain the identity of the signer and the reason for signing.

For example, to confirm 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 does not verify, then the document has been modified.

Another purpose of use is to verify the clinical content of a document. When a physician has verified that a report is complete and correct, the physician signs the document with purpose of signature being "verification". If there is ever a need, the digital signature provides a mechanism to show that the "verification" was attested to by the physician.

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 they are using has been verified.

37.4.2 One Signature signing multiple documents

The Detached Signature Option supports a single signature document that simultaneously signs multiple documents. For example, when a doctor verifies and signs a diagnostic report, the digital signature can also sign the source data that was used to prepare the diagnostic report. The digital signature for a mammography diagnostic report may sign:

1. The examination procedure notes
2. The DICOM Mammography images that were read by the radiologist
3. The verified diagnostic report

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 other reports in the XDS Document Registry, e.g., a later lab report, the digital signature indicates that this other information not used to prepare the report.

37.4.2.1 Signing a SubmissionSet

A variant of a Signature signing multiple documents is one where the group of documents being signed is also defined by a Document Sharing SubmissionSet.

37.4.3 Processing by XDS Document Consumer

Among other uses, the Detached Signature Option supports use of Document Sharing infrastructure (e.g., XDS, XDR, XDM, and XCA). The following sections describe how common queries can be performed in a Document Sharing environment where document digital signatures are used.

- Search for signatures, given a document

  The signatures that apply to a specific document can be found by querying (e.g., the XDS Document Registry) to obtain the "SIGNS" association linkages to that specific

document. The “SIGNS” associations link the Digital Signature documents with the documents signed.

- Search for documents, given a signature

  The signature document itself contains a manifest that lists the document IDs for all of the signed documents. It might also contain a SubmissionSet uniqueId for a submission set. The documents can be obtained through the Document Sharing system. It is possible that authorization or other limits may prevent retrieval of some of these documents.

- Search for signatures

  The signature documents are identified as a 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.

- Ignore signature documents in query

  The digital signature type document can also be suppressed in queries that are intended to retrieve only source documents. In an environment with extensive use of data 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.

37.4.4 Sign a document by Enveloping - Use Case Description

When a clinician needs to bind both a document and the signature into one document (for example, because there is no Document Sharing infrastructure to carry the document, the digital signature, and the association), then the Enveloping Signature Option needs to be used.

The Enveloping Signature method encapsulates the signed document inside of the digital signature document. The result is one new document that is externally the signature document, and embedded inside that document is the document that is signed.

Since it is unclear whether (or which) metadata should refer to the signed document or to the enveloping signature document, IHE does not specify metadata to be used for an Enveloping Signature document in a Document Sharing infrastructure.

37.5 Security Considerations

Digital Signatures rely on a Private Key / Public Key Management Infrastructure (aka PKI) that must exist and be configured. The definition and configuration of PKI is outside the scope of this document content profile. The PKI should adhere to ISO TS-17090 standards for PKI in healthcare.

The Detached Signature Option allows for independent management of signature document and content documents; thus, there is a risk they will be made unavailable through revision or access control.

Content Creator and Content Consumer shall be grouped with CT Time Client Actor as Digital Signatures require a reliable date and time. There is a risk that the clock can be subverted, so operational controls should be used to audit clock modifications.

Content Creator and Content Consumer should be grouped with ATNA Secure Node or Secure Application to record an Audit Message when a signature is created or validated.

37.6 Cross Profile Considerations

When used with a Document Sharing infrastructure (e.g., XDS, XDR, XDM, or XCA):

- ITI TF-3: 5.5.6 Document Sharing Metadata is used
- The “SIGNS” association type is used to indicate relationship between signed documents and the signature document

When no Document Sharing infrastructure is used, then the Encapsulating Option should be used.

Volume 3 – Cross-Transactions and Content Specifications

5 IHE Content Specifications

Editor please add Section 5.5

5.5 Document Digital Signature (DSG) Document Content

Document Digital Signature content shall conform to XAdES schema for signatures, with extensions and restrictions defined in the following. IHE is 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.

5.5.1 References

5.5.1.1 Normative References

[XAdES]: XML Advanced Electronic Signatures XAdES http://www.w3.org/TR/XAdES/ -- aka. ETSI TS 101 903

[W3C XMLDSIG] XML-Signature Syntax and Processing. W3C Recommendation. Donald Eastlake, Joseph Reagle, David Solo. February 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[ASTM-E1762-05]ASTM E1762-95(2013) – 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

5.5.1.2 Informative References

[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 http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=8179&curItemNr=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

[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

[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

[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

[ISO17090 (1,2,3)] ISO/TS 17090 – Health Informatics Digital Signatures for Healthcare http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35489&ICS1=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&scopelist=PROGRAMME

[IETF RFC3280] IETF/RFC 3280 regarding X.509v3 PKIX Private Key Infrastructure RFC3280 http://www.faqs.org/rfcs/rfc3280.html

5.5.2 Signature Specification

The following constraints define the Digital Signature block. This block is common to the detached signature and Enveloping signature.

- Shall conform to XAdES-X-L – for support of Long Term signatures. The XAdES-X-L specification adds the timestamp of the signing and inclusion of the certificate and statement of revocation..
- Shall use the hash algorithm sha256.
- Shall use the canonicalization algorithm "Canonical XML 1.1 with Comments" (http://www.w3.org/2006/12/xml-c14n11#WithComments).
- The policy may be identified as **urn:ihe:iti:dsg:detached:2014** when the signature document is a Detached Signature and **urn:ihe:iti:dsg:enveloping:2014** when the signature document is an Enveloping Signature to indicate that the signature document complies with the DSG Profile.
- Shall include a "CommitmentTypeIndication" element for the Purpose(s) of Signature (aka purposeOfSignature). The Purpose can be the action being attested to, or the role associated with the signature. The value shall come from ASTM E1762-95(2013) and reproduced in Table 5.5.2-1. Where a coding scheme is needed the value "1.2.840.10065.1.12" shall be used.

Note that Content Creators and Content Consumers should be capable of being configured to other conformance policies to support local policy. For example some environments may choose a different XAdES profile, hashing algorithm, policy identifier, or signature purpose vocabulary. Content Creators would thus create Digital Signature blocks that are not conformant to this profile. Content Consumers can validate these Digital Signature blocks, and be capable of configured behavior according to the local policy.

Table 5.5.2-1: Digital Signature Purposes from ASTM E1762-95(2013)

Code	Term	Definition
1.2.840.10065.1.12.1.1	Author's Signature	The signature of the primary or sole author of a health information document. There can be only one primary author of a health information document.

Code	Term	Definition
1.2.840.10065.1.12.1.2	Co-Author's Signature	The signature of a health information document co-author. There can be multiple co-authors of a health information document.
1.2.840.10065.1.12.1.3	Co-participant's Signature	The signature of an individual who is a participant in the health information document but is not an author or co-author. (e.g., a surgeon who is required by institutional, regulatory, or legal rules to sign an operative report, but who was not involved in the authorship of that report.)
1.2.840.10065.1.12.1.4	Transcriptionist/Recorder Signature	The signature of an individual who has transcribed a dictated document or recorded written text into a digital machine -readable format.
1.2.840.10065.1.12.1.5	Verification Signature	A signature verifying the information contained in a document. (e.g., a physician is required to countersign a verbal order that has previously been recorded in the medical record by a registered nurse who has carried out the verbal order.)
1.2.840.10065.1.12.1.6	Validation Signature	A signature validating a health information document for inclusion in the patient record. (e.g., a medical student or resident is credentialed to perform history or physical examinations and to write progress notes. The attending physician signs the history and physical examination to validate the entry for inclusion in the patient's medical record.)
1.2.840.10065.1.12.1.7	Consent Signature	The signature of an individual consenting to what is described in a health information document.
1.2.840.10065.1.12.1.8	Signature Witness Signature	The signature of a witness to any other signature.
1.2.840.10065.1.12.1.9	Event Witness Signature	The signature of a witness to an event. (Example the witness has observed a procedure and is attesting to this fact.)
1.2.840.10065.1.12.1.10	Identity Witness Signature	The signature of an individual who has witnessed another individual who is known to them signing a document. (e.g., the identity witness is a notary public.)
1.2.840.10065.1.12.1.11	Consent Witness Signature	The signature of an individual who has witnessed the health care provider counselling a patient.
1.2.840.10065.1.12.1.12	Interpreter Signature	The signature of an individual who has translated health care information during an event or the obtaining of consent to a treatment.
1.2.840.10065.1.12.1.13	Review Signature	The signature of a person, device, or algorithm that has reviewed or filtered data for inclusion into the patient record. (e.g., (1) a medical records clerk who scans a document for inclusion in the medical record, enters header information, or catalogues and classifies the data, or a combination thereof; (2) a gateway that receives data from another computer system and interprets that data or changes its format, or both, before entering it into the patient record.)
1.2.840.10065.1.12.1.14	Source Signature	The signature of an automated data source. (e.g., (1) the signature for an image that is generated by a device for inclusion in the patient record; (2) the signature for an ECG derived by an ECG system for inclusion in the patient record; (3) the data from a biomedical monitoring device or system that is for inclusion in the patient record.)

Code	Term	Definition
1.2.840.10065.1.12.1.15	Addendum Signature	The signature on a new amended document of an individual who has corrected, edited, or amended an original health information document. An addendum signature can either be a signature type or a signature sub-type (see ASTM E1762-Section 8.1). Any document with an addendum signature shall have a companion document that is the original document with its original, unaltered content, and original signatures. The original document shall be referenced via an attribute in the new document, which contains, for example, the digest of the old document. Whether the original, unaltered, document is always displayed with the addended document is a local matter, but the original, unaltered, document must remain as part of the patient record and be retrievable on demand.
1.2.840.10065.1.12.1.16	Modification Signature	The signature on an original document of an individual who has generated a new amended document. This (original) document shall reference the new document via an additional signature purpose. This is the inverse of an addendum signature and provides a pointer from the original to the amended document.
1.2.840.10065.1.12.1.17	Administrative (Error/Edit) Signature	The signature of an individual who is certifying that the document is invalidated by an error(s), or is placed in the wrong chart. An administrative (error/edit) signature must include an addendum to the document and therefore shall have an addendum signature sub-type (see ASTM E1762-Section 8.1). This signature is reserved for the highest health information system administrative classification, since it is a statement that the entire document is invalidated by the error and that the document should no longer be used for patient care, although for legal reasons the document must remain part of the permanent patient record.
1.2.840.10065.1.12.1.18	Timestamp Signature	The signature by an entity or device trusted to provide accurate timestamps. This timestamp might be provided, for example, in the signature time attribute.

5.5.3 Detached Signature

500 The Detached Signature utilizes the XML Signature - Reference element (ds:reference) to identify and provide a hash for each document that is signed. This set of Reference elements is considered the manifest. The URI type shall be used and hold the document uniqueID. Using the Data Type “OID URN” form to encode the DocumentEntry.uniqueId. See ITI TF-3: Table 4.2.3.1.7-2.

505 **urn:oid:1.3.6.1.4.1.21367.2005.3.7**

5.5.3.1 SubmissionSet Signature

The SubmissionSet Signature is a variant of the Detached Signature used to digitally sign a complete SubmissionSet. The signature can later be validated to assure that the SubmissionSet is complete and the same as when it was created.

510 The SubmissionSet Signature shall be a Detached Signature that has Reference elements for:

a. the SubmissionSet uniqueID with a hash value of “0”

b. the document uniqueID for each of the documents contained in the SubmissionSet not including the SubmissionSet Signature document

The SubmissionSet Signature creation is informatively described here with the Content Creator grouped with an XDS Document Source and is equally applicable with grouping the Content Creator with the other Document Sharing infrastructure (e.g., XDR, and XDM). The document publication transaction is not specific to the SubmissionSet Signature process or content, and is included here only to show overall workflow.

Informative process for creating a SubmissionSet Signature:

1. A set (n) of Documents of interest are gathered, or generated to be published
2. A SubmissionSet is created for the Documents, for example in preparation for using the Provide and Register Document Set-b [ITI-41] transaction or equivalent
3. A Digital Signature document is created which includes Reference elements of:
   a. The SubmissionSet.uniqueId is included in the manifest, with a zero hash value (the value "0").
   b. All of the (n) documents to be included in the SubmissionSet, other than the signature document, are listed in the manifest with their hash.
   c. The signature document is processed according to Section 5.5.2, and thus signed.
4. The signature document would be added to the SubmissionSet according to Section 5.5.6. The SubmissionSet may, but is not required, include all the "SIGNS" association defined in Section 5.5.6.4 with associations to all the other documents in the SubmissionSet. The "SIGNS" association is redundant in this case as the SubmissionSet already groups these documents.
5. The SubmissionSet with the (n) documents and the Digital Signature document is submitted using the Provide and Register Document Set-b [ITI-41] ransaction, or equivalent from the other Document Sharing infrastructures.

5.5.4 Enveloping Signature

The Enveloping Signature utilizes the XML Signature – "Include" capability where the full content of the signed document is encoded inside the signature document in the Object element (ds:object).

The signed document shall be base64 encoded, unless some other policy overrides.

The object element Encoding shall be specified (http://www.w3.org/2000/09/xmldsig#base64).

5.5.5 Signature Verification

There are three levels of signature verification:

1. verifying that the Digital Signature block itself has integrity through verifying the signature across the XML-Signature,

2. confirming that the signer was authentic, not revoked, and appropriate to the signature purpose,
3. confirming that the signed Documents of interest are unmodified using the hash algorithm.

The Content Consumer shall verify the Digital Signature block has integrity.

The Content Consumer shall be able to be configured with local policy on PKI trust models, and management that supports the confirmation that the signer was authentic, not revoked, and appropriate to the signature purpose. The Content Consumer shall use this configuration when confirming the validity of the signature.

The Content Consumer shall be able to confirm the validity of the documents that are signed.

- Workflow or local policy may direct that all or a subset of the signed documents be validated. There are use cases where only one document within a signed set of documents is all that is called for by the workflow.
- The document may not be accessible to the user, for example authorization denied, so confirmation of valid signed content may be impossible.
- If there is a SubmissionSet unique ID included in the manifest, then the Content Consumer shall be able to verify that the submission set reference in the manifest is the one containing the documents which are listed in the manifest and the documents listed in the manifest are the complete list of documents in the submission set on the XDS Registry.

The decision on what degree of verification is needed is determined by the application and use case.

The Content Consumer shall be able to validate content that uses SHA256 as well as SHA1.

5.5.6 Document Sharing Metadata

This section applies when the Content Creator or Content Consumer is utilizing a Document Sharing Profile for transport. This section defines the source for all required Document Sharing attributes and as many optional attributes as makes sense for implementers' applications.

5.5.6.1 Document Sharing – DocumentEntry Metadata

The Signature Document shall have a compliant DocumentEntry with the following constraints:

5.5.6.1.1 XDSDocumentEntry.formatCode

The XDSDocumentEntry.formatCode shall be **urn:ihe:iti:dsg:detached:2014** when the signature document is a Detached Signature and **urn:ihe:iti:dsg:enveloping:2014** when the signature document is an Enveloping Signature. The formatCode codeSystem shall be **1.3.6.1.4.1.19376.1.2.3**.

5.5.6.1.2 XDSDocumentEntry.classCode

Shall be **urn:oid:1.3.6.1.4.1.19376.1.2.1.1.1**

Coding scheme= URN
code value = urn:oid:1.3.6.1.4.1.19376.1.2.1.1.1
Code value display name = “Digital Signature”

5.5.6.1.3 XDSDocumentEntry.typeCode

Where policy does not define a workflow specific typeCode, the following code should be used:

Coding schema = “ASTM”

Code value = “E1762”

Code value display name = ”Full Document”

5.5.6.1.4 XDSDocumentEntry.author

The author should represent the signer.

5.5.6.1.5 XDSDocumentEntry.eventCodeList

The eventCodeList shall contain the signature Purpose(s) from the Digital Signature block “CommitmentTypeIndication” element, using Table 5.5.2-1.

5.5.6.1.6 XDSDocumentEntry.mimeType

Shall be “text/xml”

5.5.6.1.7 XDSDocumentEntry.title

Should be the same as the display name for the signature purpose

5.5.6.1.8 XDSDocumentEntry.language

The language of the signature content shall be ‘art’ as in “artificial”.

5.5.6.2 Document Sharing – SubmissionSet Metadata

This document content profile makes no changes to the structure of Submission Sets.

5.5.6.3 Document Sharing - Folder Metadata

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

5.5.6.4 Document Associations

When Detached Signature Option is used, the Content Creator shall use the “SIGNS” associationType Document Relationship to associate the signature (sourceObject) to the documents that it signs (targetObjects). See ITI TF-3: 4.2.2.

When SubmissionSet Signature Option is used, the Content Creator may use the "SIGNS" associationType Document Relationship to associate the signature (sourceObject) to the documents that it signs (targetObjects). See ITI TF-3: 4.2.2.

5.5.7 Security Considerations

See XAdES specification for risk assessment and mitigation plan on Digital Signatures.

5.5.7.1 Content Creator

When Content Creator is grouped with an ATNA Secure Node or Secure Application, shall create an Audit Message indicating the Signature Creation event.

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(113031, DCM, "Signed Manifest")
	EventActionCode	M	"C" (Create)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("urn:ihe:iti:dsg", "IHE Transactions", "Document Digital Signature")
Audit Source (Content Consumer) (1)			
ActiveParticipant (User/System that requested Signature Creation) (0..n)			
ActiveParticipant (Patient indicated in the Signature Document) (0..n)			
ParticipantObjectIdentification (Digital Signature Document)(1)			

5.5.7.2 Content Consumer

When Content Consumer is grouped with an ATNA Secure Node or Secure Application, shall create an Audit Message indicating the Signature Verification event.

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110007, DCM, "Report Verification")
	EventActionCode	M	"R" (Read)
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("urn:ihe:iti:dsg", "IHE Transactions", "Document Digital Signature")
Audit Source (Content Consumer) (1)			
ActiveParticipant (User/System that requested Signature Validation) (0..n)			
ActiveParticipant (Patient indicated in the Signature Document) (0..n)			
ParticipantObjectIdentification (Digital Signature Document)(1)			

