



5

IHE IT Infrastructure Technical Framework Supplement

10

Secure Retrieve (SeR)

15

Revision 1.5 – Trial Implementation

20

Date: July 2, 2021
Author: IHE ITI Technical Committee
Email: iti@ihe.net

25

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

Foreword

30 This is a supplement to the IHE IT Infrastructure Technical Framework V17.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on July 2, 2021 for trial implementation and may be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure
35 Technical Framework. Comments are invited and can be submitted at http://www.ihe.net/ITI_Public_Comments.

This supplement describes changes to the existing technical framework documents.

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

40 *Amend Section X.X by the following:*

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

45

General information about IHE can be found at www.ihe.net.

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

50 Information about the structure of IHE Technical Frameworks and Supplements can be found at http://www.ihe.net/IHE_Process and <http://www.ihe.net/Profiles>.

The current version of the IHE IT Infrastructure Technical Framework can be found at <https://profiles.ihe.net/ITI/TF/index.html>.

55 CONTENTS

	Introduction to this Supplement.....	5
	Open Issues and Questions	6
	Closed Issues	6
60	IHE Technical Frameworks General Introduction.....	9
	9 Copyright Licenses	9
	10 Trademark	9
	IHE Technical Frameworks General Introduction Appendices.....	10
	Appendix A – Actors	10
65	Appendix B – Transactions.....	10
	Appendix D – Glossary.....	11
	Volume 1 – Profiles	12
	Copyright Licenses.....	12
	Domain-specific additions	12
70	39 Secure Retrieve (SeR) Profile.....	13
	39.1 SeR Actors, Transactions, and Content Modules.....	14
	39.1.1 Actor Descriptions and Actor Profile Requirements.....	15
	39.1.1.1 Authorization Decisions Manager.....	15
	39.1.1.2 Authorization Decisions Verifier	15
75	39.2 SeR Actor Options	16
	39.3 SeR Required Actor Groupings	16
	39.4 SeR Overview	17
	39.4.1 Concepts.....	17
	39.4.2 Use Cases	17
80	39.4.2.1 Use Case #1: Environment with a centralized Access Decision Manager	17
	39.4.2.1.1 Environment with a centralized Access Decision Manager Use Case Description.....	17
	39.4.2.1.2 Environment with a centralized Access Decision Manager Process Flow	18
	39.5 SeR Security Considerations.....	19
85	39.6 SeR Cross Profile Considerations	19
	Volume 2 – Transactions	20
	3.79 Authorization Decisions Query [ITI-79].....	20
	3.79.1 Scope	20
	3.79.2 Actor Roles.....	20
90	3.79.3 Referenced Standards	20
	3.79.4 Messages	21
	3.79.4.1 XACMLAuthorizationDecisionQuery Request	21
	3.79.4.1.1 Trigger Events	21
	3.79.4.1.2 Message Semantics.....	21
95	3.79.4.1.2.1 Example of a SOAP v1.2 XACMLAuthorizationDecisionQuery Request message.....	24
	3.79.4.1.3 Expected Actions	26

	3.79.4.2 XACMLAuthorizationDecisionQuery Response	27
	3.79.4.2.1 Trigger Events	27
100	3.79.4.2.2 Message Semantics	27
	3.79.4.2.2.1 Example of a SOAP v1.2 XACMLAuthorizationDecisionQuery Response message	28
	3.79.4.2.3 Expected Actions	29
	3.79.5 Security Considerations.....	30
105	3.79.5.1 Security Audit Considerations.....	30
	3.79.5.1.1 Authorization Decisions Verifier audit message	30
	3.79.5.1.2 Authorization Decisions Manager audit message.....	32
	3.79.5.2 Authorization Decisions Manager Specific Security Considerations	34
	3.79.5.3 Authorization Decisions Verifier Specific Security Considerations	34
110	Volume 2 Namespace Additions	35
	Volume 2 Appendices.....	36
	Volume 3 – Content Modules.....	37
	Volume 4 – National Extensions	38
115		

Introduction to this Supplement

This supplement defines new functionalities for an XDS environment with a unique and centralized Access Control system. As a Trial Implementation Supplement, this profile is limited to those deployment models and their policies where a central authorization authority can make complete and definitive decisions, yet support federated identity/authentication. These use-cases specifically mean that neither XDS Document Source nor XDS Document Repository Actors need to have any more fine-grain policies to enforce. The supplement describes how to create a “system of trust” between the actor that can perform Access Decisions (on behalf of Consent Docs, Policies and Creation/Access/Disclosure rules) and XDS Actors that actually store clinical data and documents. Access decisions are often based on metadata (e.g., document types, practiceSetting); therefore, the source of truth for metadata (i.e., the XDS Document Registry) is the best place to make the decisions. With the objective to keep the data close to the decision point, the XDS Document Registry in many implementations, is a good candidate to perform access control decisions (Authorization Decisions Manager or Policy Decision Point). In a typical XDS environment, there are many XDS Document Repositories that store documents. These systems are not aware of Consent Documents published by patients, and cannot apply Access/Creation/Disclosure Policies to requests for Document retrieval; then the replication of Access Control functionalities is unfeasible and/or too expensive (due to integration burdens and total cost of ownership).

The objective of the Secure Retrieve Profile is the definition of a mechanism to convey Authorization Decisions between XDS Actors, attesting that the reliable Policy Decision Point (PDP) has already made an access decision.

The starting requirements/constraints upon which this profile is developed are described below:

- A unique PDP performs access decision for all XDS Document Consumer and all XDS Document Repositories involved in the Affinity Domain.
- XDS Document Repositories cannot manage the whole set of information needed to perform access decisions (XDS Document Repositories are not required to store metadata. If the Repository stores metadata, the metadata might be insufficient to perform an access decision).
- The XDS infrastructure is not fully federated; a clear separation of duties and responsibilities between PDP and XDS Document Repositories is needed (Repositories store clinical documents; PDP evaluates access rights to those contents).
- The XDS Document Repositories must enforce access decision made by the Policy Decision Point.
- A technical pattern that reduces behavioral and transactional changes for the Consumer side is clearly preferred (lower costs for deployment and for security reasons).

This supplement is a standalone profile because it defines a flexible pattern that could be used by any Service Provider that queries for Authorization Decisions already granted by a trusted

155 Authorization Decisions Manager (or PDP). However, the focus is to add Access Control functionalities to the XDS environment.

This profile introduces two new actors (Authorization Decisions Manager and Authorization Decisions Verifier) and one new transaction (Authorization Decisions Query).

160 This profile does not describe how Authorization Decisions are performed. However, this profile relies on XACM-SAML framework, so these standards could be good candidates to implement Authorization Requests.

This profile describes how a Service Provider (e.g., Document Repository) can discover the existence of Authorization Decisions granted to an entity and for specific documents.

Open Issues and Questions

None

165 Closed Issues

1. Which is the best technical approach for the solution?

- It is suggested an evaluation of both the technical approaches: SAML token vs. JWT Bearer token. A comparison between the two standards will be formalized in a document. First step: evaluation of the efficiency of the two solutions proposed.
- 170 ○ A JWT token is only OAuth which is REST. What we may end up with is an equivalent of this in MHD. Right now, we are doing this for XDS, so the strategy should be:
 - Focus on SAML and SOAP, and advancing XUA.
 - Let MHD handle the RESTful equivalent after this is in TI.
- 175 ○ Volume 1 should be independent of the standards selected. Volume 2 may eventually contain an extra piece that shows how OAuth, REST and MHD meet the same volume 1 need as the SAML/SOAP pieces that are developed this year.
- Therefore, the plan is to proceed with SAML and SOAP for now, but not mention this in volume 1, only in volume 2.
- 180 2. I've introduced a transaction to "Request Retrieval Token". This allows in the same environment simple Consumer and Consumer compliant with SeR guideline. This is, from my point of view, acceptable because there are certain types of docs (administrative docs and so on...) that probably can be shared without Retrieval Token. In my perspective this choice brings flexibility to the solution. Is this reasonable?
- 185 ○ This can be addressed silently defining Domain Policies that state that some documents can be retrieved without Retrieval Token. No reasons to profile this feature.
- 3. Many different patterns have been analyzed. An evaluation spreadsheet was produced. For further details see ftp site: ftp://ftp.ihe.net/IT_Infrastructure/iheitiyr12-2014-

- 190 2015/Technical_Cmte/Workitems/SecureRetrieve_SeR/CRAC%20Standards%20Pattern
%20Selection%20Criteria%20Matrix%20-%2020140323.xls
- 195 4. Which is the best drafting approach for the supplement? (Suggestion to postpone this decision/discussion, after a deep analysis of the problem. This is something that can be addressed after the first face to face meeting, once we have clear the SCOPE and the USE CASES that can be covered)
- The supplement is drafted as an independent supplement focused on an XDS environment. The pattern selected, allows to be applied for future applications to other use cases. Transaction [ITI-79] is profiled taking this in mind (extensible payload for the XACMLAuthorizationDecisionQuery Request message)
- 200 5. There was a proposal: Use Artifact Resolution Protocol (defined in SAML 2.0 core specification) instead of XACMLAuthzDecisionQuery. Rationale: The transaction [ITI-79] defines a standard semantic to check if an authorization token exists, but XACMLAuthzDecision Query is used to request and perform Authorization Decision.
- The proposal was rejected: The use case does not require the sharing of SAML Artifact. The XACMLAuthzDecisionQuery does not require that the Authorization Decisions Manager performs access decisions following the XACML standard. XACML Authorization Query Request message just conveys needed parameters to locate an authorization. In addition to that, Artifact Resolution protocol seems to add some requirements that broke the basic use case “In all cases, the artifact MUST exhibit a single-use semantic such that once it has been successfully resolved, it can no longer be used by any party.” And again: “The responder MUST enforce a one-time-use property on the artifact by ensuring that any subsequent request with the same artifact by any requester results in an empty response as described above”. For the XDS use case, the Authorization Decisions Manager could request the same
- 205
- 210 authorization many times; the one-shot authorization is not useful in this use case.
- 215
6. It was suggested to use Attribute Name:
urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:subject in accordance to XSPA instead of the subject-id. The proposal was rejected. The using of the XSPA guideline does not add value, and add requirements that do not match with SeR use case..
- 220 7. This profile mandates the grouping between XDS Actors and XUA Actors (see Section 3). Readers are asked to provide feedback on this requirement. It is obvious that XUA environment (and SAML 2.0 token) is helpful for entity identification. Are there any other preferred approaches to perform this identification?
- No other approaches are suggested. XUA grouping is confirmed.
- 225 8. Readers should focus on the XACML encoding defined for the XDSDocumentEntry.uniqueId and for the XUA Attribute Patient ID. Both this attribute are identified by the same @Category and same @AttributeId. This could create problems, because the Authorization Decisions Manager should interpret which is the

- 230 docID and which is the patient ID. It is not clear to the tech committee how much the impact is.
- A new urn is defined for patient ID.
9. This profile defines a mandatory grouping between Authorization Decisions Manager and Document Registry. It is an obvious grouping, but implementations could also use other approaches. Readers are asked to provide feedback on this requirement.
- 235 ○ The profile does not profile the transaction to request Authorizations. This access decision is likely performed during the Query Request processing and requires input parameters local defined by the Domain. However, the performing of these decisions needs a lot of information managed by the Registry or conveyed within the Query Request. In accordance to this a grouping approach is proposed.
- 240 10. The pattern described in this profile requires the Pull of authorization from an Authorization Decisions Manager. This approach is compliant with XACML standard. For efficiency reasons a Push approach could be better. In a Push environment when an Authorization is granted for a resource, this authorization is sent to the XDS Document Repository that stores this resource. This approach is not described in standard
- 245 specification yet.
- The Pull approach is chosen to reduce computational load on the central Authorization Decision Manager

IHE Technical Frameworks General Introduction

250 The [IHE Technical Framework General Introduction](#) is shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to this document where appropriate.

9 Copyright Licenses

255 IHE technical documents refer to, and make use of, a number of standards developed and published by several standards development organizations. Please refer to the IHE Technical Frameworks General Introduction, [Chapter 9 - Copyright Licenses](#) for copyright license information for frequently referenced base standards. Information pertaining to the use of IHE International copyrighted materials is also available there.

10 Trademark

260 IHE® and the IHE logo are trademarks of the Healthcare Information Management Systems Society in the United States and trademarks of IHE Europe in the European Community. Please refer to the IHE Technical Frameworks General Introduction, [Chapter 10 - Trademark](#) for information on their use.

IHE Technical Frameworks General Introduction Appendices

265 The [IHE Technical Framework General Introduction Appendices](#) are components shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to these documents where appropriate.

270 *Update the following appendices to the General Introduction as indicated below. Note that these are **not** appendices to this domain's Technical Framework (TF-1, TF-2, TF-3 or TF-4) but rather, they are appendices to the IHE Technical Frameworks General Introduction located [here](#).*

[Appendix A](#) – Actors

275 *Add the following **new or modified** actors to the [IHE Technical Frameworks General Introduction Appendix A](#):*

Actor	Definition
Authorization Decisions Manager	Actor that can perform Access Control decision, evaluating requests for authorization. The result of this evaluation is the creation of an Authorization Decision that certifies the decision made
Authorization Decisions Verifier	This actor queries for Authorization Decisions related to the Requester Entity before disclosing specific documents. An Authorization Decision is stored and managed by the Authorization Decisions Manager and certifies that a decision was made by a trustable actor.

[Appendix B](#) – Transactions

280 *Add the following **new or modified** transactions to the [IHE Technical Frameworks General Introduction Appendix B](#):*

Transaction	Definition
Authorization Decisions Query [ITI-79]	Transaction used by the service provider (Authorization Decisions Verifier) to request valid authorization decisions granted for the Requester Entity to disclose specific documents.

285 **Appendix D – Glossary**

*Add the following **new or modified** glossary terms to the [IHE Technical Frameworks General Introduction Appendix D](#):*

Glossary Term	Definition
Access Decision Manager	A complex system that is responsible for access/creation/disclosure decisions performed according to Domain Policies, Consent Documents, etc. This actor can implement additional functionalities typical of a PDP (Policy Decision Point), PAP (Policy Administration Point) and a PIP (Policy Information Point).
Authorization Decision	A security token that describes which documents can be accessed by a specific entity
Requester Entity	The entity identified within the identity assertion. This entity asks for resources (documents). This entity performs query to the registry and try to retrieve documents from repositories. Authorization Decisions are created and associated with the Requester Entity.

290

Volume 1 – Profiles

Copyright Licenses

NA

Domain-specific additions

NA

295

<i>Add new Section 39</i>

39 Secure Retrieve (SeR) Profile

This profile defines a framework able to enforce a centralized Access Control system, conveying between actors involved in an XDS environment the evidence of the reliable decisions already made by an Access Decision Manager.

The main objective of this profile is to create a system of trust between the actor that performs access decisions (Authorization Decisions Manager), and actors that store clinical data (XDS Document Repositories). This split of responsibilities is needed in many environments where systems that expose clinical data are not able to replicate and repeat access decisions.

This type of approach is useful in many situations:

- XDS environments with many XDS Document Repositories which expose clinical documents without an access control system already implemented. These systems require minimal integration burden to support functionalities defined in this profile.
- Federation of repositories in a new Affinity Domain. The federation of repositories requires the subscription of the whole set of domain policies for content Creation/Access/Disclosure. A centralized Access Decision Manager coupled with the central XDS Document Registry allows the management of accesses to local Repositories without requiring the development of complex Access Control systems.
- Environments where Consent Documents, Policies and Data Access Rules can be collected, managed and discovered only in a centralized way.
- Sharing infrastructure with strong enforcement of Access Control systems. In many organizational and jurisdictional environments, access to clinical data is managed by Servers that store/register clinical data and cannot be regulated by the Consumer itself.

In those scenarios, this profile defines how to create a “logical federation” between an Access Decision Manager (responsible for enabling/denying accesses) and XDS Document Repositories (that store documents and expose them without knowledge related to the user/role/consent documents/policies etc.). Actors that store clinical data could only trust a decision made by the Access Decision Manager

Access Decision Manager functionalities are out of scope for this profile because typically they are domain specific and locally defined. It is out of scope of the profile to cover all the Access Control Decision issues. This profile allows the creation of a system where the existence of a document that cannot be accessed by a specific user is totally obscured from the Consumers.

Creation, management and enforcement of policies are out of scope for this profile. However, this profile takes in consideration best practices and common implementations for Access Decision Manager functionalities.

This profile allows addressing the following security risks (related to XDS Document Repository exposure):

- The Document Repository does not know the access control decision that should be enforced. Therefore, if it denies access to data, there is a failure of availability. If it

provides the document inappropriately, there is a risk to confidentiality. The SeR Profile allows the Repository to be aware of the decision made, only asking for the existence of Authorizations granted by the trusted Access Decision Manager and enforcing that decision. In accordance with Affinity Domain policies, the XDS Document Repository can make further access control decisions.

- A separation of duties between Document Consumer (that requests authorization and documents) and the Policy Decision Point is created. The SeR Profile moves the decisions and enforcement into the service layer by grouping decisions with the Registry and enforcement with the Repository (instead of the Consumer).

39.1 SeR Actors, Transactions, and Content Modules

This section defines the actors, transactions, and/or content modules in this profile.

Figure 39.1-1 shows the actors directly involved in the SeR Profile and the relevant transactions between them. If needed for context, other actors that may be indirectly involved due to their participation in other related profiles are shown in dotted lines. Actors which have a mandatory grouping are shown in conjoined boxes.

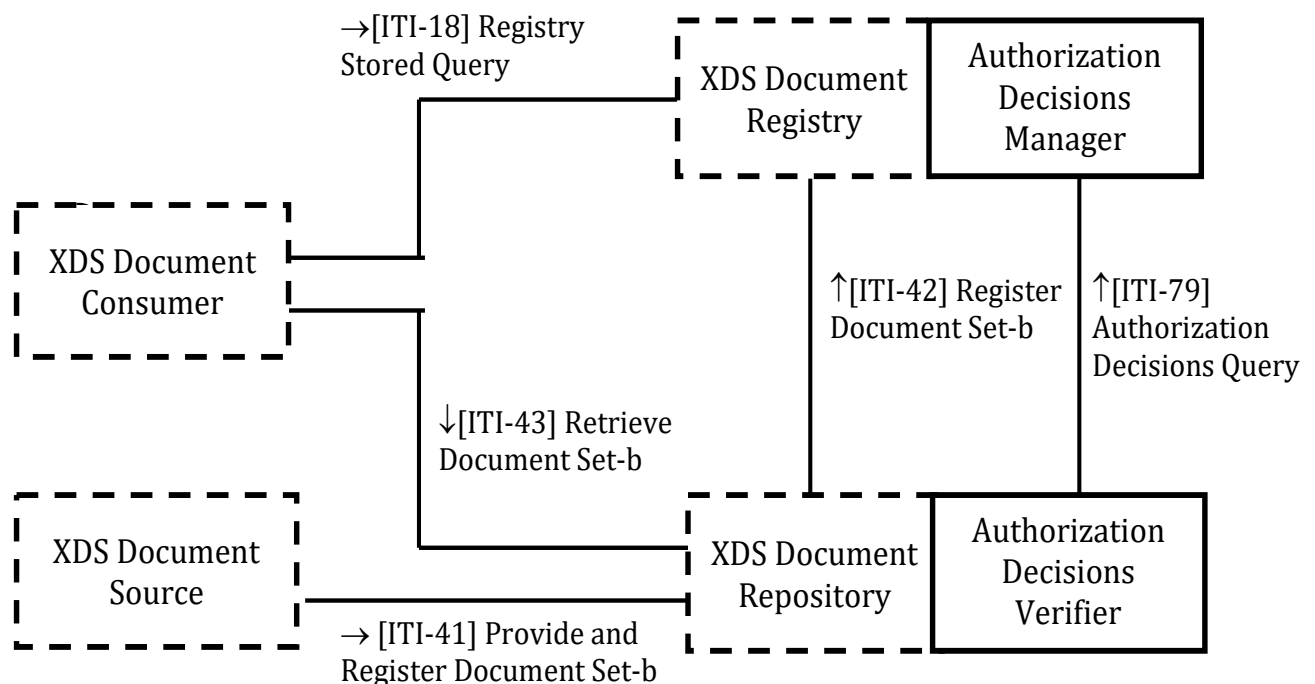


Figure 39.1-1: SeR Actor Diagram

Table 39.1-1 lists the transactions for each actor directly involved in the SeR Profile. To claim compliance with this profile, an actor shall support all required transactions (labeled “R”) and may support the optional transactions (labeled “O”).

Table 39.1-1: SeR Profile - Actors and Transactions

Actors	Transactions	Optionality	Reference
Authorization Decisions Manager	Authorization Decisions Query [ITI-79]	R	ITI TF-2: 3.79
Authorization Decisions Verifier	Authorization Decisions Query [ITI-79]	R	ITI TF-2: 3.79

39.1.1 Actor Descriptions and Actor Profile Requirements

Most requirements are documented in Transactions (Volume 2) and Content Modules (Volume 3). This section documents any additional requirements on profile's actors.

39.1.1.1 Authorization Decisions Manager

The Authorization Decisions Manager is responsible for the management of access control decisions in the entire XDS domain. From the Access Control point of view, this actor is the unique Policy Decision Point (PDP) of the entire domain for all documents because it may decide on the outcome of an incoming authorization request in order to provide access to specific resources (documents). The Authorization Decisions Manager completes the Authorization Decision creating and storing a security token. This security token does not need to be exposed to other systems, and it certifies the decision made. This actor could implement additional Access Control functionalities required in the specific implementation scenario.

(Refer to the White Paper IHE ITI Access Control White Paper for further information about PDP and Access Control Systems.)

39.1.1.2 Authorization Decisions Verifier

The Authorization Decisions Verifier is the actor that verifies if the Requester Entity is authorized to access specific resources by querying the Authorization Decisions Verifier. This actor enforces the Access Decision made by the trusted Policy Decision Point, so it acts as a Policy Enforcement Point (PEP). This actor enables the secure exposure of documents, allowing access only to Requester Entities previously authorized by the Policy Decision Point.

The Requester Entities (XDS Document Consumer) convey at least the following information to the Authorization Decisions Verifier:

- Requester Entity that obtains authorization (e.g., using an identity assertion)
- The unique ID of the document that can be accessed (within the Retrieve Document Set-b Request)

(Refer to the White Paper IHE ITI Access Control White Paper for further information about PEP and Access Control Systems).

39.2 SeR Actor Options

Options that may be selected for each actor in this profile, if any, are listed in the Table 39.2-1. Dependencies between options when applicable are specified in notes.

Table 39.2-1: SeR - Actors and Options

Actor	Option Name	Reference
Authorization Decisions Manager	No options defined	--
Authorization Decisions Verifier	No options defined	--

39.3 SeR Required Actor Groupings

SeR Actors are involved in an XDS document sharing infrastructure. The groupings between XDS Actors and SeR Actors enforce the system of trust between the XDS Document Registry that localizes the XDS DocumentEntries and the XDS Document Repositories that store XDS documents. The mandatory grouping between the XDS Document Registry and the Authorization Decisions Manager is needed to leave the protocols and semantics of the Authorization Request transaction unspecified. The Authorization Decisions Manager needs metadata, entity identification, policies applicable etc.

This profile requires the identification of the entity that actually performs queries and retrieves of documents. Authorization Decisions are granted to a specific entity and can be used only by that entity to get access to document entries.

Grouping with XUA Actors shall be supported. Other approaches for entity identification could be defined by local domain policies.

An actor from this profile (Column 1) shall implement all of the required transactions and/or content modules in this profile *in addition to* all of the transactions required for the grouped actor (Column 2).

Section 39.5 describes some optional groupings that may be of interest for security considerations and Section 39.6 describes some optional groupings in other related profiles.

Table 39.3-1: SeR - Required Actor Groupings

SeR Actor	Actor to be grouped with	Reference	Content Bindings Reference
Authorization Decisions Manager	XDS Document Registry	ITI TF-1: 10.1	--
	XUA X-Service Provider	ITI TF-1: 13.4	--
	ATNA Secure Node or Secure Application	ITI TF-1: 9.1	--
Authorization Decisions Verifier	XDS Document Repository	ITI TF-1: 10.1	--
	XUA X-Service Provider	ITI TF-1: 13.4	--

SeR Actor	Actor to be grouped with	Reference	Content Bindings Reference
	ATNA Secure Node or Secure Application	ITI TF-1: 9.4	--

39.4 SeR Overview

39.4.1 Concepts

This section describes the primary use-cases for the SeR Profile. In this use case, the storing facility relies on a trusted actor able to evaluate access rights.

The Authorization Decisions Manager is grouped with the XDS Document Registry. It acts as a Policy Decision Point (PDP) and implements functions of Policy Information Point (PIP) and Policy Administration Point (PAP). The Authorization Decisions Manager in this use-case act as a PIP because it manages the whole set of information needed to perform an access decision:

- Consent Documents subscribed by patients
- Security & Privacy Metadata
- Access Policies
- Patients and Providers Master Data and relationship between them
- Etc.

The Authorization Decisions Manager may implement functions of a PAP, administering and maintaining Affinity Domain Policies.

39.4.2 Use Cases

39.4.2.1 Use Case #1: Environment with a centralized Access Decision Manager

This use-case describes how an XDS Document Repository without internal Access Control mechanisms uses Authorization Decisions made by a third party.

39.4.2.1.1 Environment with a centralized Access Decision Manager Use Case Description

The XDS Document Repositories are all in the same XDS Affinity Domain, but are unable to perform access decisions. When an entity tries to retrieve some documents from an XDS Repository, the XDS Document Repository lacks the information needed to make an access control decision. The Authorization Decisions Manager can make the decision at the time of the query to the XDS Registry. This decision is enforced by the XDS Document Repository grouped with an Authorization Decisions Verifier.

For example:

Mr. White comes to his GP, Dr. Brown, to show him a Laboratory Report. This Laboratory Report is shared in an XDS infrastructure. Using his EHR, Dr. Brown queries for Mr. White's Laboratory Reports shared in the XDS infrastructure. The Query Response returns some

440 DocumentEntries to the XDS Document Consumer. Each XDSDocumentEntry in the response is authorized for the retrieval. Dr. Brown uses his XDS Document Consumer to retrieve these documents. XDS Document Repository verifies the authorization for the Requester Entity for each document requested before providing documents.

No other access control decisions are needed at this level.

445 Each Authorization Decision has a time slot of validity. Dr. Brown can retrieve documents until the Authorization expires. The Repository discloses **only** documents requested and authorized.

There are conditions where XDS Document Repository might not be providing documents:

- The Requester Entity does not have authorization according to the Authorization Decisions Query
- 450 • The authorization was granted too long ago and the Authorization Decision is expired

The user attempting to retrieve from the XDS Document Repository is different from the user that was authorized (there is a mismatch between the user that performs the retrieve and the user that queries for documents).

39.4.2.1.2 Environment with a centralized Access Decision Manager Process Flow

455

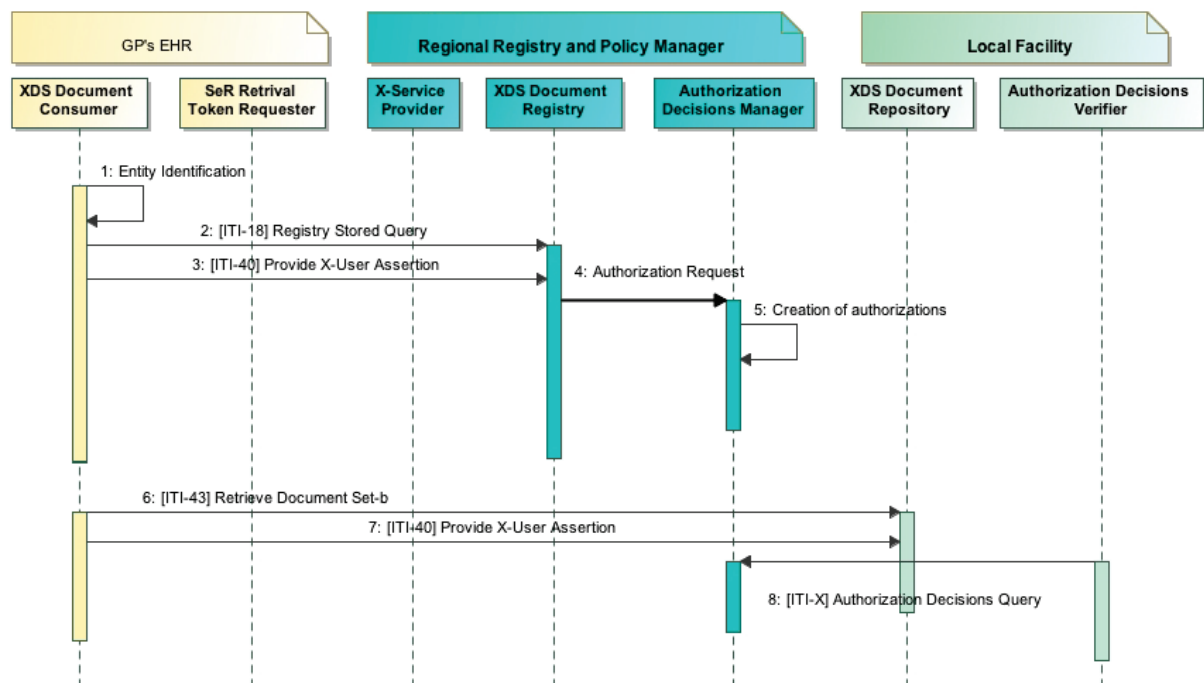


Figure 39.4.2.1.2-1: Basic Process Flow in SeR Profile

39.5 SeR Security Considerations

- 460 To prevent interaction with malicious third parties, a closed system of trust based on TLS digital identities is strongly recommended. Authorization Decisions Manager should accept queries only from a restricted set of Secure Nodes/Applications. The Authorization Decisions Verifier should perform queries only to the domain-identified Authorization Decisions Manager.
- Authorization Decisions are collected by the Authorization Decisions Manager. These security
465 tokens should not be exposed to other systems. Encryption of this token (when stored by the Authorization Decisions Manager) could avoid the disclosure of sensitive information.
- The centralized Access Control system introduces a single point-of-failure risk in the XDS environment. A failure of the Authorization Decisions Manager could result in legitimate access being denied.
- 470 This profile introduces an XDS Error Code in order to codify an additional reason for document retrieve failure. See [ITI TF-3: Table 4.2.4.1-2](#). Adding more technical details within the failure response could be used to refine malicious requests. For example, if the error created by the Authorization Decisions Verifier conveys the reason of the failure, such as “the authorization is expired” or “the authorization is released in a different Functional Context”, it could provide
475 information to the malicious Document Consumer that can try to refine subsequent requests.
- The SeR Profile does not define how to perform the Access Decision. However, this profile supports the creation of a system where the existence of a document that cannot be accessed by a specific user is not revealed. Each document returned within the Query Response should be considered Authorized for the retrieval at the time of the Query Request.
- 480 If the Authorization Decisions Verifier is allowed to perform new access decision when it receives an XACMLAuthorizationDecisionsQuery Request message, performances can be not adequate. In order to avoid that, a previous Query is recommended.

39.6 SeR Cross Profile Considerations

- 485 An XDS Document Consumer that participates in an XDS environment using SeR framework shall be grouped with an XUA X-Service User.
- An X-Service User involved in a SeR framework shall be able to identify the specific Requester Entity conveying its logical identity (user ID, application ID, etc.) within the <Subject>/<NameID> element.

Volume 2 – Transactions

490 *Add Section 3.79*

3.79 Authorization Decisions Query [ITI-79]

3.79.1 Scope

This transaction is used by the Authorization Decisions Verifier to query for authorization decisions, granted and managed by the Authorization Decisions Manager. These authorization
495 decisions are created for an entity that is authorized to disclose specific documents.

The Authorization Decisions Verifier asks for authorizations based on the Requester Entity and the requested documents identifiers.

This transaction is based on SOAP v1.2 exchange protocol and Synchronous Web services (see [ITI TF-2: Appendix V](#)).

500 3.79.2 Actor Roles

Actor:	Authorization Decisions Manager
Role:	This actor stores and manages authorization decisions granted for an entity and for specific documents.
Actor:	Authorization Decisions Verifier
Role:	This actor queries for authorization decisions granted based on the Requester Entity and requested documents identifiers.

3.79.3 Referenced Standards

OASIS SOAP v1.2

505 OASIS Security Assertion Markup Language (SAML) v2.0

OASIS eXtensible Access Control Markup Language (XACML) v2.0

OASIS Multiple resource profile of XACML v2.0

OASIS SAML 2.0 profile for XACML v2.0

510 OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0
for Healthcare Version 2.0 (not normative)

3.79.4 Messages

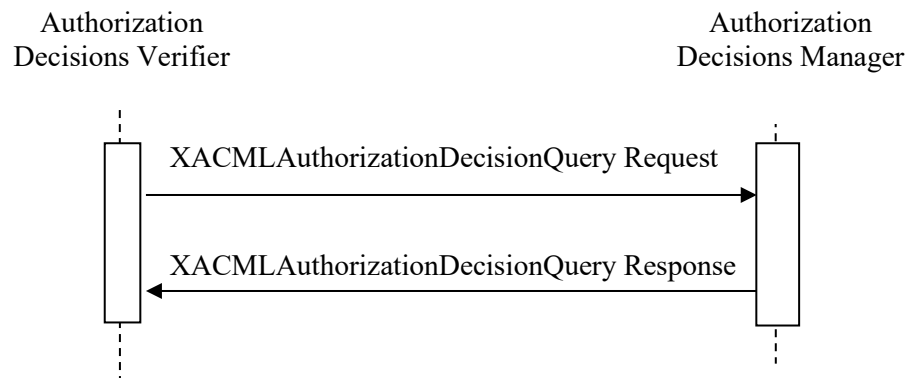


Figure 3.79.4-1: Interaction Diagram

3.79.4.1 XACMLAuthorizationDecisionQuery Request

515 This message enables the Authorization Decisions Verifier to query the Authorization Decisions
 Manager for authorizations. This message relies on the SAML v2.0 extension for XACML and
 uses the element `<XACMLAuthzDecisionQuery>` to convey the document identifiers and the
 subject identifier. The Authorization Decisions Verifier can ask for authorization for many
 documents in one query, so the Request message complies with the Multiple resource profile of
 520 XACML v2.0. Actors involved support XUA and use SAML identity assertions to identify
 entities (see ITI TF-1: 39.5 and ITI TF-1: 39.6). SAML attribute elements shall be mapped into
 xacml-context attribute elements as defined in SAML 2.0 Profile of XACML v2.0 (Section 2).

3.79.4.1.1 Trigger Events

525 The Authorization Decisions Verifier sends this message when it needs to verify whether there is
 an Authorization to disclose specific documents to an entity requesting them. The trigger event is
 the grouped XDS Document Repository receiving a Retrieve Document Set Request message
 (see [ITI TF-2: 3.43.4.1](#)) and a Provide X-User Assertion [ITI-40] transaction from an XDS
 Document Consumer that identifies the specific Requester Entity within a SAML Assertion.

3.79.4.1.2 Message Semantics

530 The XACMLAuthorizationDecisionQuery Request message shall use SOAP v1.2 message
 encoding.

The WS-Addressing Action header shall have this value:

- `urn:ihe:iti:2014:ser:XACMLAuthorizationDecisionQueryRequest`

535 The body of the message shall use an `<XACMLAuthzDecisionQuery>` element (defined in the
 SAML 2.0 Profile for XACML v2.0) to convey Authorization Query parameters.

This element shall contain the following attribute:

- `@ReturnContext`: shall be set to “false” because the content of the XACMLAuthorizationDecision Request is not needed within the Authorization Result.

IHE does not define constraints for other attributes (see OASIS SAML 2.0 Profile of XACML Version 2.0 Section 4 for details).

The `<XACMLAuthzDecisionQuery>` element shall have only one child element `<Request>`. This element shall comply with OASIS Multiple resource profile of XACML v2.0. This element shall have the following child elements:

- It shall have one child element `<Subject>`. This element identifies the Requester Entity. The `<Subject>` element shall have at least one child element `<Attribute>` characterized by `@AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"` and `@DataType="http://www.w3.org/2001/XMLSchema#string"`. The `<AttributeValue>` child element shall convey the subject identifier. This element shall have the same value of the `<Subject>/<NameID>` element conveyed within the SAML assertion. See the [Provide X-User Assertion](#) (ITI-40) transaction for details. Any other SAML attribute related to the subject shall be added as additional XACML attribute. Table 3.79.4.1.2-1 defines which XUA attributes are identified as related to the subject (each attribute with “XACML Category” equal to `urn:oasis:names:tc:xacml:1.0:subject-category:access-subject`)
- It shall have one or more `<Resource>` elements that identify resources. There is one `<Resource>` element for each document requested by the Requester Entity. In the XDS environment, a `<Resource>` element identifies a document. Each document is identified by two required `<Attribute>` child elements.
 - The first `<Attribute>` element shall have `@AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"` and `@DataType="http://www.w3.org/2001/XMLSchema#string"`. The `<AttributeValue>` child element stores the value of the `XDSDocumentEntry.uniqueId`;
 - The second `<Attribute>` element shall have `@AttributeId="urn:ihe:iti:ser:2016:document-entry:repository-unique-id"` and `@DataType="http://www.w3.org/2001/XMLSchema#anyURI"`. The `<AttributeValue>` child element stores the value of the `XDSDocumentEntry.repositoryUniqueId`.

Any other SAML attribute related to the resource requested shall be added as additional XACML attribute (e.g., `homeCommunityId`). Table 3.79.4.1.2-1 defines which XUA attributes are identified as related to the resource (each attribute with “XACML Category” equal to `urn:oasis:names:tc:xacml:1.0:resource`)

Attributes that belong to the XACML environment category (e.g., XUA attributes with “XACML Category” equal to urn:oasis:names:tc:xacml:1.0:environment in Table 3.79.4.1.2-1) shall be added to an <Environment> element.

The <Action> element identifies the action that the Authorization Decisions Manager has to authorize. This element shall have a child element <Attribute> with @AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" and @DataType=http://www.w3.org/2001/XMLSchema#anyURI. This attribute shall have a child element <AttributeValue> characterized by value: urn:ihe:iti:2007:RetrieveDocumentSetResponse

Additional attributes that belong to the XACML action category (e.g., XUA attributes with “XACML Category” equal to urn:oasis:names:tc:xacml:1.0:action in Table 3.79.4.1.2-1) shall be added to an <Action> element.

The mapping of attributes from SAML v2.0 assertion defined in the Provide X-User Assertion [ITI-40] transaction into XACML query attributes is defined below. For each attribute from [ITI-40], the XACML Category and @AttributeId are identified:

Table 3.79.4.1.2-1: [ITI-40] Attributes mapping into XACML Query Attributes

[ITI-40] Attribute	XACML Category	AttributeId	DataType
Subject ID	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xacml:1.0:subject:subject-id	http://www.w3.org/2001/XMLSchema#string
Subject Organization	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xspa:1.0:subject:organization	http://www.w3.org/2001/XMLSchema#string
Subject Organization ID	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xspa:1.0:subject:organization-id	http://www.w3.org/2001/XMLSchema#anyURI
Home Community ID (Note 1)	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:ihe:iti:xca:2010:homeCommunityId	http://www.w3.org/2001/XMLSchema#anyURI
National Provider Identifier (NPI)	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xspa:1.0:subject:npi	http://www.w3.org/2001/XMLSchema#string
Subject Role	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xacml:2.0:subject:role	http://www.w3.org/2001/XMLSchema#anyURI
Authz-Consent	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:ihe:iti:bppc:2007:docid	http://www.w3.org/2001/XMLSchema#anyURI
Patient Identifier	urn:oasis:names:tc:xacml:1.0:resource	urn:ihe:iti:ser:2016:patient-id	http://www.w3.org/2001/XMLSchema#string
PurposeOfUse	urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	http://www.w3.org/2001/XMLSchema#anyURI

Note 1: To enable authorization decisions for this [ITI-79] transaction, Home Community Id identifies the requesting user’s community identity as identified in the SAML header in [ITI-40]. I.E. it is not the homeCommunityId of the community where the requested document resides.

Any SAML 2.0 Attribute codified using the HL7 CD or CE dataType shall be codified into a XACML Attribute using the percentage urn encoding and DataType <http://www.w3.org/2001/XMLSchema#anyURI> as defined below:

```
"urn:ihe:iti:2014:ser:[codeSystem]:[codeSystemName]:[code]:[displayName]"
```

For example:

```
600 <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name=" urn:oasis:names:tc:xacml:2.0:action:purpose">
    <saml:AttributeValue>
605         <value xmlns="urn:hl7-org:v3" xsi:type="CD"
            code="RECORDMGT"
            displayName="records management"
            codeSystem="2.16.840.1.113883.1.11.20448"
            codeSystemName="Purpose of Use" />
610 </saml:AttributeValue>
    </saml:Attribute>
```

Shall be codified in a urn:

```
<Attribute AttributeId="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
    DataType="http://www.w3.org/2001/XMLSchema#anyURI">
615 <AttributeValue>urn:ihe:iti:2014:ser:2.16.840.1.113883.1.11.20448:Purpose%20
    f%20Use:RECORDMGT:records%20management</AttributeValue>
</Attribute>
```

620 Additional SAML 2.0 <Attribute> elements useful as authorization query parameters may be identified by domain policies. Any additional <Attribute> can be provided to the Authorization Decisions Verifier using a SAML v2.0 assertion. OASIS SAML 2.0 Profile of XACML Version 2.0, Section 2 provides guidance in mapping SAML attributes into XACML attributes. Domain Policies should define to which XACML category (Subject, Resource, Action or Environment) each additional Attribute belongs.

625 **3.79.4.1.2.1 Example of a SOAP v1.2 XACMLAuthorizationDecisionQuery Request message**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xsi:schemaLocation="http://www.w3.org/2003/05/soap-
envelope soap-envelope.xsd"
    xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xacml-
saml="urn:oasis:xacml:2.0:saml:assertion:schema:os">
    <soap:Header
        xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd"
        xmlns:wsa="http://www.w3.org/2005/08/addressing">
```



```

    <wsa:Action>urn:ihe:iti:2014:ser:XACMLAuthorizationDecisionQueryReq
uest</wsa:Action>
    <wsa:MessageID>urn:uuid:9376254e-da05-41f5-9af3-
ac56d63d8ebd</wsa:MessageID>
    <wsa:To>https://AuthorizationDecisionsManager</wsa:To>
  </soap:Header>
  <soap:Body
xsi:schemaLocation="urn:oasis:xacml:2.0:saml:assertion:schema:os
access_control-xacml-2.0-saml-assertion-schema-os.xsd">
    <xacml-sampl:XACMLAuthzDecisionQuery xmlns:xacml-
sampl="urn:oasis:xacml:2.0:saml:protocol:schema:os" xacml-
sampl:InputContextOnly="false" xacml-sampl:ReturnContext="false">
      <Request
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
        <!-- Requester Entity identifier -->
        <Subject>
          <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string">

            <AttributeValue>admin</AttributeValue>
          </Attribute>
        </Subject>
        <!-- DOC 1 -->
        <Resource>
          <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>documentID1</AttributeValue>
          </Attribute>
          <Attribute
            AttributeId="urn:ihe:iti:ser:2016:document-
entry:repository-unique-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI">>
            <AttributeValue>urn:oid:1.2.3.4.5</AttributeValue>
          </Attribute>
        </Resource>
        <!-- DOC 2 -->
        <Resource>
          <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>documentID2</AttributeValue>
          </Attribute>
          <Attribute
            AttributeId="urn:ihe:iti:ser:2016:document-
entry:repository-unique-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI">>

```

```

                                <AttributeValue>
urn:oid:1.2.3.4.5</AttributeValue>
                                </Attribute>
                                </Resource>
                                <!-- DOC 3 -->
                                <Resource>
                                    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                <AttributeValue>documentID3</AttributeValue>
                                </Attribute>
                                <Attribute
                                    AttributeId="urn:ihe:iti:ser:2016:document-
entry:repository-unique-id"
                                    DataType="http://www.w3.org/2001/XMLSchema#anyURI">>
                                <AttributeValue>
urn:oid:1.2.3.4.5</AttributeValue>
                                </Attribute>
                                </Resource>
                                <Action>
                                    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:action-id"
                                    DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                                <AttributeValue>urn:ihe:iti:2007:RetrieveDocumentSetResponse
                                </AttributeValue>
                                </Attribute>
                                </Action>
                                <Environment/>
                                </Request>
                                </xacml-samlp:XACMLAuthzDecisionQuery>
                                </soap:Body>
                                </soap:Envelope>

```

3.79.4.1.3 Expected Actions

- 630 When the Authorization Decisions Manager receives an XACMLAuthorizationDecisionQuery Request message, it evaluates each Authorization Request conveyed within the XACMLAuthorizationDecision (one for each <Resource> element). The Authorization Decisions Manager shall verify the existence of Authorization Decisions that match the XACML Query parameters:
- 635
- The Requester Entity identified within the XACMLAuthorizationDecisionQuery (<Subject>/<Attribute> element with @AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id") is an entity that has Authorization Decisions already granted;

AND

- 640
 - Among these authorizations, there is an authorization for each document identified within the XACMLAuthorizationDecisionQuery (<Resource>/<Attribute> elements with @AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" and "urn:ihe:iti:xds-b:2007:document-entry:repository-unique-id").

645 If other parameters (such as attributes taken from an [ITI-40] identity assertion) are specified within the XACMLAuthorizationDecisionQuery Request message and if domain policies require the creation of authorizations related to these parameters, then the Authorization Decisions Manager shall verify the match with these additional parameters (e.g., An authorization is created for document A for entity X acting for PurposeOfUse Y, the same entity cannot retrieve the documents acting for PurposeOfUse Z).

650 If authorization decisions that match the query parameters of the XACMLAuthorizationDecisionQuery Request message were not cached by the Authorization Decisions Manager, this actor can make a new access decision based on those query parameters.

655 The Authorization Decisions Manager shall produce a XACMLAuthorizationDecisionQuery Response message that conveys the results of this evaluation. One Result for each <Resource> shall be sent in the response message.

3.79.4.2 XACMLAuthorizationDecisionQuery Response

660 The XACMLAuthorizationDecisionQuery Response message is created by the Authorization Decisions Manager in response to the XACMLAuthorizationDecisionQuery Request. This message conveys to the Authorization Decisions Verifier the results of the evaluation made by the Authorization Decisions Manager. For each Resource (document) specified within the Request message, the Authorization Decisions Manager provides an Authorization Result, that shall be used by the Authorization Decisions Verifier / XDS Document Repository to determine which of the requested documents to return to the Document Consumer in response to the [ITI-43] Retrieve Document Set request, in accordance with local policies. This message relies on the XACML extension of SAML v2.0 protocol standard. Authorization Results are conveyed using an XACMLAuthzDecisionStatement.

3.79.4.2.1 Trigger Events

670 This message is created by the Authorization Decisions Manager after the evaluation of the XACML AuthorizationDecisionQuery Request message. The Authorization Decisions Manager identifies Authorization Decisions applicable to the Documents/Requester Entity and produces a result of the evaluation done.

3.79.4.2.2 Message Semantics

The XACMLAuthorizationDecisionQuery Response message is based on OASIS SAML 2.0 Profile of XACML Version 2.0. That profile relies on SAML v2.0 protocol standard.

675 The Addressing Action header of the SOAP message shall be:

urn:ihe:iti:2014:ser:XACMLAuthorizationDecisionQueryResponse

The XACMLAuthorizationStatement (defined in the OASIS SAML 2.0 Profile of XACML Version 2.0) is conveyed within a SAML v2.0 Assertion. The Assertion does not need to be signed. The SAML StatusCode of the Response message shall be
 680 urn:oasis:names:tc:SAML:2.0:status:Success.

The <Issuer> of the Authorization Assertion should identify the trusted Authorization Decisions Manager (SOAP endpoint of the Web Service).

See Section 3.1 of the OASIS SAML 2.0 Profile of XACML Version 2.0 document for further details on the message structure. As specified in the OASIS Multiple resource profile of
 685 XACML v2.0, the XACML <Response> element shall contain one <Result> element for each <Resource> element identified within the XACMLAuthorizationDecisionQuery Request message. Each <Result> element shall contain a @ResourceId attribute that identifies the <AttributeValue> value of the related resource.

As defined in the XACML v2.0 standard, there are four possible values associated with the
 690 <Decision>. The Authorization Decisions Manager shall associate codes to the result as described below:

- Permit: if a valid authorization decision exists allowing the disclosure of the requested document to the Requester Entity
- Deny: if no valid authorization decisions exist for the identified Document/Requester
 695 Entity, or if authorization decision does not allow disclosure of the Document to the Requester Entity
- Indeterminate: if the Authorization Decisions Manager cannot discover if authorization decisions are granted (e.g., Internal Errors, or DB unreachable for network problems, ...)
- NotApplicable: if access to the requested document is not managed by the Authorization
 700 Decisions Manager. If the Authorization Decisions Manager cannot determine if the Requester Entity can access the resource requested.

3.79.4.2.2.1 Example of a SOAP v1.2 XACMLAuthorizationDecisionQuery Response message

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xsi:schemaLocation="http://www.w3.org/2003/05/soap-envelope
soap-envelope.xsd"
  xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xacml-
saml="urn:oasis:xacml:2.0:saml:assertion:schema:os">
  <soap:Header xsi:schemaLocation="http://www.w3.org/2005/08/addressing
ws-addr.xsd"
    xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsa:Action>urn:ihe:iti:2014:XACMLAuthorizationDecisionQueryResponse</wsa:Ac
tion>
    <wsa:RelatesTo>urn:uuid:9376254e-da05-41f5-9af3-
```

```

ac56d63d8ebd</wsa:RelatesTo>
    <wsa:MessageID>urn:uuid:7534324t-mm56-45t5-6tg4-
gt56d63g6hym</wsa:MessageID>
    </soap:Header>
    <soap:Body xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol saml-
schema-protocol-2.0.xsd">
        <samlp:Response ID="a123456" Version="2.0" IssueInstant="2014-04-
16T14:53:55Z">
            <samlp:Status>
                <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
                <samlp:StatusMessage>OK</samlp:StatusMessage>
            </samlp:Status>
            <saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
                ID="a9812368" IssueInstant="2006-05-31T13:20:00.000">
                <saml:Issuer>https://XACMLPDP.example.com</saml:Issuer>
                <saml:Statement xsi:type="xacml-
saml:XACMLAuthzDecisionStatementType"
xsi:schemaLocation="urn:oasis:xacml:2.0:saml:assertion:schema:os
access_control-xacml-2.0-saml-assertion-schema-os.xsd"
                    xmlns:xacml-
saml="urn:oasis:xacml:2.0:saml:assertion:schema:os">
                        <Response
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                            <Result ResourceId="DocumentID1">
                                <Decision>Deny</Decision>
                            </Result>
                            <Result ResourceId="DocumentID2">
                                <Decision>Permit</Decision>
                            </Result>
                            <Result ResourceId="DocumentID3">
                                <Decision>Permit</Decision>
                            </Result>
                        </Response>
                    </saml:Statement>
                </saml:Assertion>
            </samlp:Response>
        </soap:Body>
    </soap:Envelope>

```

705

3.79.4.2.3 Expected Actions

When the Authorization Decisions Verifier receives a XACMLAuthorizationDecisionQuery Response, the XDS Document Repository shall enforce the decision results according to local policy.

- 710 If a Deny decision is returned, the XDS Document Repository shall not disclose the document, unless local policies allow it.
- If a Permit decision is returned, the XDS Document Repository shall disclose the document, unless additional local decisions are applied.
- 715 If NotApplicable or Indeterminate decisions are returned, local policies determine what action is appropriate for the XDS Document Repository to perform.
- If one or more of the requested documents are not authorized, then the Document Repository shall send a status `urn:ihe:iti:2007:ResponseStatusType:PartialSuccess` in the Retrieve Document Set Response message (see [ITI TF-2: 3.43.5](#)).
- 720 If all the requested documents are not authorized, then the Document Repository shall send a status `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure` in the Retrieve Document Set Response message (see [ITI TF-2: 3.43.5](#)).
- The XDS Document Repository shall generate an Error of type:
- DocumentAccessNotAuthorized

3.79.5 Security Considerations

- 725 Relevant Security Considerations are defined in ITI TF-1: 39.5. The Authorization Decisions Query transaction requires TLS communication between actors involved.
- This transaction mandates the creation of Authorizations associated at least with the Requester Entity and with the document requested. If additional parameters need to be associated to the authorization, then the same parameters shall be provided within the Authorization Decisions Query transaction.
- 730

3.79.5.1 Security Audit Considerations

Both the actors involved in the Authorization Decisions Query transaction are recommended to record the “Query” event creating audit messages in accordance to the following structure.

The audit message shall identify:

- 735
- The entity that requires authorization
 - The documents have been requested
 - The overall result of the Authorization processing

3.79.5.1.1 Authorization Decisions Verifier audit message

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110112, DCM, “Query”)
	EventActionCode	M	E = Execute
	EventDateTime	M	<i>not specialized</i>
	EventOutcomeIndicator	M	<i>not specialized</i>
	EventTypeCode	M	EV(“ITI-79”, “IHE Transactions”, “Authorization Decisions Query”)
Source (Authorization Decisions Verifier) (1)			
Destination (Authorization Decisions Verifier) (1)			
Query Parameters (1)			
Requester Entity (1)			
Authorization Result (1)			

740

Source: AuditMessage/ ActiveParticipant	UserID	U	<i>not specialized</i>
	AlternativeUserID	MC	the process ID as used within the local operating system in the local system of logs
	UserName	U	<i>not specialized</i>
	UserIsRequestor	U	<i>not specialized</i>
	RoleIDCode	M	EV (110153, DCM, “Source”)
	NetworkAccessPointTypeCode	U	“1” for machine (DNS) name “2” for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Authorization Decisions Manager SOAP URI
	AlternativeUserID	U	the process ID as used within the local operating system in the local system of logs
	UserName	U	<i>not specialized</i>
	UserIsRequestor	U	<i>not specialized</i>
	RoleIDCode	M	EV (110152, DCM, “Destination”)
	NetworkAccessPointTypeCode	U	“1” for machine (DNS) name “2” for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Requester Entity: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	“1” (person)
	ParticipantObjectTypeCodeRole	M	“11” (security user entity)
	ParticipantObjectDataLifeCycle	U	<i>not specialized</i>
	ParticipantObjectIDTypeCode	M	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	ParticipantObjectSensitivity	U	<i>not specialized</i>

	ParticipantObjectID	M	The Requester Entity who wants to retrieve documents (identified in the Attribute with AttributeId urn:oasis:names:tc:xacml:1.0:subject:subject-id)
	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectQuery</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

Query Parameters: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	“2” (SYSTEM)
	ParticipantObjectTypeCodeRole	M	“24” (query)
	<i>ParticipantObjectDataLifeCycle</i>	<i>U</i>	<i>not specialized</i>
	ParticipantObjectIDTypeCode	M	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	<i>ParticipantObjectSensitivity</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectID</i>	<i>M</i>	<i>not specialized</i>
	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	ParticipantObjectQuery	U	The <Request>, base 64 encoded
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

Authorization Result: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	“2” (SYSTEM)
	ParticipantObjectTypeCodeRole	M	“13” (security resource)
	<i>ParticipantObjectDataLifeCycle</i>	<i>U</i>	<i>not specialized</i>
	ParticipantObjectIDTypeCode	M	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	<i>ParticipantObjectSensitivity</i>	<i>U</i>	<i>not specialized</i>
	ParticipantObjectID	M	Content of StatusCode element (overall result of the authorization)
	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectQuery</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

745

3.79.5.1.2 Authorization Decisions Manager audit message

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110112, DCM, “Query”)
	EventActionCode	M	E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV(“ITI-79”, “IHE Transactions”, “Authorization Decisions Query”)
Source (Authorization Decisions Verifier) (1)			
Destination (Authorization Decisions Verifier) (1)			
Query Parameters (1)			
Requester Entity (1)			
Authorization Result (1)			

Source: AuditMessage/ ActiveParticipant	UserID	U	not specialized
	AlternativeUserID	MC	the process ID as used within the local operating system in the local system of logs
	UserName	U	not specialized
	UserIsRequestor	U	not specialized
	RoleIDCode	M	EV (110153, DCM, “Source”)
	NetworkAccessPointTypeCode	U	“1” for machine (DNS) name “2” for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Authorization Decisions Manager SOAP URI
	AlternativeUserID	U	the process ID as used within the local operating system in the local system of logs
	UserName	U	not specialized
	UserIsRequestor	U	not specialized
	RoleIDCode	M	EV (110152, DCM, “Destination”)
	NetworkAccessPointTypeCode	U	“1” for machine (DNS) name “2” for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

750

Requester Entity: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	“1” (person)
	ParticipantObjectTypeCodeRole	M	“11” (security user entity)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The person who wants to create retrieve documents (identified in the Attribute with AttributeID urn:oasis:names:tc:xacml:1.0:subject:subject-id)

	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectQuery</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

Query Parameters: AuditMessage/ ParticipantObjectIdentification (1)	<i>ParticipantObjectTypeCode</i>	<i>M</i>	“2” (SYSTEM)
	<i>ParticipantObjectTypeCodeRole</i>	<i>M</i>	“24” (query)
	<i>ParticipantObjectDataLifeCycle</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectIDTypeCode</i>	<i>M</i>	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	<i>ParticipantObjectSensitivity</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectID</i>	<i>M</i>	<i>not specialized</i>
	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectQuery</i>	<i>U</i>	The <Request>, base 64 encoded
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

Authorization Result: AuditMessage/ ParticipantObjectIdentification (1)	<i>ParticipantObjectTypeCode</i>	<i>M</i>	“2” (SYSTEM)
	<i>ParticipantObjectTypeCodeRole</i>	<i>M</i>	“13” (security resource)
	<i>ParticipantObjectDataLifeCycle</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectIDTypeCode</i>	<i>M</i>	EV(“ITI-79”, “IHE Transaction”, “Authorization Decisions Query”)
	<i>ParticipantObjectSensitivity</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectID</i>	<i>M</i>	Content of StatusCode element (overall result of the authorization)
	<i>ParticipantObjectName</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectQuery</i>	<i>U</i>	<i>not specialized</i>
	<i>ParticipantObjectDetail</i>	<i>U</i>	<i>not specialized</i>

3.79.5.2 Authorization Decisions Manager Specific Security Considerations

755 None

3.79.5.3 Authorization Decisions Verifier Specific Security Considerations

None

Volume 2 Namespace Additions

760 Add the following terms to the [IHE FormatCodes](#):

Urn namespace
urn:ihe:iti:ser:2016:document-entry:repository-unique-id
urn:ihe:iti:ser:2016:patient-id
urn:ihe:iti:2014:ser:XACMLAuthorizationDecisionQueryRequest

Volume 2 Appendices

765 Not applicable

770

Volume 3 – Content Modules

Add the following ErrorCode in [ITI TF-3: Table 4.2.4.1-2: Error Codes](#)

Error Code ¹	Discussion	Transaction (See Note 1)
DocumentAccessNotAuthorized	The document requested is not authorized to be disclosed to the Requester Entity	RS

775

Volume 4 – National Extensions

Not applicable