Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'interieur DFI

RS 816.111

Complément 2.1 à l'annexe 5 de l'ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient

Profils d'intégration nationaux selon l'art. 5, al. 1, let. c ODEP-DFI

Authorization Decision Request (CH:ADR) and Privacy Policy Query (CH:PPQ)

Complément 2.1 à l'annexe 5 ODEP-DFI : Adaptations nationales

Édition 5 : 4 mai 2023

Entrée en vigueur : 1er juin 2023

Table of contents

1 Introduction

Le présent document a été établi en application des règles suisses énoncées dans l'ordonnance sur le dossier électronique du patient (ODEP ; RS 816.11). L'ODEP et l'ODEP-DFI (RS 816.111) sont publiées dans le Recueil officiel (en français, allemand et italien)[1].

Le dossier électronique du patient (DEP) est un système composé de plusieurs communautés et communautés de référence utilisant un profil IHE XDS. Le patient non seulement donne son consentement à la création et à l'utilisation d'un dossier, mais il peut également, via le portail d'accès destiné aux patients, définir explicitement des droits d'accès et déterminer si les professionnels de la santé qui bénéficient d'un droit d'accès peuvent ou non déléguer ce droit à d'autres professionnels de la santé. Ces règles d'accès sont enregistrées au sein de la communauté de référence du patient.

Les acteurs IHE des communautés ou communautés de référence qui doivent appliquer ces droits d'accès (p. ex. registres des documents) doivent donc agir en tant que fournisseurs de services chargés d'appliquer les décisions (Policy Enforcing Service Providers) et implémenter un point d'application de la décision (Policy Enforcement Point, PEP), tel que défini par la spécification XACML. Ils doivent implémenter des interfaces pour consulter les décisions relatives aux accès émanant du point de décision de la politique (XACML Policy Decision Point, PDP) de la communauté de référence du patient.

La complexité et la flexibilité liées à la définition des droits d'accès que la loi garantit aux patients exigent que les portails d'accès destinés aux patients et ceux destinés aux professionnels de la santé fonctionnent comme des acteurs Policy Source et Policy Consumer des politiques CH:PPQ afin de pouvoir faire des ajouts, des requêtes, des mises à jour et des suppressions dans le point de stockage de ces politiques (Policy Repository), qui est un point d'administration de la politique (XACML Policy Administration Point, PAP). Le présent document décrit les normes d'interopérabilité pour l'administration et l'application des droits d'accès des patients.

The Swiss Electronic Patient Record (EPR) is a system with multiple IHE XDS-based (reference) communities, where the patient not only consents to the creation and usage of the EPR. The patient can also explicitly define access rules through the patient portal and specify whether healthcare professionals are allowed to delegate obtained permissions to other healthcare professionals. These access rules are stored in the patient's reference community.

IHE actors of the (reference) communities having to enforce these access policies (e.g., Document Registries) must therefore act as a Policy Enforcing Service Provider implementing an XACML Policy Enforcement Point (PEP). These actors may need to implement interfaces to request policy decisions from the XACML Policy Decision Point (PDP) of the patient's reference community.

The complexity and flexibility of access rule definitions that were granted to patients by law, require the patient portals and healthcare professional portals to act as CH:PPQ Policy Source and Consumer to add, query, update and delete policies in the CH:PPQ Policy Repository, an XACML Policy Administration Point (PAP). The interoperability standards to manage the patient's access rules and to enforce them, are specified in this document.

This document fulfils the Swiss regulations of the Ordinance on the Electronic Patient Record (EPRO, SR 816.11). The EPRO and the EPRO-FDHA (SR 816.111) are published in Official Compilation of Federal Legislation (available in German, French and Italian)[1].

[1] German: https://www.admin.ch/opc/de/classified-compilation/20111795/index.html; French: https://www.admin.ch/opc/fr/classified-compilation/20111795/index.html; Italian: https://www.admin.ch/opc/it/classified-compilation/20111795/index.html.

2 Volume 1 – Integration Profiles

2.1 Authorization Decision Request [CH:ADR]

According to Swiss EPR regulations, patients have the right to decide who is allowed to access and modify data in their EPR and under which circumstance (cf. emergency access).

The access restrictions concern following actors:

a. Document Registry;
b. Document Repository;
c. Restricted Metadata Update Responder;
d. Policy Repository;
e. Patient Audit Record Repository;
f. Imaging Document Source;

Each of them is grouped with an X-Service Provider, which means that they shall be able to

g. use the CH:XUA assertion obtained from the X Service User to determine whether the user who initiated the transaction is allowed to access the requested information stored in a patient's EPR;
h. and interpret (enforce) this decision.

Exactly this is the purpose of the Authorization Decision Request (CH:ADR) profile: it computes authorization decisions and defines how to enforce them for each particular request type.

CH:ADR constitutes an adaptation of the IHE Secure Retrieve (SeR) profile to EPR requirements, and uses the same technology stack: SAML 2.0 profile of XACML v2.0 as data format and Web Services according to IHE ITI TF 2[2] , Appendix V as transport protocol. The XACML data-flow model serves as the underlying processing model.

CH:ADR defines two actors and one transaction:

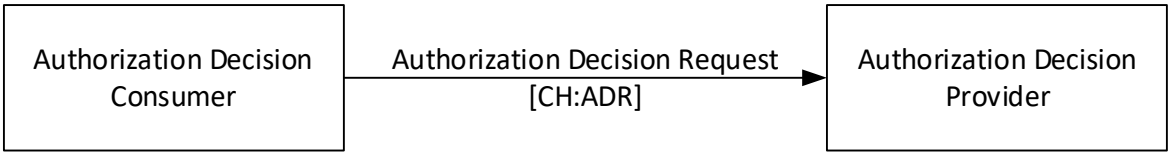

Figure 1: CH:ADR actor diagram

Actor:	Authorization Decision Provider
Role:	This actor computes authorization decisions
Actor:	Authorization Decision Consumer
Role:	This actor queries and enforces authorization decisions

Table 1: CH:ADR actors and roles

Table 2 lists the transactions for each actor directly involved in the CH:ADR Profile. To claim compliance with this profile, an actor shall support all required transactions (labeled "R") and may support the optional transactions (labeled "O").

Actors	Transactions	Optionality	Section
Authorization Decision Consumer	Authorization Decision Request [CH:ADR]	R	3.1
Authorization Decision Provider	Authorization Decision Request [CH:ADR]	R	3.1

Table 2: CH:ADR actors and transactions

[2] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

Besides privacy policies created by a patient, an essential role for making authorization decisions is played by the CH:XUA assertion provided by the requesting user. Therefore, an Authorization Decision Consumer MUST be able to obtain this assertion and forward it to the Authorization Decision Provider. This implies the groupings shown in Table 3:

Actors	Actor to be grouped with	Reference
`Authorization Decision Consumer`	X-Service User	Amendment 1 of Annex 5 EPRO-FDHA, Section 1.6
`Authorization Decision Provider`	X-Service Provider	Amendment 1 of Annex 5 EPRO-FDHA, Section 1.6

Table 3: CH:ADR required actors groupings

The actors “Authorization Decision Consumer” and “Authorization Decision Provider” can be seen as EPR-specific implementations respectively of Policy Enforcement Point (PEP) and Policy Decision Point (PDP) as defined in the XACML specification. The Policy Repository acts as an XACML Policy Administration Point (PAP). The Authorization Decision Provider MAY use the CH:PPQ profile or any other mechanism to retrieve policies from the Policy Repository.

Privacy policies of a patient are stored only in the reference community of this patient. Therefore, if the community where the Authorization Decision Consumer operates is not the reference community of the patient whose EPR the user wants to access, then the Authorization Decision Consumer SHALL query Authorization Decision Providers of other communities until one of them turns out to be the patient’s reference community.

The following actors are grouped with both X-Service Provider and Authorization Decision Consumer, and therefore called “Policy Enforcing Service Providers”:

i. XDS Document Registry;
j. CH:PPQ Policy Repository;
k. CH:ATC Patient Audit Record Repository;
l. RMU Update Responder.

All other actors grouped with X-Service Provider use indirect mechanisms to obtain authorization decisions whenever necessary – for example, by issuing a Registry Stored Query and in this way delegating the Authorization Decision Consumer function to the Document Registry. In other words, every Authorization Decision Consumer is an X-Service Provider, but not every X-Service Provider is an Authorization Decision Consumer. The figure below shows the correspondence between these actors, see also section 3.1.7 for details.

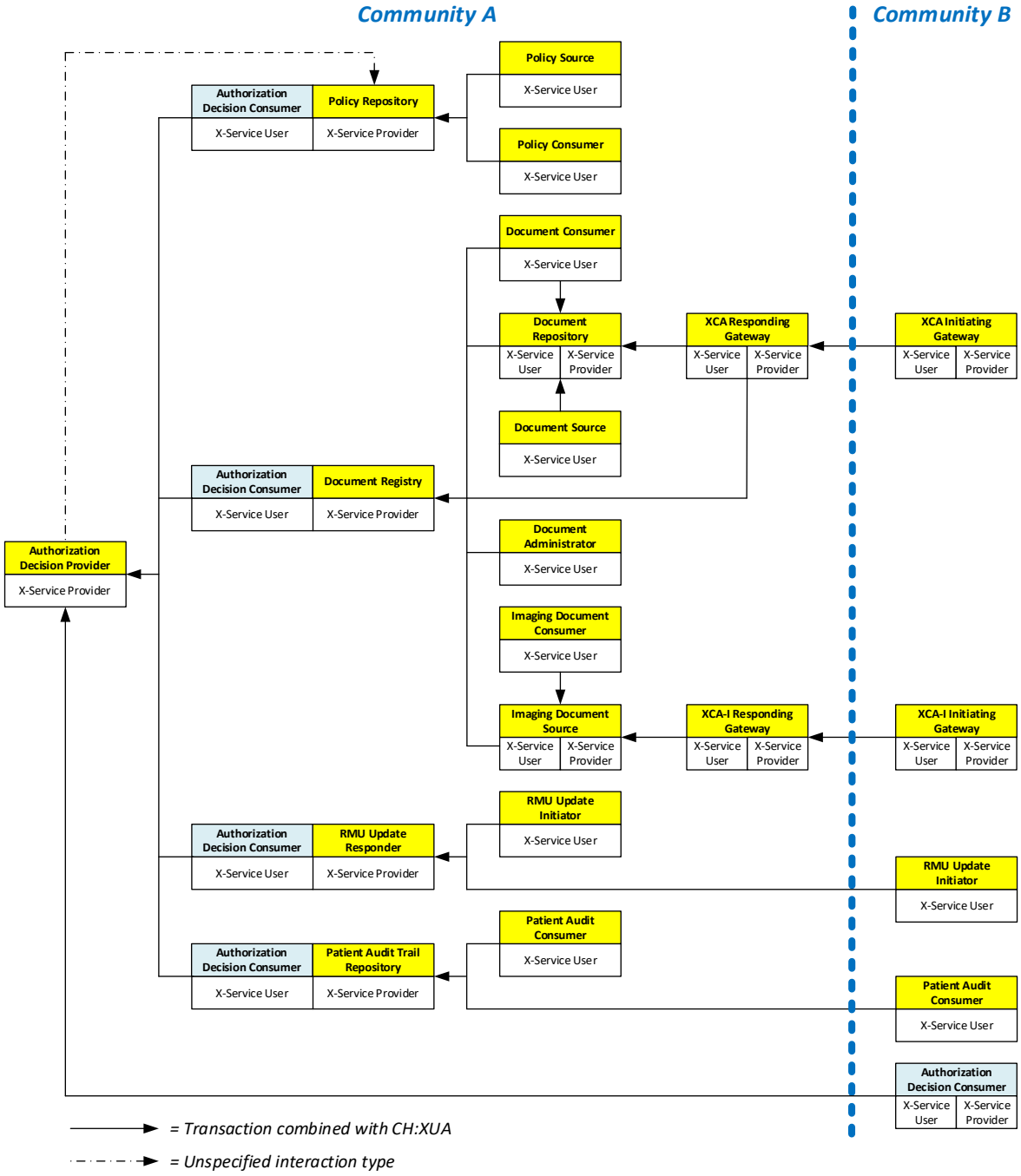

Figure 2: Correspondence between Authorization Decision Consumers and X-Service Providers

2.2 Privacy Policy Query [CH:PPQ]

According to Swiss EPR regulations, patients have the right to decide who is allowed to access and modify data in their EPR and under which circumstance (cf. emergency access). The reference community of the patient is responsible for storing and considering these decisions.

For that, the EPR specifications prescribe to use XACML 2.0 format, and define the Policy Repository as an XACML Policy Administration Point (PAP) that holds privacy policies of patients onboarded in the given reference community. Each reference community provides a patient portal that allows patients to manage their privacy policies[3].

The Privacy Policy Query (CH:PPQ) profile defines a programmatic interface to the Policy Repository. Its transactions allow to add, query, update, and delete XACML policies and policy sets. In that

[3] XACML distinguishes between "policies" and "policy sets". In the given document, the both will be referred to as "policies", unless explicitly stated otherwise.

way, this profile is somehow similar to XDS, but operates on another storage and another type of information. Same as XDS, CH:PPQ mandates the usage of CH:XUA.

CH:PPQ defines three actors and two transactions between them:

Figure 3: Privacy Policy Query (CH:PPQ) actor diagram

While the Policy Repository constitutes a specific implementation of a XACML Policy Administration Point (PAP), for the two other actors there is no correspondence in XACML. In this way, the Policy Source and Policy Consumer are introduced as entirely new actors.

The transactions between the profile's actors use SAML 2.0 profile of XACML v2.0 with EPR-specific extensions as data format and Web Services according to IHE ITI TF 2, Appendix V as transport protocol.

Actor:	Policy Repository
Role:	This actor stores policies and policy sets and provides the possibility to add, query, update and delete them
Actor:	Policy Source
Role:	This actor initiates addition, update and deletion of policies and policy sets
Actor:	Policy Consumer
Role:	This actor queries policies and policy sets

Table 4: CH:PPQ actors and roles

Table 5 lists the transactions for each actor directly involved in the CH:PPQ Profile. To claim compliance with this profile, an actor shall support all required transactions (labeled "R") and may support the optional transactions (labeled "O").

Actors	Transactions	Optionality	Section
`Policy Source`	Privacy Policy Feed [CH:PPQ-1]	R	3.2
`Policy Repository`	Privacy Policy Feed [CH:PPQ-1]	R	3.2
	Privacy Policy Retrieve [CH:PPQ-2]	R	3.3
`Policy Consumer`	Privacy Policy Retrieve [CH:PPQ-2]	R	3.3

Table 5: CH:PPQ actors and transactions

Actors	Actor to be grouped with	Reference
`Policy Source`	X-Service User	Amendment 1 of Annex 5 EPRO-FDHA, Section 1.6
`Policy Repository`	X-Service Provider	Amendment 1 of Annex 5 EPRO-FDHA, Section 1.6
	Authorization Decision Consumer	Amendment 2.1 of Annex 5 EPRO-FDHA, Section 2.1
`Policy Consumer`	X-Service User	Amendment 1 of Annex 5 EPRO-FDHA, Section 1.6

Table 6: CH:PPQ required actor groupings

Rules on authoring policies and policy sets are given in section 4.

3 Volume 2 – Transactions

3.1 Authorization Decision Request [CH:ADR]

3.1.1 Scope

This transaction is used by the Authorization Decision Consumer to query for authorization decisions, computed by the Authorization Decision Provider.

This transaction is based on synchronous Web services as described in IHE ITI TF-2[4], Appendix V.

3.1.2 Referenced Standards

a. IHE ITI TF-2[4], Appendix V "Web Services for IHE transactions" https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html

b. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

c. The home page of the "OASIS eXtensible Access Control Markup Language" technical committee: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml references all XACML related protocols and specifications for implementers of this profile.

I. OASIS Multiple Resource Profile of XACML v2.0

II. https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-mult-profile-spec-os.pdf

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

IV. https://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html

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

VI. (Original: https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf) Please be aware of the errata of the specification document as published on the XACML technical committee home page:

VII. **Errata**: http://www.oasis-open.org/committees/download.php/24548/access_control-xacml-2.0-core-spec-os-errata.zip (spec and schema)

VIII. OASIS SAML 2.0 profile of XACML v2.0

IX. (Original: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf) Please be aware of the errata of the specification document as published on the XACML technical committee home page:

X. **Errata**: www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf

3.1.3 XML Namespaces

In addition to XML namespaces defined in IHE ITI TF-2[5], Appendix V.2.4, the following namespaces and namespace prefixes will be used in message definitions:

Prefix	Namespace	Specification
saml	urn:oasis:names:tc:SAML:2.0:assertion	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
samlp	urn:oasis:names:tc:SAML:2.0:protocol	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
xacml-context	urn:oasis:names:tc:xacml:2.0:context:schema:os	OASIS eXtensible Access Control Markup Language (XACML) v2.0

[4] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022
[5] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022

Prefix	Namespace	Specification
xacml-saml	urn:oasis:names:tc:xacml:2.0: profile:saml2.0:v2:schema:assertion	OASIS SAML 2.0 profile of XACML v2.0
xacml-samlp	urn:oasis:names:tc:xacml:2.0: profile:saml2.0:v2:schema:protocol	OASIS SAML 2.0 profile of XACML v2.0

Table 7: Trigger events of CH:ADR request

3.1.4 Interaction Diagram

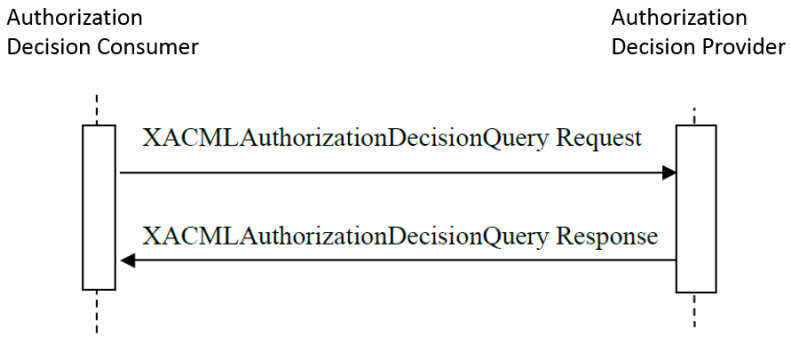

Figure 4: Sequence diagram of the CH:ADR transaction of the CH:ADR profile

3.1.5 CH:ADR Request

Authorization Decision Consumer uses this message to query the Authorization Decision Provider for authorization decisions. The request is an XML document compliant to the SAML v2.0 profile for XACML, and contains information about which Subject (user) wants to perform which Action on which Resources. Multiple resources MAY be referenced in a single request as defined in the Multiple Resource Profile of XACML v2.0.

3.1.5.1 Trigger Events

The Authorization Decision Consumer sends this message when it receives a request from an X-Service User and needs to determine whether the requesting user is allowed to access the requested resources. The trigger events are summarized in Table 8:

Trigger Event	Transaction	Client (X-Service User)	Policy Enforcing Service Provider
XDS	Registry Stored Query [ITI-18]	Document Consumer[6]	Document Registry
	Register Document Set-b [ITI-42]	Document Repository[7]	
	Update Document Set [ITI-57]	Document Administrator	
CH:ATC	Retrieve ATNA Audit Event [ITI-81]	Patient Audit Consumer	Patient Audit Record Repository
RMU	Restricted Update Document Set [ITI-92]	Update Initiator	Update Responder
CH:PPQ	Privacy Policy Feed [CH:PPQ-1]	Policy Source	Policy Repository
	Privacy Policy Retrieve [CH:PPQ-2]	Policy Consumer	

Table 8: Trigger events of CH:ADR request

[6] As Document Repositories and Imaging Document Sources are not grouped with an Authorization Decision Consumer, they use this transaction to indirectly query authorization decisions on data retrieval requests Retrieve Document Set [ITI-43] and Retrieve Imaging Document Set [RAD-69].

[7] As Document Repositories are not grouped with an Authorization Decision Consumer, they use this transaction to indirectly query authorization decisions on data submission requests Provide and Register Document Set-b [ITI-41] and Provide & Register Imaging Document Set – MTOM/XOP [RAD-68].

3.1.5.2 Message Semantics

The CH:ADR request message SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[8], Appendix V "Web Services for IHE Transaction".

The WS-Addressing header <wsa:Action> SHALL contain the value

```
urn:e-health-suisse:2015:policy-enforcement:AuthorizationDecisionRe-
quest
```

The WS-Security header <wse:Security> SHALL contain a CH:XUA assertion.

The SOAP body SHALL contain a single element <xacml-samlp:XACMLAuthzDecisionQuery> with the following attributes:

a. @ReturnContext SHOULD be set to "false", because the content of the CH:ADR request is not needed within the Authorization Result.

b. @InputContextOnly SHALL be set to "false", as the Authorization Decision Provider may have further information and rules, other than the parameters included in the request, to determine a decision. This should not be restricted by the Authorization Decision Consumer.

CH:ADR does not define further constraints for other attributes of this element (see OASIS SAML 2.0 profile of XACML v2.0 for details).

The only child element of <xacml-samlp:XACMLAuthzDecisionQuery> SHALL be <xacml-context:Request> containing the following elements:

c. Exactly one element <xacml-context:Subject>;

d. One or more elements <xacml-context:Resource>;

e. Exactly one element <xacml-context:Action>;

f. Exactly one element <xacml-context:Environment>.

Their contents will be described in separate sub-sections below, but they have in common that they all represent lists of child elements <xacml-context:Attribute>. Each of those child elements is characterized by XML attributes @AttributeId and @DataType, and carries values in elements <xacml-context:AttributeValue>.

In each case, only required contents (i.e. required elements <xacml-context:Attribute>) will be described; Authorization Decision Consumers MAY provide any additional contents, Authorization Decision Providers MAY process or ignore them.

3.1.5.2.1 Element <xacml-context:Subject>

This element identifies the requesting user. Its contents do not depend on the trigger event and represent a mapping of the CH:XUA assertion.

The following child elements <xacml-context:Attribute> SHALL be provided:

[8] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022

@AttributeId	@DataType	Contents of <xacml-context:AttributeValue>
urn:oasis:names:tc:xacml:1.0:subject:subject-id	http://www.w3.org/2001/XMLSchema#string	Text contents of the CH:XUA assertion element `/Assertion/Subject/NameID`
urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier	http://www.w3.org/2001/XMLSchema#string	Contents of the CH:XUA assertion attribute `/Assertion/Subject/NameID /@NameQualifier`
urn:ihe:iti:xca:2010:homeCommunityId	http://www.w3.org/2001/XMLSchema#anyURI	Text contents of the CH:XUA assertion element `/Assertion/AttributeStatement /Attribute[@name="urn:ihe:iti:xca:2010:homeCommunityId"] /AttributeValue`
urn:oasis:names:tc:xacml:2.0:subject:role	urn:hl7-org:v3#CV	Element `<hl7:CodedValue>` with all attributes (except @xsi:type) copied from the CH:XUA assertion element `/Assertion/AttributeStatement /Attribute[@name="urn:oasis:names:tc:xacml:2.0:subject:role"] /AttributeValue/hl7:Role`
urn:oasis:names:tc:xspa:1.0:subject:organization-id	http://www.w3.org/2001/XMLSchema#anyURI	Text contents of the CH:XUA assertion element `/Assertion/AttributeStatement /Attribute[@name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"]/AttributeValue` As there can be multiple organization IDs in a CH:XUA assertion, implementers SHALL map them either to separate elements `<xacml-context:Attribute>` with the same @AttributeId, or to multiple repetitions of `<xacml-context:AttributeValue>` in the same single `<xacml-context:Attribute>`.
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	urn:hl7-org:v3#CV	Element `<hl7:CodedValue>` with all attributes (except @xsi:type) copied from the CH:XUA assertion element `/Assertion/AttributeStatement /Attribute[@name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"] /AttributeValue/hl7:PurposeOfUse`

Table 9: Required attributes of the element <xacml-context:Subject>

3.1.5.2.2 Element <xacml-context:Resource>

This element depends on the trigger event (section 3.1.5.1) and identifies a particular object (for trigger events CH:PPQ and CH:ATC) or a class of objects (trigger events XDS and RMU) to which the requesting user tries to access.

3.1.5.2.2.1 Trigger event CH:PPQ

For the trigger event CH:PPQ, a separate repetition of the element <xacml-context:Resource> SHALL be provided for each policy or policy set being tried to be created, updated, read or deleted in a CH:PPQ request.

In each repetition, the following child elements <xacml-context:Attribute> SHALL be provided:

@AttributeId	@DataType	Contents of <xacml-context:AttributeValue>
urn:oasis:names: tc:xacml:1.0: resource:resource-id	http://www.w3.org/2001/ XMLSchema#anyURI	ID of the policy or policy set being tried to be created, updated, read or deleted
urn:e-health-suisse: 2015:epr-spid	urn:hl7-org:v3#II	Element `<hl7:InstanceIdentifier>` with attribute `@root` equal to the field CX.4.2 and attribute `@extension` equal to the field CX.1 of the CH:XUA assertion element `/Assertion /AttributeStatement/Attribute [@name="urn:oasis:names:tc:xacml: 2.0:resource:resource-id"] /AttributeValue`
urn:e-health-suisse:2015: policy-attributes: referenced-policy-set	http://www.w3.org/2001/ XMLSchema#anyURI	ID of the policy or policy set referenced from the Policy Set being tried to be queried, added, updated or deleted. It is used in particular to ensure that a healthcare professional can only delegate access rights which do not exceed his own access level granted by the patient. Example: A user tries to add a policy set with ID c969c7cd-9fe9-4fdc-83c5-a7b5118922a3 (as in Resource attribute with @AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id") that puts a healthcare professional onto exclusion list, i.e. this policy set contains a reference to the policy set with the ID "urn:e-health-suisse:2015: policies:exclusion-list". That is the value to be populated in the Resource attribute with @AttributeId="urn:e-health-suisse:2015:policy-attributes:referenced-policy-set".

Table 10: Required attributes of the element <xacml-context:Resource> for the trigger event CH:PPQ

3.1.5.2.2.2 Trigger events XDS and RMU

For the trigger events XDS and RMU, exactly three repetitions of the element <xacml-context:Resource> SHALL be provided — one for each possible confidentiality level of documents in EPR (normal, restricted, secret).

In each repetition, the following child elements <xacml-context:Attribute> SHALL be provided:

@AttributeId	@DataType	Contents of <xacml-context:AttributeValue>
urn:oasis:names:tc: xacml:1.0:resource: resource-id	http://www.w3.org/2001/ XMLSchema#anyURI	A string of the form "urn:e-health-suisse:2015:epr-subset: <epr-spid>:<conf-level>", where: • <epd-spid> is the EPR-SPID of the patient, • <conf-level> is the confidentiality level name corresponding to the given repetition of <xacml-context:Resource>, i.e. "normal", "restricted", or "secret". For example, for a patient with the EPR-SPID "8901", <xacml-context:Resource> repetitions with the following attribute values will have to be provided: • urn:e-health-suisse:2015:epr-subset: 8901:normal • urn:e-health-suisse:2015:epr-subset: 8901:restricted • urn:e-health-suisse:2015:epr-subset: 8901:secret

@AttributeId	@DataType	Contents of <xacml-context:AttributeValue>
urn:e-health-suisse: 2015:epr-spid	urn:hl7-org:v3#II	Element `<hl7:InstanceIdentifier>` with attribute `@root` equal to the field CX.4.2 and attribute `@extension` equal to the field CX.1 of the CH:XUA assertion element `/Assertion /AttributeStatement/Attribute [@name="urn:oasis:names:tc:xacml: 2.0:resource:resource-id"] /AttributeValue`
urn:ihe:iti:xds-b: 2007: confidentiality-code	urn:hl7-org:v3#CV	Confidentiality level code corresponding to the given repetition of <xacml-context:Resource>, in HL7v3 Coded Value format, e.g.: `<hl7:CodedValue code="17621005" codeSystem= "2.16.840.1.113883.6.96" displayName="normal"/>`
urn:ihe:iti:xca:2010: homeCommunityId	http://www.w3.org/2001/ XMLSchema#anyURI	OID of the Authorization Decision Consumer's community in the URN format

Table 11: Required attributes of the element <xacml-context:Resource> for the trigger events XDS and RMU

3.1.5.2.2.3 Trigger event CH:ATC

For the trigger event CH:ATC, exactly one repetition of the element <xacml-context:Resource> SHALL be provided.

The following child elements <xacml-context:Attribute> SHALL be provided:

@AttributeId	@DataType	Contents of <xacml-context:AttributeValue>
urn:oasis:names:tc: xacml:1.0:resource: resource-id	http://www.w3.org/2001/ XMLSchema#anyURI	A string of the form "urn:e-health-suisse:2015:epr-subset: <epr-spid>:patient-audit-trail-records", where <epd-spid> is the EPR-SPID of the patient specified in the query parameter "entity-id". For example, for a patient with the EPR-SPID "8901", the following value will be created: • urn:e-health-suisse:2015:epr-subset: 8901:patient-audit-trail-records
urn:e-health-suisse: 2015:epr-spid	urn:hl7-org:v3#II	Element `<hl7:InstanceIdentifier>` with attribute `@root` equal to the field CX.4.2 and attribute `@extension` equal to the field CX.1 of the CH:XUA assertion element `/Assertion /AttributeStatement/Attribute [@name="urn:oasis:names:tc:xacml: 2.0:resource:resource-id"] /AttributeValue`

Table 12: Required attributes of the element <xacml-context:Resource> for the trigger event CH:ATC

3.1.5.2.3 Element <xacml-context:Action>

This element identifies the action the requesting user tries to perform.

The following child element <xacml-context:Attribute> SHALL be provided:

a. @AttributeId: fixed value "urn:oasis:names:tc:xacml:1.0:action:action-id"

b. @DataType: fixed value "http://www.w3.org/2001/XMLSchema#anyURI"

c. Contents of <xacml-context:AttributeValue>: fixed value depending from the trigger transaction (see **Fehler! Verweisquelle konnte nicht gefunden werden.Fehler! Verweisquelle konnte nicht gefunden werden.**):

   I. For ITI-18 – urn:ihe:iti:2007:RegistryStoredQuery

   II. For ITI-42 – urn:ihe:iti:2007:RegisterDocumentSet-b

   III. For ITI-57 – urn:ihe:iti:2010:UpdateDocumentSet

IV. For ITI-81 – urn:e-health-suisse:2015:patient-audit-administration:RetrieveAtnaAudit

V. For ITI-92 – urn:ihe:iti:2018:RestrictedUpdateDocumentSet

VI. For PPQ-1 – one of:

- urn:e-health-suisse:2015:policy-administration:AddPolicy
- urn:e-health-suisse:2015:policy-administration:UpdatePolicy
- urn:e-health-suisse:2015:policy-administration:DeletePolicy

VII. For PPQ-2 – urn:e-health-suisse:2015:policy-administration:PolicyQuery

3.1.5.2.4 Element <xacml-context:Environment>

The EPR does not specify any required attributes in the element <xacml-context:Environment> within <xacml-samlp:XACMLAuthzDecisionQuery>. Therefore this child element MAY be empty. The Authorization Decision Provider MAY process or ignore any provided attributes.

3.1.5.3 Expected Actions

The Authorization Decision Provider SHALL compute and return Authorization Decisions that match the XACML Query parameters according to the rules defined in XACML policies.

The Authorization Decision Provider SHALL create a CH:ADR response message that conveys the results of the evaluation of the patient's privacy policies against the request. One result for each Resource SHALL be included in the response message.

3.1.6 CH:ADR Response

The CH:ADR response message is created by the Authorization Decision Provider in response to the CH:ADR request. This message conveys to the Authorization Decision Consumer the results of the evaluation made by the Authorization Decision Provider. For each Resource specified within the re-quest message, the Authorization Decision Provider provides an Authorization Decision that SHALL be used by the Authorization Decision Consumer to determine which of the requested objects are to be returned or transactions to be allowed in response to the corresponding trigger transactions.

3.1.6.1 Trigger Events

This message is created by the Authorization Decision Provider after the evaluation of the CH:ADR request message. The Authorization Decision Provider MUST only return Authorization Decisions applicable to the request.

3.1.6.2 Message Semantics

The CH:ADR response message SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[9], Appendix V "Web Services for IHE Transaction".

The WS-Addressing header <wsa:Action> SHALL contain the value

```
urn:e-health-suisse:2015:policy-enforcement:XACMLAuthzDecisionResponse
```

The body of the SOAP message SHALL contain a single element <samlp:Response**>**, which SHALL contain a single element <samlp:Status> and a single element <saml:Assertion>:

The element <samlp:Status> contains a single element <samlp:StatusCode>, whose attribute @Value SHALL be set as follows:

a. If status codes of all decisions are "urn:e-health-suisse:2015:error:not-holder-of-patient-policies" (see below), @Value SHALL equal to "urn:e-health-suisse:2015:error:not-holder-of-patient-policies".

[9] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

b. Otherwise, @Value SHALL be set as defined in section 4.10 “Element <samlp:Response>: XACMLAuthzDecision Response” of OASIS SAML 2.0 profile of XACML v2.0 (errata).

The assertion in <saml:Assertion> SHALL contain following elements:

c. Exactly one element <saml:Issuer> SHALL identify the Authorization Decision Provider by containing the home community ID of its community encoded as an URN and an XML attribute @NameQualifier equal to "urn:e-health-suisse:community-index".

d. Exactly one element <saml:Statement> of the type “xacml-saml:XACMLAuthzDecisionStatementType” with a single element <xacml-context:Response>.

As specified in the OASIS multiple resource profile of XACML v2.0, the <xacml-context:Response> element SHALL contain an element <xacml-context:Result> for each element <xacml-context:Resource> contained within the CH:ADR request message.

Contents of <xacml-context:Result> are the following:

e. Attribute @ResourceId SHALL contain the resource ID of the corresponding <xacml-context:Resource> (provided there in the element <xacml-context:Attribute> with @AttributeId equal to “urn:oasis:names:tc: xacml:1.0:resource:resource-id”).

f. Child element <xacml-context:Decision> SHALL hold the actual decision code, i.e. one of:

I. “Permit”: if the evaluation was successful and the Subject is authorized to perform the Action on the Resource;

II. “Deny”: if the evaluation was successful and the Subject is explicitly prohibited to perform the Action on the Resource.

III. “NotApplicable”: if the evaluation was successful, but the Subject is neither explicitly authorized nor explicitly prohibited to perform the Action on the Resource.

IV. “Indeterminate”: either the evaluation of policies failed, or the policies are not available because the community of the Authorization Decision Provider is not the reference community of the given patient.

g. Child element <xacml-context:Status> SHALL contain a element <xacml-context:StatusCode>, whose attribute @Value SHALL be set as follows:

I. When policies are not available because the community of the Authorization Decision Provider is not the reference community of the given patient, @Value SHALL equal to “urn:e-health-suisse:2015:error:not-holder-of-patient-policies”.

II. Otherwise, @Value SHALL be set as defined in section B.9 “Status Codes” of OASIS eXtensible Access Control Markup Language (XACML) v2.0.

Other elements of <xacml-context:Status> MAY be optionally provided as well.

3.1.6.3 Expected Actions

On receiving a CH:ADR response message, the Policy Enforcing Service Provider SHALL enforce the decision as described below.

Note that Registry Stored Query [ITI-18] and Privacy Policy Retrieve [CH:PPQ-2] are the only transactions allowing partial success; all others obey the principle of atomicity (“all or nothing”).

If the decision is “Deny” or “NotApplicable”:

Transaction	Effect
ITI-18	XDS Document Registry SHALL NOT disclose in the Registry Stored Query [ITI-18] response document entries with the confidentiality code for which such a decision was returned.
ITI-42	XDS Document Registry SHALL reject the whole request containing a document entry with the confidentiality code for which such a decision was returned, and return an error message to the XDS Document Repository in response to Register Document Set-b [ITI-42].
ITI-57 ITI-92	If the request references a document entry, whose confidentiality code stored in the Document Registry (i.e. the current value and not the possibly different new value specified in

	the given metadata update request) is the one for which such a decision was returned, then the XDS Document Registry/RMU Update Responder SHALL reject the whole request, and return an error message to the XDS Document Administrator/RMU Update Initiator in response to Update Document Set [ITI-57] or Restricted Update Document Set [ITI-92].
ITI-81	CH:ATC Patient Audit Record repository SHALL NOT disclose the related patient audit records in the Retrieve ATNA Audit Event [ITI-81] response.
PPQ-1	Policy Repository SHALL reject the whole request containing (for AddPolicy and UpdatePolicy) or referencing (for DeletePolicy) a policy or policy set for which such a decision was returned, and return an error message to the Policy Source in the Privacy Policy Feed [CH:PPQ-1] response.
PPQ-2	CH:PPQ Policy Repository SHALL NOT disclose in Privacy Policy Retrieve [CH:PPQ 2] response policies and policy sets for which such a decision was returned.

Table 13: Effects of the authorization decisions "Deny" and "NotApplicable"

If the decision is “Permit”:

Transaction	Effect
ITI-18	XDS Document Registry SHALL disclose in the Registry Stored Query [ITI-18] response the following objects (depending on the stored query type): a) document entries with the confidentiality code for which such a decision was returned, if they reference in the attribute “DocumentEntry.patientId” the same patient as the CH:XUA assertion does; b) submission sets, if they reference in the attribute “SubmissionSet.patientId” the same patient as the CH:XUA assertion does; c) associations that relate to at least one object from subsets a) or b); d) references to objects from subsets a), b), and c).
ITI-42	XDS Document Registry SHALL process the request if the decision Permit was retuned for all confidentiality codes occurring in contained document entries and at the same time the attribute “SubmissionSet.patientId” references the same patient as the CH:XUA assertion does.
ITI-57 ITI-92	XDS Document Registry/RMU Update Responder SHALL process the request if the decision Permit was retuned for all current confidentiality codes of the document entries referenced in the request and at the same time the attribute “SubmissionSet.patientId” references the same patient as the CH:XUA assertion does.
ITI-81	CH:ATC Patient Audit Record repository SHALL disclose related patient audit records in the Retrieve ATNA Audit Event [ITI-81] response, if they reference in the element “Patient” the same patient as the CH:XUA assertion does.
PPQ-1	CH:PPQ Policy Repository SHALL process the request if the decision Permit was returned for all policy sets contained (for AddPolicy and UpdatePolicy) or referenced (for DeletePolicy) in the request and all these policy sets reference in the element “Resource” the same patient as the CH:XUA assertion does.
PPQ-2	CH:PPQ Policy Repository SHALL disclose in Privacy Policy Retrieve [CH:PPQ-2] response policies and policy sets for which such a decision was returned and which at the same time either do not reference any patient in the element “Resource” or reference the same patient as the CH:XUA assertion does.

Table 14: Effects of the authorization decision "Permit"

If the decision is “Indeterminate”:

Transaction	Effect
ITI-18 ITI-42 ITI-57 ITI-81 ITI-92	The Authorization Decision Consumer SHALL query Authorization Decision Providers of other communities (as listed in the Community Portal Index (CPI)), until a response contains a decision code other than Indeterminate. If all available Authorization Decision Providers return the decision “Indeterminate”, then the Authorization Decision Consumer SHALL apply the same rules as if the decision were “Deny”.
PPQ-1 PPQ-2	CH:PPQ Policy Repository SHALL apply the same rules as if the decision were “Deny”.

Table 15: Effects of the authorization decision "Deny"

3.1.7 Indirect decision queries

3.1.7.1 Decision querying and enforcement for Retrieve Document Set [ITI-43]

To determine whether the requesting user is allowed to retrieve documents referenced in an Retrieve Document Set [ITI-43] request, the XDS Document Repository SHALL create for each of these documents an Registry Stored Query [ITI-18] of the type “GetDocuments” with the parameter “returnType” set to “ObjectRef”, and send this query to the XDS Document Registry along with the CH:XUA assertion obtained from the XDS Document Consumer.

If the corresponding Registry Stored Query response contains the entryUUID of the document, then the document SHALL be supplied to the Document Consumer. If the corresponding Registry Query Response does not contain the entryUUID of the document, then the document SHALL NOT be supplied to the Document Consumer.

3.1.7.2 Decision querying and enforcement for Retrieve Imaging Document Set [RAD-69]

The Retrieve of images SHALL be enforced according to the access rights formulated by the patient.

If a Retrieve Imaging Document Set [RAD-69] request addresses a DICOM object, and the CH:XUA token contained in the request references a user and a patient, the DICOM object SHALL be delivered to the user only if the repositories of the community contain a KOS object which references the study instance id and the user is authorized to access the KOS object.

The Imaging Document Source actor SHALL perform the following steps when processing each element “StudyRequest” of a Retrieve Imaging Document Set [RAD-69] request:

In the XDS infrastructure:

a. Query the XDS metadata of KOS objects of the DICOM study by sending a Registry Stored Query [ITI-18] of type “FindDocumentsByReferenceId” with the following parameters:
   I. $XDSDocumentEntryPatientId: MPI-PID of the patient.
   II. $XDSDocumentEntryStatus: fixed value “urn:oasis:names:tc:ebxml-regrep:StatusType:Approved”.
   III. $XDSDocumentEntryFormatCode: fixed value “1.2.840.10008.5.1.4.1.1.88.59^^1.2.840.10008.2.6.1” (format code of KOS objects according to section 2.3 annex 3, in the HL7v2 CE format).
   IV. $XDSDocumentEntryReferenceIdList: StudyInstanceUID in the CXi format, e.g. “2.16.5.4.3.2.1.0^^^^urn:ihe:iti:xds: 2016:studyInstanceUID”.
b. The CH:XUA token contained in the original Retrieve Imaging Document Set [RAD-69] request SHALL be used for this query.
c. This query may return metadata of more than one KOS object. If no KOS objects have been found, then no DICOM contents SHALL be returned.
d. Retrieve the contents of the found KOS objects by sending a Retrieve Document Set [ITI-43] query. The CH:XUA token contained in the original Retrieve Imaging Document Set [RAD-69] request SHALL be used for this query.
e. Match the DICOM object references in the KOS object and in the Retrieve Imaging Document Set [RAD-69] request. DICOM objects not referenced in both, the KOS object and the Retrieve Imaging Document Set [RAD-69] request SHALL NOT be returned in the response.

3.1.8 Security Considerations

Relevant Security Considerations are defined in IHE ITI TF-1[10], chapter 9.4. The CH:ADR profile requires all actors to be grouped with Secure Node or Secure Application implementing the “STX: TLS 1.2 floor using BCP195 Option” defined in the IHE ITI TF-2[11], chapter 3.19.6.2.3. Relevant XDS

[10] IHE IT Infrastructure (ITI) Technical Framework, Volume 1, Revision 19.0, June 17, 2022
[11] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022

Affinity Domain Security background is discussed in the XDS Security Considerations section (IHE ITI TF-1[10], chapter 10.7). The involved actors SHALL record audit events according to the following definitions:

3.1.8.1 Authorization Decision Consumer Audit Message

	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("ADR", "e-health-suisse", "Authorization Decision Query")
Source (Authorization Decision Consumer) (1)			
Human Requestor (0..n)			
Destination (Authorization Decision Provider) (1)			
Audit Source (Authorization Decision Consumer) (1)			
Requester Entity (1)			
Resource (1..n)			

Where:

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	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	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address
Human Requestor: AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP Endpoint URI
	AlternativeUserID	U	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address
Audit Source: AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

Requester Entity: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCode	M	“1” (person)
	ParticipantObjectTypeCodeRole	M	“11” (security user entity)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	Subject Role (value of the attribute “urn:oasis:names:tc:xacml:2.0:subject:role”)
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Subject ID (value of the attribute “urn:oasis:names:tc:xacml:1.0:subject:subject-id”)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Resource: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCode	M	“2” (system)
	ParticipantObjectTypeCodeRole	M	For ADR due toXDS and RMU: “3” (report) For ADR due to PPQ: “13” (security resource) For ADR due to ATC: “17” (data repository)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	*U*	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Resource-ID (value of the attribute “urn:oasis:names:tc:xacml:1.0:resource:resource-id”)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	C	Authorization result (when available): type = fixed string "decision", value = one of "Permit", "Deny", "NotApplicable", "Indeterminate".

Table 16: Authorization Decision Consumer Audit Message

3.1.8.2 Authorization Decision Provider Audit Message

	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(“ADR”, “e-health-suisse”, “Authorization Decision Query”)
Source (Authorization Decision Consumer) (1)			
Human Requestor (0..n)			

Destination (Authorization Decision Provider) (1)
Audit Source (Authorization Decision Provider) (1)
Requester Entity (1)
Resource (1..n)

Where:

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	*U*	*not specialized*
	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
Human Requestor: AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP Endpoint URI
	AlternativeUserID	M	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
Audit Source: AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
Requester Entity: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"11" (security user entity)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	Subject Role (value of the attribute "urn:oasis:names:tc:xacml:2.0:subject:role"
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Subject ID (value of the attribute "urn:oasis:names:tc:xacml:1.0:subject:subject-id")
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Resource:	ParticipantObjectTypeCode	M	"2" (system)

AuditMessage/ ParticipantObject Identification (1..n)	ParticipantObjectTypeCodeRole	M	For ADR due toXDS or RMU: “3” (report) For ADR due to PPQ: “13” (security resource) For ADR due to ATC: “17” (data repository)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	*U*	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Resource-ID (value of the attribute “urn:oasis:names:tc:xacml:1.0:resource:resource-id”)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	C	Authorization result (when available): type = fixed string "decision", value = one of "Permit", "Deny", "NotApplicable", "Indeterminate".

Table 17: Authorization Decision Provider Audit Message

3.2 Privacy Policy Feed [CH:PPQ-1]

3.2.1 Scope

This transaction is used by the Policy Source to add, update, or delete privacy policies and policy sets stored in the Policy Repository.

3.2.2 Referenced Standards

Privacy Policy Feed [CH:PPQ-1] messages shall be transmitted using synchronous Web Services, according to the requirements specified in IHE ITI TF-2[12], Appendix V.

a. IHE ITI TF-2[12], Appendix V “Web Services for IHE transactions” https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html

b. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

c. The home page of the "OASIS eXtensible Access Control Markup Language" technical committee: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacmlreferences all XACML related protocols and specifications for implementers of this profile.

   I. OASIS Multiple Resource Profile of XACML v2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-mult-profile-spec-os.pdf

   II. OASIS eXtensible Access Control Markup Language (XACML) v2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf Please be aware of the errata of the specification document as published on the XACML technical committee home page:

   III. Errata: http://www.oasis-open.org/committees/download.php/26986/access_control-xacml-2.0-core-spec-os-errata.doc

   IV. OASIS SAML 2.0 profile of XACML v2.0

   V. (Original: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)

   VI. Please be aware of the errata of the specification document as published on the XACML technical committee home page:

[12] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022

Errata: www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf

3.2.3 XML Namespaces

In addition to XML namespaces defined in IHE ITI TF-2[13], Appendix V.2.4, the following namespaces and namespace prefixes will be used:

Prefix	Namespace	Specification
epr	urn:e-health-suisse:2015:policy-administration	XSD document is available for download from the website of the Federal Office of Public Health[14]
hl7	urn:hl7-org:v3	HL7v3 specification on HL7.org
saml	urn:oasis:names:tc:SAML:2.0:assertion	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
xacml	urn:oasis:names:tc:xacml:2.0:policy:schema:os	OASIS eXtensible Access Control Markup Language (XACML) v2.0
xacml-context	urn:oasis:names:tc:xacml:2.0:context:schema:os	OASIS eXtensible Access Control Markup Language (XACML) v2.0
xacml-saml	urn:oasis:names:tc:xacml:2.0:profile:saml2.0:v2:schema:assertion	OASIS SAML 2.0 profile of XACML v2.0
xacml-samlp	urn:oasis:names:tc:xacml:2.0:profile:saml2.0:v2:schema:protocol	OASIS SAML 2.0 profile of XACML v2.0

Table 18: XML Namespaces

3.2.4 Interaction Diagram

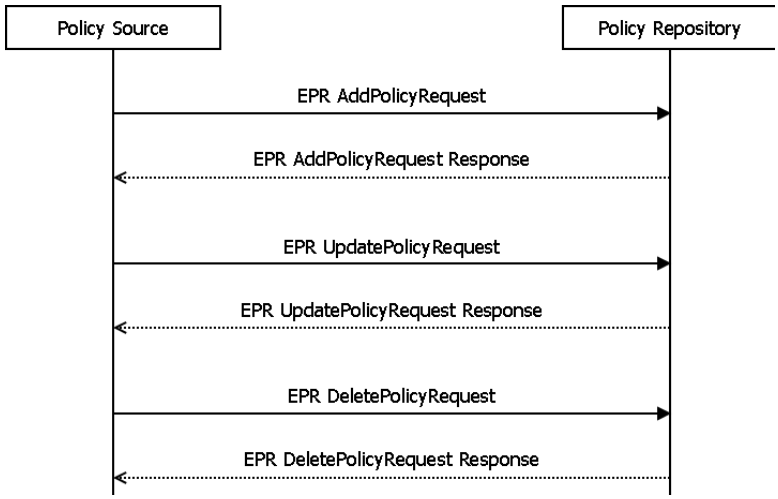

Figure 5: Sequence diagrams for the Privacy Policy Feed [CH:PPQ-1] transaction

3.2.5 AddPolicyRequest and UpdatePolicyRequest

3.2.5.1 Trigger Events

The Policy Source sends these messages when it needs to add new or update existing policies and/or policy sets stored in the Policy Repository.

[13] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

[14] Office fédéral de la santé publique OFSP, Législation Dossier électronique du patient (LDEP), https://www.bag.admin.ch/ldep > Supplément de 1er juin 2023 à l'édition 5 du complément 2.1 à l'annexe 5 ODEP-DFI.zip.

3.2.5.2 Message Semantics

The AddPolicyRequest and UpdatePolicyRequest request messages SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[15], Appendix V “Web Services for IHE Transaction”.

The WS-Addressing header <wsa:Action> SHALL contain the value:

a. For AddPolicyRequest: “urn:e-health-suisse:2015:policy-administration:AddPolicy”.

b. For UpdatePolicyRequest: “urn:e-health-suisse:2015:policy-administration:UpdatePolicy”.

The WS-Security header <wse:Security> SHALL contain a CH:XUA Assertion.

The SOAP body SHALL contain a single element <epr:AddPolicyRequest> or <epr:UpdatePolicyRequest> (an EPR-specific XML schema epr-policy-administration-combined-schema-1.3-local.xsd is used, because the SAML 2.0 profile of XACML v2.0 does not define messages suitable for these requests). The only child of this root element SHALL be the element <saml:Assertion>.

The assertion in <saml:Assertion> SHALL contain following elements:

c. Exactly one element <saml:Issuer> SHALL identify the Authorization Decision Provider by containing the home community ID of its community encoded as an URN and an XML attribute @NameQualifier equal to "urn:e-health-suisse:community-index".

d. Exactly one element <saml:Statement> of the type “xacml-saml:XACMLPolicyStatementType” with one or more policies and policy sets contained in child elements <xacml:Policy> and <xacml:PolicySet>.

3.2.5.3 Expected Actions

The Policy Repository SHALL perform an Authorization Decision Request [CH:ADR] to determine whether the requesting user has the permission to fulfil the given CH:PPQ request.

If yes, the Policy Repository SHALL add (for AddPolicyRequest) or update (for UpdatePolicyRequest) policies and policy sets contained in the CH:PPQ request, and create a CH:PPQ response message according to the success or failure of the transaction as defined below.

Otherwise, the Policy Repository SHALL create a CH:PPQ error response message.

3.2.6 AddPolicyRequest Response and UpdatePolicyRequest Response

3.2.6.1 Trigger Events

The AddPolicyRequest response or UpdatePolicyRequest response message is created by the Policy Repository in response to the AddPolicyRequest or UpdatePolicyRequest message, respectively.

3.2.6.2 Message Semantics

The AddPolicyRequest and UpdatePolicyRequest response messages SHALL use SOAP 1.2 encoding and comply with all requirements described in ITI TF-2[15], chapter Appendix V “Web Services for IHE Transaction”.

The WS-Addressing header <wsa:Action> SHALL contain the value:

a. For AddPolicyRequest Response:
“urn:e-health-suisse:2015:policy-administration:AddPolicyResponse”.

b. For UpdatePolicyRequest Response:
“urn:e-health-suisse:2015:policy-administration:UpdatePolicyResponse”.

The SOAP body SHALL contain a single element <epr:PolicyRepositoryResponse> with the attribute @status set to:

c. On success: “urn:e-health-suisse:2015:response-status:success”.

[15] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

d. On failure: "urn:e-health-suisse:2015:response-status:failure".

There is no notion of partial success in Privacy Policy Feed [CH:PPQ-1]. If at least one policy or policy set within the request cannot be added or updated, the entire request SHALL result in a failure response.

In case of an update failure due to unknown Policy Set IDs, a SOAP Fault MUST be returned to the Policy Source. The element <soap12:Detail> of this Fault SHALL contain a single element <epr:UnknownPolicySetId>.

3.2.7 DeletePolicyRequest

3.2.7.1 Trigger Events

The Policy Source sends this message when it needs to delete existing policies and policy sets from the Policy Repository.

3.2.7.2 Message Semantics

The DeletePolicyRequest request message SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[16], Appendix V "Web Services for IHE Transaction".

The WS-Addressing header <wsa:Action> SHALL contain the value:

```
urn:e-health-suisse:2015:policy-administration:DeletePolicy
```

The WS-Security header <wse:Security> SHALL contain a CH:XUA assertion.

The SOAP body SHALL contain a single element <epr:DeletePolicyRequest>. The only child of this root element SHALL be the element <saml:Assertion>.

The assertion in <saml:Assertion> SHALL contain following elements:

a. Exactly one element <saml:Issuer> SHALL identify the Authorization Decision Provider by containing the home community ID of its community encoded as an URN and an XML attribute @NameQualifier equal to "urn:e-health-suisse:community-index".

b. Exactly one element <saml:Statement> of the type "epr:XACMLPolicySetIdReferenceStatementType" with one or more policy IDs or policy set IDs contained in child elements <xacml:PolicySetIdReference>.

3.2.7.3 Expected Actions

The Policy Repository SHALL perform an Authorization Decision Request [CH:ADR] to determine whether the requesting user has the permission to fulfil the given CH:PPQ request.

If yes, the Policy Repository SHALL delete policies and policy sets referenced in the CH:PPQ request, and create a CH:PPQ response message according to the success or failure of the transaction as defined below.

Otherwise, the Policy Repository SHALL create a CH:PPQ error response message.

3.2.8 DeletePolicyRequest Response

3.2.8.1 Trigger Events

The DeletePolicyRequest response message is created by the Policy Repository in response to the DeletePolicyRequest message.

3.2.8.2 Message Semantics

The DeletePolicyRequest response message SHALL use SOAP 1.2 encoding and comply with all requirements described in ITI TF-2[17], Appendix V "Web Services for IHE Transaction".

[16] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022
[17] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

The WS-Addressing header <wsa:Action> SHALL contain the value:

```
urn:e-health-suisse:2015:policy-administration:DeletePolicyResponse
```

The SOAP body SHALL contain a single element <epr:PolicyRepositoryResponse> with the attribute @status set to:

a. On success: “urn:e-health-suisse:2015:response-status:success”.

b. On failure: “urn:e-health-suisse:2015:response-status:failure”.

There is no notion of partial success in Privacy Policy Feed [CH:PPQ-1]. If at least one policy or policy set referenced within the request cannot be deleted, the entire request SHALL result in a failure response.

In case of a deletion failure due to an unknown policy ID or policy set ID, a SOAP Fault MUST be returned to the Policy Source. The element <soap12:Detail> of this Fault SHALL contain a single element <epr:UnknownPolicySetId>.

3.2.9 Security Considerations

Relevant Security Considerations are defined in IHE ITI TF-1[18], chapter 9.4. The CH:PPQ profile requires all actors to be grouped with Secure Node or Secure Application implementing the “STX: TLS 1.2 floor using BCP195 Option” defined in the IHE ITI TF-2[19], chapter 3.19.6.2.3. Relevant XDS Affinity Domain Security background is discussed in the XDS Security Considerations section (see IHE ITI TF-1[18], chapter 10.7). The involved actors SHALL record audit events according to the following definitions:

3.2.9.1 Policy Source Audit Message

	Field Name	Opt	Value Constraints
Event	EventID	M	EV (110106, DCM,“Export”)
	EventActionCode	M	a. For Add Policy: C = Create b. For Update Policy: U = Update c. For Delete Policy: D = Delete
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV(“PPQ-1”, “e-health-suisse”, “Privacy Policy Feed”)
Source (Policy Source) (1)			
Human Requestor (0..n)			
Destination (Policy Repository) (1)			
Audit Source (Policy Source) (1)			
Patient (1..1)			
Policy or Policy Set (0..n)			

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	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

[18] IHE IT Infrastructure (ITI) Technical Framework, Volume 1, Revision 19.0, June 17, 2022.
[19] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

	NetworkAccessPointID	U	The machine name or IP address.
Human Requestor : AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	U	not specialized
	RoleIDCode	U	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address.
Audit Source: AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

Patient: (AuditMessage/ ParticipantObject Identification)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Policy or Policy Set: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"13" (security resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	*M*	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	ID of the policy or policy set from the CH:PPQ request message. For Add and Update requests, only IDs of top-level policies and policy sets are required; IDs of nested policies and policy sets should be omitted
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Table 19: Policy Source Audit Message

3.2.9.2 Policy Repository Audit Message

	Field Name	Opt	Value Constraints
Event	EventID	M	EV (110107, DCM,“Import”)
	EventActionCode	M	a. For Add Policy: C = Create b. For Update Policy: U = Update c. For Delete Policy: D = Delete
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV(“PPQ-1”, “e-health-suisse”, “Privacy Policy Feed”)
Source (Policy Source) (1)			
Human Requestor (0..n)			
Destination (Policy Repository) (1)			
Audit Source (Policy Repository) (1)			
Patient (1..1)			
Policy or Policy Set (0..n)			

Source: AuditMessage/ ActiveParticipant	UserID	*M*	*not specialized*
	AlternativeUserID	U	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, “Source”)
	NetworkAccessPointTypeCode	M	“1” for machine (DNS) name, “2” for IP address
	NetworkAccessPointID	U	The machine name or IP address.
Human Requestor (if known): AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	M	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.
Audit Source AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
Patient (AuditMessage/ ParticipantObject Identification)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Policy or Policy Set: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCode	M	"2" (system object)
	ParticipantObjectTypeCodeRole	M	"13" (security resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	*M*	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	ID of the policy or policy set from the CH:PPQ request message. For Add and Update requests, only IDs of top-level policies and policy sets are required; IDs of nested policies and policy sets SHOULD be omitted
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Table 20: Policy Repository Audit Message

3.3 Privacy Policy Retrieve [CH:PPQ-2]

3.3.1 Scope

This transaction is used by the Policy Consumer to retrieve privacy policies and policy sets from the Policy Repository.

3.3.2 Referenced Standards

Same as in the Privacy Policy Feed [CH:PPQ-1] transaction, see Section 3.2.2.

3.3.3 XML Namespaces

Same as in the Privacy Policy Feed [CH:PPQ-1] transaction, see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

3.3.4 Interaction Diagrams

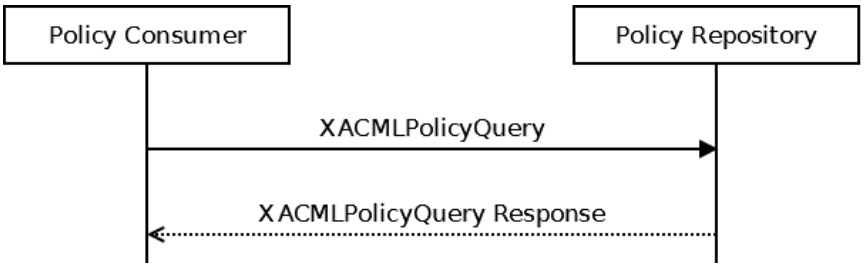

Figure 6: Sequence diagrams for the Privacy Policy Retrieve [CH:PPQ-2] transaction

3.3.5 Policy Query Request

3.3.5.1 Trigger Events

The Policy Consumer sends this message when it needs to retrieve existing XACML policies or policy sets stored in a Policy Repository.

3.3.5.2 Message Semantics

The XACMLPolicyQuery request message SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[20], Appendix V “Web Services for IHE Transaction”.

The WS-Addressing header <wsa:Action> SHALL contain the value:

```
urn:e-health-suisse:2015:policy-administration:PolicyQuery
```

The WS-Security header <wse:Security> SHALL contain a CH:XUA assertion.

The SOAP body SHALL contain a single element <xacml-samlp:XACMLPolicyQuery>.

Two different query flavors are supported:

a. Retrieval of all policies and policy sets related to a particular patient. In this case, the only child of <xacml-samlp:XACMLPolicyQuery> SHALL be the element <xacml-context:Request>. Its elements <xacml-contect:Subject>, <xacml-contect:Action> and <xacml-contect:Environment> SHOULD be empty as there is no use for them. Its element <xacml-contect:Resource> SHALL contain a single child element <xacml-contect:Attribute> with
   i. XML attribute @AttributeId equal to ”urn:e-health-suisse:2015:epr-spid”,
   ii. XML attribute @DataType equal to of ”urn:hl7-org:v3#II”,
   iii. Contents of <xacml-contect:AttributeValue> set to the EPR SPID of the patient in HL7v3 Instance Identifier format, e.g.:

   <hl7:InstanceIdentifier xsi:type="hl7:II" root="2.16.756.5.30.1.127.3.10.3" extension="8901" />

   The request MAY contain more than one Resource, but they all SHALL reference the same patient.

b. Retrieval of policies and policy sets directly referenced by their IDs (also useful for not patient-related policies). In this case, <xacml-samlp:XACMLPolicyQuery> SHALL contain one or more elements <xacml:PolicyIdReference> and/or <xacml:PolicySetIdReference> holding IDs of policies and policy sets, respectively.

[20] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022.

3.3.5.3 Expected Actions

All policies satisfying the Resource definitions within a Request SHALL be returned if allowed by CH:ADR. Only policies and policy sets directly matching the search criteria shall be considered.

3.3.6 PolicyQuery Response

The PolicyQuery Response message is created by the Policy Repository in response to the PolicyQuery Request.

3.3.6.1 Trigger Events

This message is created by the Policy Repository after the evaluation of a PolicyQuery Request message. The Policy Repository identifies policies and policy sets applicable to be returned to the requester. Only policies and policy sets directly matching search criteria shall be considered, the ones referenced from them transitively SHALL NOT be returned.

3.3.6.2 Message Semantics

The Policy Query Response message SHALL use SOAP 1.2 encoding and comply with all requirements described in IHE ITI TF-2[21], Appendix V "Web Services for IHE Transaction".

The WS-Addressing header <wsa:Action> SHALL contain the value:

```
urn:e-health-suisse:2015:policy-administration:PolicyQueryResponse
```

The body of the SOAP message SHALL contain a single element <samlp:Response>, which SHALL contain a single element <samlp:Status> and a single element <saml:Assertion>:

The element <samlp:Status> contains a single element <samlp:StatusCode>, whose attribute @Value SHALL be set as defined in section 4.10 "Element <samlp:Response>: XACMLAuthzDecision Response" of OASIS SAML 2.0 profile of XACML v2.0 (errata).

The assertion in <saml:Assertion> SHALL contain following elements:

a. Exactly one element <saml:Issuer> SHALL identify the Authorization Decision Provider by containing the home community ID of its community encoded as an URN and an XML attribute @NameQualifier equal to "urn:e-health-suisse:community-index".
b. Exactly one element <saml:Statement> of the type "xacml-saml:XACMLPolicyStatementType" with one or more policies and policy sets contained in child elements <xacml:Policy> and <xacml:PolicySet>.

3.3.7 Security Considerations

Relevant Security Considerations are defined in IHE ITI TF-1[22], chapter 9.4. The CH:PPQ profile requires all actors to be grouped with Secure Node or Secure Application implementing the "STX: TLS 1.2 floor using BCP195 Option" defined in the IHE ITI TF-2[23], chapter 3.19.6.2.3. Relevant XDS Affinity Domain Security background is discussed in the XDS Security Considerations section (see IHE ITI TF-1[22], chapter 10.7). The involved actors SHALL record audit events according to the following definitions:

3.3.7.1 Policy Consumer Audit Message

	Field Name	Opt	Value Constraints
Event	EventID	M	EV (110112, DCM,"Query")
	EventActionCode	M	E = Execute
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*

[21] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022
[22] IHE IT Infrastructure (ITI) Technical Framework, Volume 1, Revision 19.0, June 17, 2022
[23] IHE IT Infrastructure (ITI) Technical Framework, Volume 2, Revision 19.0, June 17, 2022

	EventTypeCode	M	EV(“PPQ-2”, “e-health-suisse”, “Privacy Policy Retrieve”)
Source (Policy Consumer) (1)			
Human Requestor (0..n)			
Destination (Policy Repository) (1)			
Audit Source (Policy Consumer) (1)			
Patient (1..1)			
Query Parameters (1..1)			

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	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.

Human Requestor : AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	U	not specialized
	RoleIDCode	U	EV(110152, DCM, “Destination”)
	NetworkAccessPointTypeCode	M	“1” for machine (DNS) name, “2” for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Audit Source: AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

Patient: (AuditMessage/ ParticipantObject Identification)	ParticipantObjectTypeCode	M	“1” (person)
	ParticipantObjectTypeCodeRole	M	“1” (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

	ParticipantObjectTypeCode	M	“2” (system object)

Query Parameters: AuditMessage/ ParticipantObject Identification	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Value of the attribute /XACMLPolicyQuery/@ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	The XACML Policy Query, base64 encoded
	ParticipantObjectDetail	M	Attribute *type* — fixed string "QueryEncoding", attribute *value* — name the character encoding, such as "UTF-8", used to encode the query before base64 encoding.

Table 21: Policy Consumer Audit Message

3.3.7.2 Policy Repository Audit Message

	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("PPQ-2", "e-health-suisse", "Privacy Policy Retrieve")
Source (Policy Consumer) (1)			
Human Requestor (0..n)			
Destination (Policy Repository) (1)			
Audit Source (Policy Repository) (1)			
Patient (1..1)			
Query Parameters (1..1)			
Source: AuditMessage/ ActiveParticipant	UserID	*M*	*not specialized*
	AlternativeUserID	U	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address.
Human Requestor: AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination:	UserID	M	SOAP endpoint URI.

AuditMessage/ ActiveParticipant	*AlternativeUserID*	M	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.
Audit Source AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
Patient (AuditMessage/ ParticipantObjectIdenti fication)	ParticipantObjectTypeCode	M	“1” (person)
	ParticipantObjectTypeCodeRole	M	“1” (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*
Query Parameters: AuditMessage/ ParticipantObjectIdentification	ParticipantObjectTypeCode	M	“2” (system object)
	ParticipantObjectTypeCodeRole	M	“24” (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Value of the attribute /XACMLPolicyQuery/@ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	The XACML Policy Query, base64 encoded
	ParticipantObjectDetail	M	Attribute *type* — fixed string “QueryEncoding”, attribute *value* — name the character encoding, such as “UTF-8”, used to encode the query before base64 encoding.

Table 22: Policy Repository Audit Message

4 Volume 3 – Content Profiles - Submission Rules for Policies and Policy Sets

The collection of EPR base and template policies are available for download from the website of the Federal Office of Public Health[24]. It contains the following parts:

a. Base Policies,
b. Base Policy Sets,
c. Templates for Patient Bootstrap Policy Sets,
d. Templates for Patient User Assignment Policy Sets.

4.1 Base Policies and Base Policy Sets

Base Policies and Base Policy Sets have fixed IDs and are not related to a particular patient. They belong to the static configuration of a reference community and therefore MUST be stored in the CH:PPQ Policy Repository.

4.2 Patient Bootstrap Policy Sets and Patient User Assignment Policy Sets

These two groups of policy sets relate to a particular patient.

The difference between those groups of policy sets is the following:

a. **Bootstrap Policy Sets** SHALL be fed into the CH:PPQ Policy Repository during the on-boarding of a patient. This SHALL be done by the EPR role Policy Administrator (PADM).
b. **User Assignment Policy Sets** are created when
   I. the patient grants permission to a healthcare professional, a group of healthcare professionals, or a representative,
   II. the patient adds a healthcare professional onto the exclusion list,
   III. a healthcare professional with delegation permission delegates access rights to another healthcare professional.

The CH:PPQ Policy Source SHALL create Patient Policies from the template policies by setting actual data (e.g. EPR-SPIDs of patients or references to Base Policy Sets) and generate policy set IDs as UUIDs.

Patient Policy Sets stored in and returned by a CH:PPQ Policy Repository SHALL be compliant to the templates and SHALL pass the Schematron validation available for download from the website of the Federal Office of Public Health[24].

[24] Office fédéral de la santé publique OFSP, Législation Dossier électronique du patient (LDEP), https://www.bag.admin.ch/ldep > Supplément de 1er juin 2023 à l'édition 5 du complément 2.1 à l'annexe 5 ODEP-DFI.zip

5 List of figures

6 List of tables