



HL7 Implementation Guide for CDA® Release 2: Digital Signatures and Delegation of Rights, Release 1

DRAFT STANDARD FOR TRIAL USE

October 2014

Sponsored by:

**Structured Documentation Work Group
Attachments Work Group
Security Work Group**

Publication of this draft standard for trial use and comment has been approved by Health Level Seven International (HL7). This draft standard is not an accredited American National Standard. The comment period for use of this draft standard shall end 24 months from the date of publication. Suggestions for revision should be submitted at <http://www.hl7.org/dstucomments/index.cfm>.

Following this 24 month evaluation period, this draft standard, revised as necessary, will be submitted to a normative ballot in preparation for approval by ANSI as an American National Standard. Implementations of this draft standard shall be viable throughout the normative ballot process and for up to six months after publication of the relevant normative standard.

Copyright © 2014 Health Level Seven International ® ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher. HL7 International and Health Level Seven are registered trademarks of Health Level Seven International. Reg. U.S. Pat & TM Off.

IMPORTANT NOTES:

HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document**, you are not authorized to access or make any use of it. To obtain a free license, please visit <http://www.HL7.org/implement/standards/index.cfm>.

If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material"), the following describes the permitted uses of the Material.

A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS, who register and agree to the terms of HL7's license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.

INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.

B. HL7 ORGANIZATION MEMBERS, who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

C. NON-MEMBERS, who register and agree to the terms of HL7's IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.

NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.

Please see <http://www.HL7.org/legal/ippolicy.cfm> for the full license terms governing the Material.

Acknowledgements and Copyrights

The editors appreciate the support and sponsorship of the HL7 Attachments Special Interest Group, the HL7 Security Special Interest Group, and the Structured Documents Working Group (SDWG) and all the volunteers, staff, and contractors participating in the S&I Framework.

This document contains content from the World Wide Web Consortium (W3C) recommendation **XAdES XML Advanced Electronic Signatures (XAdES)**, February 2003, <http://www.w3.org/TR/2003/NOTE-XAdES-20030220/>

This document contains content from the Organization for the Advancement of Structured Information Standards (OASIS); "OASIS", "SAML" and "Security Assertion Markup Language" are trademarks of [OASIS](http://www.oasis-open.org), the open standards consortium where the SAML specification is owned and developed. <https://www.oasis-open.org/standards#samlev2.0>

This document contains content reprinted, with permission, from E1762-95 Standard Guide for Electronic Authentication of Health Care Information, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM International, www.astm.org.

Co-Chair:	Calvin Beebe Mayo Clinic cbeebe@mayo.edu	Co-Editor:	Robert Dieterle Enablecare, LLC rdieterle@enablecare.us
Co-Chair:	Diana Behling Iatric Systems Diana.Behling@iatric.com	Co-Editor:	Dan Kalwa CMS daniel.kalwa@cms.hhs.gov
Co-Chair:	Robert H. Dolin, MD Lantana Consulting Group bob.dolin@lantanagroup.com	Co-Editor:	Zachary May ESAC, Inc zachary.may@esacinc.com
Co-Chair:	Austin Kreisler SAIC – Science Applications International Corp AUSTIN.J.KREISLER@leidos.com	Co-Editor:	Viet Nguyen, MD Systems Made Simple viet.nguyen@systemsmadesimple.com
Co-Chair:	Patrick Lloyd ICode Solutions patrick.e.loyd@gmail.com	Co-Editor:	Mark Pilley, MD StrategicHealthSolutions, LLC m.pilley@strategichs.com
Co-Chair:	Brett Marquard River Rock Associates brett@riverrockassociates.com	Co-Editor:	Bob Yench RTY, LLC
Current Work Group also includes all those who participated in the ONC S&I Framework and provided comments on the ballot: Swati Albal, Nalini Ananth, Peter Bachman, Greg Beech, Steven Beller, Rob Benjamin, Victor Beraja, Jennifer Bessette, Steve Blackford, Michael Brody, Robin Bronson, Susan Broughton, Jennifer Brush, Lynn Chapple, Laura Cohen, Melanie Combs-Dyer, George Cook, Joyce Davis, Cletis Earle, Sue Farrington, Kari Gaare, Craig Gabron, John Gachago, Parag Gajare, Dawn Gallagher, Darlene Gandara, Reed Gelzer, Denesecia Green, Allen Helms, Geanelle Herring, Judith Hutman, Robin Isgett, Lenel James, Donna Jones, Joe Keochinda, Lester Keepper, Patrice Kuppe, Sweta Ladwa, Cynthia Levy, Cherie Little, Carole Magoffin, Kishore Metla, Sheri Mitchell, John Moehrke, Brandon Morstad, Lee Mosbrucker, Lisa Nelson, Kyle Pearson, Donald Potts, Patricia Powles, Martin Prah, Trebba Putnam, Vaishnavi Rao, Matt Reid, Keith Salzman, Joy Sam, Brian Scheller, Rita Scichilone, Christine Stahlecker, Melinda Thomas, Serafina Versaggi, Kathy Wallace, Diana Warner, Daidi Zhong			

TABLE OF CONTENTS

TABLES AND FIGURES.....	6
1 INTRODUCTION.....	7
1.1 PURPOSE	7
1.2 AUDIENCE	8
1.2.1 REQUISITE KNOWLEDGE.....	8
1.3 ORGANIZATION OF THIS GUIDE	9
1.3.1 CONVENTIONS	9
1.3.2 KEYWORDS	9
1.3.3 CARDINALITY	9
2 USE CASE	11
2.1 ASSUMPTIONS	11
2.2 SCOPE	11
2.2.1 IN-SCOPE	11
2.2.2 OUT OF SCOPE	11
2.3 ACTORS	12
2.4 SCENARIO – SIGNING A CDA DOCUMENT	12
2.4.1 USER STORY 1 – DIGITAL SIGNATURE BY AUTHORIZED SIGNER	12
2.4.2 USER STORY 2 – DIGITAL SIGNATURE BY DELEGATED SIGNER.....	13
2.5 BASE FLOWS.....	15
2.6 REQUIREMENTS.....	17
2.7 INFORMATION INTERCHANGE REQUIREMENTS.....	17
2.8 SYSTEM REQUIREMENTS.....	17
3 DIGITAL SIGNATURE PROCESSES	18
3.1 CREATING A DIGITAL SIGNATURE.....	18
3.1.1 DIGITAL SIGNATURE STANDARD	18
3.1.2 COMPUTATION OF THE DIGEST	18
3.1.3 SIGNATURE PROCESS	19
3.2 CREATING A DELEGATION OF RIGHTS ARTIFACT	19
3.2.1 OVERVIEW OF THE DELEGATION OF RIGHTS PROCESS	20
3.2.2 PRE-CONDITIONS	21
3.2.3 DELEGATION OF RIGHTS STANDARDS.....	21
3.2.4 CREATING A SAML-BASED DELEGATION OF RIGHTS ASSERTION.....	22
3.2.5 CREATING A DELEGATION OF RIGHTS ARTIFACT	23
3.2.6 VALIDATING THE DELEGATION OF RIGHTS ARTIFACT	23
3.3 INCORPORATING DIGITAL SIGNATURE AND DELEGATION OF RIGHTS ARTIFACTS INTO A CDA DOCUMENT	24

3.3.1	SPECIFICATIONS FOR THE ED DATA TYPE	27
3.3.2	SPECIFICATIONS FOR THUMBNAIL.....	27
3.4	VERIFYING AN XADES-BASED SIGNATURE	28
3.4.1	VERIFYING THE SIGNERS SIGNATURE	28
3.4.2	VERIFYING THE VALIDATION SIGNATURE	29
3.4.3	VERIFYING THE DELEGATION OF RIGHTS ARTIFACT	29
4	DATA REQUIREMENTS.....	30
4.1	DOCUMENT SIGNATURE	30
4.2	DELEGATION OF RIGHTS ASSERTION.....	38
4.3	VALIDATED DELEGATION OF RIGHTS ASSERTION.....	40
4.4	CODE SETS.....	40
4.5	PURPOSE OF SIGNATURE AND ROLE WITHIN A SIGNED CDA (EXAMPLE).....	41
5	RISKS	46
6	APPENDIX A: EXAMPLES.....	47
6.1	XADES-X-L DIGITAL SIGNATURE	47
6.2	SAML DELEGATION OF RIGHTS ARTIFACT	51
6.3	XADES-X-L DIGITAL SIGNATURE APPLIED TO SAML DELEGATION OF RIGHTS	54
7	APPENDIX B: SIGNING CERTIFICATE INFORMATION	57
8	APPENDIX C: CREATION OF THE DIGEST	58
9	APPENDIX D: MULTIPLE SIGNERS SCENARIO	59
9.1	MULTIPLE SIGNERS.....	59
9.2	ACTIVITY DIAGRAM	60
9.3	BASE FLOW.....	60
10	APPENDIX E: SIGNATURE PURPOSE	62
11	APPENDIX F: GLOSSARY	63

TABLES AND FIGURES

LIST OF TABLES

TABLE 2-1. BASE FLOW FOR USER STORY 1	16
TABLE 2-2. BASE FLOW FOR USER STORY 2	16
TABLE 2-3. INFORMATION INTERCHANGE REQUIREMENTS	17
TABLE 2-4. SYSTEM REQUIREMENTS	17
TABLE 4-1. DOCUMENT SIGNATURE	30
TABLE 4-2. DELEGATION OF RIGHTS ASSERTION	38
TABLE 4-3. VALIDATED DELEGATION OF RIGHTS ASSERTION	40
TABLE 4-4. CODE SETS.....	40
TABLE 7-1. SIGNING CERTIFICATE INFORMATION	57
TABLE 9-1. SIGNATURE ROLES AND PURPOSES FOR MULTIPLE SIGNERS	59
TABLE 9-2. BASE FLOW FOR MULTIPLE SIGNERS SCENARIO	60
TABLE 10-1. SIGNING PURPOSE	62
TABLE 11-1. GLOSSARY	63

LIST OF FIGURES

FIGURE 2-1. ACTIVITY DIAGRAM 1.....	13
FIGURE 2-2. ACTIVITY DIAGRAM 2.....	15
FIGURE 3-1. DELEGATION OF RIGHTS PROCESS.....	21
FIGURE 3-2. LEGALAUTHENTICATOR EXAMPLE.....	24
FIGURE 3-3. AUTHENTICATOR EXAMPLE.....	25
FIGURE 3-4. SIGNATURETEXT STRUCTURE	26
FIGURE 3-5. SIGNATURETEXT STRUCTURE WITH DELEGATION OF RIGHTS.....	26
FIGURE 6-1. HEADER DETAIL	41
FIGURE 6-2. AUTHENTICATOR DETAIL	42
FIGURE 6-3. SDTC:SIGNATURETEXT DETAIL	43
FIGURE 6-4. SIGNERROLE DETAIL	44
FIGURE 6-5. SIGNATUREPURPOSE DETAIL.....	45
FIGURE 9-1. ACTIVITY DIAGRAM FOR MULTIPLE SIGNERS	60

1 INTRODUCTION

The HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1 is a collaboration between Health Level Seven (HL7) the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator (ONC) Standards and Interoperability (S&I) Framework Electronic Submission of Medical Documentation (esMD) Initiative.

This implementation guide defines a method to imbed digital signatures in a CDA¹ document and provides an optional method of specifying delegation of right assertions that may be included with the digital signatures. This implementation guide will allow health plans, payers, and providers to accurately authenticate the Authorized Signer(s)² of a CDA document and trust the validity and authenticity of signed medical documentation.

This implementation guide specifies the content of the `sdtc:signatureText`³ element when included as part of the `legalAuthenticator` and/or `authenticator` participant occurrences. Examples of the `sdtc:signatureText` are defined in the HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm) Draft Standard for Trial Use Release 2⁴ (C-CDA) and can be found in Appendix A: Example.

1.1 Purpose

This document provides guidance on the use of digital signatures imbedded in a CDA document to:

- Provide a non-repudiation signature that attests to the role and signature purpose (see Table 4-4. Code Sets for role and signature purpose code sets) of each Authorized Signer to the document.
- Provide for a delegation of rights where the signer is a Delegated Signer⁵ and not the Authorized Signer responsible individual or organization (e.g., the signer is acting as an authorized agent).
- Provide a medical/legal attestation for administrative and clinical purposes such as documenting transfer of clinical care (e.g. the Longitudinal Coordination of Care initiative)⁶.
- Provide for both digital co-signatures and counter signatures.

For example, an Authorized Signer may play a role in the document, such as ‘author’, and would therefore be represented in the `author` participation declared in the header. The Authorized Signer will also be represented as an `authenticator` in the header. In the `sdtc:signatureText` for the `authenticator`, the Authorized Signer will have a `signerRole`. If this Authorized Signer claims to be an anesthesiologist, signing as an author, then this information would be represented in the `signerRole` as the `claimedRole` and `signaturePurpose`. Through appropriate use of both `signerRole` and `signaturePurpose`, digital signatures can accommodate co-signatures on any CDA (e.g. multiple Authorized Signers can indicate that they are co-authors). In addition, since the XAdES-X-L standard used by this guide supports counter signatures, any digital signature may be countersigned.

¹ HL7 Version 3 Clinical Document Architecture (CDA®) - http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

² Authorized Signer – see Actors (Section 2.3) for definition

³ HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2, Volume 2 – Templates and Supporting Material, September 2013. Section 1.1.1.10

⁴ HL7 documents are available at <http://www.hl7.org>

⁵ Delegated Signer – see Actors (Section 2.3) for definition

⁶ [http://wiki.siframework.org/Longitudinal+Coordination+of+Care+\(LCC\)](http://wiki.siframework.org/Longitudinal+Coordination+of+Care+(LCC))

It is intended to:

- Identify a method of incorporating digital signatures and delegation of right assertions into the header of a CDA document.
- Identify a digital signature standard for a CDA document that supports the exchange of a signed:
 - Digest of the message;
 - Timestamp;
 - Role of the signer;
 - Purpose of signature.
- Identify a digital signature standard for:
 - The public certificate of the signer;
 - Long term validation data, including Online Certificate Status Protocol (OCSP) response and/or Certificate Revocation List (CRL).
- Identify a standard to assert a delegation of rights that supports the exchange of:
 - The certificate ID of both parties;
 - The purpose of the delegation;
 - The effective date range of the assertion.
- Identify a method to validate an existing delegation of rights assertion.

The ability to provide Digital Signatures and Delegation of Rights Assertion artifacts can be achieved with existing standards. The capability may be provided as a service by third parties or incorporated directly into or provided in conjunction with EHRs and payer systems. A method to support validation of an existing delegation of rights assertion is presented in this guide, see Section 3.2.6 Validating the Delegation of Rights Artifact.

1.2 Audience

This guide is intended to assist analysts, developers, providers, agents⁷, payers, review contractors, and other health care organizations that require guidance on how to imbed a digital signature in a CDA document.

The intended audiences for this guide are:

- Providers and payers that wish to imbed digital signatures in a CDA document.
- Providers that wish to submit digitally-signed medical documentation for administrative purposes.
- Payers that wish to process digitally-signed medical documentation sent by a provider.
- Software analysts and developers that may develop products to assist payers, providers, and their agents in applying digital signatures to a CDA document.

1.2.1 REQUISITE KNOWLEDGE

- XML-Signature Syntax and Processing (XML-DSIG), <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>
- XML Advanced Electronic Signatures (XAdES), <http://www.w3.org/TR/2003/NOTE-XAdES->

⁷ Agent - Regional Health Information Organizations (RHIO), Health Information Exchanges (HIE), Release of Information (ROI) vendors, claim clearinghouses, and other entities that handle health information on behalf of a Provider under a Business Associate Agreement (BAA).

[20030220/](#)

- OASIS Security Assertion Markup Language (SAML 2.0), <https://www.oasis-open.org/standards#samlv2.0>, used in this guide to convey the delegation of rights assertion
- ASTM International E 1762-95, Standard Guide for Electronic Authentication of Health Care Information, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM International, www.astm.org.
- Washington Publishing Company, Healthcare Provider Taxonomy Code Set, <http://www.wpc-edi.com/reference/>
- HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2

1.3 Organization of This Guide

1.3.1 CONVENTIONS

This guide adheres to the following conventions:

- Text formatted as `monoSpacedCamelCase` indicates a literal data element representation from an underlying standard and that the definition is bound to that standard.
- Terms with initial caps, e.g., Signed, indicate a specific definition for the context of this document.
- Elements not prefaced with “hl7:”, “sdhc:”, “ds:”, or “saml:” are elements from the XAdES specification.

1.3.2 KEYWORDS

The keywords **SHALL**, **SHOULD**, **MAY**, **NEED NOT**, **SHOULD NOT**, and **SHALL NOT** in this document are to be interpreted as described in the HL7 Version 3 Publishing Facilitator's Guide.⁸

SHALL: an absolute requirement

SHALL NOT: an absolute prohibition against inclusion

SHOULD/SHOULD NOT: best practice or recommendation. There may be valid reasons to ignore an item, but the full implications must be understood and carefully weighed before choosing a different course

MAY/NEED NOT: truly optional; can be included or omitted as the author decides with no implications

1.3.3 CARDINALITY

The cardinality indicator (0..1, 1..1, 1..*, etc.) specifies the allowable occurrences within a document instance. The cardinality indicators are interpreted with the following format “m...n” where m represents the least and n the most:

⁸ HL7, Version 3 Publishing Facilitator's Guide. <http://www.hl7.org/v3ballot/html/help/pfg/pfg.htm>

0..1 zero or one

1..1 exactly one

1..* at least one

0..* zero or more

1..n at least one and not more than n

2 USE CASE

The use case covered by this IG is the application of one or more Digital Signature(s) to a CDA by an Authorized Signer or Delegated Signer to satisfy administrative or clinical policy requirements.

2.1 Assumptions

- All Authorized Signers and Delegated Signers have obtained a digital identity from a recognized Certificate Authority (CA).
- Registration Authorities exist and are able to identity proof individuals and organizations based on policy requirements.
- Registration Authorities may be part of a Certificate Authority or a standalone entity/function recognized by the Certificate Authority that issues the required signing certificate.
- Certificate Authorities exist and are capable of providing the necessary digital credentials for signing.
- Technology exists to utilize the digital credentials for signing a CDA document.
- The signature on a document attests to the signer's role, purpose of the signature, and the accuracy of the signed documentation for which they are responsible.
- Document revisions or addenda are signed at the time the revisions or addenda are completed, indicating the appropriate action(s).

2.2 Scope

The scope of this Use Case is the application of a Digital Signature(s) to a CDA document.

2.2.1 IN-SCOPE

- Solutions for individual or organizational Digital Signatures for discrete CDA documents to attest to the validity and authenticity of the information within the document or actions performed on the document.
- Defining delegation of rights between the Authorized Signer and the Delegated Signer.
- Content of the Digital Signature artifact and the delegation of rights assertion.
- Validation of signature artifacts and delegation of rights assertion(s) by recipient.
- Defining long-term validation of Digital Signature and Delegation of Rights artifacts.

2.2.2 OUT OF SCOPE

- Transport and message standards for the exchange of signed CDAs.
- Encryption of CDAs for security or privacy.
- A definition of electronic transactions between a Registration Authority (RA) and a CA.
- A definition of electronic transactions between a Payer and a RA or a CA.
- A definition of electronic transactions between a Provider and a RA or a CA.
- Consent, privacy, and use of the signed CDA document in situations other than providing documentation to payers for the sake of program or benefits administration.
- Policies that determine who is an Authorized Signer and the conditions under which a Delegated Signer is allowed.
- Policies that determine when a CDA document must be created and signed.
- Issues related to the cost of technology or technology services to utilize digital credentials to sign a CDA document.

2.3 Actors

There are four actors that have responsibilities related to the conformance requirements defined in this document:

- Authorized Signer – An entity (`legalAuthenticator` or `authenticator`) that affixes a Digital Signature to a CDA document to satisfy policy requirements.
- Delegated Signer – An entity that was delegated authority to sign a CDA on behalf of an Authorized Signer.
- Delegation Validator – A service that electronically verifies that the Delegation of Rights Artifact is valid.
- Recipient – An entity that receives and validates a signed CDA.

2.4 Scenario – Signing a CDA Document

One or more Authorized Signer(s) must attest to the patient's condition, actions taken, and/or plan of care with respect to information contained in a specific CDA document. This attestation must be done in a manner that supports non-repudiation and verification by a third party of the artifacts created at the time of signing. The Authorized Signer(s) has/have a need to send the signed CDA document to a third party as documentation for administrative or clinical purposes.

This guide outlines two user stories. The first user story details a CDA Digital Signature by an Authorized Signer. The second user story details a CDA Digital Signature by a Delegated Signer including the creation, validation and use of a delegation of rights assertion. An individual CDA may be signed by any number of Authorized Signers and/or their Delegated Signer(s). The user stories depict only one signer for simplicity, not as a constraint of this guide. Each Authorized Signer (or their Delegated Signer) must have a separate `legalAuthenticator` or `authenticator` participant occurrence that contains the `sdhc:signatureText` element.

2.4.1 USER STORY 1 – DIGITAL SIGNATURE BY AUTHORIZED SIGNER

The Authorized Signer digitally signs the document attesting to their role and the purpose of their signature. The Authorized Signer sends the signed document to the Recipient. The Recipient receives the Signed Document and authenticates the Authorized Signer's digital certificate, the signature artifact, and validates the data integrity of the document.

In order to participate in digital signing, the Authorized Signer obtains and maintains a non-repudiation digital identity by obtaining an X.509v3 digital signing certificate.⁹ Entities approved by a Registration Authority will receive the X.509v3 certificate from a Certificate Authority to incorporate into their business process.

The Authorized Signer creates a Digital Signature artifact attesting to their role, purpose of signature, and date/time of the signature and inserts it into the `sdhc:signatureText` element. The Authorized Signer, who has satisfied any requirements for a specific exchange of documentation with a Recipient, sends (directly or through a delegated agent) the digitally signed CDA document in a secure transaction to the Recipient using appropriate transmission methods.

⁹ In the United States for CMS, the X.509v3 digital signing certificate must come from a Federal Bridge cross-certified Certificate Authority.

2.4.1.1 ACTIVITY DIAGRAM 1

The Activity Diagram illustrates the use case flows graphically and represents the flow of events and information between the actors. It also displays the main events/actions that are required for the data exchange and the role of each system in supporting the exchange. Figure 2-1 illustrates the flow for User Story 1 - the digital signing of a CDA document by the Authorized Signer.

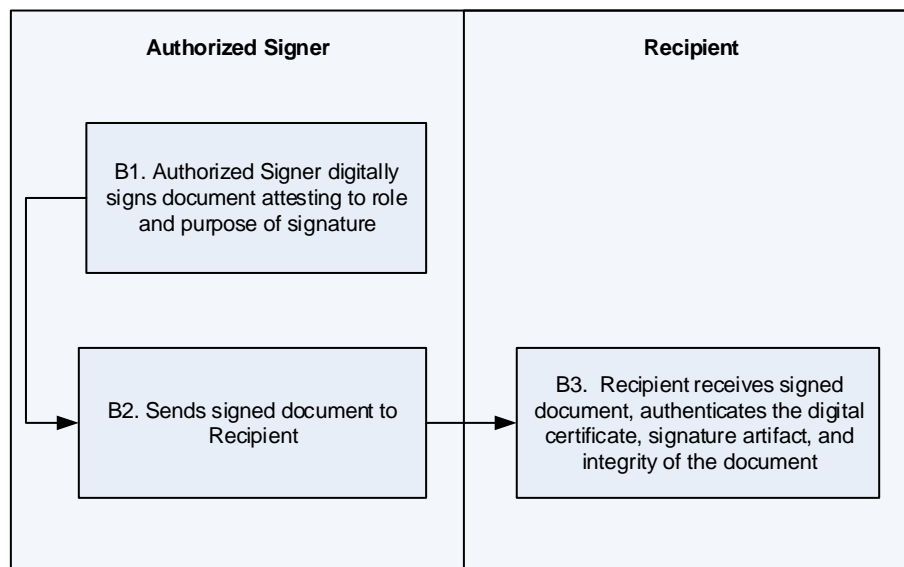


FIGURE 2-1. ACTIVITY DIAGRAM 1

2.4.2 USER STORY 2 – DIGITAL SIGNATURE BY DELEGATED SIGNER

In certain situations, the Authorized Signer may not be available or able to sign the CDA. In such a situation, the Authorized Signer may delegate the responsibility to a third party to sign on their behalf. The validity of such a delegation is a matter of both law and policy which are outside of the scope of this document. While it is possible to use multiple methods of asserting a delegation of rights, this guide focuses on the creation, use and validation of a computable, cryptographically verifiable method of delegation using a signed SAML 2.0 assertion.

The Authorized Signer and any Delegated Signer must obtain and maintain a non-repudiation digital identity. Both actors initiate the process to obtain an X.509v3 digital signing certificate.¹⁰ Entities approved by a Registration Authority will receive the X.509v3 certificate from a Certificate Authority to incorporate into their business process.

The Authorized Signer creates and digitally signs a Delegation of Rights assertion to permit a Delegated Signer to sign a CDA document on their behalf. It is the responsibility of the Delegated Signer to ensure that the Delegation of Rights is validated prior to incorporating the Delegation of Rights artifacts into the CDA.

¹⁰ In the United States for CMS, the X.509v3 digital signing certificate must come from a Federal Bridge cross-certified Certificate Authority.

The Delegated Signer creates a Digital Signature artifact attesting to their role, purpose of signature, and date/time of the signature and includes the signature artifact and the validated Delegation of Rights artifacts and inserts them into the `sdtc:signatureText` element. The Authorized Signer or Delegated Signer, who has satisfied any requirements for a specific exchange of documentation with a Recipient, sends (directly or through a delegated agent) the digitally signed CDA document in a secure transaction to the Recipient using appropriate transmission methods.

2.4.2.1 ACTIVITY DIAGRAM 2

Figure 2-2 illustrates the flow for User Story 2 - the digital signing of a CDA document *with* a delegation of rights.

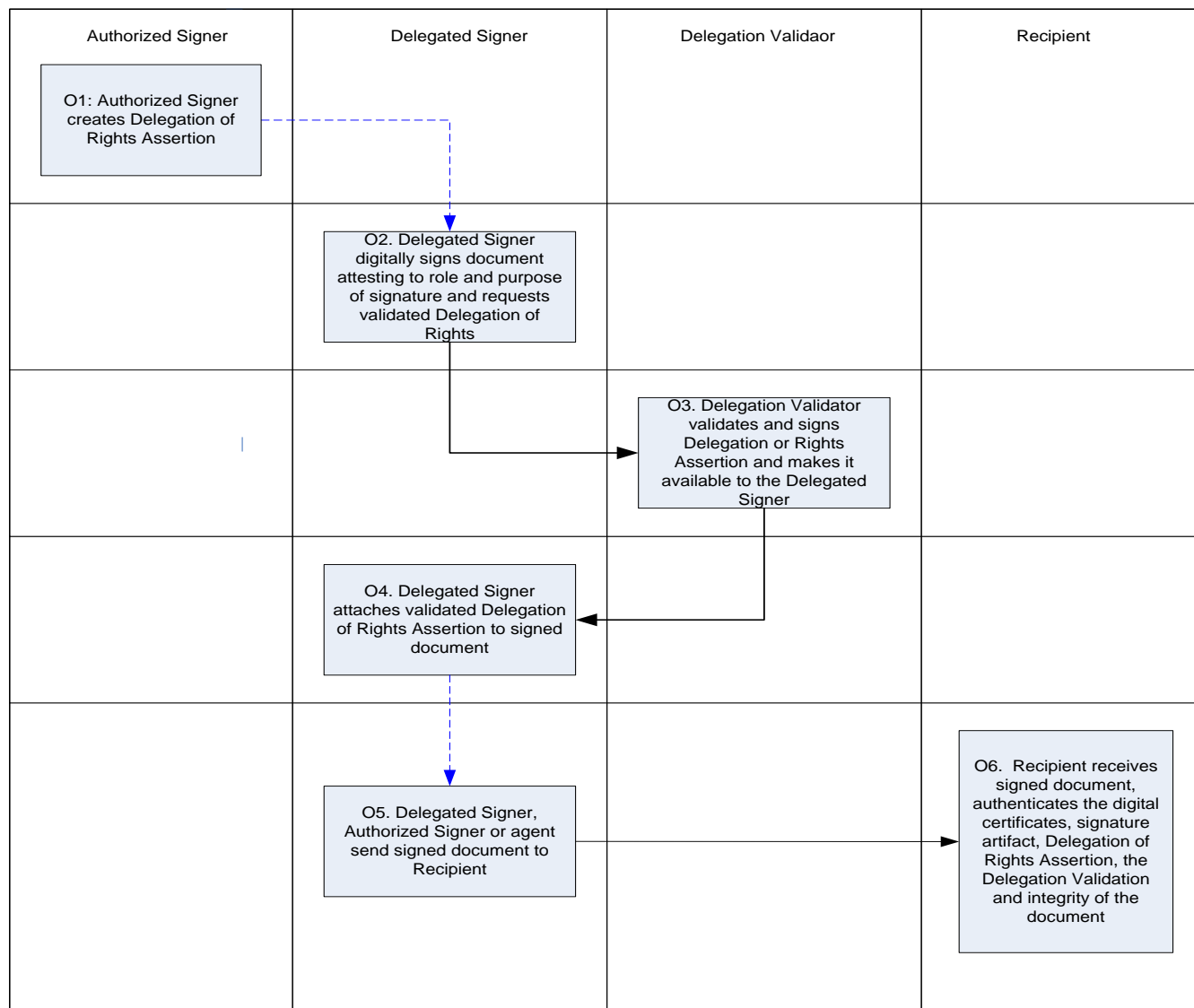


FIGURE 2-2. ACTIVITY DIAGRAM 2

2.5 Base Flows

The Base Flows presents the step-by-step process of the information exchange depicted in the activity diagrams (above). It indicates the actor who performs the action, the description of the event/action, and the associated inputs (records/data required to undertake the action) and outputs (records/data produced by actions taken).

Notes:

- Prior to this base flow, the actors have been identity proofed, and received an X.509 signing certificate from a CA that is used in their signing application.

- This signing process can occur as many times as necessary – once for each Authorized Signer or Delegated Signer that must attest to the contents of an individual CDA.
- Specific requirements for signing a CDA document are defined by Recipient policy.
- In addition to meeting the requirements defined by the CDA for use of `legalAuthenticator` and/or `authenticator` participant occurrences, the `signerRole` and `signaturePurpose` add clarity and should follow Recipient policy.

Table 2-1. Base Flow for User Story 1

Step	Actor	Role	Event/Description	Inputs	Outputs
B1	Authorized Signer	Attests to action on Document	Authorized Signer completes applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signed Document
B2	Authorized Signer	Document Sender	Authorized Signer sends signed Document to Recipient	Digitally Signed Document	Digitally Signed Document
B3	Recipient	Receiver and validator of Document	Recipient receives Document, authenticates Signature Artifacts and validates data integrity of submission from the Authorized Signer	Digitally Signed Document	Success or failure of Signature Artifact validation and Data integrity authentication

Table 2-2. Base Flow for User Story 2

Step	Actor	Role	Event/Description	Inputs	Outputs
O1	Authorized Signer	Delegation of Rights Creator	Authorized Signer creates and signs Delegation of Rights Assertion	Authorized Signer and Delegated Signer Digital Certificate Information	Delegation of Rights Assertion available
O2	Delegated Signer	Attests to action on Document	Delegated Signer applies a non-repudiation Digital Signature attesting to the role and signature purpose and requests validated Delegation of Rights Assertion	Document	Digitally Signed Document and request for validated Delegation of Rights Assertion
O3	Delegation Validator	Delegation of Rights Validator	Delegation Validator validates and signs Delegation of Rights Assertion	Delegated Signer request for a validated Delegation of Rights Assertion	Validated Delegation of Rights Assertion
O4	Delegated Signer	Applying Delegation of Rights Assertion	Delegated Signer associates the validated Delegation of Rights Assertion with the signed document	Validated Delegation of Rights Assertion and Digitally Signed Document	Digitally Signed Document with validated Delegation of Rights Assertion
O5	Delegated Signer	Document Sender	Delegated Signer sends signed Document with Validated Delegation of Rights Assertion to Recipient	Digitally Signed Document, with validated Delegation of Rights Assertion	Digitally Signed Document, with validated Delegation of Rights Artifacts
O6	Recipient	Receiver and validator of Document	Recipient receives Document, authenticates Signature Artifacts including the Delegation of Rights Assertions, and validates data integrity	Digitally Signed Document with a Delegation of Rights Assertion	Success or failure of Signature Artifact validation, Delegation of Rights Artifacts validation, and Data integrity authentication

2.6 Requirements

- Documentation of patient's condition, actions taken, and/or plan of care as documented in the CDA are digitally signed with the date/time, role and action (e.g., creation, review, etc.). The specific policies for Recipients should be followed.
- The signature(s) is/are added when the document is created, attesting to the contents of the document, role and purpose of the signature.

2.7 Information Interchange Requirements

The Information Interchange Requirements define the system's name and role. They also specify the actions associated with the actual transport of content from the sending system to the receiving system.

Table 2-3. Information Interchange Requirements				
Initiating System	Action	Information Interchange Requirement Name	Action	Receiving System
Authorized Signer Information System	Send	Link for Delegation of Rights Assertion	Receive	Delegated Signer Information System
Delegated Signer Information System	Send	Request for validated Delegation of Rights Assertion	Receive	Authorized Signer Information System
Authorized Signer Information System	Send	Validated Delegation of Rights Assertion	Receive	Delegated Signer Information System
Authorized Signer Information System	Send	Digitally Signed Document	Receive	Recipient Information System
Delegated Signer Information System	Send	Digitally Signed Document with validated Delegation of Rights Assertion	Receive	Recipient Information System

2.8 System Requirements

This section lists the requirements internal to the system necessary to participate successfully in the transaction. System requirements may also detail a required workflow that is essential to the Use Case.

Table 2-4. System Requirements	
System	System Requirement
Recipient Information System	Verify Delegation of Rights (if any), Digital Signatures, traceability to registered provider, and validate integrity of Document
Authorized Signer Information System	Incorporate signing Digital Certificate Create Delegation of Rights if required Respond to request to Validate Delegation of Rights Assertion Perform actions on a Document (create, modify, read) Apply non-repudiation Digital Signature to Delegation of Rights Assertion, and Documents and creates Signature Artifacts
Delegated Signer Information System (usually the same as Authorized Signer Information System)	Incorporate signing Digital Certificate Request Validated Delegation of Rights Perform actions on a Document (create, modify, read) Apply non-repudiation Digital Signature to Documents, creates Signature Artifacts and attaches validated Delegation of Rights Assertion

3 DIGITAL SIGNATURE PROCESSES

This section describes the standards, and process required to create a Digital Signature and apply it to a CDA document. The following sections describe the detailed requirements to:

- Define the standards and process for creating a Digital Signature.
- Define the standards and process for creating and validating a Delegation of Rights.
- Define the standards and process for adding the Digital Signature and where appropriate the Delegation of Rights artifact to a CDA document.
- Define the process for validating the Digital Signatures and Delegation of Rights artifact on a Signed CDA document.

Notes:

1. This implementation guide stores the Digital Signature artifacts described in this section in the `sdtc:signatureText` element.
2. The process defined in this IG provides for a signature over the entire CDA excluding all occurrences in the header for `legalAuthenticator` and `authenticator`. By excluding `legalAuthenticator` and `authenticator` participant occurrences from the calculation of the Digest, each additional signing event (e.g. additional authenticators) will not alter the information signed by a prior signer and therefore will not invalidate their Digital Signature.
3. Through appropriate use of both `signerRole` and `signaturePurpose`, Digital Signatures can accommodate co-signatures on any CDA (e.g. multiple Authorized Signers can indicate that they are co-authors). In addition, since the XAdES-X-L standard used by this guide supports counter signatures, any Digital Signature may be counter signed.
4. The UTC incorporated in each Digital Signature will permit the Recipient to determine the order in which each signature was applied.

3.1 Creating a Digital Signature

This section identifies the Digital Signature standards and process used to create a Digital Signature using an X.509v3 signing certificate.

3.1.1 DIGITAL SIGNATURE STANDARD

The standard used in this guide to sign a CDA document is XAdES-X-L, an extension to the W3C XML Digital Signature (XML-DSIG) standard that adds support for long term signature verification via timestamps, certificates, revocation lists, and additional features.

3.1.2 COMPUTATION OF THE DIGEST

It should be noted that excluding the `legalAuthenticator` and `authenticator` participant occurrences from the calculation of the Digest does not remove them from the CDA.

When digitally signing a CDA document, the Digest of the Signed Data Object is the entire document contents including the `ClinicalDocument` start and end tags *excluding* all occurrences of (and elements contained within) the beginning and end tags for `authenticator` and `legalAuthenticator`. The Digest is computed using the method defined in XML-DSIG on the remaining CDA contents and `SignedProperties`.

By excluding `legalAuthenticator` and `authenticator` participant occurrences from the calculation of the Digest, the information signed by each Authorized Signer and Delegated Signer will not be altered by subsequent signing events. This allows for multiple Authorized Signers and Delegated Signers on any CDA as long as each `sdhc:signatureText` element used for signing is included in either a `legalAuthenticator` or `authenticator` participant occurrence and these occurrences are excluded from the calculation of the Digest.

It should be noted that excluding the `legalAuthenticator` and `authenticator` participant occurrences from the calculation of the Digest does not remove them from the CDA.

3.1.3 SIGNATURE PROCESS

The signer creates the XAdES-X-L Digital Signature and populates it with all required elements including:

1. The signer's public X.509v3 signing certificate
2. The Digest of the CDA (see Section 3.1.2 and the `SignedProperties`)
3. The Signed Digest
4. The following signed elements:
 - a. Coordinated Universal Time (UTC)
 - b. Role (see Table 4-4)
 - c. Signature Purpose (see Table 4-4)
5. A signed OCSP or CRL in the `RevocationValues` element

Conformance Statements: XAdES-X-L

ESMD-1: XAdES-X-L digital signatures **SHALL** include each signer's public X.509v3 certificate in the `SigningCertificate` property element.

ESMD-2: XAdES-X-L digital signatures **SHALL** include Coordinated Universal Time (UTC).

ESMD-3: XAdES-X-L digital signatures **SHALL** include a Role from the role code set defined in Table 4-4.

ESMD-4: XAdES-X-L digital signatures **SHALL** include a Signature Purpose from the Signature Purpose code set defined in Table 4-4.

ESMD-5: XAdES-X-L digital signatures **SHALL** include a certification path that was valid at the time of signature in `CertificateValues` property element.

ESMD-6: XAdES-X-L digital signatures **SHALL** include an OCSP or CRL response in the `RevocationValues` property element.

3.2 Creating a Delegation of Rights Artifact

The Delegation of Rights process enables an Authorized Signer to assign a right to another party (a Delegated Signer) to sign a CDA document on their behalf.

This guide provides for two methods of providing a Delegation of Rights:

- Computable (as defined below)
- Non-computable -- such as an image of an executed Power of Attorney.

This guide focuses on the creation, use and validation of a computable Delegation of Rights Artifact. The process presented here is broadly applicable to any situation in which a right must be delegated to another party digitally. In this guide, we are focused on the use of Delegation of Rights Artifact to convey the right to sign a CDA from an Authorized Signer to a Delegated Signer

The following actors may take part in the Delegation of Rights Process:

- An Authorized Signer is the individual or organization that assigns the right.
- A Delegated Signer is the individual or organization that receives the right.
- A Delegation Validator is a third party trusted by the Authorized Signer to confirm that an existing Delegation of Rights is still valid.

Additionally, the following terms are defined:

- A “Delegation of Rights Assertion” is an assertion created by the Authorized Signer prior to being signed.
- A “Delegation of Rights Artifact” is an assertion created *and* digitally signed by the Authorized Signer.
- A “Validated Delegation of Rights” artifact includes the Digital Signature of the Delegation Validator applied to a Delegation of Rights Artifact.

3.2.1 OVERVIEW OF THE DELEGATION OF RIGHTS PROCESS

In general, the Delegation of Rights process proceeds as follows:

1. The Authorized Signer creates and digitally signs a Delegation of Rights Assertion; the resulting Delegation of Rights Artifact is provided to the Delegated Signer (Section 3.2.3).
2. When creating a Digital Signature, the Delegated Signer requests a Validated Delegation of Rights Artifact from the Delegation Validator.
3. Assuming the Delegation of Rights is still valid, the Delegation Validator issues a Validated Delegation of Rights Artifact (Section 3.2.6).
4. The Delegated Signer signs a CDA document on behalf of the Authorized Signer (Section 3.1.3) and includes the Validated Delegation of Rights Artifact as proof of the granted right to sign.

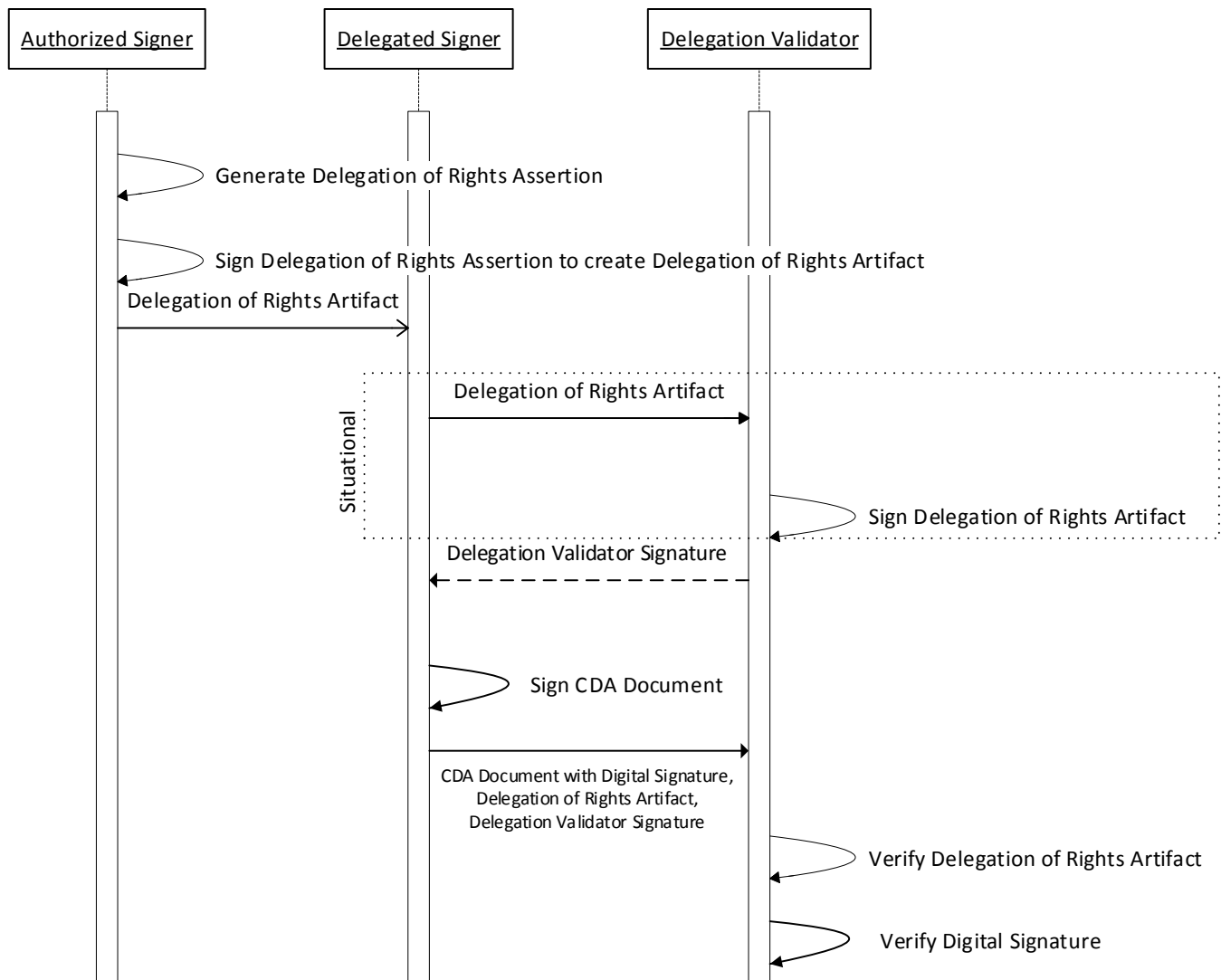


FIGURE 3-1. DELEGATION OF RIGHTS PROCESS

3.2.2 PRE-CONDITIONS

- Authorized Signer, Delegated Signer, and Delegation Validator have obtained X.509v3 digital certificates in compliance with industry-accepted requirements.
- Authorized Signer, Delegated Signer, and Delegation Validator support the required standards for the delegation of rights.
- Minimal cryptographic algorithm specified by policy.

3.2.3 DELEGATION OF RIGHTS STANDARDS

This guide uses the OASIS Security Assertion Markup Language (SAML) 2.0 standard to support the Delegation of Rights. OASIS SAML 2.0 specifies a data format for exchanging authentication and authorization data between parties.

While OASIS specifies the use of the XML Digital Signature (XML-DSIG) standard to sign SAML 2.0 assertions, the Delegation of Rights requires a long term validation. This guide establishes the use of the XML Advanced Electronic Signatures standard with eXtended validation for the long term (XAdES-X-L). XAdES-X-L is an extension of XAdES, which is itself an extension to XML-DSIG. XAdES-X-L adds support for long term signature verification via timestamps, certificates, revocation lists, and additional features.

This guide establishes use of the XAdES-X-L standard to support the Delegation Validator Signature.

Name of Specification	Purpose
OASIS SAML 2.0	Delegation of Rights Assertion
XAdES-X-L	Authorized Signer signs assertion to create Delegation of Rights Artifact
XAdES-X-L	Delegation Validator signs Delegation of Rights Artifact to create Validated Delegation of Rights Artifact

The Delegation of Rights Artifact is meant to prove that a Delegated Signer is authorized to sign a CDA document on behalf of the Authorized Signer.

The Authorized Signer shall create and deliver a signed SAML 2.0 assertion to the Delegated Signer. The Delegated Signer shall act as the Signer and digitally sign a CDA document.

OASIS defines a number of specifications to support the exchange of SAML 2.0 assertions; however, delivery of the SAML 2.0 assertions between actors is outside the scope of this implementation guide.

3.2.4 CREATING A SAML-BASED DELEGATION OF RIGHTS ASSERTION

The Delegation of Rights Artifact shall contain a signed SAML assertion compliant with “saml-core-2.0-os: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) 2.0¹¹.” The following constraints apply to a Delegation of Rights Artifact:

1. The Subject of the assertion must be included and must be the Delegated Signer.
2. The SubjectConfirmation method must be holder-of-key.
3. The SubjectConfirmationData element must include a KeyInfo element.
4. The SubjectConfirmationData KeyInfo type must be X509Data.
5. The SubjectConfirmationData KeyInfo element must contain the X509IssuerSerial of the X.509v3 certificate that holds the public key used to verify the Signature on the document (i.e., the public certificate of the Delegated Signer).
6. The SAML 2.0 assertion must be signed by the Authorized Signer.
7. The Signature element must include a KeyInfo element.
8. The Signature KeyInfo type must be rawX509Certificate.
9. The Signature KeyInfo element must contain the X.509v3 certificate that holds the public key that will be used to verify the signature of the SAML 2.0 assertion (i.e., the public certificate of the Authorized Signer).

This guide makes the following recommendations to limit the use of the Delegation of Rights Artifact:

¹¹ <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

- The assertion should use `NotBefore` and `NotOnOrAfter` elements within the `SubjectConfirmationData` element to bind use of the assertion to a reasonable time frame.
- The assertion should define an `Attribute` of the `Subject` that describes their business relationship.
- The assertion shall have an `Attribute` statement, defined by policy, showing that the right to sign is conferred.

3.2.5 CREATING A DELEGATION OF RIGHTS ARTIFACT

The following steps must be taken for an Authorized Signer to issue a Delegation of Rights Artifact to a Delegated Signer:

1. Authorized Signer creates Delegation of Rights Assertion that includes the following:
 - a. Issuer/ID of Delegated Signer X.509v3 signing certificate,
 - b. Issuer/ID of Authorized Signer X.509v3 signing certificate,
 - c. Start and End date of assertion,
 - d. Right to sign is delegated;
2. Authorized Signer signs the Delegation of Rights assertion using the XAdES-X-L standard syntax;
3. The resultant signed Delegation of Rights Assertion is the Delegation of Rights Artifact.

3.2.6 VALIDATING THE DELEGATION OF RIGHTS ARTIFACT

Once an Authorized Signer provides a Delegation of Rights Artifact to a Delegated Signer, the Authorized Signer needs a method to “revoke” the Delegation of Rights Artifact prior to its expiration date. Without such a method, the Delegation of Rights Artifact presents a security risk whereby the Delegated Signer can sign for the Authorized Signer and use the Delegation of Rights Artifact as the proof of the right after the Authorized Signer has terminated the relationship or signing right.

There are multiple possible methods for validating an existing Delegation of Rights Assertion prior to its expiration date. These include:

- The Authorized Signer publishing to a revocation list.
- A CA using its own process to issue a Delegation of Rights Artifact and publish a revocation list.
- Validation of the Delegation of Rights Artifact by the issuing system.

The methods that employ a revocation list require both management of the list and a process to access the list and validate that a revocation has not occurred at the time of use. This guide specifies the third approach as a preferred method that does not rely on revocation lists. When the Delegated Signer attempts to invoke a SAML 2.0-based delegated right, the Authorized Signer’s system, which issued the assertion, validates the delegation at the time of use by signing the Delegation of Rights Artifact using a system certificate.

To ensure that a Delegation of Rights Artifact is valid at the time of signature, the Delegated Signer must take the following steps immediately prior to using a Delegation of Rights Artifact:

1. Delegated Signer **SHOULD** request a Delegation of Rights Artifact from the Delegation Validator Server/Service
2. Delegation Validator Server/Service **SHALL** perform the following actions:
 - a. Verifies that the Delegation of Rights Assertion has not been revoked.

- b. Signs the Delegation of Rights Artifact using the XAdES-X-L standard syntax and populates the `RevocationValues` element with the current OCSP or signed CRL.
3. The result of this process is the Validated Delegation of Rights Artifact.
4. Delegation Validator SHALL return the Validated (Signed) Delegation of Rights Artifact to the Delegated Signer or an error.
5. Delegated Signer SHALL include the Validated Delegation of Rights Artifact as part of the Delegated Signer's Digital Signature to prove that the right to sign has been delegated.

3.3 Incorporating Digital Signature and Delegation of Rights Artifacts into a CDA Document

The `sdtc:signatureText` element is specified in Consolidated-CDA R2. It provides a “textual or multimedia depiction of the signature by which the participant endorses his or her participation and that he or she agrees to assume the associated accountability.” The `sdtc:signatureText` element holds the Digital Signature by containing a signature data block (i.e., the XAdES-X-L elements) within the CDA header.

The `legalAuthenticator`, if present, **MAY** contain zero or one [0..1] `sdtc:signatureText` (CONF:30810).

```
<legalAuthenticator>
  <time value="20120915223615-0800" />
  <signatureCode code="S" />
  <assignedEntity>
    <id extension="5555555555" root="2.16.840.1.113883.4.6" />
    <code code="207QA0505X" displayName="Adult Medicine"
codeSystem="2.16.840.1.113883.6.101" codeSystemName="NUCC" />
    <addr>
      <streetAddressLine>1004 Healthcare Drive </streetAddressLine>
      <city>Portland</city>
      <state>OR</state>
      <postalCode>99123</postalCode>
      <country>US</country>
    </addr>
    <telecom use="WP" value="tel:+1(555)555-1004" />
    <assignedPerson>
      <name>
        <given>Patricia</given>
        <given qualifier="CL">Patty</given>
        <family>Primary</family>
        <suffix qualifier="AC">M.D.</suffix>
      </name>
    </assignedPerson>
  </assignedEntity>
</legalAuthenticator>
```

FIGURE 3-2. LEGALAUTHENTICATOR EXAMPLE

The authenticator, if present, **MAY** contain zero or one [0..1] `sdtc:signatureText` (CONF:30811).

```
<authenticator>
  <time value="201209151030-0800" />
  <signatureCode code="S" />
  <assignedEntity>
    <id extension="5555555555" root="2.16.840.1.113883.4.6" />
    <code code="207QA0505X" displayName="Adult Medicine"
codeSystem="2.16.840.1.113883.6.101" codeSystemName="NUCC" />
    <addr>
      <streetAddressLine>1004 Healthcare Drive </streetAddressLine>
      <city>Portland</city>
      <state>OR</state>
      <postalCode>99123</postalCode>
      <country>US</country>
    </addr>
    <telecom use="WP" value="tel:+1(555)555-1004" />
    <assignedPerson>
      <name>
        <given>Patricia</given>
        <given qualifier="CL">Patty</given>
        <family>Primary</family>
        <suffix qualifier="AC">M.D.</suffix>
      </name>
    </assignedPerson>
  </assignedEntity>
</authenticator>
```

FIGURE 3-3. AUTHENTICATOR EXAMPLE

The XAdES-X-L syntax is inserted within the `sdtc:signatureText` element. The `sdtc:signatureText` element is then inserted under the appropriate participant occurrence of `legalAuthenticator` or `authenticator`, depending on the capacity in which the Authorized Signer acted when creating the Digital Signature.

By excluding `legalAuthenticator` and `authenticator` participant occurrences from the calculation of the Digest, the information signed by each Authorized Signer and Delegated Signer will not be altered by subsequent signing events. This allows for multiple Authorized Signers and Delegated Signers on any CDA as long as each `sdtc:signatureText` element used for signing is included in either a `legalAuthenticator` or `authenticator` participant occurrences and these occurrences are excluded from the calculation of the Digest.

A Delegated Signer must include a valid Delegation of Rights. A computable Delegation of Rights is described in Section 3.3.23.2. The Authorized Signer must sign the Delegation of Rights Assertion that contains the delegation information and the certificate ID of the Delegated Signer.

If a Delegation of Rights is required, the Validated Delegation of Rights Artifact (Section 3.2.6) is included with the correct XML tags along with the Digital Signature of the Delegated Signer in the same `sdtc:signatureText` element. All of the allowed MIME types defined in the base CDA specification are also allowed in this guide.

The structure of the XML Digital Signature in the `sdtc:signatureText` element is:

```
<sdtc:signatureTEXT mediaType="text/xml" representation="B64">
  <thumbnail mediaType="text/plain" representation = "TXT">
    Text representation of the signature (see Section 3.3.2)
  </thumbnail>
  <digitalSignature>
    <authorizedSigner>
      XAdES-X-L signature of Authorized Signer
    </authorizedSigner>
  </digitalSignature>
</sdtc:signatureText>
```

FIGURE 3-4. SIGNATURETEXT STRUCTURE

The structure of the XML Digital Signature in the `sdtc:signatureText` element with delegation of rights is:

```
<sdtc:signatureText mediaType="text/xml" representation="B64">
  <thumbnail mediaType="text/plain" representation = "TXT">
    Text representation of the signature (see Section 3.3.2)
  </thumbnail>
  <digitalSignature>
    <delegatedSigner>
      XAdES-X-L signature of Delegated Signer
    </delegatedSigner>
    <delegationofRights>
      <dorType>
        Value from Table 4-4 DoR Type
      </dorType>
      <dorValidation> [for DoRType 1.2.1]
        XAdES-X-L signature of Delegation Validator
      </dorValidation>
      <dorSaml>
        SAML 2.0 Assertion signed by Authorized Signer with XAdES-X-L
      </dorSaml>
    </delegationofRights>
  </digitalSignature>
</sdtc:signatureText>
```

FIGURE 3-5. SIGNATURETEXT STRUCTURE WITH DELEGATION OF RIGHTS

The content of `sdtc:signatureText` will be one of the following:

1. For a signature by the Authorized Signer:
 - a. `authorizedSigner` only
2. For a signature by a Delegated Signer:
 - a. no `authorizedSigner`
 - b. `delegatedSigner`
 - c. `delegationofRights`

The `sdtc:signatureText` element is associated with the appropriate Participant occurrence within the CDA header (depending on whether the Signer acted in the capacity of an authenticator or a legalAuthenticator). All Digital Signature and Delegation of Rights artifacts are held within the `sdtc:signatureText` element, which contains the following:

- 1) Text description of the Digital Signature (see Section 3.3.2)
- 2) The signers Digital Signature [XAdES-X-L]
 - a. One of `authorizedSigner` or `delegatedSigner`
- 3) If the signer is a Delegated Signer, then the `delegationofRights` block is included.

3.3.1 SPECIFICATIONS FOR THE ED DATA TYPE

The `sdtc:signatureText` element has an ED data type and is to be specified with the following values:

```
representation = "B64"  
mediaType = "application"
```

3.3.2 SPECIFICATIONS FOR THUMBNAIL

The `sdtc:signatureText` element is an ED data type and permits the definition of a `thumbnail` to provide a human readable version of the Digital Signature:

```
<thumbnail mediaType="text/plain" representation="TXT">
```

The `thumbnail` text string SHOULD contain the following elements for an Authorized Signer:

1. "Digitally Signed by Authorized Signer"
2. Signers name
3. Date and time of signature
4. Role
5. Purpose

Example (Authorized Signer):

Digitally signed by Authorized Signer John Doe on 4/21/2013 at 15:30 EDT as Physician for the purpose of Author's signature.

The `thumbnail` text string SHOULD contain the following elements for a Delegated Signer

1. "Digitally Signed by Delegated Signer"
2. Signers name
3. Date and time of signature
4. Role
5. Purpose
6. "Delegate right to sign by"
7. Name of the right delegator

Example (Delegated Signer):

Digitally signed by Delegated Signer John Doe on 4/21/2013 at 15:30 EDT as Physician for the purpose of Co-author's signature. Delegated right to sign by Jane Doe.

Conformance Statements: `sdtc:signatureText`

ESMD-7: `sdtc:signatureText` **SHALL** contain exactly one `authorizedSigner` or exactly one `delegatedSigner` block with one `[XAdES-X-L]`.

ESMD-8: if `sdtc:signatureText` contains one `delegatedSigner` then `sdtc:signatureText` **SHALL** contain exactly one `delegationofRights`.

ESMD-9: if `sdtc:signatureText` contains one `delegationofRights` then, `delegationofRights` **SHALL** contain exactly one `dorType`.

ESMD-10: if `dorType` is “1.2.1” then `delegationofRights` **SHALL** contain exactly one `dorValidation`.

ESMD-11: if `dorType` is “1.2.1” then `delegationofRights` **SHALL** contain exactly one `dorSaml`.

ESMD-12: `sdtc:signatureText/representation` **SHALL** be “B64”.

ESMD-13: `sdtc:signatureText/mediaType` **SHALL** be “application”.

ESMD-14: `sdtc:signatureText/thumbnail representation` **SHALL** be “TXT”.

ESMD-15: `sdtc:signatureText/thumbnail mediaType` **SHALL** be “text/plain”.

ESMD-16: `sdtc:signatureText/thumbnail` **SHALL** contain a textual representation of the digital signature that contains the following elements described in Section 3.3.2.

3.4 Verifying an XAdES-based Signature

A Recipient is the receiver of the signed CDA document and should verify the Digital Signatures using the following steps to verify the identity of the Authorized Signer(s) and the Delegated Signer(S) and the integrity of the CDA document¹². The following steps provide technical verification of the signer’s signature and do not discuss the requirements that policy may place on verification of Certificate content, CDA document types, delegation, etc. XAdES-X-L is used to encapsulate all validation artifacts (such as path to issuer and revocation list) to avoid any dependency on availability of such resources at the time of validation.

3.4.1 VERIFYING THE SIGNERS SIGNATURE

1. Verify the X.509v3 Certificate contained in the `x509Certificate` element. Specifically, verify that:
 - a. The certificate was current at the time of signature.
 - b. The certificate has been issued for an acceptable purpose.
 - c. The trust anchor is acceptable by verifying the complete chain to the issuing CA’s root certificate.
 - d. The `altName` field includes the required identification (NPI within the US realm) or an Alternative ID.
 - e. The CRL or OCSP included in the XAdES-X-L was signed by the issuing CA at a date and time, acceptable by policy, relative to the date of the Digital Signature.

¹² Verification of the Digital Signatures in a Validated Delegation of Rights Artifact is identical (see Section 3.2).

- f. The signing certificate is not on the signed CRL or is indicated as valid on the signed OSCP response included in the XAdES-X-L `RevocationValues` element.
2. Inspect signature date/time for constancy with signature and timestamp policy.
3. Verify that the role of the signer is appropriate.
4. Inspect the signature purpose is reasonable and appropriate given the document content and the signer identity.
5. Decrypt the signed Digest with the public key from the X.509v3 public digital certificate.
6. Compute the Digest of the CDA document using the serialization and algorithm specified in the signature.
7. Verify that the signed Digest matches the computed Digest.
8. Use and verification of optional fields in the Digital Signature is based on trading partner agreement and outside of the scope of this document.

If any of these steps fails, the Signature cannot be verified.

3.4.2 VERIFYING THE VALIDATION SIGNATURE

If a Delegation of Rights assertion is signed by a Delegation Validator, then the following steps should be performed to verify the validation signature on the Delegation of Rights Artifact:

1. Verify the Delegation Validator Signature.
2. Verify that the `SigningTime` element falls within appropriate time frame as defined by Recipient policies.

If any of these steps fail, the Delegation Validator Signature cannot be verified. If these steps are successful, the validity of the Delegation of Rights Artifact has been confirmed and the Recipient should proceed to verify the SAML 2.0-based Delegation of Rights Artifact.

3.4.3 VERIFYING THE DELEGATION OF RIGHTS ARTIFACT

If a Digital Signature has an associated Delegation of Rights Artifact, it should be verified using the following steps to confirm that the Delegated Signer has the right to sign the CDA document on behalf of the Authorized Signer:

1. Confirm that any limitations defined within the Delegation of Rights Assertion are met, including:
 - a. Current date falls within `NotBefore` and `NotOnOrAfter` elements.
 - b. Attribute of the Subject describes a business relationship appropriate for signing a CDA document.
 - c. Attribute statement, defined by policy showing that the right to sign is conferred.
2. Use the X.509v3 certificate referenced in the `Signature KeyInfo` element to validate the identity of the entity that signed the assertion (i.e., the Authorized Signer).
3. Verify that the signer of the Delegation of Rights Assertion (i.e., the Authorized Signer) meets appropriate policy requirements.
4. Verify the signature contained in the `Signature` element of the assertion.
5. Confirm that the `SubjectConfirmationData KeyInfo` element references the same X.509v3 certificate that holds the public key that will be used to verify the Signature on the CDA document (i.e., the certificate of the Delegated Signer).

If any of these steps fails, Delegation of Rights cannot be confirmed.

4 DATA REQUIREMENTS

These tables list the data elements and data element sets that will be available within the certificate information, document signature, and delegation of rights assertion of the CDA document. Each data element listed below is necessary for some aspect of the Use Case; however, the table does not specify exactly how they may be used together. The usage and cardinality constraints in the following tables are based on the XML-DSIG, XAdES, and SAML 2.0 specifications.

4.1 Document Signature

An asterisk (*) indicates the element is not part of the base XAdES or XML-DSIG specification but is a name-spaced element added to fulfill the requirements of this guide.

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
*digitalSignature	R	[1..1]	Container element which contains all digital signature and delegation of rights artifacts.	
*authorizedSigner	O	[0..1]	Container element which contains <code>Signature</code> element for the Authorized Signer. <code>sdsc:signatureText</code> must contain either the <code>authorizedSigner</code> element or the <code>delegatedSigner</code> element.	
*delegatedSigner	O	[0..1]	Container element which contains the <code>Signature</code> element for the Delegated Signer. <code>sdsc:signatureText</code> must contain either the <code>authorizedSigner</code> element or the <code>delegatedSigner</code> element.	
*delegationofRights	R	[1..1]	Container element for the Delegation of Rights Artifact (SAML 2.0) elements.	Required if the signer is a Delegated Signer
*dorType	R	[1..1]	Indicates the type of delegation of rights being asserted.	Required if the <code>delegationofRights</code> element is present. See Table 4-4. Code Sets: <code>dorType</code> for values.
*dorValidation	R	[1..1]	Container element for Delegation Validator XAdES signature artifact	
Signature	O	[0..1]	Root element of an XML digital signature	
SignedInfo	R	[1..1]	Used to specify the canonicalization algorithm, a signature algorithm, and one or more references	May also contain an optional <code>ID</code> attribute that will allow it to be referenced by other signatures and objects.
CanonicalizationMethod	R	[1..1]	Specifies the canonicalization algorithm applied to the <code>SignedInfo</code> element prior to performing signature	When not present, the standard canonicalization

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
			calculations. Indicates method used for canonicalizing XML node sets resulting after retrieving (and processing when required) the data objects covered by the time-stamp token(s)	method as specified by XML-DSIG <i>MUST</i> be used
SignatureMethod	R	[1..1]	Specifies the algorithm used for digital signature generation and validation.	This algorithm identifies all cryptographic functions involved in the signature operation (e.g. hashing, public key algorithms, MACs, padding, etc.)
Reference	RE	[0..*]	Specifies a digest algorithm and digest value, and optionally an identifier of the object being signed, the type of the object, and/or a list of transforms to be applied prior to digesting. The identification (URI) and transforms describe how the digested content was created.	The <code>Type</code> attribute facilitates the processing of referenced data. An optional <code>ID</code> attribute permits a <code>Reference</code> to be referenced from elsewhere.
Transforms	RE	[0..1]	Contains an ordered list of <code>Transform</code> elements	
Transform	R	[1..*]	Describes how the signer obtained the data object that was digested. The output of each <code>Transform</code> serves as input to the next <code>Transform</code> . The input to the first <code>Transform</code> is the result of dereferencing the <code>URI</code> attribute of the <code>Reference</code> element. The output from the last <code>Transform</code> is the input for the <code>DigestMethod</code> algorithm.	If the <code>Transforms</code> element is used, at least one <code>Transform</code> element must be used. When transforms are applied the signer is not signing the native (original) document but the resulting (transformed) document
DigestMethod	R	[1..1]	Identifies the digest algorithm to be applied to the signed object	
DigestValue	R	[1..1]	Contains the base64 encoded value of the digest	
SignatureValue	R	[1..1]	Contains the actual base64 encoded value of the digital signature	
KeyInfo	RE	[0..1]	Contains public key information for validating signatures. May contain keys, names, certificates, and other PKI management information.	If <code>KeyInfo</code> is omitted, the recipient is expected to be able to identify the key based on application context.
KeyName	O	[0..1]	Contains a string value which may be used by the signer to communicate a key identifier to the recipient.	The name of the digital signer is required, but it is not required that <code>KeyName</code> be used.
KeyValue	O	[0..1]	Contains a single public key that may be useful in validating the signature	Must contain exactly one of any of the following elements: 1. <code>DSAPublicKey</code> 2. <code>RSAKeyValue</code> 3. Externally-defined public keys values represented as <code>PCDATA</code> or element types from an external namespace

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
RetrievalMethod	O	[0..1]	Conveys a reference to <code>KeyInfo</code> information that is stored at another location. For example, several signatures in a document might use a key verified by an X509v3 certificate chain appearing once in the document or remotely outside the document; each signature's <code>KeyInfo</code> can reference this chain using a single <code>RetrievalMethod</code> element instead of including the entire chain with a sequence of <code>X509Certificate</code> elements.	
X509Data	R	[1..1]	Contains one or more identifiers of keys or X509 certificates (or certificates' identifiers or a revocation list). Must contain at least one or more [1..*] of the following elements: <code>X509IssuerSerial</code> , <code>X509SKI</code> , <code>X509SubjectName</code> , <code>X509Certificate</code> , <code>X509CRL</code>	Any <code>X509IssuerSerial</code> , <code>X509SKI</code> , and <code>X509SubjectName</code> elements that appear MUST refer to the certificate or certificates containing the validation key.
Object	R	[1..*]	Parent element to all XAdES extension elements, which are added on to the base XMLDSIG core element (detailed in the rows above).	While the <code>Object</code> element may be repeated for purposes other than XAdES, such use is out of scope for this guide.
QualifyingProperties	R	[1..1]	Acts as a container element for all the qualifying information that should be added to an XML signature. <code>QualifyingProperties</code> are split into properties that are cryptographically bound to (i.e. signed by) the XML signature (<code>SignedProperties</code>), and properties that are not cryptographically bound to the XML signature (<code>UnsignedProperties</code>).	The <code>SignedProperties</code> MUST be covered by a <code>ds:Reference</code> element of the XML signature.
SignedProperties	R	[1..1]	Properties that are cryptographically bound (i.e., signed) to the XML signature	
SignedSignatureProperties	R	[1..1]	Contains properties that qualify the XML signature that has been specified with the <code>Target</code> attribute of the <code>QualifyingProperties</code> container element.	The optional <code>Id</code> attribute can be used to make a reference to the <code>UnsignedProperties</code> element.
SigningTime	R	[1..1]	Specifies the time at which the signer (purportedly) performed the digital signature process.	This element is optional within the XAdES specification, but required for the purposes of this guide.
SigningCertificate	R	[1..1]	Contains references to certificates and digest values computed on them. The certificate used to verify the signature SHALL be identified in the sequence. The signature policy MAY mandate other certificates be present, that MAY include all the certificates up to the point of trust.	This element is optional within the XAdES specification, but required for the purposes of this guide. This element contains the sequence of certificate identifiers and digests computed on the certificates. This information is further elaborated within the

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
				Cert elements CertDigest and IssuerSerial (listed below).
CertDigest	R	[1..1]	Contains the digest of one of the certificates referenced in the sequence. It contains two elements: <code>ds:DigestMethod</code> indicates the digest algorithm, and <code>ds:DigestValue</code> contains the value of the digest..	The optional URI attribute serves to indicate where the referenced certificate can be found.
IssuerSerial	R	[1..1]	Contains the identifier of one of the certificates referenced in the sequence. Should the <code>ds:X509IssuerSerial</code> element appear in the signature to denote the same certificate, its value MUST be consistent with the corresponding <code>IssuerSerial</code> element.	
SignaturePolicyIdentifier	R	[1..1]	Contains elements that specify ways to identify the set of rules governing the creation and validation of the digital signature.	Must contain exactly one of the following: <code>SignaturePolicyID</code> or <code>SignaturePolicyImplied</code>
SignaturePolicyID	RE	[0..1]	Appears when the signature policy contains an explicit and unambiguous identifier of a signature policy together with a hash value of the signature policy, so it can be verified that the policy selected by the signer is the one being used by the verifier. An explicit signature policy has a globally unique reference which is bound to a digital signature by the signer as part of the signature calculation. In these cases, for a given explicit signature policy there shall be one definitive form that has a unique binary encoded value.	The <code>SigPolicyId</code> element contains an identifier that uniquely identifies a specific version of the signature policy. The <code>SigPolicyHash</code> element contains the identifier of the hash algorithm and the hash value of the signature policy. The <code>SigPolicyQualifier</code> element can contain additional information qualifying the signature policy identifier.
SignaturePolicyImplied	O	[0..1]	Appears when the digital signature can avoid the inclusion of the aforementioned identifier and hash value. This will be possible when the signature policy can be unambiguously derived from the semantics of the type of data object(s) being signed, and some other information, e.g. national laws or private contractual agreements, that mention that a given signature policy MUST be used for this type of data content. In such cases, the signature will contain a specific empty element indicating that this implied way to identify the signature policy is used instead of the identifier and hash value.	Use of this field is based on a signature policy that is agreed to by both the signer and the intended recipient. Details of such a policy are out of the scope of this document.
SignatureProductionPlace	O	[0..1]	In some transactions the purported place where the signer was at the time of signature creation MAY need to be indicated. This element specifies an address associated with the signer at a particular geographical (e.g. city) location.	Must contain no more than one of each of the following elements: <code>City</code> , <code>StateorProvince</code> , <code>PostalCode</code> , <code>CountryName</code> .
SignerRole	R	[1..1]	Property that contains a sequence of roles that the signer can play.	This element is optional within the XAdES

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
				specification, but required for the purposes of this guide. It must contain at least one of the two elements: <code>ClaimedRoles</code> , <code>CertifiedRoles</code> .
<code>ClaimedRoles</code>	R	[1..1]	Contains a sequence of roles (using <code>ClaimedRole</code> element(s)) claimed by the signer but not certified. Additional contents types MAY be defined on a domain application basis and be part of this element.	
<code>ClaimedRole</code>	R	[1..*]	Indicates role of signer	From Healthcare Taxonomy Data Set
<code>CertifiedRoles</code>	O	[0..1]	Contains one or more wrapped DER-encoded attribute certificates for the signer (using <code>CertifiedRole</code> elements).	
<code>CertifiedRole</code>	R	[1..*]	Indicates role of signer	
<code>*SignaturePurpose</code>	R	[1..*]	Contains a signature purpose claimed by the signer.	From ASTM E 1762-95
<code>SignedDataObjectProperties</code>	O	[0..1]	Contains properties that qualify some of the signed data objects.	May include any of the following elements: <code>DataObjectFormat</code> , <code>CommitmentTypeIndication</code> , <code>AllDataObjectsTimeStamp</code> , <code>IndividualDataObjectsTimeStamp</code>
<code>DataObjectFormat</code>	O	[0..*]	Provides information that describes the format of the signed data object. This element SHOULD be present when the signed data is to be presented to human users on verification if the presentation format is not implicit within the data that has been signed. Must include the <code>ObjectReference</code> attribute, which must reference the <code>ds:Reference</code> element of the <code>ds:Signature</code> corresponding with the data object qualified by this property.	If used, this element must include at least one of any the following elements: <code>Description</code> , <code>ObjectIdentifier</code> , <code>MimeType</code> , <code>Encoding</code> . These properties may not be repeated within the <code>DataObjectFormat</code> element.
<code>CommitmentTypeIndication</code>	O	[0..*]	Identifies the type of commitment made by the digital signer by either explicitly using a commitment type indication in the digital signature, or by implicitly or explicitly using the semantics of the signed data object. A commitment type definition includes the object identifier for the commitment as well as a sequence of qualifiers.	Must contain exactly one <code>CommitmentTypeId</code> element. Must contain either <code>AllSignedDataObjects</code> element, or <code>ObjectReference</code> element(s). May contain <code>CommitmentTypeQualifiers</code> element.
<code>CommitmentTypeId</code>	O	[0..1]	Unequivocally identifies the type of commitment made by the signer. Required if <code>CommitmentTypeIndication</code> element is used.	Must include exactly one <code>Identifier</code> element (which indicates URI of commitment). May include no more than one of each of the following elements: <code>Description</code> and

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
				DocumentationReferences.
AllDataObjectsTimeStamp	O	[0..*]	Contains the time-stamp computed before the signature production, over the sequence formed by ALL the <code>ds:Reference</code> elements within the <code>ds:SignedInfo</code> referencing whatever the signer wants to sign except the <code>SignedProperties</code> element. The application MUST compose the <code>Include</code> elements to refer to all the <code>ds:Reference</code> elements except the one referencing the <code>SignedProperties</code> element. Their corresponding <code>referencedData</code> attribute MUST be present and set to "true".	May contain more than one <code>Include</code> element. May contain no more than 1 <code>CanonicalizationMethod</code> elements. Must contain at least one of the following two elements: <code>EncapsulatedTimeStamp</code> or <code>XMLTimeStamp</code> .
IndividualDataObjectsTimeStamp	O	[0..*]	Contains the time-stamp computed before the signature production, over a sequence formed by SOME <code>ds:Reference</code> elements within the <code>ds:SignedInfo</code> . Note that this sequence cannot contain a <code>ds:Reference</code> computed on the <code>SignedProperties</code> element. The application MUST compose the <code>Include</code> elements to refer to those <code>ds:Reference</code> elements that are to be time-stamped. Their corresponding <code>referencedData</code> attribute MUST be present and set to "true".	May contain more than one <code>Include</code> element. May contain no more than 1 <code>CanonicalizationMethod</code> elements. Must contain at least one of the following two elements: <code>EncapsulatedTimeStamp</code> or <code>XMLTimeStamp</code> .
UnsignedProperties	R	[1..1]	Contains properties that are not bound/signed by the digital signature.	May contain at most one of each of the following elements: <code>UnsignedSignatureProperties</code> , <code>UnsignedDataObjectProperties</code>
UnsignedSignatureProperties	R	[1..1]	Contains properties that qualify the XML signature that has been specified with the <code>Target</code> attribute of the <code>QualifyingProperties</code> container element.	The optional <code>Id</code> attribute can be used to make a reference to the <code>UnsignedProperties</code> element.
CounterSignature	O	[0..*]	Provides support for multiple imbedded signatures. Each counter-signature is carried in one <code>CounterSignature</code> element added to the <code>Signature</code> element to which the counter-signature is applied.	In a qualified <code>Signature</code> the contents of the <code>CounterSignature</code> element are one or more signatures (i.e. <code>ds:Signature</code> elements) of the <code>SignatureValue</code> in the qualified <code>Signature</code> . A counter-signature can itself be qualified by a <code>CounterSignature</code> property.
SignatureTimeStamp	O	[0..*]	A container for a time-stamp token over the <code>ds:SignatureValue</code> element to protect against repudiation in case of a key compromise.	The application MUST compose one <code>Include</code> element with an URI referencing the <code>ds:SignatureValue</code>

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
				element. The input for the time-stamp has is, in consequence, the <code>ds:SignatureValue</code> element.
<code>CompleteCertificateRefs</code>	R	[1..1]	Contains a sequence of references to the full set of CA certificates that have been used to validate the digital signature up to (but not including) the signing certificate.	Must contain exactly one <code>CertRefs</code> element. The <code>CertRef</code> element must contain at least one <code>Cert</code> element.
<code>CompleteRevocationRefs</code>	RE	[1..1]	Contains a full set of references to the revocation data that have been used in the validation of the signer and CA certificates.	Must contain at most one of any of the following elements: <code>CRLRefs</code> , <code>OCSPRefs</code> , <code>OtherRefs</code> .
<code>CRLRefs</code>	RE	[0..1]	Contains sequences of references to CRLs via the <code>CRLRef</code> element. Identification of a CRL is made using 1) the digest of the entire DER encoded CRL (<code>DigestAlgAndValue</code> element); and 2) a set of data (<code>CRLIdentifier</code> element) including the issuer (<code>Issuer</code> element), the time when the CRL was issued (<code>IssueTime</code> element) and optionally the number of the CRL (<code>Number</code> element).	The <code>Identifier</code> element can be dropped if the CRL could be inferred from other information. Its <code>URI</code> attribute could serve to indicate where the identified CRL is archived. Must contain at least one <code>CRLRef</code> element. [1..*]
<code>OCSPRefs</code>	RE	[0..1]	Contains sequences of references to OCSP data via the <code>OCSPRef</code> element. Identification of an OCSP response is made using 1) a set of data (<code>OCSPIdentifier</code> element) including the name of the server that has produced the referenced response (<code>ResponderID</code> element) and the time indication in the "ProducedAt" field of the referenced response (<code>ProducedAt</code> element); and 2) the digest computed on the DER encoded <code>OCSPResponse</code> (as defined in the <code>DigestAlgAndValue</code> element), since it MAY be needed to differentiate between two OCSP responses by the same server with their "ProducedAt" fields within the same second.	The optional <code>URI</code> attribute could serve to indicate where the OCSP response identified is archived Must contain at least one <code>OCSPRef</code> element. [1..*]
<code>AttributeCertificateRefs</code>	O	[0..1]	Contains the references to the full set of Attribute Authorities certificates that have been used to validate the attribute certificate. This property MAY be used only when a user attribute certificate is present within the digital signature.	Must contain exactly one <code>CertRefs</code> element.
<code>AttributeRevocationRefs</code>	O	[0..1]	Contains the references to the full set of Attribute Certificate Revocation List and/or OCSP responses that have been used in the validation of the attribute certificate(s) present in the signature. This property MAY be used only when a user attribute certificate is present in the signature within the signature.	Must contain at most one of any of the following elements: <code>CRLRefs</code> , <code>OCSPRefs</code> , <code>OtherRefs</code> .

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
SigAndRefsTimeStamp	RE	[1..*]	Contains a time-stamp which covers the signature and references to validation data. When an OCSP response is used, it is necessary to time-stamp in particular that response in the case the key from the responder would be compromised. Since the information contained in the OCSP response is user specific and time specific, an individual time-stamp is needed for every signature received.	<p>The application MUST compose the following sequence of <code>Include</code> elements:</p> <ul style="list-style-type: none"> - One <code>Include</code> element whose <code>URI</code> attribute references the <code>ds:SignatureValue</code> element of the qualified digital signature; - One <code>Include</code> element per each present <code>SignatureTimeStamp</code>. The <code>URI</code> attribute in each <code>Include</code> element will reference one <code>SignatureTimeStamp</code> element; - One <code>Include</code> element whose <code>URI</code> attribute references the <code>CompleteCertificateRefs</code> property element; - One <code>Include</code> element whose <code>URI</code> attribute references the <code>CompleteRevocationRefs</code> property element; - One element whose <code>URI</code> attribute references the <code>AttributeCertificateRefs</code> element if this property is present; - One element whose <code>URI</code> attribute references the <code>AttributeRevocationRefs</code> element if this property is present.
RefsOnlyTimeStamp	O	[0..*]	<p>Contains a time-stamp which covers only references to validation data. Time-Stamping each digital signature with Complete Validation Data as defined above (<code>SigAndRefsTimeStamp</code> element) may not be efficient, particularly when the same set of CA certificates and CRL information is used to validate many signatures.</p> <p>Time-Stamping CA certificates will stop any attacker from issuing bogus CA certificates that could be claimed to exist before the CA key was compromised. Any bogus time-stamped CA certificates will show that the certificate was created after the legitimate CA key was compromised. In the same way, time-stamping CA CRLs, will stop any attacker from issuing bogus CA CRLs which could be claimed to exist before the CA key was compromised.</p>	<p>The application MUST compose the following sequence of <code>Include</code> elements:</p> <ul style="list-style-type: none"> - One <code>Include</code> element whose <code>URI</code> attribute references the <code>CompleteCertificateRefs</code> property element; - One <code>Include</code> element whose <code>URI</code> attribute references the <code>CompleteRevocationRefs</code> property element; - One element whose <code>URI</code> attribute references the <code>AttributeCertificateRefs</code> element if this property is present; - One element whose <code>URI</code> attribute references the <code>AttributeRevocationRefs</code> element if this property is present.

Table 4-1. Document Signature				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
CertificateValues	R	[1..1]	Contains the full set of certificates that have been used to validate the digital signature, including the signer's certificate. However, it is not necessary to include one of those certificates into this property, if the certificate is already present in the <code>ds:KeyInfo</code> element of the signature. Both the signer certificate and all certificates referenced in the <code>CompleteCertificateRefs</code> property (when present) element MUST be present either in the <code>ds:KeyInfo</code> element of the signature or in the <code>CertificateValues</code> property element. In addition, all the certificates referenced in <code>AttributeCertificateRefs</code> (when present) MUST also be present in the <code>CertificateValues</code> element.	This element is optional within the XAdES specification, but required for the purposes of this guide. Must contain one of the following elements: <code>EncapsulatedX509Certificate</code> , <code>OtherCertificate</code> . The <code>EncapsulatedX509Certificate</code> element is able to contain the base64 encoding of a DER-encoded X.509v3 certificate. The <code>OtherCertificate</code> element is a placeholder for potential future new formats of certificates.
RevocationValues	RE	[1..1]	Contains the values of the revocation information which are to be shipped with the digital signature. This property MAY also include the revocation data for any time-stamping units that have provided the time-stamp tokens if this information is not already included in the time-stamp token as part of the digital signature..	This element is optional within the XAdES specification, but required for the purposes of this guide. Must contain no more than one of any the following elements: <code>CRLValues</code> , <code>OCSPValues</code> , <code>OtherValues</code> .

4.2 Delegation of Rights Assertion

Table 4-2. Delegation of Rights Assertion				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
saml:Assertion	R	[1..1]	Specifies the basic information that is common to all assertions.	Must include the following elements: <code>Issuer</code> , <code>ds:Signature</code> , <code>Subject</code> . Must include the following attributes: <code>Version</code> , <code>ID</code> , <code>IssueInstant</code> . <code>Version</code> attribute must be "2.0".
saml:Issuer	R	[1..1]	The SAML authority that is making the claim(s) in the assertion. The issuer SHOULD be unambiguous to the intended relying parties.	

Table 4-2. Delegation of Rights Assertion				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
ds:Signature	R	[1..1]	Digital Signature Artifact encrypted by signer's private key. The ds:Signature element also contains the ds:Object element, which in turn contains required XAdES-specific elements. See Table 4-1. Document Signature for detailed digital signature elements.	Must include ds:KeyInfo element. ds:KeyInfo element must be "rawX509Certificate" and must contain the X.509v3 certificate that holds the public key that will be used to verify the signature of the Assertion (i.e., the public certificate of the Delegator).
saml:Subject	R	[1..1]	The subject of the statement(s) in the assertion. Identified by BaseID, NameID or EncryptedID. A Subject element SHOULD NOT identify more than one principal. The subject MUST be the Delegatee.	Must include element SubjectConfirmation. Should contain an Attribute element that describes the business relationship between Delegator and Delegatee.
saml:SubjectConfirmation	R	[1..1]	Provides the means for a relying party to verify the correspondence of the subject of the assertion with the party with whom the relying party is communicating. The Method attribute provides a reference that identifies a protocol or mechanism to be used to confirm the subject.	The Method attribute must be "holder-of-key." Must include element SubjectConfirmationData.
saml:SubjectConfirmationData		[1..1]	Specifies additional data that allows the subject to be confirmed or constrains the circumstances under which the act of subject confirmation can take place. The time period specified by the NotBefore and NotOnOrAfter attributes SHOULD fall within the overall assertion validity period as specified by the Conditions element's NotBefore and NotOnOrAfter attributes. If both attributes are present, the value for NotBefore MUST be less than (earlier than) the value for NotOnOrAfter.	The following attributes are optional within the SAML 2.0 specification, but are required for the purposes of this guide: NotBefore, NotOnOrAfter. Must include ds:KeyInfo element, which must also include ds:X509Data element. The ds:X509Data element must contain the X509IssuerSerial element, relating to the X.509v3 certificate that holds the public key of the Delegatee.
saml:Conditions		[0..1]	Conditions that MUST be evaluated when assessing the validity of and/or when using the assertion.	May contain the following attributes: NotBefore, NotOnOrAfter, AudienceRestriction, OneTimeUse, ProxyRestriction
saml:Attribute		[0..1]	Identifies an attribute by name and optionally includes its value(s). It is used within an attribute statement to express particular attributes and values associated with an assertion subject.	The assertion should define an Attribute of the Subject that describes their business relationship.
saml:AttributeStatement		[1..1]		

4.3 Validated Delegation of Rights Assertion

Table 4-3. Validated Delegation of Rights Assertion				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
saml:Assertion	R	[1..1]	Delegation of Rights Assertion as described in Table 4-2. Delegation of Rights Assertion.	
ds:Signature	R	[1..1]	Digital Signature artifacts encrypted by signer's private key for Delegation of Rights Assertion as described in Table 4-2. Delegation of Rights Assertion.	Includes XAdES-X-L elements. This element is contained within the saml:Assertion element.
ds:Signature	R	[1..1]	Digital Signature artifacts to provide for a validated Delegation of Rights Assertion.	Includes XAdES-X-L elements. Reference to the Delegation of Rights Assertion is contained within this ds:Signature element.

4.4 Code Sets

Table 4-4. Code Sets				
Data Element	Usage	Cardinality	Code Set	Additional Notes
Role	R	[1..1]	Healthcare Taxonomy Data Set OR Personal and Legal Relationship Role Type	Healthcare Provider Taxonomy (HIPAA) 2.16.840.1.114222.4.11.1066 2.16.840.1.113883.11.20.12.1 – A personal and legal relationship records the role of a person in relation to another person, or a person to himself or herself. This value set is to be used when recording relationships based on personal or family ties or through legal assignment of responsibility.
Signature Purpose	R	[1..1]	ASTM E 1762-95	See Appendix E: Signature Purpose
Delegation of Rights Assertion Action	R	[1..1]	'Authorized Signer'	
dorType (Delegation of Rights Type)	R	[1..1]	1.1.0 – PDF of executed 1.2.0 – Computable SAML Assertion (no validation) 1.2.1 – Computable SAML Assertion (with system validation)	User extensible

4.5 Purpose of Signature and Role within a Signed CDA (Example)

Figure 4-1 shows the CDA containing a header and a body, with the key header elements on the right including participation types, some of which are optional but are included for illustrative purposes.

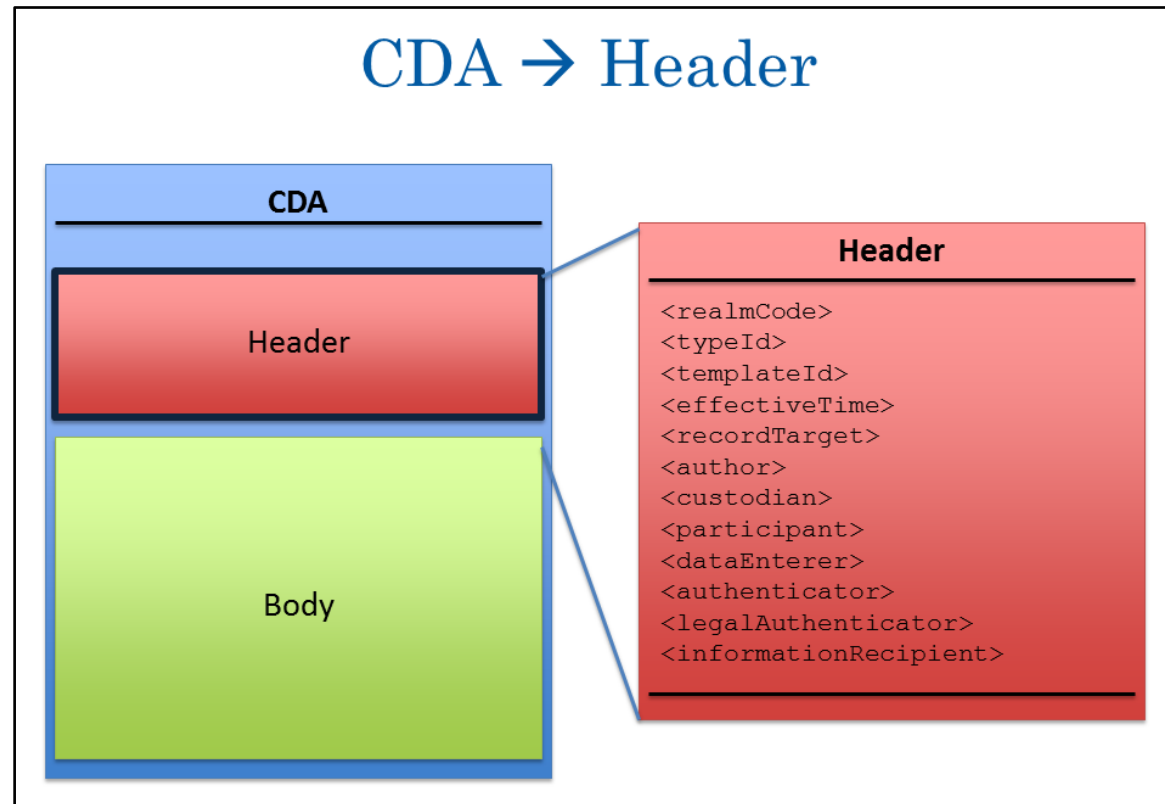


FIGURE 4-1. HEADER DETAIL

Figure 4-2 shows the header elements, and on the right the authenticator element which contains four important top-level tags under it.

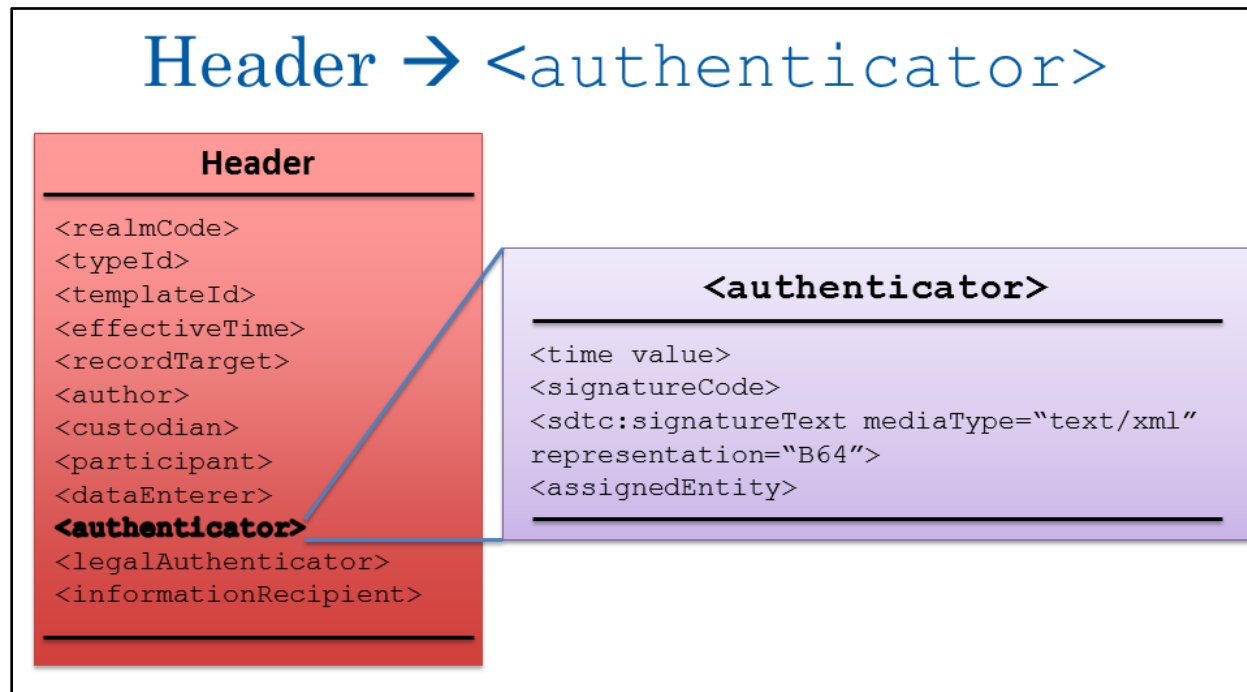


FIGURE 4-2. AUTHENTICATOR DETAIL

The `sdtc:signatureText` tag contains the `ds:Signature` tag, which further contains the `ds:Object` tag. The `ds:Object` tag contains the XAdES elements. Further nested under the `ds:Object` tag is `QualifyingProperties` tag, which contains both `SignedProperties` and `UnsignedProperties`.

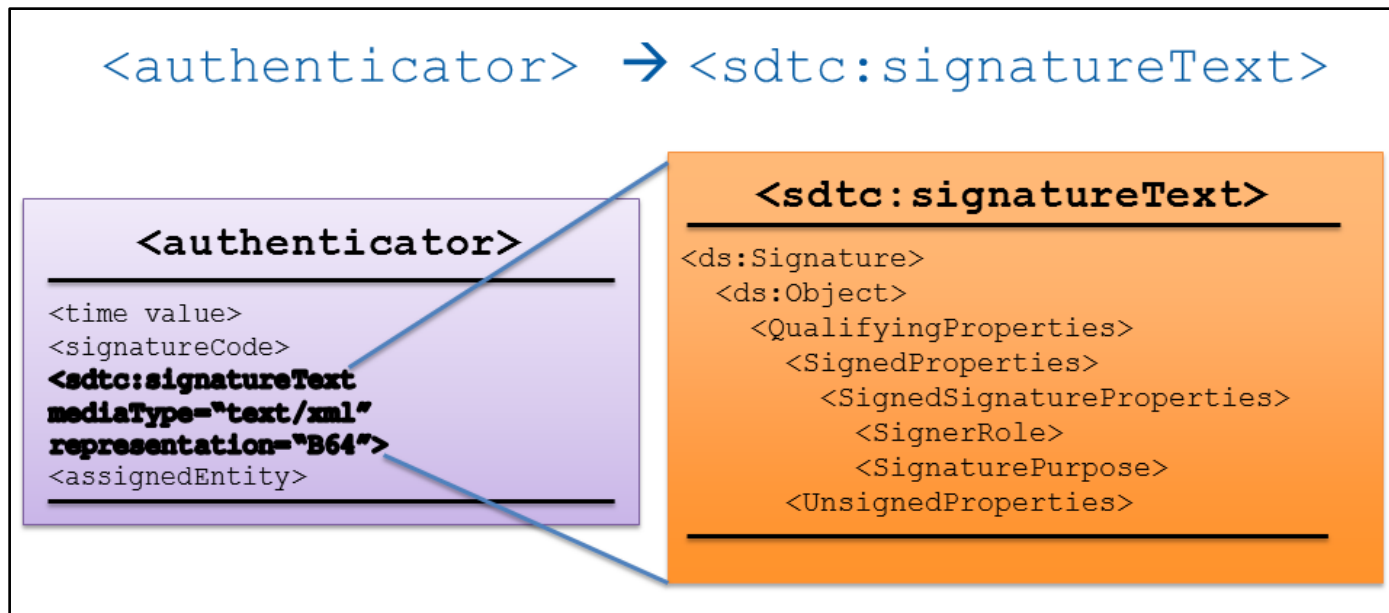


FIGURE 4-3. SDTC:SIGNATURETEXT DETAIL

Within SignedProperties, there is the SignedSignatureProperties tag, which contains the SignerRole tag. This tag indicates the role of the Authorized Signer. The SignerRole tag can either contain a ClaimedRoles or CertifiedRoles tag. The ClaimedRoles tag contains the ClaimedRole tag, which is used to specify the asserted role of the signer using the Healthcare Taxonomy Code Set. In this example, the code is set to Trauma Surgery (2086S0127X). Role can also be indicated using CertifiedRoles, however the CertifiedRole tag calls for a base64encrypted data type.

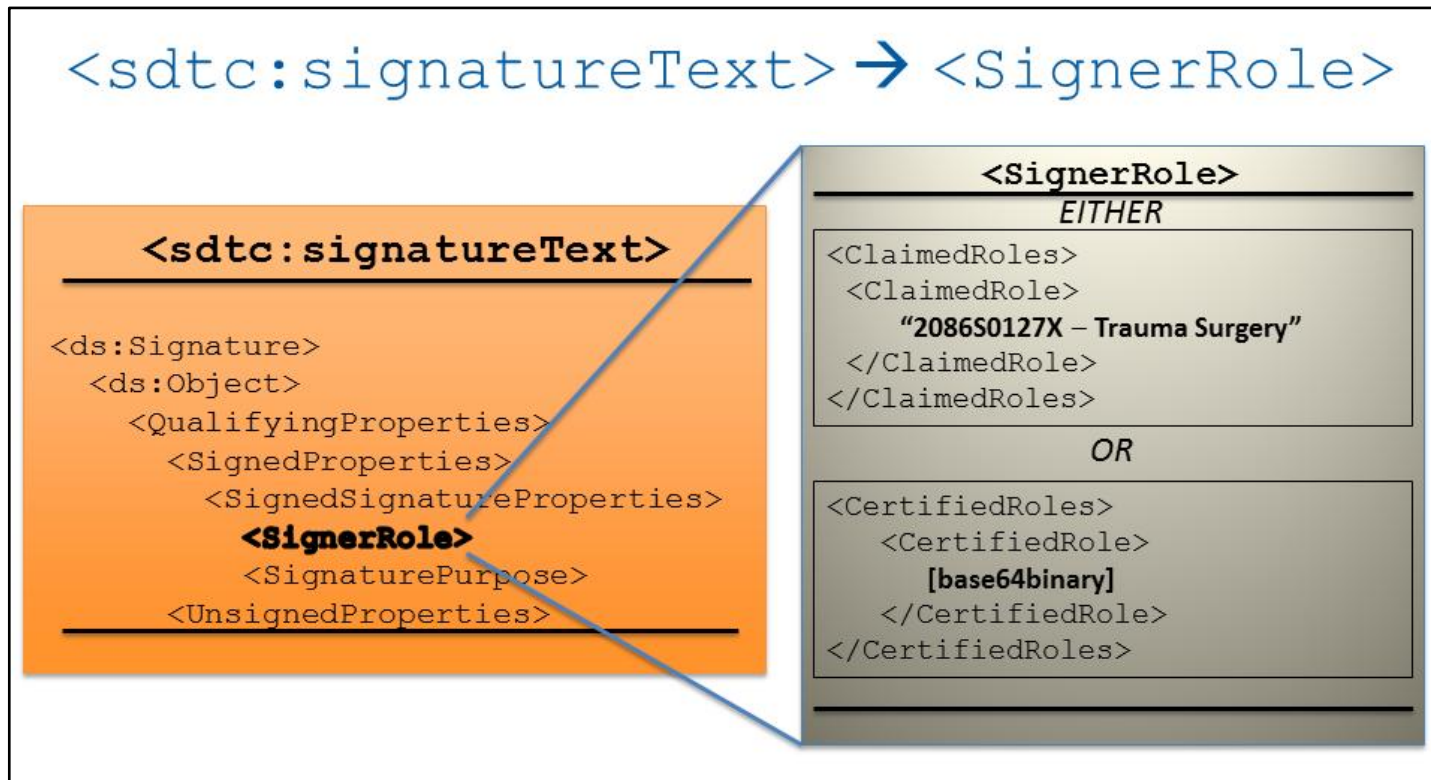


FIGURE 4-4. SIGNERROLE DETAIL

Within SignedSignatureProperties, we can also indicate the SignaturePurpose using the ASTM E-1762 code set – in this case, to provide more granularity and clarity as to the Signer’s role. In this example, the Signer indicates she is signing as a coauthor.

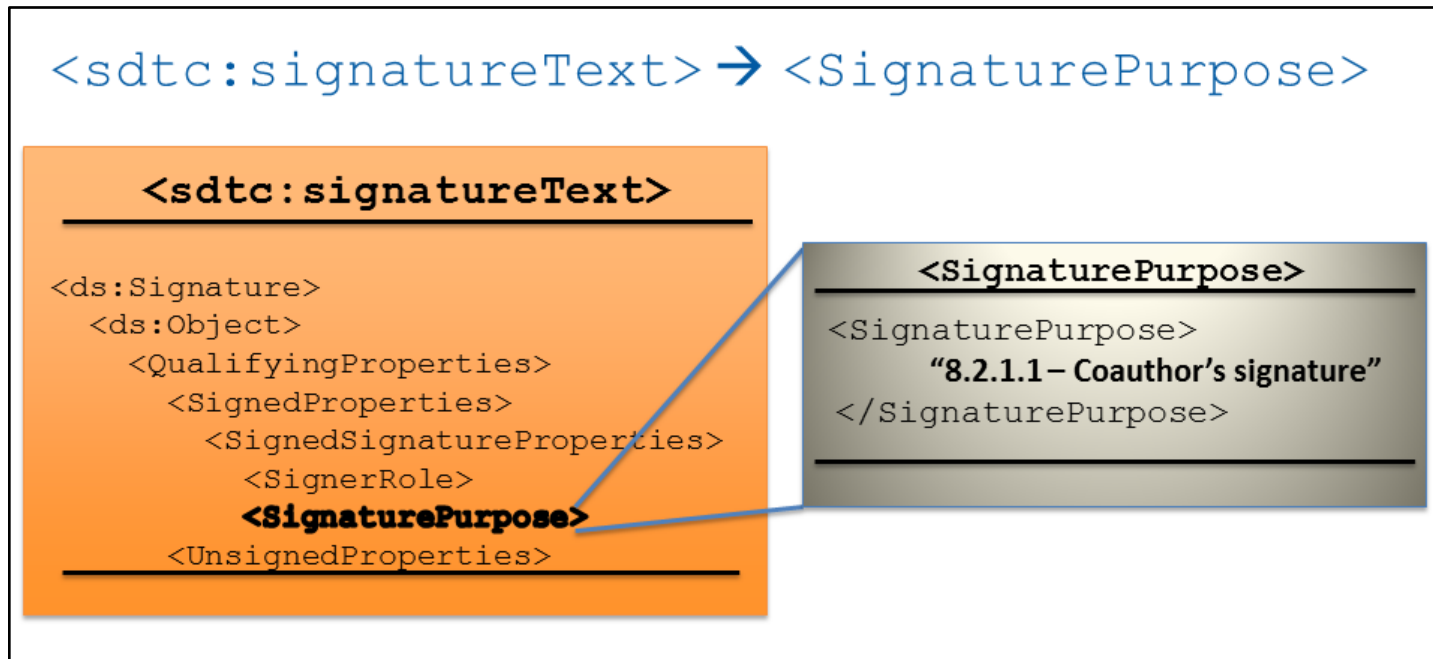


FIGURE 4–5. SIGNATUREPURPOSE DETAIL

5 RISKS

- Signature by a patient or their authorized representative:
 - a. Level of Assurance may be lower than that allowed by provider and payers
 - b. Definition and verification of authorized representative
- Production, verification and validation of Delegation of Rights:
 - a. Definition of appropriate business relationship
 - b. Definition of rights delegated
 - c. Policy issues related to who can delegate and the allowed recipient of the delegation
 - d. Revocation issues
 - e. Validation issues (how do we know the delegation was valid on use)
- Timestamp fabrication:
 - a. May be minimized by certified signing module
 - b. May be minimized by use of timestamp services

6 APPENDIX A: EXAMPLES

The following XML examples present an XAdES-X-L Signature, a SAML 2.0 based Delegation of Rights Artifact, and an XAdES-X-L Signature for that Delegation of Rights Artifact.

6.1 XAdES-X-L Digital Signature

```
<legalAuthenticator>
  <time value="20090227130000+0500"/>
  <signatureCode code="S"/>
  <!-- SignatureText START -->
  <sdct:signatureText mediaType="text/xml" representation="B64">
    <!-- XAdES WORK (Signed CDA): START -->
    <thumbnail mediaType="text/plain" representation="TXT">Digitally signed by John Doe on 2013-04-01 at 18:30 CDT as
    Physician for the purpose of Author.
    </thumbnail>
    <digitalSignature>
      <authorizedSigner>
        <ds:Signature>
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512" />
            <ds:Reference>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha512" />
              <ds:DigestValue>2c2dc2c30d3dd3fca22e3ccf02ca0f4db8a5d6494b6319df28b70fb76c7b246fed
              13840ca913be70802e2345c6dd3a6087ab00c41f64e80e61e2c6bc24d105fe</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>oRrea2fzFswyLeE+a36P2C/xQB4BMk6LJPAyym873qgjS1loqR3fbZLYvm/yJ6iGCANc9+mbP4U/
          kwIyn63QQhjHIST/i3Z9bwwo6QV9EewHGybkNEFvK+7C51JI88bNR9pihp/3Y5Afp9+a0o566fKX
          HNNksd5a5cSytqfPTYoiZq5LQdLYkjzLSyCy0YhGDiG6DKk0uBjAdkNlt1Z7GtaP2XhpcKQ1x3XI
          n1S8T1HjBqKNw6ZIZ64+8GtA+kwwayXOVpdYL1r6M6iq1HrbLLSqGFY1+RQCe0+9qjSTHQRgg+eT
          y7K2x1Rg9zMg3tLkAtUyLOsP/jNa7RU5HwC/Q==</ds:SignatureValue>
        </ds:Signature>
      </authorizedSigner>
    </digitalSignature>
  </sdct:signatureText>
  <ds:Object>
    <QualifyingProperties>
      <SignedProperties>
        <SignedSignatureProperties>
          <SigningTime>2012-04-26T16:04:56Z</SigningTime>
          <SigningCertificate>
            <Cert URI="http://www.example.com/">
              <CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512" />
                <ds:DigestValue>
xmlns="http://www.w3.org/2000/09/xmldsig#">bJrQQeyoztdAP06nsoRQ5oX5oAg=</ds:DigestValue>
```

```

        </CertDigest>
        <IssuerSerial>
            <X509IssuerName>X.509 distinguished name of certificate</X509IssuerName>
            <X509SerialNumber>certificate serial number</X509SerialNumber>
        </IssuerSerial>
    </Cert>
</SigningCertificate>
<SignaturePolicyIdentifier>...</SignaturePolicyIdentifier>
<SignatureProductionPlace>
    <City>City</City>
    <State>State</State>
    <PostalCode>Zip</PostalCode>
    <CountryName>Country</CountryName>
</SignatureProductionPlace>
<SignerRole>
    <ClaimedRoles>
        <ClaimedRole>"2086S0127X - Trauma Surgery"</ClaimedRole>
    </ClaimedRoles>
</SignerRole>
    <SignaturePurpose>"8.2.1.1 - Author's signature"</SignaturePurpose>
</SignedSignatureProperties>
<SignedDataObjectProperties>
    <DataObjectFormat>
        <Description>string</Description>
        <ObjectIdentifier>
            <Identifier>http://www.example.com</Identifier>
            <Description>string</Description>
            <DocumentationReferences>
                <DocumentationReference>http://www.example.com</DocumentationReference>
            </DocumentationReferences>
        </ObjectIdentifier>
        <MimeType>string</MimeType>
        <Encoding>http://www.example.com</Encoding>
    </DataObjectFormat>
    <CommitmentTypeIndication>
        <CommitmentTypeId>
            <Identifier>http://www.example.com</Identifier>
            <Description>string</Description>
            <DocumentationReferences>
                <DocumentationReference>http://www.example.com</DocumentationReference>
            </DocumentationReferences>
        </CommitmentTypeId>
        <ObjectReference>http://www.example.com</ObjectReference>
        <CommitmentTypeQualifiers>
            <CommitmentTypeQualifier>text</CommitmentTypeQualifier>

```



```

        </CommitmentTypeQualifiers>
    </CommitmentTypeIndication>
    <AllDataObjectsTimeStamp>
        <Include URI="http://www.example.com/" />
        <CanonicalizationMethod Algorithm="http://www.example.com/">text</CanonicalizationMethod>
        <EncapsulatedTimeStamp>EncapsulatedPKIDataType</EncapsulatedTimeStamp>
    </AllDataObjectsTimeStamp>
    <IndividualDataObjectsTimeStamp>
        <Include URI="http://www.example.com/" />
        <CanonicalizationMethod Algorithm="http://www.example.com/">text</CanonicalizationMethod>
        <EncapsulatedTimeStamp>EncapsulatedPKIDataType</EncapsulatedTimeStamp>
    </IndividualDataObjectsTimeStamp>
</SignedDataObjectProperties>
</SignedProperties>
<UnsignedProperties>
    <UnsignedSignatureProperties>
        <!-- Added by XAdES-T -->
        <SignatureTimeStamp>...</SignatureTimeStamp>
        <!-- Added by XAdES-C -->
        <CompleteCertificateRefs>
            <CertRefs>
                <Cert URI="http://www.example.com/">
                    <CertDigest>...</CertDigest>
                    <IssuerSerial>...</IssuerSerial>
                </Cert>
            </CertRefs>
        </CompleteCertificateRefs>
        <CompleteRevocationRefs>
            <OCSPRefs>
                <OCSPRef>
                    <OCSPIdentifier URI="http://www.example.com/">...</OCSPIdentifier>
                    <DigestAlgAndValue>...</DigestAlgAndValue>
                </OCSPRef>
            </OCSPRefs>
            <OtherRefs>
                <OtherRef>text</OtherRef>
            </OtherRefs>
        </CompleteRevocationRefs>
        <!-- Added by XAdES-X. Choose one: -->
        <SigAndRefsTimeStamp>
            <Include URI="http://www.example.com/" />
            <ds:CanonicalizationMethod Algorithm="http://www.example.com/">text</ds:CanonicalizationMethod>
            <EncapsulatedTimeStamp>GpM7</EncapsulatedTimeStamp>
        </SigAndRefsTimeStamp>
        <RefsOnlyTimeStamp>

```

```

        <Include URI="http://www.example.com/">
        <ds:CanonicalizationMethod Algorithm="http://www.example.com/">text</ds:CanonicalizationMethod>
        <EncapsulatedTimeStamp>GpM7</EncapsulatedTimeStamp>
    </RefsOnlyTimeStamp>
    <!-- Added by XAdES-X-L -->
    <CertificateValues>
        <EncapsulatedX509Certificate>GpM7</EncapsulatedX509Certificate>
    </CertificateValues>
    <RevocationValues>
        <CRLValues>
            <EncapsulatedCRLValue>GpM7</EncapsulatedCRLValue>
        </CRLValues>
        <OCSPValues>
            <EncapsulatedOCSPValue>GpM7</EncapsulatedOCSPValue>
        </OCSPValues>
        <OtherValues>
            <OtherValue>text</OtherValue>
        </OtherValues>
    </RevocationValues>
    </UnsignedSignatureProperties>
</UnsignedProperties>
</QualifyingProperties>
</ds:Object>
</ds:Signature>
</authorizedSigner>
</digitalSignature>
<!-- XAdES WORK (Signed CDA): END -->
</signatureText>
<!-- SignatureText END -->
    <assignedEntity>
    <id extension="999999999" root="2.16.840.1.113883.4.6"/>
    <addr>
        <streetAddressLine>Street</streetAddressLine>
        <city>City</city>
        <state>State</state>
        <postalCode>Zip</postalCode>
        <country>US</country>
    </addr>
    <telecom use="WP" value="tel:555-555-1002"/>
    <assignedPerson>
        <name>
            <given>First</given>
            <family>Last</family>
        </name>
    </assignedPerson>

```

```

    </assignedEntity>
</legalAuthenticator>

```

6.2 SAML Delegation of Rights Artifact

```

<legalAuthenticator>
  <time value="20090227130000+0500"/>
  <signatureCode code="S"/>
  <sdtc:signatureText mediaType="text/xml" representation="B64">
    <thumbnail mediaType="text/plain" representation="TXT">Digitally signed by John Doe on 2013-04-01 at 18:30 CDT as
Physician for the purpose of Author. Delegate right to sign by Jane Doe.
    </thumbnail>
    <!-- Delegation artifact begin -->
    <digitalSignature>
      <delegationOfRights>
        <dorType>"1.2.0 - Computable SAML Assertion (no validation)"</dorType>
        <dorSaml>
          <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="550e8400-e29b-41d4-
a716-446655440000" Version="2.0" IssueInstant="2012-01-01T12:00:00Z">
            <saml:Issuer Format="urn:oasis:names:SAML:2.0:nameid-
format:entity">http://example.provider.com</saml:Issuer>
            <saml:Subject>
              <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">CN=John D.,O=AoR
Delegated Signer Inc.,ST=VA,C=US</saml:NameID>
              <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                <saml:SubjectConfirmationData xsi:type="saml:KeyInfoConfirmationDataType">
                  <ds:KeyInfo> <!-- identifier of Delegatee/Signer certificate -->
                    <ds:X509Data>
                      <ds:X509IssuerName>X.509 distinguished name of certificate</ds:X509IssuerName>
                      <ds:X509SerialNumber>certificate serial number</ds:X509SerialNumber>
                    </ds:X509Data>
                  </ds:KeyInfo>
                </saml:SubjectConfirmationData>
              </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions>
              NotBefore="2013-08-01T12:00:00Z"
              NotOnOrAfter="2013-08-16T12:10:00Z">
            </saml:Conditions>
            <saml:AttributeStatement>
              <saml:Attribute
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                Name="http://example.hih.com/esMDBusinessPartner"
                FriendlyName=" Business Partner">

```

```

        <saml:AttributeValue>...</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Saml>
</ds:Signature>
  <ds:Reference URI="#550e8400-e29b-41d4-a716-446655440000"/>
    <!--Additional XML Sig data here-->
    <ds:SignatureValue>base64SignatureValue</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <!-- certificate of Delegator -->
        <ds:X509Certificate>base64X509certificate</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <ds:Object>
      <QualifyingProperties>
        <SignedProperties>
          <SignedSignatureProperties>
            <SigningTime>2012-04-26T16:04:56Z</SigningTime>
            <SigningCertificate>
              <Cert URI="http://www.example.com/">
                <CertDigest>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
                  <ds:DigestValue
                    xmlns="http://www.w3.org/2000/09/xmldsig#">bJrQQeyoztdAPO6nsoRQ5oX5oAg=</ds:DigestValue>
                </CertDigest>
                <IssuerSerial>
                  <X509IssuerName>X.509 distinguished name of certificate </X509IssuerName>
                  <X509SerialNumber>certificate serial number </X509SerialNumber>
                </IssuerSerial>
              </Cert>
            </SigningCertificate>
            <SignaturePolicyIdentifier>...</SignaturePolicyIdentifier>
            <SignerRole>
              <ClaimedRoles>
                <ClaimedRole>Any text</ClaimedRole>
              </ClaimedRoles>
            </SignerRole>
          </SignedSignatureProperties>
        </SignedProperties>
        <UnsignedProperties>
          <UnsignedSignatureProperties>
            <SignatureTimeStamp>...</SignatureTimeStamp>
            <CompleteCertificateRefs>
              <CertRefs>

```

```

        <Cert URI="http://www.example.com/">
          <CertDigest>...</CertDigest>
          <IssuerSerial>...</IssuerSerial>
        </Cert>
      </CertRefs>
    </CompleteCertificateRefs>
    <CompleteRevocationRefs>
      <OCSPRefs>
        <OCSPRef>
          <OCSPIdentifier URI="http://www.example.com/">
            ...
          </OCSPIdentifier>
          <DigestAlgAndValue>...</DigestAlgAndValue>
        </OCSPRef>
      </OCSPRefs>
    </CompleteRevocationRefs>
    <SigAndRefsTimeStamp>
      <Include URI="http://www.example.com/">
        <ds:CanonicalizationMethod
          Algorithm="http://www.example.com/">Text</ds:CanonicalizationMethod>
        <EncapsulatedTimeStamp>GpM7</EncapsulatedTimeStamp>
      </SigAndRefsTimeStamp>
    <CertificateValues>
      <EncapsulatedX509Certificate>GpM7</EncapsulatedX509Certificate>
    </CertificateValues>
  </UnsignedSignatureProperties>
</UnsignedProperties>
</QualifyingProperties>
</ds:Object>
</ds:Signature>
</saml:Assertion>
</delegationOfRights>
</digitalSignature>
</sdtc:signatureText>
<assignedEntity>
  <id extension="999999999" root="2.16.840.1.113883.4.6"/>
  <addr>
    <streetAddressLine>Street</streetAddressLine>
    <city>City</city>
    <state>State</state>
    <postalCode>Zip</postalCode>
    <country>US</country>
  </addr>
  <telecom use="WP" value="tel:555-555-1002"/>
</assignedPerson>

```

```

    <name>
      <given>First</given>
      <family>Last</family>
    </name>
  </assignedPerson>
</assignedEntity>
</legalAuthenticator>

```

6.3 XAdES-X-L Digital Signature Applied to SAML Delegation of Rights

```

<legalAuthenticator>
  <time value="20090227130000+0500"/>
  <signatureCode code="S"/>
  <sdtc:signatureText mediaType="text/xml" representation="B64">
    <thumbnail mediaType="text/plain" representation="TXT">
      Digitally signed by Bob Doe on 2013-04-01 at 18:30 CDT as Physician for the purpose of Co-Author. Delegated right
      to sign by Jane Doe.
    </thumbnail>
    <digitalSignature>
      <delegationOfRights>
        <dorType>"1.2.1 - Computable SAML Assertion (with system validation)"</dorType>
        <dorValidation>
          <ds:Signature Id="signatureOID" xmlns:ds=http://www.w3.org/2000/09/xmldsig#
            xmlns:xad="http://uri.etsi.org/01903/v1.1.1#">
            <SignedInfo>
              <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
              <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
              <Reference>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>base64ManifestDigestValue</DigestValue>
              </Reference>
            </SignedInfo>
            <SignatureValue>base64SignatureValue</SignatureValue>
            <KeyInfo>
              <X509Data>
                <!-- signing certificate for Delegation Verifier-->
                <X509Certificate>base64X509certificate</X509Certificate>
              </X509Data>
            </KeyInfo>
          </ds:Signature>
          <ds:Object>
            <QualifyingProperties>
              <SignedProperties>
                <SignedSignatureProperties>
                  <SigningTime>2012-04-26T16:04:56Z</SigningTime>
                  <SigningCertificate>

```

```

<!-- identifier of signing certificate -->
<Cert>
  <CertDigest>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
    <DigestValue>base64 digest value</DigestValue>
  </CertDigest>
  <IssuerSerial>
    <X509IssuerName>X.509 distinguished name of certificate</X509IssuerName>
    <X509SerialNumber>certificate serial number</X509SerialNumber>
  </IssuerSerial>
</Cert>
<Cert> <!-- identifier of signing certificate's parent -->
  <CertDigest>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
    <DigestValue>base64 digest value</DigestValue>
  </CertDigest>
  <IssuerSerial>
    <X509IssuerName>X.509 distinguished name of parent's certificate</X509IssuerName>
    <X509SerialNumber>certificate serial number</X509SerialNumber>
  </IssuerSerial>
</Cert>
</SigningCertificate>
<SignaturePolicyIdentifier>id</SignaturePolicyIdentifier>
</SignedSignatureProperties>
</SignedProperties>
<UnsignedProperties>
  <UnsignedSignatureProperties>
    <RevocationValues>
      <OCSPValues>
        <EncapsulatedOCSPValue>base64OCSPResponse</EncapsulatedOCSPValue>
      </OCSPValues>
    </RevocationValues>
  </UnsignedSignatureProperties>
</UnsignedProperties>
</QualifyingProperties>
<!-- reference to XAdES Signed Properties -->
<Reference Type=http://uri.etsi.org/01903/v1.1.1#SignedProperties URI="#SignedProperties">
  <Transforms>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-200103015#WithComments"></Transform>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>base64DigestValue</DigestValue>
</Reference>
<!-- reference to SAML Assertion -->
<Reference URI="550e8400-e29b-41d4-a716-446655440000">

```

```

        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-200103015#WithComments"></Transform>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>base64DigestValue</DigestValue>
      </Reference>
    </ds:Object>
  </ds:Signature>
</ds:Signature>
</delegationOfRights>
</digitalSignature>
</signatureText>
<assignedEntity>
  <id extension="999999999" root="2.16.840.1.113883.4.6"/>
  <addr>
    <streetAddressLine>Street</streetAddressLine>
    <city>City</city>
    <state>State</state>
    <postalCode>Zip</postalCode>
    <country>US</country>
  </addr>
  <telecom use="WP" value="tel:555-555-1002"/>
</assignedPerson>
  <name>
    <given>First</given>
    <family>Last</family>
  </name>
</assignedPerson>
</assignedEntity>
</legalAuthenticator>

```


7 APPENDIX B: SIGNING CERTIFICATE INFORMATION

Table 7-1. Signing Certificate Information				
Data Element	Usage	Cardinality	Data Element Description	Additional Notes
Version	R	[1..1]	Version of X.509	All must be version 3(X.509v3)
Serial Number	R	[1..1]	Unique Serial Number of Certificate from the CA	
Algorithm ID	R	[1..1]	Algorithm used by the CA to sign the certificate	
Issuer	R	[1..1]	Name of CA that issued certificate	
Validity	R	[1..1]	Period of time for which the certificate is valid	Not Before, Not After
Subject	R	[1..1]	Subject Name -- Name of whom the certificate is issued to	
Subject Public Key Info	R	[1..1]	The subject's public key	
Issuer Unique Identifier	R	[1..1]		
Subject Unique Identifier	C(R/O)	[1..1]	NPI or Alternate Payer ID	For billing entities only
Extensions	R	[1..*]	Describes specific purpose of use, values, and critical or non-critical identifier	Object Identifier for each extension; non-repudiation "flag" must be set
Certificate Signature Algorithm	R	[1..1]	Algorithm used to sign the certificate	
Certificate Signature	R	[1..1]		

8 APPENDIX C: CREATION OF THE DIGEST

A signature attests to one's participation in the CDA. A digest is the result of a mathematical algorithm that takes all of the bits of the thing to be signed (in this case, the CDA document excluding the `legalAuthenticator` and `authenticator` tags in the CDA header), and computes a string of characters (the digest/hash). The string has two important characteristics:

1. It is highly improbable to recreate the same digest using different data input
2. It's mathematically impossible to create the original document given only the original digest.

A 30-page CDA may result in a digest string of 30 characters. Using a private key, the Signer encrypts the 30-character string—the encrypted digest is an inherent part of the digital signature. The Signer then sends the CDA document with included digital signature and encrypted digest, along with the Signer's public certificate/key, to the Recipient.

The Recipient receives it and uses the same algorithm to create the digest, then uses the Signer's public key to decrypt the Signer's encrypted digest. If the Recipient's calculation of the digest and the Signer's digest are identical, it proves two important things:

1. The original data has been unaltered from the time it was signed
2. The Signer was actually the person who signed the document

If any part of the document used to compute the digest is modified, the computation of the digest is altered and prior signatures invalidated. The `legalAuthenticator` and `authenticator` are excluded from the calculation of the digest because those items will be modified as each signature is added.

9 APPENDIX D: MULTIPLE SIGNERS SCENARIO

9.1 Multiple Signers

This guide supports multiple signatures on the same CDA document through the inclusion of additional `authenticator` elements.

Consider a surgical scenario where there are 5 contributors (all identified as Authorized Signers per local policy) to a CDA document. The signers may include Surgeon A, Surgeon B, the Anesthesiologist, Nurse A, and Nurse B. Surgeon A is also empowered by local policy to act in the capacity as the `legalAuthenticator`; the remaining four contributors will sign only as `authenticators`.

Although the timing of the application of multiple digital signatures is out of scope for this guide (with the exception of the `legalAuthenticator`, which by definition would logically be the final signature applied) all Authorized Signers in this scenario may sign the same CDA document at any time without altering the signature digest.

The processes outlined in user stories 1 and 2 do not change when multiple signers are signing the same CDA document. Through appropriate use of both `signerRole` and `signaturePurpose`, Digital Signatures can accommodate co-signatures on any CDA (e.g. multiple Authorized Signers can indicate that they are co-authors). In addition, since the XAdES-X-L standard used by this guide supports counter signatures, any Digital Signature may be counter signed.

In this scenario, it is assumed that workflow presents a specific version of a CDA document to the Authorized Signers; the document's `id` (OID) and `versionNumber` being within the scope of the computed digest, these values are set and remain immutable throughout the signing activity.

Of the five Authorized Signers, the `legalAuthenticator` is asserting legal responsibility for the CDA document in its entirety per the definitions in the base CDA R2 standard.

Below is a table illustrating the different designations that might appear in this scenario of treatment with five care providers.

Table 9-1. Signature Roles and Purposes for Multiple Signers				
Actor	CDA Participant Type	Signer Role	Signature Purpose	Description
Surgeon A	<code>legalAuthenticator</code>	Trauma Surgery - 2086S0127X	Author's signature - 8.2.1.1	Chief surgeon ultimately responsible for the document
Surgeon B	<code>authenticator</code>	Orthopaedic Trauma - 207XX0801X	Coauthor's signature - 8.2.1.2	Consulting specialty surgeon who was present during the surgery
Anesthesiologist	<code>authenticator</code>	Anesthesiology - Critical Care Medicine - 207LC0200X	Coauthor's signature - 8.2.1.2	Anesthetized patient and was present during surgery
Nurse A	<code>authenticator</code>	Nurse Anesthetist, Certified Registered - 367500000X	Co-participant's signature - 8.2.1.3	Assisted Anesthesiologist and was present during surgery
Nurse B	<code>authenticator</code>	Registered Nurse - 163W00000X	Consent witness signature - 8.2.1.11	Served as witness for consent to spouse to operate
System	<code>Author</code>	N/A	N/A	System responsible for generating the CDA document

9.2 Activity Diagram

Figure 9-1 illustrates the flow for the scenario of multiple signers digitally signing a CDA document.

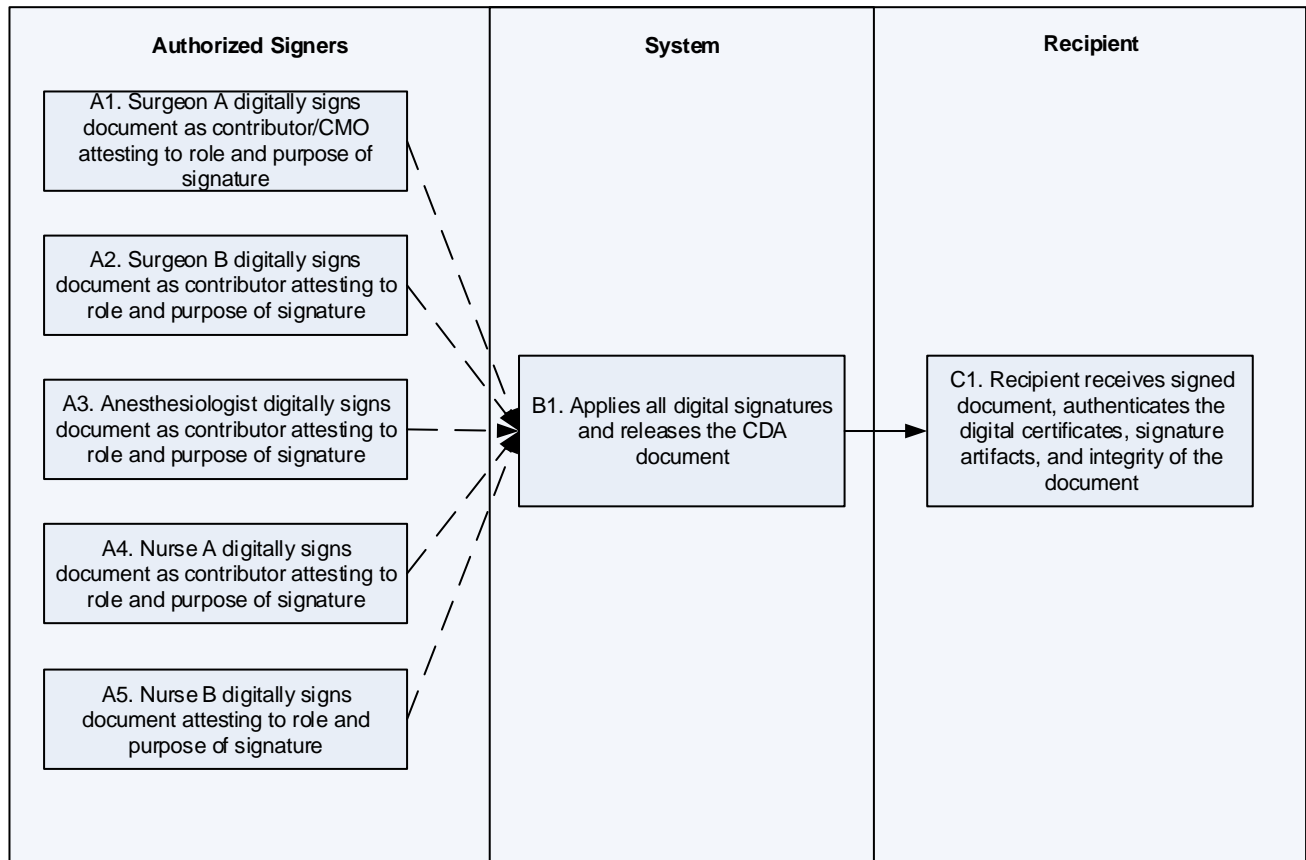


FIGURE 9-1. ACTIVITY DIAGRAM FOR MULTIPLE SIGNERS

9.3 Base Flow

The Base Flows presents the step by step process of the information exchange depicted in the activity diagrams (above). It indicates the actor who performs the action, the description of the event/action, and the associated inputs (records/data required to undertake the action) and outputs (records/data produced by actions taken).

Step	Actor	Role	Event/Description	Inputs	Outputs
A1	Authorized Signer – Surgeon A	Attests to action on Document	Authorized Signer completes and applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signature Artifacts
A2	Authorized Signer – Surgeon B	Attests to action on Document	Authorized Signer completes and applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signature Artifacts
A3	Authorized Signer - Anesthesiologist	Attests to action on Document	Authorized Signer completes and applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signature Artifacts

Table 9-2. Base Flow for Multiple Signers Scenario					
Step	Actor	Role	Event/Description	Inputs	Outputs
A4	Authorized Signer – Nurse A	Attests to action on Document	Authorized Signer completes and applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signature Artifacts
A5	Authorized Signer – Nurse B	Attests to action on Document	Authorized Signer completes an applies a non-repudiation Digital Signature attesting to the role and signature purpose	Document	Digitally Signature Artifacts
B1	System	Generates CDA	Assembles all Digital Signature Artifacts and creates new version of CDA that contains Digital Signatures. Document has new OID and <code>versionNumber</code> .	Digital Signature Artifacts from Authorized Signers	Digitally Signed (New) Document
C1	Recipient	Receiver and Validator of Document	Recipient receives Document, authenticates Signature Artifacts including the Delegation of Rights Assertions, and validates data integrity	Digitally Signed Document with a Delegation of Rights Assertion	Success or failure of Signature Artifact validation, Delegation of Rights Artifacts validation, and Data integrity authentication

10 APPENDIX E: SIGNATURE PURPOSE

Table 10-1. Signing Purpose ¹³	
Purpose Code	Purpose Description
8.2.1.1	Author's signature
8.2.1.2	Coauthor's signature
8.2.1.3	Co-participant's signature
8.2.1.4	Transcriptionist/Recorder signature
8.2.1.5	Verification signature
8.2.1.6	Validation signature
8.2.1.7	Consent signature
8.2.1.8	Witness signature
8.2.1.9	Event witness signature
8.2.1.10	Identity witness signature
8.2.1.11	Consent witness signature
8.2.1.12	Interpreter signature
8.2.1.13	Review signature
8.2.1.14	Source signature
8.2.1.15	Addendum signature
8.2.1.16	Administrative signature
8.2.1.17	Timestamp signature
8.2.1.18	Other

¹³ This document contains content reprinted, with permission, from E1762-95 Standard Guide for Electronic Authentication of Health Care Information, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM International, www.astm.org.

11 APPENDIX F: GLOSSARY

Table 11-1. Glossary	
Term	Definition
CDA (Clinical Document Architecture)	(HL7). A document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients.
Certificate Authority	(NIST). An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certificate Policy	
Delegation of Rights	The ability to delegate rights or authority to another to act in a specific capacity on behalf of the grantor of the right.
Digest	The result of applying a hash function to a message. Also known as "hash value." A hash function is a function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions are specified in FIPS 180-3 and are designed to satisfy the following properties: (1) (One-way) it is computationally infeasible to find any input that maps to any new pre-specified output, and (2) (Collision resistant) it is computationally infeasible to find any two distinct inputs that map to the same output.
Digital Signature	(NIST). The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made. The use of the terms "Digital Signature", "Digitally Signed", "Signed" and other variations are used in the context as described in this document.
Electronic Health Record	Clinical information for a specific patient that is stored electronically within an EHR-S.
Electronic Health Record System (EHR-S)	This IG uses this term in the same context as stated in the "HL7 EHR System Functional Model White Paper" Section 4 Definitions (HL7 2004 www.hl7.org): "It is important to note that the DSTU does not attempt to establish another definition for EHR Systems, but chooses to utilize existing definitions that include the concept of EHR Systems as a system (at least one) or a system-of- systems that cooperatively meet the needs of the end user."
Entity	An "entity" is an organization or a person that fulfills a role, e.g., Signer, Payer, Provider.
Non-repudiation	(NIST). A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party. This service prevents an entity from successfully denying involvement in a previous action.
Registration Authority	(NIST). An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
SAML (Security Assertion Markup Language)	(OASIS). A standard which defines a framework for exchanging security information between online business partners.
Signer	The use of the term "Signer" indicates the entity that has applied a Digital Signature to a CDA document as described in this implementation guide. All other participants who may otherwise sign a document are out of scope.