Acknowledgements and Copyrights


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, the open standards consortium where the SAML specification is owned and developed. https://www.oasis-open.org/standards#samlv2.0
## TABLE OF CONTENTS

1 **INTRODUCTION** ................................................................................................................. 6  
1.1 PURPOSE .......................................................................................................................... 6  
1.2 AUDIENCE ...................................................................................................................... 7  
1.2.1 RELEVANT DOCUMENTATION ............................................................................. 7  
1.2.2 REQUISITE KNOWLEDGE .................................................................................... 7  
1.3 ORGANIZATION OF THIS GUIDE ................................................................................ 8  
1.3.1 CONVENTIONS ......................................................................................................... 8  
1.3.2 KEYWORDS ............................................................................................................... 8  
2 **USE CASE** ....................................................................................................................... 9  
2.1 ASSUMPTIONS ............................................................................................................... 9  
2.2 SCOPE ............................................................................................................................ 9  
2.2.1 IN-SCOPE ............................................................................................................... 9  
2.2.2 OUT OF SCOPE ....................................................................................................... 9  
2.3 ACTORS .......................................................................................................................... 9  
2.4 SCENARIO 1 – SIGNING A CDA DOCUMENT ............................................................... 10  
2.4.1 USER STORY .......................................................................................................... 10  
2.4.2 BASE FLOW ........................................................................................................... 12  
2.5 REQUIREMENTS ............................................................................................................ 13  
2.6 INFORMATION INTERCHANGE REQUIREMENTS ...................................................... 13  
2.7 SYSTEM REQUIREMENTS ............................................................................................. 13  
3 **DIGITAL SIGNATURE PROCESSES** ........................................................................... 15  
3.1 CREATING A DIGITAL SIGNATURE ............................................................................. 15  
3.1.1 DIGITAL SIGNATURE STANDARD ...................................................................... 15  
3.1.2 COMPUTATION OF THE DIGEST ......................................................................... 15  
3.1.3 SIGNATURE PROCESS ............................................................................................. 16  
3.2 CREATING A DELEGATION OF RIGHTS ...................................................................... 16  
3.2.1 OVERVIEW OF THE DELEGATION OF RIGHTS PROCESS ................................ 17  
3.2.2 PRE-CONDITIONS ................................................................................................... 18  
3.2.3 DELEGATION OF RIGHTS STANDARDS ............................................................... 18  
3.2.4 CREATING A SAML-BASED DELEGATION OF RIGHTS ASSERTION ............... 19  
3.2.5 CREATING A DELEGATION OF RIGHTS ARTIFACT ........................................ 20  
3.2.6 VALIDATING THE DELEGATION OF RIGHTS ARTIFACT ..................................... 20  
3.3 INCORPORATING DIGITAL SIGNATURE AND DELEGATION OF RIGHTS ARTIFACTS INTO A CDA DOCUMENT .................................. 20  
3.3.1 SPECIFICATIONS FOR THE ED DATA TYPE ..................................................... 21  
3.4 VERIFYING AN XAdES-BASED SIGNATURE ............................................................... 22  
3.4.1 VERIFYING THE SIGNERS SIGNATURE ................................................................. 22
# TABLE OF CONTENTS

3.4.2 VERIFYING THE VALIDATION SIGNATURE ................................................................................. 23
3.4.3 VERIFYING THE DELEGATION OF RIGHTS ARTIFACT ................................................................. 23

4 DATA REQUIREMENTS .......................................................................................................................... 24
  4.1 SIGNING CERTIFICATE INFORMATION ......................................................................................... 24
  4.2 DOCUMENT SIGNATURE (XAdES-X-L ELEMENTS) ..................................................................... 24
  4.3 DELEGATION OF RIGHTS ASSERTION ......................................................................................... 34
  4.4 VALIDATED DELEGATION OF RIGHTS ASSERTION ................................................................. 35
  4.5 CODE SETS .................................................................................................................................. 36

5 APPENDIX A: EXAMPLE ....................................................................................................................... 37
  5.1 XAdES-X-L DIGITAL SIGNATURE ................................................................................................. 37
  5.2 SAML DELEGATION OF RIGHTS ASSERTION ............................................................................ 40
  5.3 XAdES-X-L DIGITAL SIGNATURE APPLIED TO SAML DELEGATION OF RIGHTS .................... 43

6 APPENDIX B: GLOSSARY ..................................................................................................................... 45
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE 2-1</td>
<td>INFORMATION INTERCHANGE REQUIREMENTS</td>
<td>12</td>
</tr>
<tr>
<td>TABLE 2-2</td>
<td>INFORMATION INTERCHANGE REQUIREMENTS</td>
<td>13</td>
</tr>
<tr>
<td>TABLE 2-3</td>
<td>SYSTEM REQUIREMENTS</td>
<td>13</td>
</tr>
<tr>
<td>TABLE 4-1</td>
<td>SIGNING CERTIFICATE INFORMATION</td>
<td>24</td>
</tr>
<tr>
<td>TABLE 4-2</td>
<td>DOCUMENT SIGNATURE</td>
<td>24</td>
</tr>
<tr>
<td>TABLE 4-3</td>
<td>DELEGATION OF RIGHTS ASSERTION</td>
<td>34</td>
</tr>
<tr>
<td>TABLE 4-4</td>
<td>VALIDATED DELEGATION OF RIGHTS ASSERTION</td>
<td>35</td>
</tr>
<tr>
<td>TABLE 4-5</td>
<td>CODE SETS</td>
<td>36</td>
</tr>
<tr>
<td>TABLE 6-1</td>
<td>GLOSSARY</td>
<td>45</td>
</tr>
</tbody>
</table>

# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIGURE 2-1</td>
<td>ACTIVITY DIAGRAM</td>
<td>11</td>
</tr>
<tr>
<td>FIGURE 3-1</td>
<td>DELEGATION OF RIGHTS PROCESS</td>
<td>18</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

The HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1 is a collaboration between HL7 and the Centers for Medicare & Medicaid Services (CMS) Electronic Submission of Medical Documentation (esMD) Initiative. This implementation guide defines a means to attach digital signatures to a CDA document, as well as provide a method of specifying delegation of right assertions.

The esMD Initiative provides solutions that address gaps identified by CMS when requesting and receiving medical documentation for administrative purposes. Through the participation of additional stakeholders, the outputs of the initiative have expanded to reflect the requirements of other payers, providers, and stakeholders. The esMD Initiative focuses on identifying the requirements, core data sets, and standards to support specific use cases, including the application of digital signatures on CDA documents.

This implementation guide will allow CMS, other health plans, payers, and providers to accurately authenticate the signer(s) of CDA documents and trust the validity and authenticity of signed medical documentation. Examples in this guide focus on the use of digitally-signed documents and delegation of right assertions within a CDA document for administrative purposes. However, the use of signed documents and delegation of right assertions is not limited to administrative use cases, thus, the processes in this guide are meant to be applicable to other uses.

This IG relies on the definition and constraints of the sdct:signatureText element as defined in the HL7 Implementation Guide for CDA Release 2: IHE Health Story Consolidation, Release 2 – US Realm.

1.1 Purpose

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

- Provide a non-repudiation signature that attests to the role and signature purpose of each signer of the document.
- Provide a non-repudiation signature that attests to the role and signature purpose of each contributor to the document in support of administrative requirements.
- Provide delegation of rights where the signer is not the responsible individual or organization (e.g., the signer is acting as an authorized agent).
- Provide a medical/legal attestation for the purpose of documenting transfer of clinical care (e.g. the Longitudinal Coordination of Care initiative)\(^1\)

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

\(^1\) [http://wiki.siframework.org/Longitudinal+Coordination+of+Care+LCC]
• Identify a digital signature standard for:
  o The public certificate of the signer
  o 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:
  o The certificate ID of both parties
  o The purpose of the delegation
  o 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 also presented in this guide.

1.2 Audience
This guide is intended to assist analysts, developers, providers, agents, payers, review contractors, and any other health care organization that require guidance on the application of digital signatures to a CDA document.

The intended audiences for this guide are:

• Providers and payers that wish to apply digital signatures to 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 RELEVANT DOCUMENTATION
This guide is not intended to compete with any other HL7 implementation guide for Digital Signatures. This guide is specific to Digital Signatures embedded in a CDA.

1.2.2 REQUISITE KNOWLEDGE

• OASIS Security Assertion Markup Language (SAML), [https://www.oasis-open.org/standards#samlv2.0](https://www.oasis-open.org/standards#samlv2.0), used in this guide to convey the delegation of rights assertion.

---

2 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).
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 “sdtc:”, “ds:”, or “saml:” are elements from the XAdES specification.

1.3.2 KEYWORDS

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119\(^3\). The following definitions are excerpted from the RFC:

**MUST** or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

**MUST NOT** or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

**SHOULD** or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

**SHOULD NOT** or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

**MAY** or the adjective "OPTIONAL", mean that an item is truly optional. One software supplier may choose to include the item to enable certain capabilities while another software supplier may omit the same item. In either case, the communication partner cannot be expected to either provide it (sender) or process it (receiver) without clear and voluntary agreement between the partners.

An implementation which does not include items marked as optional **MUST** be prepared to interoperate with another implementation which does include the optional item, but is not obligated to support the optional item. In the same vein an implementation that includes a particular item marked as optional **MUST** be prepared to interoperate with other implementations which do not support the optional item.

\(^3\) [http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
2 USE CASE
The use case covered by this IG is the application of one or more Digital Signature(s) to a CDA by a provider to satisfy administrative requirements.

2.1 Assumptions
- All Payers and Providers have obtained a digital identity from a recognized Certificate Authority (CA).
- 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 to a CDA document by a Provider (or on behalf of a provider) for submission to a Payer for administrative purposes. This IG is intended to provide a standard for the use of Digital Signatures for Health Plans and Payers to receive the required authentication on medical documentation in support of administrative requirements.

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 signer and the authorized individual.
- Creation of the digital signature artifact and the delegation of rights assertion by the signer
- 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 an RA or a CA.
- A definition of electronic transactions between a Provider and an 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.
- Signature by a patient or their authorized representative.

2.3 Actors
There are three actors that have responsibilities related to the conformance requirements defined in this document:
• Provider – An entity (legalAuthenticator or authenticator) that affixes a Digital Signature to a CDA document
• Delegatee – A Signer that with delegated authority from a Provider
• Payer – Verifies that the Signature and, where appropriate Delegation of Rights artifacts are valid

2.4 Scenario 1 – Signing a CDA Document
A Provider or its delegated agent must attest to actions taken (e.g. creation, modification, review) with respect to a specific CDA document at the time the action is taken/completed. 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 Provider or its delegated agent has a need to send the Signed CDA document to a third.

2.4.1 USER STORY
In order to participate in digital signing, the Provider and any delegated agent must obtain and maintain a non-repudiation digital identity. Both actors initiate the process to obtain an X.509v3 digital signing certificate.\(^4\) Entities approved by a Registration Authority will receive Credentials from a Certificate Authority to incorporate into their business process.

If required, the Provider creates and digitally signs a Delegation of Rights assertion to permit a delegated agent to sign a CDA document on their behalf. It is the responsibility of the Delegatee to ensure that the Delegation of Rights is validated prior to incorporating the Delegation of Rights artifacts in the CDA. When a Provider or their delegated agent completes an attestable action with respect to a CDA document, the Provider or delegated agent will create a digital signature artifact attesting to the date/time, action taken by encrypting a Digest of the CDA document, the date/time, and action code with the private key of signing digital certificate.

The Provider, who has satisfied any payer registration that may be required for a specific exchange of documentation with a payer, sends (directly or through a delegated agent) the digitally signed CDA document in a secure transaction to the payer using appropriate transmission methods. Upon receiving the digitally signed CDA document, the Payer validates the following: each Digital Certificate and its chain to the appropriate Certificate Policy (CP), delegation of rights artifacts, where required, and digital signature artifact. Additionally, the Payer decrypts the Digest (hash) of the CDA document and validates data integrity of the CDA document received.

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.

\(^4\) In the United States, the X.509v3 digital signing certificate must come from a Federal Bridge cross-certified Certificate Authority.
Delegatee Payer Provider

B1. Provider completes action on a document and digitally signs document

O2. Delegatee completes action on document on behalf of Provider and digitally signs document and requests validated Delegation of Rights


O4. Delegatee attaches validated Delegation of Rights Assertion to signed document

O5. Delegatee sends signed document and signed Delegation of Rights Assertion to Payer

B2. Provider sends signed document to Payer

O3. Provider system validates and signs Delegation of Rights Assertion and makes available to Delegatee

Notes:
- The following are alternative paths (B1+B2+B3, and O1+O2+O3+O4+O5)
- Activities related to Delegatee (O1, O2, O3, O4, and O5) occur only if there is a need for a Delegation of Rights

### 2.4.2 BASE FLOW

The Base Flow presents the step by step process of the information exchange depicted in the activity diagram (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 Provider or Delegatee that must attest to the contents of an individual CDA

<table>
<thead>
<tr>
<th>Step</th>
<th>Actor</th>
<th>Role</th>
<th>Event/Description</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>O1</td>
<td>Provider</td>
<td>Delegation of Rights Creator</td>
<td>Provider creates and signs Delegation of Rights Assertion</td>
<td>Provider and Delegatee Digital Certificate Information</td>
<td>Delegation of Rights Assertion available</td>
</tr>
<tr>
<td>B1</td>
<td>Provider</td>
<td>Attests to action on Document</td>
<td>Provider completes action on a Document and applies a non-repudiation digital signature attesting to the action</td>
<td>Document</td>
<td>Digitally Signed Document and Signature Artifact</td>
</tr>
<tr>
<td>O2</td>
<td>Delegatee</td>
<td>Attests to action on Document</td>
<td>Delegatee completes action on a Document and applies a non-repudiation digital signature attesting to the action and requests validated Delegation of Rights Assertion</td>
<td>Document</td>
<td>Digitally Signed Document and Signature Artifact and request for validated Delegation of Rights Assertion</td>
</tr>
<tr>
<td>O3</td>
<td>Provider</td>
<td>Delegation of Rights Validator</td>
<td>Provider system validates and signs Delegation of Rights Assertion</td>
<td>Delegatee request for a validated Delegation of Rights Assertion</td>
<td>Validated Delegation of Rights Assertion</td>
</tr>
<tr>
<td>O4</td>
<td>Delegatee</td>
<td>Applying Delegation of Rights Assertion</td>
<td>Delegatee associates the validated Delegation of Rights Assertion with the signed document</td>
<td>Validated Delegation of Rights Assertion</td>
<td>Digitally Signed Document Signature Artifact and the validated Delegation of Rights Assertion</td>
</tr>
<tr>
<td>B2</td>
<td>Provider</td>
<td>Document Sender</td>
<td>Provider sends signed Document and Signature Artifacts to Payer</td>
<td>Digitally Signed Document and Signature Artifact</td>
<td>Digitally Signed Document and Signature Artifact</td>
</tr>
</tbody>
</table>
### 2.5 Requirements

- Documentation of services that have been delivered are digitally signed with the date/time, role and action (e.g., creation, review, etc.) at the time the action is performed or, at a minimum, prior to the time required by the relative administrative use. The specific policies for Payers should be followed for services covered by each Payer.

### 2.6 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 2-1. Information Interchange Requirements

<table>
<thead>
<tr>
<th>Step</th>
<th>Actor</th>
<th>Role</th>
<th>Event/Description</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>B3</td>
<td>Payer</td>
<td>Receiver and validator of Document</td>
<td>Payer receives Document, authenticates Signature Artifacts, where appropriate any Delegation of Rights Assertions, and validates data integrity of submission from the Provider or Delegatee</td>
<td>Digitally Signed Document and Signature Artifact, and, where appropriate, Delegation of Rights Assertion</td>
<td>Success or failure of Signature Artifact validation, Delegation of Rights Artifacts validation, and Data integrity authentication</td>
</tr>
</tbody>
</table>

#### Table 2-2. Information Interchange Requirements

<table>
<thead>
<tr>
<th>Initiating System</th>
<th>Action</th>
<th>Information Interchange Requirement Name</th>
<th>Action</th>
<th>Receiving System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Information System</td>
<td>Send</td>
<td>Link for Delegation of Rights Assertion</td>
<td>Receive</td>
<td>Delegatee Information System</td>
</tr>
<tr>
<td>Delegatee Information System</td>
<td>Send</td>
<td>Request for validated Delegation of Rights Assertion</td>
<td>Receive</td>
<td>Provider Information System</td>
</tr>
<tr>
<td>Provider Information System</td>
<td>Send</td>
<td>Validated Delegation of Rights Assertion</td>
<td>Receive</td>
<td>Delegatee Information System</td>
</tr>
<tr>
<td>Provider Information System</td>
<td>Send</td>
<td>Document and Signature Artifact</td>
<td>Receive</td>
<td>Payer Information System</td>
</tr>
<tr>
<td>Delegatee Information System</td>
<td>Send</td>
<td>Document, Signature Artifact, validated Delegation of Rights Assertion</td>
<td>Receive</td>
<td>Payer Information System</td>
</tr>
</tbody>
</table>

#### Table 2-3. System Requirements

<table>
<thead>
<tr>
<th>System</th>
<th>System Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payer Information System</td>
<td>Verify Delegation of Rights (if any), digital signatures, traceability to registered provider, and validates integrity of Document</td>
</tr>
<tr>
<td>Provider Information System</td>
<td>Incorporate signing Digital Certificate Create Delegation of Rights if required Respond to request to Validate Delegation of Rights Assertion Performs actions on a Document (create, modify, read) Apply non-repudiation Digital Signature to Delegation of Rights Assertion, and Documents and creates Signature Artifacts</td>
</tr>
</tbody>
</table>
### Table 2-3. System Requirements

<table>
<thead>
<tr>
<th>System</th>
<th>System Requirement</th>
</tr>
</thead>
</table>
| Delegatee Information System (usually the same as Provider Information System) | Incorporate signing Digital Certificate  
Request Validated Delegation of Rights  
Performs 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:

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

Notes:

1. This process requires the use of the sdtec:signatureText element as described in the “HL7 Implementation Guide for CDA Release 2: IHE Health Story Consolidation, Release 1.X – US Realm”. The full set of constraints for this element is described there and is not replicated here. The sdtec:signatureText data element is available on the legalAuthenticator and authenticator data elements; all constraints for those elements must be met for the application of the Digital Signature to be valid.

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 from the calculation of the Digest, the subsequent addition of the digital signature artifact, and any required updates to the associated participant occurrence will not alter the Digest value signed by a prior Digital Signature. This method provides for single, multiple, and co-signatures on the CDA. However, it does not make explicit provision for digital counter signatures of legalAuthenticator and authenticator occurrences except where the counter signatures are included in the optional counterSignature element in the respective XAdES.

3. The UTC incorporated in each Digital Signature will permit the signature verifier 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

When digitally signing a CDA document, the Digest of the Signed Data Object is the entire document contents starting with, and including, <ClinicalDocument> and ending with, and including, </ClinicalDocument>, 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.

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 3.1.2 and the SignedProperties)
3. The Signed Digest
4. The following signed elements:
   a. Coordinated Universal Time (UTC)
   b. Role (see Table 4.5)
   c. Signature Purpose (see Table 4.5)
5. A signed OCSP or CRL in the RevocationValues element

Conformance Statements: XAdES-X-L
ESMD-1: XAdES-X-L digital signatures SHALL include the 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 valid Role
ESMD-4: XAdES-X-L digital signatures SHALL include a valid Signature Purpose
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

3.2 Creating a Delegation of Rights
The Delegation of Rights process enables an individual or organization to assign a right to another party to act on their behalf. The process presented here is meant to be broadly applicable to any situation in which a right must be delegated to another party digitally. In order to clearly exhibit the use of a Delegation of Rights Artifact back to the Digital Signature Process detailed in Section 3.1 of this guide, the examples below focus on the signing of a CDA document.5

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

- A Delegator is the individual or organization that assigns the right.
- A Delegatee is the individual or organization that receives the right.
- A Delegation Agent is a third party trusted by the Delegator to confirm that an existing delegation of rights is still valid.

In the context of this implementation guidance, these actors might be:

5 The appropriate object must be signed by the Delegatee as their signature proves that they are the subject of the Delegation of Rights Assertion.
• Delegator – Provider responsible for medical documentation
• Delegatee – The proxy that is authorized to sign on the delegator’s behalf
• Delegation Validator – Service that verifies the Delegation of Rights Artifact is valid.

Additionally, the following terms are defined:

• A “Delegation of Rights Assertion” is an assertion created by the Delegator prior to being signed
• A “Delegation of Rights Artifact” is an assertion created and digitally signed by the Delegator
• A “Validated Delegation of Rights” artifact includes the Digital Signature of the Delegation Agent 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 Delegator issues a Delegation of Rights Artifact to the Delegatee (Section 3.2.3)
2. When creating a Digital Signature, the Delegatee requests a Validated Delegation of Rights Artifact from the Delegation Agent.
3. Assuming the DoR is still valid, the Delegation Agent issues a Validated Delegation of Rights Artifact (Section 3.xx)
4. The Delegatee/AoR Signer signs a CDA document on behalf of the Delegator (Section 3.1.3) and includes the Validated Delegation of Rights.
### 3.2.2 PRE-CONDITIONS

- Delegator, Delegatee, and Delegation Agent have obtained X.509v3 digital certificates in compliance with industry-accepted requirements.
- Delegator, Delegatee, and Delegation Agent support the required standards for the delegation of rights.

### 3.2.3 DELEGATION OF RIGHTS STANDARDS

This guide establishes use of the OASIS Security Assertion Markup Language (SAML) V2.0 standard to support Delegation of Rights. OASIS SAML specifies a data format for exchanging authentication and authorization data between parties.

SAML specifies the use of the XML Digital Signature (XML-DSIG) standard to sign SAML assertions. For delegation of rights requiring long term validation, this guide establishes 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 Agent Signature.

<table>
<thead>
<tr>
<th>Name of Specification</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>OASIS SAML</td>
<td>Delegation of Rights Assertion</td>
</tr>
</tbody>
</table>
The Delegation of Rights Artifact is meant to prove that a Delegatee is authorized to sign a CDA document on behalf of the individual or organization responsible for that document.

The Delegator (e.g. Provider, Provider Organization, or a trusted third party delegated to act on their behalf) shall create and deliver a signed SAML assertion to the Delegatee. The Delegatee shall act as the Signer and digitally sign a CDA document.

OASIS defines a number of specifications to support the exchange of SAML assertions; however, delivery of the SAML 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) V2.0”.

The following constraints apply to a Delegation of Rights Artifact:

1. The Subject of the assertion must be included and must be the Delegatee
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 that will be used to verify the Signature on the document bundle (i.e., the public certificate of the Delegatee/Signer)
6. The SAML assertion must be signed by the Delegator
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 assertion (i.e., the public certificate of the Delegator)

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

- 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.

---

* [http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)*
3.2.5 CREATING A DELEGATION OF RIGHTS ARTIFACT

The following steps must be taken for a Delegator to issue a Delegation of Rights Artifact to a Delegatee:

1. Delegator creates Delegation of Rights Assertion that includes the following:
   a. Issuer/ID of Delegatee X.509v3 signing certificate
   b. Issuer/ID of Delegator X.509v3 signing certificate
   c. Start and End date of assertion
   d. Right(s) that is/are delegated

2. Delegator signs the Delegation of Rights assertion using the XAdES-X-L standard syntax without populating the RevocationValues element

3. The resultant signed Delegation of Rights Assertion is the Delegation of Rights Artifact

3.2.6 VALIDATING THE DELEGATION OF RIGHTS ARTIFACT

Once a Delegator provides a Delegation of Rights Artifact to a Delegatee, there is no method to revoke that right prior to its expiration date. This presents a security risk whereby a malicious user can hijack assertions. To insure that a Delegation of Rights Artifact is valid at the time of signature, a Delegatee must take the following steps immediately prior to using a Delegation of Rights Artifact:

1. Signer sends Delegation of Rights Artifact to the Delegation Agent Server/Service
2. Delegation Agent Server/Service performs the following actions:
   a. Verifies that the Delegation of Rights Assertion has not been revoked
   b. Verifies that the Delegatee X.509v3 signing certificate is still valid and not revoked
   c. Populates the Delegation of Rights Artifact XAdES-X-L Revocation Values with the current OCSP or signed CRL
   d. 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. Delegatee provides Delegation of Rights Artifact to Delegation Agent
5. Delegation Agent confirms all limitations within the Delegation of Rights Assertion are met, including subject of assertion, dates of use, and purpose of use
6. Delegation Agent verifies the signature of the Delegation of Rights Artifact
7. Delegation Agent confirms trust relationship exists with Delegator
8. Delegation Agent signs Delegation of Rights Artifact to create a Delegation Agent Signature
9. Delegation Agent returns the Validated (Signed) Delegation of Rights Artifact to the Delegatee
10. Delegatee includes the Validated Delegation of Rights Artifact as part of the Delegatee’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 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 represents the digital signature by reference to a signature data block (i.e., the XAdES-X-L elements) within the CDA header.

---

7 as defined in the HL7 Implementation Guide for CDA Release 2: IHE Health Story Consolidation, Release 2 – US Realm
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 Signer acted when creating the digital signature. By excluding `legalAuthenticator` and `authenticator` from the calculation of the Digest, the subsequent addition of the digital signature artifact, and any required updates to these participant occurrences will not alter the Digest (hash) value signed by a prior digital signature.

If a Delegation of Rights is required, the Validated Delegation of Rights Artifact is inserted immediately behind the Digital Signature artifact in the same `sdtc:signatureText` element.

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

1. For a signature with no delegation of rights: `[XAdES-X-L]` for the Signer
2. For a signature with a delegation of rights: `[XAdES-X-L] [XAdES-X-L] [XAdES-X-L] [SAML]` where the first `[XAdES]` in the signers signature, the second is the Delegation Agents signature to validate the Delegation of Rights Artifact, the third is the Delegator signature on the SAML assertion, and finally, the SAML assertion that contains the Delegation of Rights.

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 3.3.1)
2) The signers Digital Signature `[XAdES-X-L]`
3) In addition the signer may have a delegated right to sign on behalf of another individual or organization. The Validated Delegation of Right Artifact `[XAdES-X-L] [XAdES-X-L] [SAML2.0]` is included immediately following the Digital Signature.

### 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”

The `thumbnail` is used provide a human readable version of the digital signature:

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

The `thumbnail` SHOULD contain the following elements:

1. “Digitally Signed by”
2. Signers name
3. Date and time of signature
4. Role
5. Purpose
6. Optionally (if there is a Delegation of Rights):
   a. “Delegate right to sign by”
b. Name of the right delegator

Example:
Digitally signed by John Doe on 4/21/2013 at 15:30 EDT as Physician for the purpose of Author.

Conformance Statements: sdtc:signatureText

ESMD-7: sdtc:signatureText SHALL contain one [XAdES-X-L] for the signer
ESMD-8: sdtc:signatureText MAY contain one Delegation of Rights
Validation signature
ESMD-10: sdtc:signatureText Delegation of Rights SHALL contain one [XAdES-X-L]
signature on the Delegation of Rights Assertion
ESMD-11: sdtc:signatureText Delegation of Rights SHALL contain one [SAML 2.0] n
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 contain the following elements described in 3.3.1

3.4 Verifying an XAdES-based Signature

A Signature Verifier is the receiver of the CDA document and must verify the signature using the
following steps to verify the identity of the Signer and the integrity of the CDA document.

3.4.1 VERIFYING THE SIGNERS SIGNATURE

1. Verify the X.509v3 Certificate contained in the X509Certificate element. Specifically,
   verify that:
   a. The certificate is current
   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 certificate has not been revoked by reviewing the OCSP response or signed CRL
      included in the XAdES-X-L RevocationValues element.
2. Verify the signature contained in the sdtc:signatureText element.
3. Verify that the signature date is appropriate.
4. Verify that the signature purpose is appropriate.
5. Decrypt the signed Digest with the public key from the X.509v3 public digital certificate.

---

8 Verification of the signature of a Delegation of Rights Artifact is identical (see Section 3.2).
7. Verify that the signed Digest matches the computed Digest.
If any of these steps fail, the Signature cannot be verified.

### 3.4.2 VERIFYING THE VALIDATION SIGNATURE

If a Delegation requires and receives a Delegation Agent Signature, they should complete the following steps to verify the validity of the Delegation of Rights Artifact:

1. Verify the Delegation Agent Signature
2. Verify that the SigningTime element falls within appropriate time frame as defined by Delegation Verifier policies.

If any of these steps fail, the Delegation Agent Signature cannot be verified. If these steps are successful, the validity of the Delegation of Rights Artifact has been confirmed and the Verifier should proceed to verify the SAML-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 Signer has the right to sign the CDA document on behalf of the Delegator:

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
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 Delegator)
3. Confirm trust in the entity that signed the assertion (i.e., the Delegator)
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 Delegatee/Signer)

If any of these steps fail, 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.

4.1 Signing Certificate Information

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

4.2 Document Signature (XAdES-X-L Elements)

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>O</td>
<td>[0..1]</td>
<td>Root element of an XML digital signature</td>
<td></td>
</tr>
<tr>
<td>SignedInfo</td>
<td>R</td>
<td>[1..1]</td>
<td>Used to specify the canonicalization algorithm, a signature algorithm, and</td>
<td>May also contain an optional ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>one or more references</td>
<td>attribute that will allow it to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>be referenced by other signatures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and objects.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CanonicalizationMethod</td>
<td>R</td>
<td>[1..1]</td>
<td>Specifies the canonicalization algorithm applied to the SignedInfo element prior to performing signature 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).</td>
<td>When not present, the standard canonicalization method as specified by XML-DSIG MUST be used.</td>
</tr>
<tr>
<td>SignatureMethod</td>
<td>R</td>
<td>[1..1]</td>
<td>Specifies the algorithm used for digital signature generation and validation.</td>
<td>This algorithm identifies all cryptographic functions involved in the signature operation (e.g. hashing, public key algorithms, MACs, padding, etc.).</td>
</tr>
<tr>
<td>Reference</td>
<td>RE</td>
<td>[0..*]</td>
<td>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.</td>
<td>The Type attribute facilitates the processing of referenced data. An optional ID attribute permits a Reference to be referenced from elsewhere.</td>
</tr>
<tr>
<td>Transforms</td>
<td>RE</td>
<td>[0..1]</td>
<td>Contains an ordered list of Transform elements.</td>
<td></td>
</tr>
<tr>
<td>Transform</td>
<td>R</td>
<td>[1..*]</td>
<td>Describes how the signer obtained the data object that was digested. The output of each Transform serves as input to the next Transform. The input to the first Transform is the result of dereferencing the URI attribute of the Reference element. The output from the last Transform is the input for the DigestMethod algorithm.</td>
<td>If the Transforms element is used, at least one Transform element must be used. When transforms are applied the signer is not signing the native (original) document but the resulting (transformed) document is signed.</td>
</tr>
<tr>
<td>DigestMethod</td>
<td>R</td>
<td>[1..1]</td>
<td>Identifies the digest algorithm to be applied to the signed object</td>
<td></td>
</tr>
<tr>
<td>DigestValue</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains the base64 encoded value of the digest</td>
<td></td>
</tr>
<tr>
<td>SignatureValue</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains the actual base64 encoded value of the digital signature</td>
<td></td>
</tr>
<tr>
<td>KeyInfo</td>
<td>RE</td>
<td>[0..1]</td>
<td>Contains public key information for validating signatures. May contain keys, names, certificates, and other PKI management information.</td>
<td>If KeyInfo is omitted, the recipient is expected to be able to identify the key based on application context.</td>
</tr>
<tr>
<td>KeyName</td>
<td>O</td>
<td>[0..1]</td>
<td>Contains a string value which may be used by the signer to communicate a key identifier to the recipient.</td>
<td>The name of the digital signer is required, but it is not required that KeyName be used.</td>
</tr>
<tr>
<td>Data Element</td>
<td>Usage</td>
<td>Cardinality</td>
<td>Data Element Description</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KeyValue</td>
<td>O</td>
<td>[0..1]</td>
<td>Contains a single public key that may be useful in validating the signature</td>
<td>Must contain exactly one of any of the following elements: 1. DSAKeyValue 2. RSAKeyValue 3. Externally-defined public keys values represented as PCDATA or element types from an external namespace</td>
</tr>
<tr>
<td>RetrievalMethod</td>
<td>O</td>
<td>[0..1]</td>
<td>Conveys a reference to KeyInfo 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 KeyInfo can reference this chain using a single RetrievalMethod element instead of including the entire chain with a sequence of X509Certificate elements.</td>
<td></td>
</tr>
<tr>
<td>X509Data</td>
<td>R</td>
<td>[1..1]</td>
<td>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: X509IssuerSerial, X509SK1, X509SubjectName, X509Certificate, X509CRL</td>
<td>Any X509IssuerSerial, X509SK1, and X509SubjectName elements that appear MUST refer to the certificate or certificates containing the validation key.</td>
</tr>
<tr>
<td>Object</td>
<td>R</td>
<td>[1..*]</td>
<td>Parent element to all XAdES extension elements, which are added on to the base XMLDSIG core element (detailed in the rows above).</td>
<td>While the Object element may be repeated for purposes other than XAdES, such use is out of scope for this guide.</td>
</tr>
<tr>
<td>QualifyingProperties</td>
<td>R</td>
<td>[1..1]</td>
<td>Acts as a container element for all the qualifying information that should be added to an XML signature. QualifyingProperties are split into properties that are cryptographically bound to (i.e. signed by) the XML signature (SignedProperties), and properties that are not cryptographically bound to the XML signature (UnsignedProperties).</td>
<td>The SignedProperties MUST be covered by a ds:Reference element of the XML signature.</td>
</tr>
<tr>
<td>SignedProperties</td>
<td>R</td>
<td>[1..1]</td>
<td>Properties that are cryptographically bound (i.e., signed) to the XML signature</td>
<td></td>
</tr>
<tr>
<td>SignedSignatureProperties</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains properties that qualify the XML signature that has been specified with the Target attribute of the QualifyingProperties container element.</td>
<td>The optional Id attribute can be used to make a reference to the UnsignedProperties element.</td>
</tr>
</tbody>
</table>
Table 4-2. Document Signature

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SigningTime</td>
<td>R</td>
<td>[1..1]</td>
<td>Specifies the time at which the signer (purportedly) performed the digital signature process.</td>
<td>This element is optional within the XAdES specification, but required for the purposes of this guide.</td>
</tr>
<tr>
<td>SigningCertificate</td>
<td>R</td>
<td>[1..1]</td>
<td>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.</td>
<td>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 Cert elements CertDigest and IssuerSerial (listed below).</td>
</tr>
<tr>
<td>CertDigest</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains the digest of one of the certificates referenced in the sequence. It contains two elements: ds:DigestMethod indicates the digest algorithm, and ds:DigestValue contains the value of the digest.</td>
<td>The optional URI attribute serves to indicate where the referenced certificate can be found.</td>
</tr>
<tr>
<td>IssuerSerial</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains the identifier of one of the certificates referenced in the sequence. Should the ds:X509IssuerSerial element appear in the signature to denote the same certificate, its value MUST be consistent with the corresponding IssuerSerial element.</td>
<td></td>
</tr>
<tr>
<td>SignaturePolicyIdentifier</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains elements that specify ways to identify the set of rules governing the creation and validation of the digital signature.</td>
<td>Must contain exactly one of the following: SignaturePolicyID or SignaturePolicyImplied</td>
</tr>
<tr>
<td>SignaturePolicyID</td>
<td>RE</td>
<td>[0..1]</td>
<td>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.</td>
<td>The SigPolicyId element contains an identifier that uniquely identifies a specific version of the signature policy. The SigPolicyHash element contains the identifier of the hash algorithm and the hash value of the signature policy. The SigPolicyQualifier element can contain additional information qualifying the signature policy identifier.</td>
</tr>
<tr>
<td>Data Element</td>
<td>Usage</td>
<td>Cardinality</td>
<td>Data Element Description</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SignaturePolicyImplied</td>
<td>O</td>
<td>[0..1]</td>
<td>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 the identifier and hash value.</td>
<td></td>
</tr>
<tr>
<td>SignatureProductionPlace</td>
<td>O</td>
<td>[0..1]</td>
<td>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.</td>
<td>Must contain no more than one of each of the following elements: City, StateorProvince, PostalCode, CountryName.</td>
</tr>
<tr>
<td>SignerRole</td>
<td>R</td>
<td>[1..1]</td>
<td>Property that contains a sequence of roles that the signer can play.</td>
<td>This element is optional within the XAdES specification, but required for the purposes of this guide. It must contain at least one of the two elements: ClaimedRoles,CertifiedRoles.</td>
</tr>
<tr>
<td>ClaimedRoles</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains a sequence of roles (using ClaimedRole 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.</td>
<td>From Healthcare Taxonomy Data Set</td>
</tr>
<tr>
<td>CertifiedRoles</td>
<td>O</td>
<td>[0..1]</td>
<td>Contains one or more wrapped DER-encoded attribute certificates for the signer (using CertifiedRole elements).</td>
<td></td>
</tr>
<tr>
<td>SignaturePurpose</td>
<td>R</td>
<td>[1..1]</td>
<td>Contains a signature purpose claimed by the signer.</td>
<td>From ASTM E 1762-95</td>
</tr>
<tr>
<td>SignedDataObjectProperties</td>
<td>O</td>
<td>[0..1]</td>
<td>Contains properties that qualify some of the signed data objects.</td>
<td>May include any of the following elements: DataObjectFormat, CommitmentTypeIndication, AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp</td>
</tr>
</tbody>
</table>
### Table 4-2. Document Signature

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataObjectFormat</td>
<td>O</td>
<td>[0..*]</td>
<td>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 ObjectReference attribute, which must reference the ds:Reference element of the ds:Signature corresponding with the data object qualified by this property.</td>
<td>If used, this element must include at least one of any the following elements: Description, ObjectIdentifier, MineType, Encoding. These properties may not be repeated within the DataObjectFormat element.</td>
</tr>
<tr>
<td>CommitmentTypeIndication</td>
<td>O</td>
<td>[0..*]</td>
<td>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.</td>
<td>Must contain exactly one CommitmentTypeId element. Must contain either AllSignedDataObjects element, or ObjectReference element(s). May contain CommitmentTypeQualifiers element.</td>
</tr>
<tr>
<td>CommitmentTypeId</td>
<td>O</td>
<td>[0..1]</td>
<td>Uniquely identifies the type of commitment made by the signer. Required if CommitmentTypeIndication element is used.</td>
<td>Must include exactly one Identifier element (which indicates URI of commitment). May include no more than one of each of the following elements: Description and DocumentationReferences.</td>
</tr>
<tr>
<td>AllDataObjectsTimeStamp</td>
<td>O</td>
<td>[0..*]</td>
<td>Contains the time-stamp computed before the signature production, over the sequence formed by ALL the ds:Reference elements within the ds:SignedInfo referencing whatever the signer wants to sign except the SignedProperties element. The application MUST compose the Include elements to refer to all the ds:Reference elements except the one referencing the SignedProperties element. Their corresponding referencedData attribute MUST be present and set to &quot;true&quot;.</td>
<td>May contain more than one Include element. May contain no more than 1 CanonicalizationMethod elements. Must contain at least one of the following two elements: EncapsulatedTimeStamp or XMLTimeStamp.</td>
</tr>
<tr>
<td>Data Element</td>
<td>Usage</td>
<td>Cardinality</td>
<td>Data Element Description</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IndividualDataObjectsTimeStamp</td>
<td>O</td>
<td>[0,1]</td>
<td>Contains the time-stamp computed before the signature production, over a sequence formed by SOME ds:Reference elements within the ds:SignedInfo. Note that this sequence cannot contain a ds:Reference computed on the SignedProperties element. The application MUST compose the Include elements to refer to those ds:Reference elements that are to be time-stamped. Their corresponding referencedData attribute MUST be present and set to &quot;true&quot;.</td>
<td>May contain more than one Include element. May contain no more than 1 CanonicalizationMethod elements. Must contain at least one of the following two elements: EncapsulatedTimeStamp or XMLTimeStamp.</td>
</tr>
<tr>
<td>UnsignedProperties</td>
<td>R</td>
<td>[1,1]</td>
<td>Contains properties that are not bound/signed by the digital signature.</td>
<td>May contain at most one of each of the following elements: UnsignedSignatureProperties, UnsignedDataObjectProperties</td>
</tr>
<tr>
<td>UnsignedSignatureProperties</td>
<td>R</td>
<td>[1,1]</td>
<td>Contains properties that qualify the XML signature that has been specified with the Target attribute of the QualifyingProperties container element.</td>
<td>The optional Id attribute can be used to make a reference to the UnsignedProperties element.</td>
</tr>
<tr>
<td>CounterSignature</td>
<td>O</td>
<td>[0,1]</td>
<td>Provides support for multiple embedded signatures. Each counter-signature is carried in one CounterSignature element added to the Signature element to which the counter-signature is applied.</td>
<td>In a qualified Signature the contents of the CounterSignature element are one or more signatures (i.e. ds:Signature elements) of the SignatureValue in the qualified Signature. A counter-signature can itself be qualified by a CounterSignature property.</td>
</tr>
<tr>
<td>SignatureTimeStamp</td>
<td>O</td>
<td>[0,1]</td>
<td>A container for a time-stamp token over the ds:SignatureValue element to protect against repudiation in case of a key compromise.</td>
<td>The application MUST compose one Include element with an URI referencing the ds:SignatureValue element. The input for the time-stamp has is, in consequence, the ds:SignatureValue element.</td>
</tr>
<tr>
<td>CompleteCertificateRefs</td>
<td>R</td>
<td>[1,1]</td>
<td>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.</td>
<td>Must contain exactly one CertRefs element. The CertRef element must contain at least one Cert element.</td>
</tr>
<tr>
<td>CompleteRevocationRefs</td>
<td>RE</td>
<td>[1,1]</td>
<td>Contains a full set of references to the revocation data that have been used in the validation of the signer and CA certificates.</td>
<td>Must contain at most one of any of the following elements: CRLRefs, OCSPRefs, OtherRefs.</td>
</tr>
</tbody>
</table>
### Table 4-2. Document Signature

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRLRefs</td>
<td>RE</td>
<td>[0..1]</td>
<td>Contains sequences of references to CRLs via the CRLRef element. Identification of a CRL is made using 1) the digest of the entire DER encoded CRL (DigestAlgAndValue element); and 2) a set of data (CRLIdentifier element) including the issuer (Issuer element), the time when the CRL was issued (IssueTime element) and optionally the number of the CRL (Number element).</td>
<td>The Identifier element can be dropped if the CRL could be inferred from other information. Its URI attribute could serve to indicate where the identified CRL is archived. Must contain at least one CRLRef element. [1..*]</td>
</tr>
<tr>
<td>OCSPRefs</td>
<td>RE</td>
<td>[0..1]</td>
<td>Contains sequences of references to OCSP data via the OCSPRef element. Identification of an OCSP response is made using 1) a set of data (OCSPIdentifier element) including the name of the server that has produced the referenced response (ResponderID element) and the time indication in the &quot;ProducedAt&quot; field of the referenced response (ProducedAt element); and 2) the digest computed on the DER encoded OCSPResponse (as defined in the DigestAlgAndValue element), since it MAY be needed to differentiate between two OCSP responses by the same server with their &quot;ProducedAt&quot; fields within the same second.</td>
<td>The optional URI attribute could serve to indicate where the OCSP response identified is archived. Must contain at least one OCSPRef element. [1..*]</td>
</tr>
<tr>
<td>AttributeCertificateRefs</td>
<td>0</td>
<td>[0..1]</td>
<td>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.</td>
<td>Must contain exactly one CertRefs element.</td>
</tr>
<tr>
<td>AttributeRevocationRefs</td>
<td>0</td>
<td>[0..1]</td>
<td>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.</td>
<td>Must contain at most one of any of the following elements: CRLRefs, OCSPRefs, OtherRefs.</td>
</tr>
<tr>
<td>Data Element</td>
<td>Usage</td>
<td>Cardinality</td>
<td>Data Element Description</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. | The application MUST compose the following sequence of Include elements:  
- One Include element whose URI attribute references the \( \text{ds:SignatureValue} \) element of the qualified digital signature;  
- One Include element per each present \( \text{SignatureTimeStamp} \). The URI attribute in each Include element will reference one \( \text{SignatureTimeStamp} \) element;  
- One Include element whose URI attribute references the \( \text{CompleteCertificateRefs} \) property element;  
- One Include element whose URI attribute references the \( \text{CompleteRevocationRefs} \) property element;  
- One element whose URI attribute references the \( \text{AttributeCertificateRefs} \) element if this property is present;  
- One element whose URI attribute references the \( \text{AttributeRevocationRefs} \) element if this property is present. |
Table 4-2. Document Signature

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
</table>
| RefsOnlyTimeStamp    | O     | [0..*]      | Contains a time-stamp which covers only references to validation data. Time-Stamping each digital signature with Complete Validation Data as defined above (SigAndRefsTimeStamp element) may not be efficient, particularly when the same set of CA certificates and CRL information is used to validate many signatures. 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. | The application MUST compose the following sequence of Include elements:  
- One Include element whose URI attribute references the CompleteCertificateRefs property element;  
- One Include element whose URI attribute references the CompleteRevocationRefs property element;  
- One element whose URI attribute references the AttributeCertificateRefs element if this property is present;  
- One element whose URI attribute references the AttributeRevocationRefs element if this property is present. |
| 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 ds:KeyInfo element of the signature.  
Both the signer certificate and all certificates referenced in the CompleteCertificateRefs property (when present) element MUST be present either in the ds:KeyInfo element of the signature or in the CertificateValues property element. In addition, all the certificates referenced in AttributeCertificateRefs (when present) MUST also be present in the CertificateValues element. | This element is optional within the XAdES specification, but required for the purposes of this guide.  
Must contain one of the following elements: EncapsulatedX509Certificate, OtherCertificate. The EncapsulatedX509Certificate element is able to contain the base64 encoding of a DER-encoded X.509v3 certificate. The OtherCertificate 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: CRLValues, OCSPValues, OtherValues. |
### 4.3 Delegation of Rights Assertion

#### Table 4-3. Delegation of Rights Assertion

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:Assertion</td>
<td>R</td>
<td>[1..1]</td>
<td>Specifies the basic information that is common to all assertions.</td>
<td>Must include the following elements: Issuer, ds:Signature, Subject. Must include the following attributes: Version, ID, IssueInstant. Version attribute must be “2.0”.</td>
</tr>
<tr>
<td>saml:Issuer</td>
<td>R</td>
<td>[1..1]</td>
<td>The SAML authority that is making the claim(s) in the assertion. The issuer SHOULD be unambiguous to the intended relying parties.</td>
<td></td>
</tr>
<tr>
<td>ds:Signature</td>
<td>R</td>
<td>[1..1]</td>
<td>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 4-2. Document Signature for detailed digital signature elements.</td>
<td>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).</td>
</tr>
<tr>
<td>saml:Subject</td>
<td>R</td>
<td>[1..1]</td>
<td>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.</td>
<td>Must include element SubjectConfirmation. Should contain an Attribute element that describes the business relationship between Delegator and Delegatee.</td>
</tr>
<tr>
<td>saml:SubjectConfirmation</td>
<td>R</td>
<td>[1..1]</td>
<td>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.</td>
<td>The Method attribute must be “holder-of-key.” Must include element SubjectConfirmationData.</td>
</tr>
</tbody>
</table>
### Table 4-3. Delegation of Rights Assertion

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:SubjectConfirmationData</td>
<td></td>
<td>[1..1]</td>
<td>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 V2.0 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.</td>
<td></td>
</tr>
<tr>
<td>saml:Conditions</td>
<td></td>
<td>[0..1]</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>saml:Attribute</td>
<td></td>
<td>[0..1]</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>saml:AttributeStatement</td>
<td></td>
<td>[1..1]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 4.4 Validated Delegation of Rights Assertion

### Table 4-4. Validated Delegation of Rights Assertion

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Data Element Description</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:Assertion</td>
<td>R</td>
<td>[1..1]</td>
<td>Delegation of Rights Assertion as described in Table 4-3. Delegation of Rights Assertion above.</td>
<td></td>
</tr>
<tr>
<td>ds:Signature</td>
<td>R</td>
<td>[1..1]</td>
<td>Digital Signature artifacts encrypted by signer’s private key for Delegation of Rights Assertion as described in Table 4-3. Delegation of Rights Assertion above. Includes XAdES-X-L elements. This element is contained within the saml:Assertion element.</td>
<td></td>
</tr>
<tr>
<td>ds:Signature</td>
<td>R</td>
<td>[1..1]</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.5 Code Sets

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Usage</th>
<th>Cardinality</th>
<th>Code Set</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>R</td>
<td>[1..1]</td>
<td>Healthcare Taxonomy Data Set</td>
<td>Healthcare Provider Taxonomy (HIPAA) 2.16.840.1.114222.4.11.1066</td>
</tr>
<tr>
<td>Signature Purpose</td>
<td>R</td>
<td>[1..1]</td>
<td>ASTM E 1762-95</td>
<td></td>
</tr>
<tr>
<td>Delegation of Rights Assertion Action</td>
<td>R</td>
<td>[1..1]</td>
<td>'Authorized Signer'</td>
<td></td>
</tr>
</tbody>
</table>
5  APPENDIX A: EXAMPLE
The following XML examples present an XAdES-X-L Signature, a SAML based Delegation of Rights Artifact, and an XAdES-X-L Signature for that Delegation of Rights Artifact.

5.1  XAdES-X-L Digital Signature
<legalAuthenticator>
  <time value="20090227130000+0500"/>
  <signatureCode code="S"/>
  <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>
    </addr>
    <telecom use="WP" value="tel:555-555-1002"/>
    <assignedPerson>
      <given>First</given>
      <family>Last</family>
    </assignedPerson>
  </assignedEntity>
</legalAuthenticator>

<!- SignatureText START -->
signatureText xmlns="urn:hl7-org:v3" mediaType="application/xml"

  <!- XAdES WORK (Signed CDA): START -->
  <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/xmlenc-sha512"/>
        <ds:DigestValue>2c2dc2c30d3dd3fc2c2e3ccf02ca0f4db8a5d6494b6319df28b70fb76c7b246fed13840ca913be70802e2345c6dd3a6087ab00c41f64e80e61e2c6bc2d4d105fe</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      oRrea2fzFswyLeE+a36P2C/xQB4BMk6LJPAYym873qjSlloqR3fbZLYvm/yJ6iGCANc9+mbP4U/
    </ds:SignatureValue>
  </ds:Signature>
</signatureText>
<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 bJrQQeyoztdAPO6nsoRQ5oX5oAg=</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>Any text</ClaimedRole>
                </ClaimedRoles>
                <CertifiedRoles>
                    <CertifiedRole>EncapsulatedPKIDataType</CertifiedRole>
                </CertifiedRoles>
            </SignerRole>
        </SignedSignatureProperties>
        <SignedDataObjectProperties>
            <DataObjectFormat>
                <Description>string</Description>
                <ObjectIdentifier>
                    <Identifier>http://www.example.com/</Identifier>
                    <Description>string</Description>
                    <DocumentationReferences>
                    </DocumentationReferences>
                </ObjectIdentifier>
                <MimeType>string</MimeType>
                <Encoding>http://www.example.com/</Encoding>
                </DataObjectFormat>
            </SignedDataObjectProperties>
        </SignedProperties>
    </SignedProperties>
</QualifyingProperties>
<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>

<AllDataObjectsTimeStamp>
  <Include URI="http://www.example.com/">
    <CanonicalizationMethod Algorithm="http://www.example.com/">
      <EncapsulatedTimeStamp>EncapsulatedPKIDataType</EncapsulatedTimeStamp>
    </CanonicalizationMethod>
    <IndividualDataObjectsTimeStamp>
      <Include URI="http://www.example.com/">
        <CanonicalizationMethod Algorithm="http://www.example.com/">
          <EncapsulatedTimeStamp>EncapsulatedPKIDataType</EncapsulatedTimeStamp>
        </CanonicalizationMethod>
      </Include>
    </IndividualDataObjectsTimeStamp>
  </Include>
</AllDataObjectsTimeStamp>

<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>
      <CRLRefs>
        <CRLRef>
          <DigestAlgAndValue>...</DigestAlgAndValue>
        </CRLRef>
      </CRLRefs>
    </CompleteRevocationRefs>
    <OCSPRefs>
      <OCSPRef>
        <!-- URI="http://www.example.com/" -->
      </OCSPRef>
    </OCSPRefs>
  </UnsignedSignatureProperties>
</UnsignedProperties>
5.2 SAML Delegation of Rights Assertion
<time value="20090227130000+0500"/>
<signatureCode code="S"/>

<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"/>
</assignedEntity>

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

<!-- SignatureText START -->
<signatureText xmlns="urn:hl7-org:v3" mediaType="application/xml">
  <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>
      <X509Certificate>base64X509certificate</X509Certificate>
    </X509Data>
  </KeyInfo>
</signatureText>

<!-- Delegation of Rights Artifact: BEGIN -->
  <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>
      <X509Certificate>base64X509certificate</X509Certificate>
    </X509Data>
  </KeyInfo>
</ds:Signature>

<!-- Delegation Verifier -->
<ds:Object>
  <QualifyingProperties>
    <SignedProperties>
      <SignedSignatureProperties>
        <SigningTime>2012-04-26T16:04:56Z</SigningTime>
        <SigningCertificate>
          <Cert>!!-- identifier of signing certificate -->
          <CertDigest>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>  
            <DigestValue>base64 digest value</DigestValue>  
          </CertDigest>
        </SigningCertificate>
      </SignedSignatureProperties>
    </SignedProperties>
  </QualifyingProperties>
</ds:Object>

</urn:hl7-org:v3" mediaType="application/xml"/>
<CertDigest>
  <IssuerSerial>
    <X509IssuerName>certificate</X509IssuerName>
    <X509SerialNumber>550e8400-e29b-41d4-a716-446655440000</X509SerialNumber>
  </IssuerSerial>
</CertDigest>

<RevocationValues>
  <CRLValues>
    <EncapsulatedCRLValue;base64X509crl
  </CRLValues>
  <OCSPValues>
    <EncapsulatedOCSPValue;base64OCSPResponse
  </OCSPValues>
</RevocationValues>

<Reference Type="http://uri.etsi.org/01903/v1.1.1#SignedProperties" URI="#SignedProperties">
  <Transforms>
    <Transform Algorithm = "http://www.w3.org/2001/REC-xml-c14n-200103015#WithComments"/>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>base64 digest value</DigestValue>
  </DigestMethod>
</Reference>

<Manifest>
  <Reference URI="http://uri.etsi.org/01903/v1.1.1#SignedProperties"/>
</Manifest>

<SignaturePolicyIdentifier>id</SignaturePolicyIdentifier>

<SignatureProperties>
  <SignatureProperty Id="purposeOfSignature" target="signatureOID">code</SignatureProperty>
</SignatureProperties>

<UnsignedProperties>
  <UnsignedSignatureProperties>
    <RevocationValues>
      <CRLValues>
        <EncapsulatedCRLValue;base64X509crl
      </CRLValues>
      <OCSPValues>
        <EncapsulatedOCSPValue;base64OCSPResponse
      </OCSPValues>
    </RevocationValues>
  </UnsignedSignatureProperties>
</UnsignedProperties>

<QualifyingProperties>
  <SignatureProperties>
    <SignatureProperty Id="purposeOfSignature" target="signatureOID">code</SignatureProperty>
  </SignatureProperties>
</QualifyingProperties>
5.3 XAdES-X-L Digital Signature Applied to SAML Delegation of Rights

<legalAuthenticator>
    <time value="20090227130000+0500"/>
    <signatureCode code="S"/>
    <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>

<!-- Delegation of Rights Artifact: END -->
<!-- SignatureText END -->
<ds:X509Data>
</ds:X509Data>

</ds:KeyInfo>
</ds:Signature>

<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 Delegee/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: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:Assertion>

<!-- Delegation Agent Signature: END -->

</signatureText>

<!-- SignatureText END -->
</legalAuthenticator>
6 APPENDIX B: GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDA (Clinical Document Architecture)</td>
<td>(HL7). A document markup standard that specifies the structure and semantics of &quot;clinical documents&quot; for the purpose of exchange between healthcare providers and patients.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>(NIST). An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.</td>
</tr>
<tr>
<td>Certificate Policy</td>
<td></td>
</tr>
<tr>
<td>Delegation of Rights</td>
<td>The ability to delegate rights or authority to another to act in a specific capacity on behalf of the grantor of the right.</td>
</tr>
<tr>
<td>Digest</td>
<td>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.</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>(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.</td>
</tr>
<tr>
<td>Electronic Health Record</td>
<td>Clinical information for a specific patient that is stored electronically within an EHR-S.</td>
</tr>
</tbody>
</table>
| 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.                                                                 |