Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

SR 816.111

Ergänzung 1 zu Anhang 5 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier (EPDV-EDI)

Nationale Anpassungen der Integrationsprofile nach Artikel 5 Absatz 1 Buchstabe b EPDV-EDI

National extensions to the IHE Technical Framework

Ergänzung 1 zu Anhang 5 EPDV-EDI : Nationale Anpassungen

Ausgabe 7: 24. April 2024

Inkrafttreten: 1. Juni 2024

Table of contents

1 Introduction

Die in diesem Abschnitt dokumentierten nationalen Anpassungen der Integrationsprofile sollen in Verbindung mit den Definitionen von Integrationsprofilen, Akteuren und Transaktionen verwendet werden, die in den Bänden 1 bis 3 der IHE IT Infrastructure und Radiology Technical Frameworks enthalten sind.

Dieses Dokument mit nationalen Anpassungen von IHE-Integrationsprofilen wurde erstellt, um die schweizerischen Regelungen der Verordnung über das elektronische Patientendossier (EPDV, SR 816.11) zu erfüllen. Die EPDV und die EPDV-EDI (SR 816.111) werden in der Amtlichen Sammlung (AS) veröffentlicht (in Deutsch, Französisch und Italienisch)[1].

The national extensions documented in this section shall be used in conjunction with the definitions of integration profiles, actors and transactions provided in Volumes 1 through 3 of the IHE IT Infrastructure and Radiology Technical Frameworks.

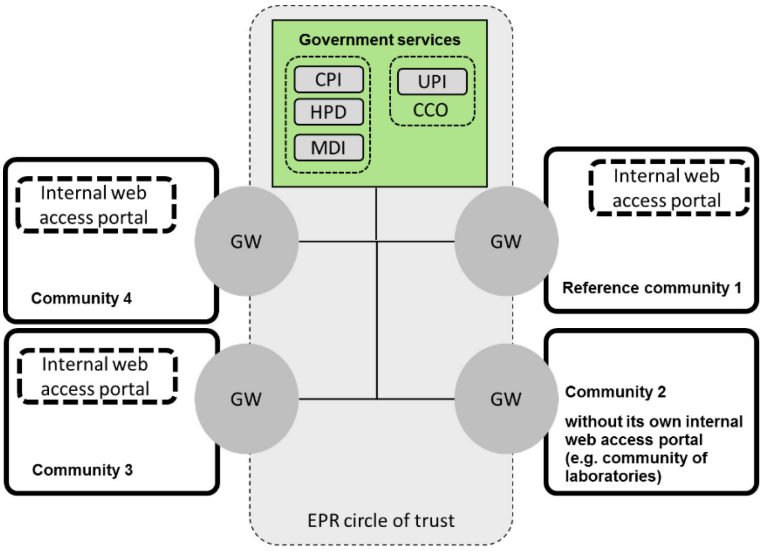
This document with national extensions of IHE integration profiles was authored in order to fulfil the Swiss regulations of the Ordinance on the Electronic Patient Record (EPRO, SR 816.11). The EPRO and the EPRO-FDHA (SR 816.111) are published in Official Compilation of Federal Legislation (available 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.

1.1 Definition of terms

1.1.1 EPR circle of trust

From an organizational perspective and in terms of the Electronic Patient Record Act (EPRA), communities are an association of healthcare professionals and their institutions. Communities who want to participate in the Swiss EPR shall comply with the certification requirements as laid down in the implementing provisions for the EPRA. Such communities and, in particular, their gateways will be listed in a community portal index (CPI) provided by the Federal Office of Public Health (FOPH) and therefore form a circle of trust by mutual recognition of their conformity related to data protection and data privacy. Furthermore, all required central services are also part of this circle of trust.



Legend:

GW: Gateway
CPI: Community portal Index
HPD: Healthcare Provider Directory
MDI: Metadata Index-Service
CCO Central Compensation Office CCO
UPI: Unique Person Identification System operated by the CCO

Figure 1: Swiss EPR circle of trust

1.1.2 Patient Identifiers (EPR-SPID, MPI-PID)

Communities in the EPR circle of trust use the national EPR sectoral patient identifier (EPR-SPID) only for cross-community communication. The Federal Central Compensation Office[2] (CCO) is the institution which issues EPR-SPID's (EPR Sectorial Personal Identification Number). The CCO is the only institution which is allowed to correlate the Social Security Number (AHVN13) with the EPR-SPID. There is no correlation possible back from the EPR-SPID to the Social Security Number. This is political intention in order to achieve highest possible patient privacy.

Within a community, patients are identified by an MPI-PID which is managed by a community Master Patient Index (MPI). Primary Systems may correlate their local patient identifier with the MPI-PID. For cross-community communication the gateways may correlate the MPI-PID to the EPR-SPID.

[2] https://www.zas.admin.ch/

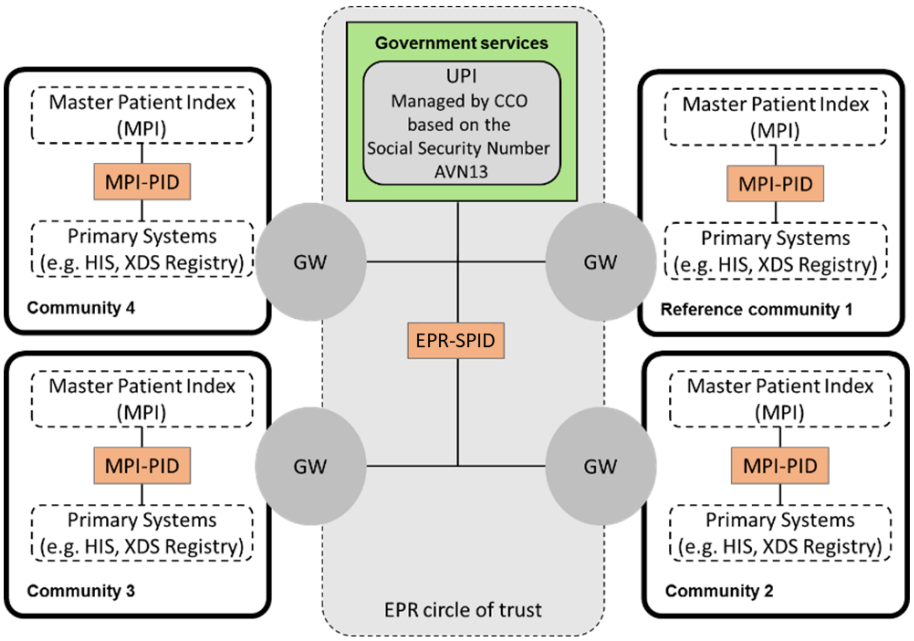


Figure 2: Swiss Patient Identifier

1.1.3 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119][3].

1.1.4 Scope of precisions

The extensions, restrictions and translations specified apply to the following IHE IT Infrastructure (ITI) integration profiles:

a. IT Infrastructure: Cross-Enterprise Document Sharing (XDS)
b. IT Infrastructure: Cross-Community Access (XCA)
c. IT Infrastructure: Cross-Enterprise Document Sharing for Imaging (XDS-I.b)
d. IT Infrastructure: Audit Trail and Node Authentication (ATNA)
e. IT Infrastructure: Cross-Enterprise User Assertion (XUA)
f. IT Infrastructure: Patient Identifier Cross-Reference HL7 V3 (PIXV3)
g. IT Infrastructure: Patient Demographic Query HL7 V3 (PDQV3)
h. IT Infrastructure: Cross-Community Patient Discovery (XCPD)
i. IT Infrastructure Technical Framework Supplement: Healthcare Provider Directory (HPD)
j. IT Infrastructure Technical Framework Supplement: XDS Metadata Update (XDS MU)
k. IT Infrastructure Technical Framework Supplement: Restricted Metadata Update (RMU)

[3] For full text of RFC2119 see https://www.ietf.org/rfc/rfc2119.txt.

1.2 Requirements on XDS and XCA

1.2.1 MetadataLevel

In Stored Queries (transactions Registry Stored Query [ITI-18] and Cross Gateway Query [ITI-38]), the parameter $MetadataLevel, whenever provided, shall equal to 1 (one). Whenever a receiving actor (e.g. a Document Registry) discovers that this requirement is violated in an incoming request, it shall reject this request and return an error with the code XDSRegistryError (see section 1.4).

1.2.2 Additional requirements on the Registry actor

Document Registries SHALL reject metadata registration requests containing Folders and/or Associations whose source and/or target objects are Folders.

1.2.2.1 Reference ID Option

The Registry SHALL support the Reference ID Option (see IHE ITI TF-1[4], chapter 10.2.6) thus to support the use case of imaging where an Imaging Source SHALL store specific values to the DocumentEntry.referenceIdList attribute.

1.2.3 Additional requirements on the Document Consumer actor

Whenever the role of the accessing user is not DADM (Document Administrator), the Document Consumer SHALL NOT display metadata of and references to objects of the following types:

a. Submission Sets not containing any DocumentEntry or Association object the accessing person is permitted to retrieve,
b. Folders,
c. Associations whose source and/or target objects are any of the above objects.

1.2.4 Metadata

1.2.4.1 DeletionStatus

An extra metadata attribute is introduced for the following use cases:

a. To submit a deletion request for a document.
b. To mark a document provided by a health care professional, that it should not be deleted after the by law determinate time period.

For the extra metadata attribute, the Predefined URN datatype is used (see IHE ITI TF-3[5], chapter 4.2.3.1.7 "Metadata Attribute Data types"). It shall have the name of urn:e-health-suisse:2019:deletionStatus. The following values are defined:

Value	Expected behavior
`urn:e-health-suisse:2019:ddeletionStatus:deletionNotRequested`	No action requested. This value can also be sent to undo the other options.
`urn:e-health-suisse:2019:deletionStatus:deletionRequested`	Document shall be deleted.
`urn:e-health-suisse:2019:deletionStatus:deletionProhibited`	This document shall not be deleted after the time period for the deletion of outdated documents as defined in the law.

Table 1: DeletionStatus in the document metadata

[4] IHE IT Infrastructure (ITI) Technical Framework, Volume 1, Revision 19.0, June 17, 2022.
[5] IHE IT Infrastructure (ITI) Technical Framework, Volume 3, Revision 19.0, June 17, 2022.

1.2.4.1.1 Expected Action

After receiving a deletionRequest equal to deletionRequested in a metadata update transaction the Registry has the options to either:

a. Store the received deletionStatus to the corresponding DocumentEntry in the Registry data store. It is then in the responsibility of the community holding the Document to delete the document and corresponding metadata in reasonable time.

b. Directly delete the corresponding metadata. It is then in the responsibility of the community holding the Document to also delete the document in reasonable time if not done directly.

After receiving a deletionRequest equal to deletionProhibited in a metadata update transaction the Registry has to store the received deletionStatus to the corresponding DocumentEntry in the Registry data store. It is then expected that the documents will not be deleted after the by law determinate time period.

1.2.4.2 Metadata Optionality

To fulfill national requirements metadata optionality is changed as follows (see IHE ITI TF-3[6], Table 4.3.1-3 "Sending Actor Metadata Attribute Optionality"):

Metadata Element	Metadata Attribute	XDS DS	XDS DR
`DocumentEntry`	Title	R	R
`DocumentEntry`	DeletionStatus	O	O
`SubmissionSet`	Author	R	R

Table 2: Metadata Optionality

1.2.4.3 SubmissionSet.Author.AuthorRole

The SubmissionSet.Author element MAY be used to track the user who made the latest changes to the document metadata. If present, the value of the AuthorRole attribute SHALL be taken from the SubmissionSet.Author.AuthorRole value set with the OID 2.16.756.5.30.1.127.3.10.1.41.

1.2.4.4 DocumentEntry.originalProviderRole

An extra metadata attribute SHALL be used to distinguish document originally provided by patients or their representatives from documents originally provided by healthcare professionals, assistants, technical users or document administrators. The extra metadata attribute SHALL be set by the Document Source actor to the role value of the current user and SHALL NOT be updated by Update Initiator or Document Administrator actors.

For the extra metadata attribute, the Predefined URN datatype SHALL be used (IHE ITI TF-3[6], chapter 4.2.3.1.7 "Metadata Attribute Data types") with name *urn:e-health-suisse:2020:originalProviderRole*. Values SHALL be taken from the value set DocumentEntry.originalProviderRole (OID: 2.16.756.5.30.1.127.3.10.1.42) and formatted as Coded String data type defined in IHE ITI TF-3[6], Table 4.2.3.1.7-2, i.e. as *Code^^^&CodeSystemID&ISO*.

1.3 Requirements on XDS-I.b

Imaging Document Sources SHALL fulfill the following requirements on the XDS Metadata and the X-User Assertion when providing KOS objects:

a. The purpose of use of the X-User Assertion SHALL be equal to "DICOM_AUTO".

b. The DocumentEntry.formatCode SHALL be equal to the coded value of "DICOM Manifest" ("1.2.840.10008.5.1.4.1.1.88.59^^1.2.840.10008.2.6.1").

c. DocumentEntry.mimeType SHALL be equal to "application/dicom".

d. The StudyInstanceUID referenced in the KOS object SHALL be conveyed in the DocumentEntry.referenceIdList (urn:ihe:iti:xds:2013:referenceIdList).

[6] IHE IT Infrastructure (ITI) Technical Framework, Volume 3, Revision 19.0, June 17, 2022.

The Document Repository SHALL enforce the requirements above when Imaging Document Sources provide KOS objects in Provide and Register Document Set [ITI-41] or Provide and Register Imaging Document Set [RAD-68] transactions. I.e., the Document Repository SHALL accept KOS objects only, if the following requirements are fulfilled:

a. The purpose of use of the X-User Assertion SHALL be equal to "DICOM_AUTO".
b. The DocumentEntry.formatCode SHALL be equal to the coded value of "DICOM Manifest" ("1.2.840.10008.5.1.4.1.1.88.59^^1.2.840.10008.2.6.1").
c. DocumentEntry.mimeType SHALL be equal to "application/dicom".

1.4 Expected actions for receiving actors receiving unexpected parameters

1.4.1 For ebXML-based profiles (e.g. XDS)

Whenever the receiving actor detects that the incoming message is invalid (e.g. a required element is missing, or a prohibited element is present, or an element has a wrong cardinality, or an element has a wrong format, or an element references an unknown entity, or an element is not consistent with other message elements, etc.), it SHALL reject this message and SHALL NOT execute the action requested in it.

The response message SHALL specify the corresponding status code and provide information about each discovered error as prescribed in IHE ITI TF-3[7], chapter 4.2.4 "Success and Error Reporting".

Note: independently from whether the incoming request message is valid or not, the receiving actor MAY create additional sub-elements RegistryError with attribute @severity set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning" to inform the sending actor about request message anomalies which are important in some regard but did not lead to rejection of the request.

1.4.2 For HL7v3-based profiles (e.g. PIXV3)

Whenever the receiving actor detects that the incoming message is invalid (e.g. a required element is missing, or a prohibited element is present, or an element has a wrong cardinality, or an element has a wrong format, or an element references an unknown entity, or an element is not consistent with other message elements, etc.), it SHALL reject this message and SHALL NOT execute the action requested in it.

The response message SHALL specify the code "AE" (application error) in both Acknowledgement.typeCode (transmission wrapper) and QueryAck.queryResponseCode (control act wrapper), and provide for each discovered error a sub-element Acknowledgement.acknowledgementDetail with the following contents:

a. typeCode – fixed value "E" (error).
b. code – error code, preferably from the HL7 code system 2.16.840.1.113883.12.357 or 2.16.840.1.113883.5.1100.
c. text – description of the error in one or more natural languages.

Note: independently from whether the incoming request message is valid or not, the receiving actor MAY create additional sub-elements Acknowledgement.acknowledgementDetail with typeCode equal to "I" (information) or "W" (warning) to inform the sending actor about request message anomalies which are important in some regard but do not lead to rejection of the request.

[7] IHE IT Infrastructure (ITI) Technical Framework, Volume 3, Revision 19.0, June 17, 2022.

1.5 Requirements on ATNA

1.5.1 Precisions on Authenticate Node [ITI-19]

All Actors grouped with the Secure Node or Secure Application Actor SHALL implement the "STX: TLS 1.2 floor using BCP195 Option" defined in the IHE ITI TF-2[8], chapter 3.19.6.2.3.

1.5.2 Precisions on Record Audit Event [ITI-20]

The following additional requirements apply to ATNA audit records generated by IHE and EPR actors:

a. The attribute //AuditSourceIdentification/@AuditEnterpriseSiteID is required and shall contain the OID of the audit source.

b. Whenever an element //PatrticipantObjectIdentification describes an XDS document, the attribute //PatrticipantObjectIdentification/@ParticipantObjectSensitivity shall contain the confidentiality code of this document (if known). The format is HL7v2 CE with the code system OID as the code system name, e.g.: `1051000195109^normal^2.16.840.1.113883.6.96`.

c. In all elements of the type CodedValueType: whenever the represented code belongs to the Swiss Metadata value set, the attribute @codeSystemName shall contain the OID of the corresponding code system instead of its symbolic name. For all other codes, this requirement is optional.

In addition to the fine-grained ATNA logging, the ERPA prescribes to log coarse-grained (and easy understandable by the patient) information about any processing of a patient's EPR, and to provide this information upon the patient's request in conformance with the national profile "Audit Trail Consumption" (CH:ATC). Thereby, ATNA audit records can serve as raw data of CH:ATC responses.

1.6 Requirements on XUA for Authentication and User Assertion

1.6.1 Introduction

The Federal Act on Electronic Patient Records (EPRA) requires a secure environment and therefore strong authentication and access control mechanisms within the EPR circle of trust.

The XUA Profile in the IHE ITI TF-1[9] defines means to communicate claims about authenticated principals (users, applications and systems) in transactions that cross enterprise boundaries. In the context of the EPR these claims are used for access control and to protocol information not available in the transaction messages.

While the requirements on the X-Service User on the authentication of principals and the method that the X-Service User (e.g., XDS Document Consumer) uses to get the Assertion, are outside of scope of the standard IHE XUA Profile (see IHE ITI TF-1[9], chapter 13 "Cross Enterprise User Assertion (XUA) "), they are of importance for the Swiss EPR.

The requirements on the X-Service User on the authentication of persons (e.g., patients, healthcare professionals) are specified in Annex 8 EPRO-FDHA and are out of the scope of this national extension. This national extension only adds some additional information, especially to bridge the IHE vocabulary used in this national extension to the vocabulary used in Annex 8 EPRO-FDHA.

The requirements on authentication of impersonal technical user (e.g., applications, systems) are not specified in Annex 8 EPRO-FDHA. The Federal Act on Electronic Patient Records allows a write only access for technical users. Consequently, this national extension specifies the method, a technical user implementing a X-Service User (XDS Document Source) shall use to retrieve an Assertion.

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

The IHE XUA Profile defines the means to communicate principal attributes (e.g. ID, Name) and session attributes (e.g. purpose of use) that appear to be needed in the use cases, leaving the definition of the standards to be used to identify these attributes and their values. Consequently, this national extension specifies the attributes and which values to be used in the Swiss EPR. Due to the special requirements of the Swiss EPR, the required attributes, their format and their possible values are not interdependent, but depend on the user role. This dependency of the attributes to the user role is taken into account by using extensions. For example the patient extension defines the attributes to be provided, their format and allowed values for an assertion to be used by patients, which differs from the requirements on the assertion to be used by a healthcare professional or other roles defined in the Swiss EPR.

A relationship is called "on behalf of"-relationship, if an authenticated person or system acts on behalf of a subject, that is registered in the community and authorized to access an EPR. For persons or systems acting on behalf of an authorized subject (responsible) inherit the access rights from their responsible. Access rights of subjects acting "on behalf of" can therefore not be managed independently.

The following roles are defined in the Swiss EPR and reflected in the extensions: A **healthcare professional** may read from and write data and documents to an EPR in a treatment context, if authorized by the patient either directly or through membership to an authorized group. An **assistant** may act on behalf of a healthcare professional and inherits the access rights of the healthcare professional she /he is acting on behalf of. A **technical user** (e.g. an application or system) may write data and documents to an EPR acting on behalf of a healthcare professional who is named to be responsible for the technical user. A **patient** may read and write data to its own EPR, e.g. read and write documents to an EPR or authorize healthcare professionals to do so. A **representative** may manage an EPR on behalf of the patient. A **policy administrator** may open or delete an EPR, i.e. read, write or delete the access policies of an EPR. A **document administrator** may correct errors on documents and document metadata level in EPR.

The roles described above may differ from the real life roles of the user. A user acting with role assistant in the Swiss EPR may be medical assistant or a healthcare professional in real life; a user acting with role representative in the Swiss EPR may be an assistant, a healthcare professional or a private person in real life; a user acting with role policy administrator or document administrator in the Swiss EPR may be an assistant, a healthcare professional or a hospital employee in real life.

While the method used by a X-Service User (e.g. Document Consumer) to determine the contents of the assertion is outside of scope of the standard IHE XUA Profile, it is of importance in the Swiss EPR. Consequently, this national extension specifies the actors and transactions for the X-Service User to claim the required attributes and to retrieve the assertion used to communicate the claims to the X-Service Provider.

In the Swiss EPR the XUA token conveys all the required information to enable actors grouped with the X-Service Provider to enforce the access rights policies. These are user identity claims (i.e. GLN of healthcare professionals or EPR-SPID of patients) as well as claims related to the current user session (i.e. purpose of use or the health record which is accessed).

For security reasons in the Swiss EPR, identity claims shall be validated, if they are claimed from sources, which are outside the certification scope of the Swiss EPR (i.e. primary systems). Consequently this national extensions defines the requirements on the validation of the identity claims to be performed when accessing a protected resource of the Swiss EPR.

To support identifier transformations and "on behalf of"-transformations, each community shall manage community-local data sources for the X-Assertion Provider actor. Annex 2 EPRO-FDHA defines in paragraphs 1.4.2, 1.6 and 8.2 operational certification requirements on these data sources.

1.6.2 Actors / Transactions

The following figures show the actors and transactions specified in this national extension in two different scenarios: Figure 3 shows the actors and transaction in a scenario, when an Actor grouped with a X-Service User (e.g. Document Consumer) communicates with one single community. Figure 4 instead shows a cross-community scenario, when an actor grouped with the X-Service User connected to a community request protected resources from a remote community.

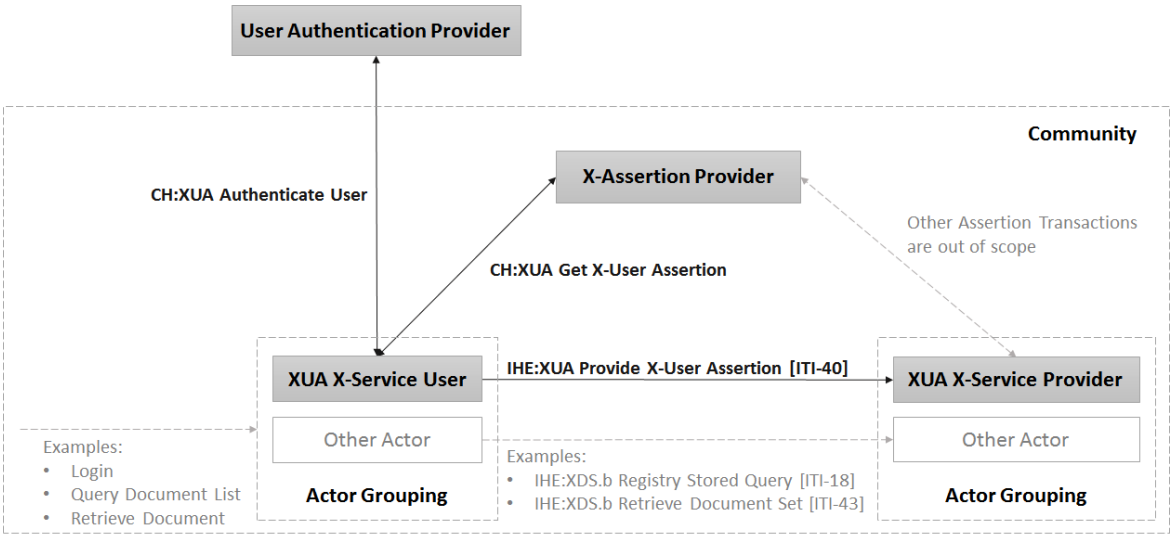


Figure 3: XUA Actors for the use within one community

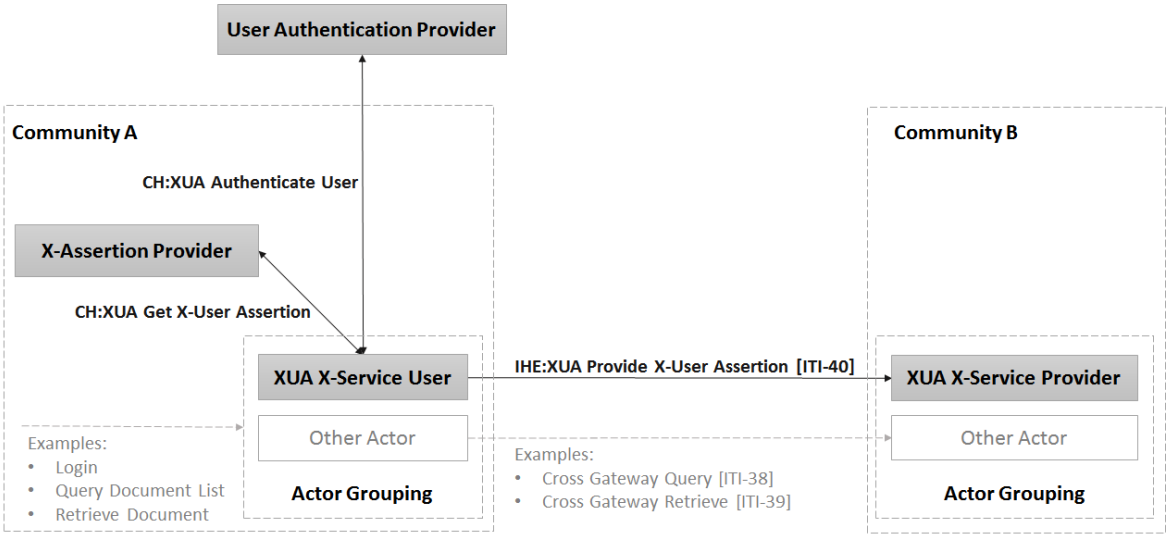


Figure 4: XUA Actors for the use in cross-community communications

1.6.2.1 Workflow Initiator Option

The Workflow Initiator option SHALL be claimed by all implementations, which require user authentication and requests to retrieve a CH:XUA compliant Assertion, i.e., patient and healthcare professional portals, primary systems, etc. The implementations usually initiate workflows to access data and documents, e.g. read or write documents from the EPR, which are triggered by a user interaction.

Actors SHALL implement the following required transactions (labelled "R") when claiming the Workflow Initiator option:

Actor	Transaction	Optionality
X-Service User	Provide X-User Assertion [ITI-40]	R
X-Service Provider	Provide X-User Assertion [ITI-40]	R
X-Assertion Provider	Get X-User Assertion	R
X-Service User	Get X-User Assertion	R
User Authentication Provider	Authenticate User	R
X-Service User	Authenticate User	R

Table 3: XUA actors and transactions in the Workflow Initiator option

1.6.2.2 Technical User Option

The Technical User option SHALL be claimed by all implementations, which do not require user authentication, but request to retrieve a CH:XUA compliant Assertion, i.e. archive systems or other primary systems accessing EPR data and documents, which are not initiated by a user interaction.

Actors SHALL perform the following required transactions (labelled "R") when claiming the Technical User option:

Actor	Transaction	Optionality
X-Service User	Provide X-User Assertion [ITI-40]	R
X-Service Provider	Provide X-User Assertion [ITI-40]	R
X-Assertion Provider	Get X-User Assertion	R
X-Service User	Get X-User Assertion	R

Table 4: XUA actors and transactions in the Technical User option

1.6.2.3 Proxy Option

The Proxy option SHALL be claimed by all implementations, which use CH:XUA assertions from other transactions and use the CH:XUA assertion when acting as an agent to request protected data from other actors, i.e. Gateways, CH:ADR Authorization Decision Consumer, etc.

Actors shall perform the following required transactions (labelled "R") when claiming the Proxy option:

Actor	Transaction	Optionality
X-Service User	Provide X-User Assertion [ITI-40]	R
X-Service Provider	Provide X-User Assertion [ITI-40]	R

Table 5: XUA actors and transactions in the Proxy option

1.6.3 Actor Grouping

The actors of this national extension SHALL be grouped with other actors as follows:

EPR Actor	Optionality	Actor to be grouped with
X-Service User	R	CT Time Client
	R	ATNA Secure Node
X-Service Provider	R	CT Time Client
	R	ATNA Secure Node
X-Assertion Provider	R	CT Time Client
	R	HPD Provider Information Consumer
User Authentication Provider	R	CT Time Client

Table 6: Required groupings of actors in this national extension

The following actors of the Swiss EPR SHALL be grouped with actors from this national extension:

EPR Actor	Optionality	Actor to be grouped with	Remark
XDS Document Consumer	R	X-Service User	Workflow Initiator
XDS Document Source	R	X-Service User	Workflow Initiator or Technical User
XDS-I.b Imaging Document Consumer	R	X-Service User	Workflow Initiator
XDS-I.b Imaging Document Source	R	X-Service Provider	Workflow Initiator or Technical User
XDS Metadata Update Document Administrator	R	X-Service User	Workflow Initiator
RMU Update Initiator	R	X-Service User	Workflow Initiator or Proxy Option
XCA(I) Initiating (Imaging) Gateway	R	X-Service User	Proxy Option
XCA(I) Responding (Imaging) Gateway	R	X-Service Provider	Proxy Option
CH:PPQ Policy Source	R	X-Service User	Workflow Initiator
CH:PPQ Policy Consumer	R	X-Service User	Workflow Initiator
CH:ADR Authorization Decision Consumer	R	X-Service User	Proxy Option
CH:ADR Authorization Decision Provider	R	X-Service Provider	
XDS Document Registry	R	X-Service Provider	
XDS Document Repository	R	X-Service Provider	
CH:PPQ Policy Repository	R	X-Service Provider	
RMU Update Responder	R	X-Service Provider	
CH:ATC Patient Audit Consumer	R	X-Service User	Workflow Initiator
CH:ATC Patient Audit Record Repository	R	X-Service Provider	

Table 7: Required groupings of actors in the EPR with actors defined in this national extension

1.6.4 Transactions

1.6.4.1 Authenticate User

1.6.4.1.1 Scope

The Authenticate User transaction is used by an X-Service User to pass identity claims to the User Authentication provider. The User Authentication Provider authenticates the user and returns a SAML 2 Authentication Assertion or an OpenID Connect ID Token. For details of the transaction and message semantics see Annex 8 EPRO-FDHA.

1.6.4.1.2 Use Case Roles

Actor: User Authentication Provider

Role: Verifies the authentication information, creates a SAML 2 Identity Assertion or an OpenID Connect ID Token and sends it to the X-Service User. This actor

corresponds to the term "Identity Provider" as defined and specified in Annex 8 EPRO-FDHA.

Actor: X-Service User

Role: Communicates authentication information to the User Authentication Provider and receives a SAML 2 Identity Assertion or an OpenID Connect ID Token. Communicates authorization information to the X-Assertion Provider and receives a SAML Authorization Assertion. Provides the SAML Authorization Assertion in the Provide X-User Assertion [ITI-40] transaction. This actor also corresponds to the term "Relying Party" as defined and specified in Annex 8 EPRO-FDHA.

1.6.4.1.3 Referenced Standards

For the referenced standards of this transaction see Annex 8 EPRO-FDHA.

1.6.4.1.4 Interaction Diagram

For details on the transaction, the message semantics and the interaction diagram see Annex 8 EPRO-FDHA.

1.6.4.2 Get X-User Assertion

1.6.4.2.1 Scope

The Get X-User Assertion transaction is used by an X-Service User to pass claims to the X-Assertion Provider. The X-Assertion Provider validates the claims and returns a XUA Token with the attributes required to enforce access rights according to the regulations of the Federal Act on Electronic Patient Records.

1.6.4.2.2 Use Case Roles

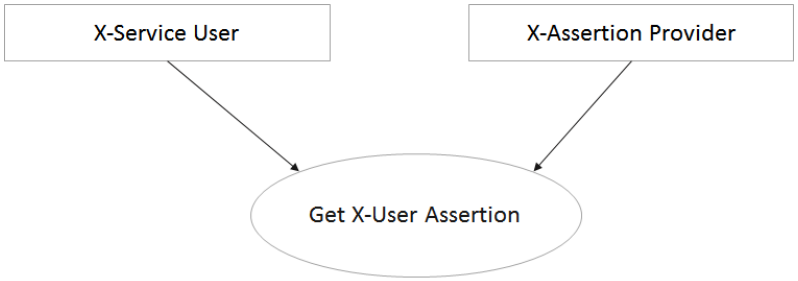


Figure 5: Use Case Roles for Get X-User Assertion

Actor: X-Service User

Role: Communicates authentication information to the User Authentication Provider and receives a SAML 2 Identity Assertion or an OpenID Connect ID Token. Communicates authorization information to the X-Assertion Provider and receives a SAML Authorization Assertion. Provides the SAML Authorization Assertion in the Provide X-User Assertion [ITI-40] transaction.

Actor: X-Assertion Provider

Role: Verifies authorization information, creates a SAML Authorization Assertion and sends it to the X-Service User.

1.6.4.2.3 Referenced Standards

The following standards are normative for this transaction:

a. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

b. Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0
https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

c. 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

d. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

e. Security Assertion Markup Language (SAML) V2.0 Technical Overview Committee Draft 02, 25 March 2008
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

f. Web Services Security: SAML Token Profile 1.1
https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

g. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

h. WS-Trust 1.3
http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html

i. OASIS eXtensible Access Control Markup Language (XACML) v2.0
https://www.oasis-open.org/standards#xacmlv2.0

j. 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

k. OASIS SAML 2.0 profile of XACML v2.0
http://docs.oasis-open.org/xacml/xacml-saml-profile/v2.0/xacml-saml-profile-v2.0.html

1.6.4.2.4 Interaction Diagram

The interactions Get X-User Assertion request and response are normative for this national extension. Other shown interactions are informative and assist with understanding or implementing this transaction.

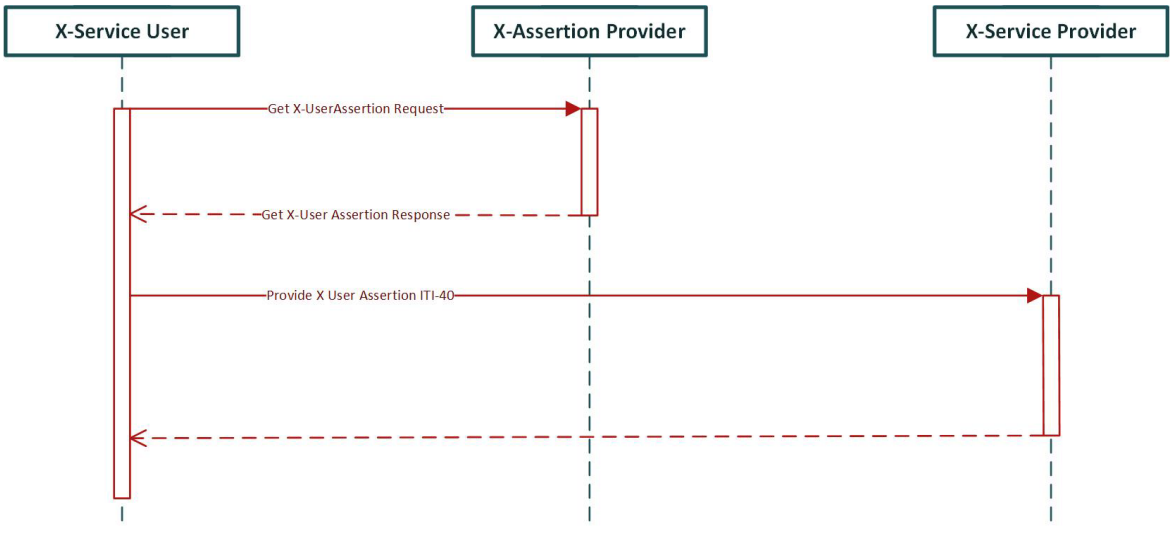


Figure 6: Get X-User Assertion interaction diagram

1.6.4.2.4.1 Trigger Events

The Get X-User Assertion transaction SHALL be executed when an X-Service User actor aims to request a protected resource from an actor grouped with the X-Service Provider and one of the following events occur:

a. the current session has no assigned XUA token;
b. the claimed attributes change during the current user session;
c. the time interval defining the validity period of the XUA token is exceeded or is expected to exceed soon.

1.6.4.2.4.2 Message Semantics

The message model of Get X-User Assertion transaction implements the message model of the Security Token Framework defined in WS-Trust 1.3.

The Get X-User Assertion response message extends the <wst:RequestSecurityTokenResponse> message defined in WS-Trust 1.3. In addition to the mandatory elements defined in WS-Trust 1.3, the Get X-User Assertion response SHALL contain a <wst:RequestedSecurityToken> element with a <saml2:Assertion> as defined in section 1.6.4.3 below or a WS-Trust 1.3 error response detailed in section 1.6.4.2.4.4, if the request was invalid, malformed or not understood for other reasons.

The Get X-User Assertion request message extends the <wst:RequestSecurityToken> message defined in WS-Trust 1.3. In addition to the elements defined in WS-Trust 1.3, the Get X-User Assertion request SHALL contain a <wst:Claims> element with the Dialect set to "http://www.bag.admin.ch/epr/2017/annex/5/amendment/2".

The <wst:Claims> element SHALL have the following child elements:

a. There SHALL be an <Attribute> element with name "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse". The <AttributeValue> child element SHALL convey a coded value of the current transaction's <PurposeOfUse>. There are four values to be distinguished within the EPR: Normal Access, Emergency Access, Automatic Upload of non DICOM Documents (for Document Sources in the role Technical User, TCU) and Automatic Upload of DICOM Contents (for Imaging Document Sources in the role Technical User, TCU) with the corresponding codes NORM, EMER, AUTO and DICOM_AUTO from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.
b. There SHALL be one <Attribute> element with name "urn:oasis:names:tc:xacml:2.0:subject:role". The <AttributeValue> child element SHALL convey a coded value of the subject's <Role>.
c. There SHALL be an <Attribute> element with name "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The <AttributeValue> SHALL convey the EPR-SPID identifier of the patient's record and the patient assigning authority formatted in CX syntax as specified in the XUA profile.

Depending on the extension used additional <Attribute> are required, as described in the following sections.

1.6.4.2.4.2.1 Healthcare Professional Extension

For healthcare professionals the Get X-User Assertion request SHALL convey the SAML 2 Identity Assertion or an OpenID Connect ID Token retrieved from the Authenticate User transaction response described above. If present, the SAML 2 Identity Assertion SHALL be contained in the Web Service security header of the SOAP message.

If present, the OpenID Connect ID Token SHALL be contained in the <BinarySecurityToken> element of the Web Service security header with the *ValueType* attribute set to *urn:e-health-suisse:2021:JWT-Identity-Token* and the *Encoding Type* attribute set to *Base64Binary*.

In the healthcare professional extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be the code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

1.6.4.2.4.2.2 Assistant Extension

For assistants the Get X-User Assertion request SHALL convey the SAML 2 Identity Assertion or an OpenID Connect ID Token retrieved from the Authenticate User transaction response described above. If present, the SAML 2 Identity Assertion SHALL be contained in the Web Service security header of the SOAP message.

If present, the OpenID Connect ID Token SHALL be contained in the <BinarySecurityToken> element of the Web Service security header with the *ValueType* attribute set to *urn:e-health-suisse:2021:JWT-Identity-Token* and the *Encoding Type* attribute set to *Base64Binary*.

The following attributes SHALL be added to the <wst:Claims> element of the Get X-User Assertion request with the assistant extension:

a. There SHALL be one <Attribute> element with name "urn:e-health-suisse:principal-id". The <AttributeValue> child element SHALL convey the GLN of the healthcare professional an assistant is acting on behalf of.
b. There SHALL be one <Attribute> element with the attribute name "urn:e-health-suisse:principal-name". The <AttributeValue> child element SHALL convey the name of the healthcare professional an assistant is acting on behalf of.

In the assistant extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be the code ASS from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

The following optional attributes MAY be used in the <wst:Claims> element of the Get X-User Assertion request in the assistant extension:

a. There MAY be one or more <Attribute> elements with name "urn:oasis:names:tc:xspa:1.0:subject:organization". If present the <AttributeValue> child element SHALL convey a plain text the subject's organization is named by.
b. There MAY be one or more <Attribute> elements with name "urn:oasis:names:tc:xspa:1.0:subject:organization-id". If present the <AttributeValue> child element SHALL convey the ID of the subject's organization or group. The ID SHALL be an OID in the format of an URN.

1.6.4.2.4.2.3 Technical User Extension

In the technical user extension the system or application SHALL be authenticated with a SAML 2 Identity Assertion in the security header of the SOAP message of the Get X-User Assertion request.

In the technical user extension the SAML 2 Identity Assertion SHALL be signed by the technical user with a private key that uniquely identifies the technical user. The SAML 2 Identity Assertion SHALL convey the unique ID of the technical User in the name identifier and a subject confirmation with bearer method in the <saml2:Subject> element.

The following attributes SHALL be added to the <wst:Claims> element of the Get X-User Assertion request with the technical user extension:

a. There SHALL be one <Attribute> element with name attribute "urn:e-health-suisse:principal-id". The <AttributeValue> child element SHALL convey the GLN of the legal responsible healthcare professional the technical user is acting on behalf of.
b. There SHALL be one or more <Attribute> elements with name attribute "urn:e-health-suisse:principal-name".The <AttributeValue> child element SHALL convey the name of the legal responsible healthcare professional the technical user is acting on behalf of.

In the technical user extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be code TCU from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

In the technical user extension the purpose of use claim ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be code AUTO or DICOM_AUTO from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.2.4.2.4 Policy Administrator Extension

For policy administrators the Get X-User Assertion request SHALL convey the SAML 2 Identity Assertion or an OpenID Connect ID Token retrieved from the Authenticate User transaction response described above. If present, the SAML 2 Identity Assertion or an OpenID Connect ID Token SHALL be contained in the Web Service security header of the SOAP message.

If present, the OpenID Connect ID Token SHALL be contained in the <BinarySecurityToken> element of the Web Service security header with the *ValueType* attribute set to *urn:e-health-suisse:2021:JWT-Identity-Token* and the *Encoding Type* attribute set to *Base64Binary*.

In the policy administrator extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be code PADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

In the policy administrator extension the purpose of use claim ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.2.4.2.5 Document Administrator Extension

For document administrators the Get X-User Assertion request SHALL convey the SAML 2 Identity Assertion or an OpenID Connect ID Token retrieved from the Authenticate User transaction response described above.

If present, the SAML 2 Identity Assertion SHALL be contained in the Web Service security header of the SOAP message.

If present, the OpenID Connect ID Token SHALL be contained in the <BinarySecurityToken> element of the Web Service security header with the *ValueType* attribute set to *urn:e-health-suisse:2021:JWT-Identity-Token* and the *Encoding Type* attribute set to *Base64Binary*.

In the document administrator extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be code DADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

In the document administrator extension the purpose of use claim ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.2.4.2.6 Patient Extension

For patients the Get X-User Assertion request SHALL convey the SAML 2 Identity Assertion or an OpenID Connect ID Token retrieved from the Authenticate User transaction response described above.

If present, the SAML 2 Identity Assertion SHALL be contained in the Web Service security header of the SOAP message.

If present, the OpenID Connect ID Token SHALL be contained in the <BinarySecurityToken> element of the Web Service security header with the *ValueType* attribute set to *urn:e-health-suisse:2021:JWT-Identity-Token* and the *Encoding Type* attribute set to *Base64Binary*.

In the patient extension the role claim ("urn:oasis:names:tc:xacml:2.0:subject:role") attribute SHALL be the code PAT from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

In the patient extension the purpose of use claim ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be the code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

The following optional attributes MAY be added to the <wst:Claims> element of the Get X-User Assertion request in the patient extension:[10]

[10] While the assistant and technical user extension use the principal claims according to the SAML 2 Delegation Specification, in the patient and representative extension the principal claims have a different meaning as explained in section 1.6.4.2.4.4.

a. There MAY be one <Attribute> element with name "urn:e-health-suisse:principal-id". If present, the <AttributeValue> child element SHALL convey the unique ID of the representative registered in the community data stores.
b. There MAY be one <Attribute> element with the attribute name "urn:e-health-suisse:principal-name". If present, the <AttributeValue> child element SHALL convey the name of the representative registered in the community data stores.

1.6.4.2.4.3 Expected Actions X-Service User

There are no further requirements defined for the X-Service User for the Get X-User Assertion transaction.

1.6.4.2.4.4 Expected Actions X-Assertion Provider

The X-Assertion Provider SHALL validate the claims as described in the following sections. If the validation succeeds, the X-Assertion Provider SHALL return SAML 2 Authorization Assertion as defined in section 1.6.4.3.4.2.

The X-Assertion Provider SHALL authenticate the transaction by validating the SAML 2 Identity Assertion or the OpenID Connect ID Token in the Web Service security header. Authentication with a SAML 2 Assertion SHALL be supported, while authentication with an OpenID Connect ID Token MAY be supported by the X-Assertion Provider.

In case the validation fails, the X-Assertion Provider SHALL respond with an error message as described in WS-Trust 1.3. The following specialization for the Swiss EPR SHALL be applied:

Error that occurred (fault string)	Fault code (fault code)	Remark
The request was invalid or malformed	`wst:InvalidRequest`	SHALL be used, if required claims are missing, wrong or if the claims are not according to the extensions defined below.
Authentication failed	`wst:FailedAuthentication`	SHALL be used, if the signature of the SAML 2 Identity Assertion or the OpenID Connect ID Token in the security header of the Get X-User Assertion Request is not from a certified identity provider nor from a technical user registered in the community as an authorized Document Source.

Table 8: Error and corresponding codes of the Get X User Assertion transaction

1.6.4.2.4.4.1 Healthcare Professional Extensions

In the healthcare professional extension the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion or the OpenID Connect ID Token conveyed in the security header. The X-Assertion Provider actor SHALL proof that the assertion or the OpenID Connect ID Token was signed by the claimed User Authentication Provider as registered in the community data stores. In addition the X-Assertion Provider actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion or the OpenID Connect ID Token is neither exceeded nor below the limit.

The SAML 2 Identity Assertion or the OpenID Connect ID Token in the security header MAY convey the GLN of the authenticated healthcare professional. If present, the X-Assertion Provider SHALL use the GLN from the SAML 2 Identity Assertion or the OpenID Connect ID Token in the <NameID> of the subject in the <Assertion> returned with the Get X-User Assertion Response message. If not,

the X-Assertion Provider actor SHALL query the community data stores to resolve the Name ID of the <Subject> element to the GLN of the healthcare professional to be returned in the <Assertion> with the Get X-User Assertion response message.

In the healthcare professional extension the X-Assertion Provider SHALL proof, that the GLN of the healthcare professional is registered in the Provider Information Directory.

The X-Assertion Provider actor SHALL query the Healthcare Provider Directory and resolve the GLN of the healthcare professional to all groups including all superior group up to the root level. The X-Assertion Provider actor SHALL add the group IDs and the group names in an ordered sequence to the Get X-User Assertion response message.

1.6.4.2.4.4.2 Assistant Extension

In the assistant extension the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion or the OpenID Connect ID Token conveyed in the security header. The X-Assertion Provider actor SHALL proof that the assertion or the OpenID Connect ID Token was signed by the claimed User Authentication Provider as registered in the community data stores. In addition the X-Assertion Provider actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion or the OpenID Connect ID Token is neither exceeded nor below the limit.

The SAML 2 Identity Assertion in the security header MAY convey the GLN of the authenticated assistant. If present, the X-Assertion Provider SHALL use the GLN from the SAML 2 Identity Assertion to resolve the attributes conveyed with the <Assertion> in the Get X-User Assertion or the OpenID Connect ID Token response message. If not, the X-Assertion Provider actor SHALL query the community data stores to resolve the Name ID of the <Subject> element to the GLN of the assistant.

The X-Assertion Provider SHALL validate, that the GLN of the assistant is registered in the community data stores and is authorized to act on behalf of the healthcare professional declared in the claim attribute "urn:e-health-suisse:principal-id" of the Get X-User Assertion request.

If present the X-Assertion Provider SHALL read the group IDs claimed in the <Attribute> element with name "urn:oasis:names:tc:xspa:1.0:subject:organization-id" from the Get X-User Assertion request and verify the membership of the healthcare professional the assistant is acting on behalf of. If true, the X-Assertion Provider SHALL query the Healthcare Provider Directory and resolve the claimed groups and all superior groups up to the root level. The X-Assertion Provider actor SHALL add the group IDs and the group names in an ordered sequence to the Get X-User Assertion response message.

If no groups are claimed in the Get X-User Assertion, the X-Assertion Provider SHALL query the Healthcare Provider Directory and resolve the GLN of the healthcare professional to all groups including all superior groups up to the root level. The X-Assertion Provider actor SHALL add the group IDs and the group names in an ordered sequence to the Get X-User Assertion response message.

1.6.4.2.4.4.3 Technical User Extension

In the technical user extension the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion conveyed in the security header.

In the technical user extension the X-Assertion Provider SHALL use the Name ID of the <Subject> element and query the community data stores for the X.509 certificate registered with the technical user. The X-Assertion Provider actor SHALL authenticate the technical user by validating the signature of the Assertion with the certificate registered with the technical user. If present, an optional <KeyInfo> element in the SAML 2 Identity Assertion with a X.509 certificate SHALL be ignored by the X-Assertion Provider.

The X-Assertion Provider actor SHALL validate, that the Name ID of the <Subject> element of Get X-User Assertion request of the technical user is registered in the community data stores as authorized to act on behalf of the healthcare professional declared in the claim attribute "urn:e-health-suisse:principal-id" of the Get X-User Assertion request. In addition the X-Assertion Provider

actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion is neither exceeded nor below the limit.

1.6.4.2.4.4.4 Policy Administrator Extension

In the policy administrator extensions the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion or the OpenID Connect ID Token conveyed in the security header. The X-Assertion Provider actor SHALL proof that the assertion or the OpenID Connect ID Token was signed by the claimed User Authentication Provider as registered in the community data stores. In addition the X-Assertion Provider actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion or the OpenID Connect ID Token is neither exceeded nor below the limit.

In the administrator extension the X-Assertion Provider SHALL use the Name ID of the <Subject> element in the SAML 2 Identity Assertion or the subject identifier of the OpenID Connect ID Token from the security header and resolve it to the unique ID of the administrator as registered in community data stores.

1.6.4.2.4.5 Document Administrator Extension

See 1.6.4.2.4.4

1.6.4.2.4.6 Patient Extension

In the patient extension the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion or the OpenID Connect ID Token conveyed in the security header. The X-Assertion Provider actor SHALL proof that the assertion or the OpenID Connect ID Token was signed by the claimed User Authentication Provider as registered in the community data stores. In addition the X-Assertion Provider actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion or the OpenID Connect ID Token is neither exceeded nor below the limit.

The X-Assertion Provider MAY accept the principal ID and name claims of a Get X-User Assertion, only if the request is performed by a X-Service User from inside the certified community without further validation. If the request is performed by a X-Service User which is not inside the certification scope of the community, the X-Assertion Provider SHALL use the Name ID of the <Subject> element in the SAML 2 Identity Assertion or the subject identifier of the OpenID Connect ID Token from the security header and resolve it to the EPR-SPID by querying the community data stores.

1.6.4.2.4.7 Representative Extension

In the representative extension the X-Assertion Provider SHALL validate the SAML 2 Identity Assertion or the OpenID Connect ID Token conveyed in the security header. The X-Assertion Provider actor SHALL proof that the assertion or the OpenID Connect ID Token was signed by the claimed User Authentication Provider as registered in the community data stores. In addition the X-Assertion Provider actor SHALL check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion or the OpenID Connect ID Token is neither exceeded nor below the limit.

The X-Assertion Provider MAY accept the principal ID and name claims of a Get X-User Assertion, only if the request is performed by a X-Service User from inside the certified community without further validation. If the request is performed by a X-Service User which is not inside of the scope of the certified community, the X-Assertion Provider SHALL use the Name ID of the <Subject> element in the SAML 2 Identity Assertion or the OpenID Connect ID Token from the security header and resolve it to the EPR-SPID of the patient by querying the community data stores.

1.6.4.2.5 Security Consideration

In the Swiss EPR all actors grouped with the X-Service User SHALL be grouped with ATNA Secure Node or Secure Application Actor with "STX: TLS 1.2 floor using BCP195 Option". In addition, the

X-Assertion Provider SHALL be grouped with the ATNA Secure Application Actor with "STX: TLS 1.2 floor using BCP195 Option" defined in the IHE ITI TF-2[11], chapter 3.19.6.2.3.

There are no requirements on the audit trail of the Get X-User Assertion transaction in this national extension. Instead there might be inherited requirements from actors grouped with the X-Service User to protocol information from the XUA Assertion in ATNA logs of the transactions.

1.6.4.3 Provide X-User Assertion [ITI-40]

This section describes the national extension for the Swiss EPR of the Provide X-User Assertion [ITI-40] transaction defined in IHE ITI TF-2[12].

1.6.4.3.1 Scope

In the Swiss EPR the Provide X-User Assertion [ITI-40] transaction is used by the X-Service User to convey an assertion to actors grouped with the X-Service Provider in order to enable the enforcement of the access rights as defined in the Federal Act on Electronic Patient Records (EPRA).

1.6.4.3.2 Use Case Roles

Actor: X-Service User

Role: Provides a SAML Authorization Assertion in the Provide X-User Assertion [ITI-40] transaction.

Actor: X-Service Provider

Role: Receives a SAML Authorization Assertion to enable grouped actors to enforce access rights policies.

1.6.4.3.3 Referenced Standards

The following standards are normative for this national extension:

a. Security Assertion Markup Language (SAML) V2.0 Technical Overview Committee Draft 02, 25 March 2008 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf

b. Web Services Security: SAML Token Profile 1.1 https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

c. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

d. OASIS SAML V2.0 Condition for Delegation Restriction Version 1.0 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation-cs-01.pdf

1.6.4.3.4 Interaction Diagrams

1.6.4.3.4.1 Trigger Events

The Provide X-User Assertion [ITI-40] transaction SHALL be executed when an X-Service User actor aims to request a protected resource from an actor grouped with the X-Service Provider, which enforces authorization.

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

1.6.4.3.4.2 Message Semantics

A SAML 2.0 Authorization Assertion SHALL be conveyed in the WS-Security SOAP Header of transaction request messages to communicate entity attributes as described in the Provide X-User Assertion [ITI-40] in IHE ITI TF-2[12].

The EPR SAML 2.0 Authorization Assertion SHALL contain child elements <Issuer>, <Signature>, <Subject>, <Conditions>, <AuthnStatement> and <AttributeStatement>. The <AttributeStatement> element carries a number of attributes that reflect the identity claims being made.

The EPR requires the following details to be conveyed within the <Assertion>:

The <Issuer> element indicates the system that issued the token and therefore confirms that the identified user was properly authenticated and that the attributes included in the token are accurate. For further details see [SAML 2.0].

The <Signature> element conveys a X.509 signature created by the X-Assertion Provider actor to guaranty the confidentiality of the claims being made and unaltered content of the assertion. For further details see [SAML 2.0].

The <Subject> element identifies the Requester Entity. This element SHALL contain a SAML 2.0 <NameID> child element with the format attribute "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" in all extensions. The further requirements depend on the extension and are defined in the corresponding sections.

The <Subject> element MAY have a second child element <SubjectConfirmation> with the following attribute: @Method="urn:oasis:names:tc:SAML:2.0:cm:bearer". The further requirements on this element depend on the extension and are defined in the corresponding sections.

The <Conditions> element specifies a validity period (timestamps) to prevent "replay" of the assertion while attributes MAY have changed. The time period is not specified in this national extension and SHALL be chosen according to the regulations of the community. An audience restriction (urn:e-health-suisse:token-audience:all-communities) specifies the intended recipient or system the assertion SHALL be valid for. The reuse of the token (signed SAML identity assertion) MAY be denied by setting a <OneTimeUse> element. For further details see [SAML 2.0].

The further requirements on this element depend on the extension and are defined in the corresponding sections.

The <AuthnStatement> element specifies the authentication procedure by which the entity's identity (e.g. a user) was verified. For further details see [SAML 2.0].

The <AttributeStatement> element identifies the Requester Entity's attributes / identity claims. The following requirements hold for the <Attribute> child elements:

a. There SHALL be one <Attribute> element with the name attribute "urn:oasis:names:tc:xspa:1.0:subject:subject-id". The <AttributeValue> child element SHALL convey the subject's real world name as plain text as defined by IHE XUA in all extensions.
b. There SHALL be one <Attribute> element with the name attribute "urn:oasis:names:tc:xacml:2.0:subject:role". The <AttributeValue> child element SHALL convey a coded value of the subject's role.
c. There SHALL be one <Attribute> element with the name attribute "urn:oasis:names:tc:xspa:1.0:subject:organization-id". The <AttributeValue> child elements SHALL convey the ID of the subject's organizations or groups registered in the HPD or empty, if not known.
d. There SHALL be one <Attribute> elements with the name attribute: "urn:oasis:names:tc:xspa:1.0:subject:organization". The <AttributeValue> child elements SHALL convey a plain text the subject's organization name as registered in the HPD or empty, if not known.
e. There SHALL be one <Attribute> element with the name attribute: "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The <AttributeValue> SHALL convey the EPR-SPID identifier of the patient's record and the patient assigning authority formatted in CX syntax as specified in the XUA profile.

f. There SHALL be one <Attribute> element with the name attribute: "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse". The <AttributeValue> child element SHALL convey a coded value of the current transaction's purpose of use.

g. There SHALL be one <Attribute> element with the name attribute:

h. "urn:ihe:iti:xca:2010:homeCommunityId". The <AttributeValue> child element SHALL convey the value of the Home Community ID (an Object Identifier) assigned to the Community that is initiating the request, using the urn format (that is, "urn:oid: " appended with the OID).

1.6.4.3.4.2.1 Healthcare Professional Extension

In the healthcare professional extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> SHALL contain the GLN of the subject with name qualifier attribute set to "urn:gs1:gln".

In the healthcare professional extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

b. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") SHALL be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

c. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") SHALL convey the identifiers of the organizations or groups the subject is assigned to. The identifiers SHALL be OID in the format of URN as registered in the healthcare provider directory.

d. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") of the <AttributeStatement> SHALL convey the name of the organizations or groups the subject is a member of.

e. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") of the <AttributeStatement> SHALL be either code NORM or EMER from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.2 Assistant Extension

The assistant extension uses the SAML 2 Condition for Delegation Restriction Version 1.0 to manage the relationship between the assistant and the healthcare professional the assistant is acting on behalf of.

In the assistant extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the GLN of the subject (responsible healthcare professional) with name qualifier attribute set to "urn:gs1:gln".

b. The <SubjectConfirmation> element SHALL contain a <NameID> child element. The <NameID> element SHALL convey the GLN of the assistant with name qualifier attribute set to "urn:gs1:gln".

c. The <SubjectConfirmation> element SHALL contain a <SubjectConfirmationData> child element with one <AttributeStatement> which conveys the assistant real name as plain text in an <Attribute> with name "urn:oasis:names:tc:xspa:1.0:subject:subject-id".

In the assistant extension the <Assertion> SHALL contain a <Conditions> element conveying the relation of the assistant to the healthcare professional the assistant is acting on behalf of. The following requirements hold for the <Conditions> element:

d. The NotBefore and NotOnOrAfter attributes of the <Conditions> element SHALL define a valid time interval.

e. The <Conditions> element SHALL contain a <AudienceRestriction> element coveying a single <Audience> child element with the value set to "urn:e-health-suisse:token-audience:all-communities".

f. The <Conditions> element SHALL contain a single <Condition> element with Type-Attribute "DelegationRestrictionType". The <Condition> element SHALL contain a single <Delegate> element with a <NameID> child element. The <NameID> element SHALL have a Format attribute with value "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" and a NameQualifier attribute with value "urn:gs1:gln" conveying the GLN of the assistant.

In the assistant extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

g. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") of the <AttributeStatement> SHALL be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

h. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") of the <AttributeStatement> SHALL convey the identifiers of the organizations or groups the subject is assigned to. The identifier SHALL be OID in the format of URN as registered in the healthcare provider directory.

i. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") of the <AttributeStatement> SHALL convey the name of the organizations or groups the subject is assigned to.

j. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") of the <AttributeStatement> SHALL be either code NORM or EMER from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.3 Technical User Extension

The technical user extension uses the SAML 2 Condition for Delegation Restriction Version 1.0 to manage the relationship between the technical user and the healthcare professional the technical user is acting on behalf of.

In the technical user extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the GLN of the subject (responsible healthcare professional) with name qualifier attribute set to "urn:gs1:gln".

b. The <SubjectConfirmation> element SHALL contain a <NameID> child element. The <NameID> element SHALL convey the unique ID the technical user is registered within the community and NameQualifier "urn:e-health-suisse:technical-user-id".

In the technical user extension the <Assertion> SHALL contain a <Conditions> element conveying the relation of the technical user to the healthcare professional the technical user is acting on behalf of. The following requirements hold for the <Conditions> element:

c. The NotBefore and NotOnOrAfter attributes of the <Conditions> element SHALL define a valid time interval.

d. The <Conditions> element SHALL contain a <AudienceRestriction> element coveying a single <Audience> child element with the value set to "urn:e-health-suisse:token-audience:all-communities".

e. The <Conditions> element SHALL contain a single <Condition> element with Type-Attribute "DelegationRestrictionType". The <Condition> element SHALL contain a single <Delegate> element with a <NameID> child element. The <NameID> element SHALL have a Format attribute with value "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" and a NameQualifier attribute with value "urn:e-health-suisse:technical-user-id" conveying the unique ID the technical user is registered with in the community.

In the technical user extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

f. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") of the <AttributeStatement> SHALL be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

g. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") SHALL convey the identifiers of the organizations or groups the subject (i.e. the responsible healthcare professional) is assigned to. The identifier SHALL be OID in the format of URN as registered in the healthcare provider directory.

h. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") SHALL convey the names of the organizations or groups the subject is assigned to.

i. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") SHALL be code AUTO or DICOM_AUTO from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.4 Policy Administrator Extension

In the document administrator extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the unique ID the administrator is registered with in the community and the name qualifier attribute set to "urn:e-health-suisse:document-administrator-id".

In the document administrator extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

b. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") SHALL be code DADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

c. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element SHALL be empty.

d. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element SHALL be empty.

e. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.5 Document Administrator Extension

In the document administrator extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the unique ID the administrator is registered with in the community and the name qualifier attribute set to "urn:e-health-suisse:document-administrator-id".

In the document administrator extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

b. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") SHALL be code DADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

c. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element SHALL be empty.

d. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element SHALL be empty.

e. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.6 Patient Extension

In the patient extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the EPR-SPID of the patient with name qualifier attribute set to "urn:e-health-suisse:2015:epr-spid".

In the patient extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

b. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") SHALL be code PAT from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

c. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element SHALL be empty.

d. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element SHALL be empty.

e. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.7 Representative Extension

In the representative extension the following requirements hold for the <Subject> element of the <Assertion>:

a. The <NameID> child element of the <Subject> element SHALL contain the unique ID the representative is registered with in the community and the name qualifier attribute set to "urn:e-health-suisse:representative-id".

In the representative extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:

b. The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") SHALL be code REP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

c. The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element SHALL be empty.

d. The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element SHALL be empty.

e. The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") SHALL be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.3 Expected Actions X-Service User

There are no further requirements defined for the X-Service User in the Provide X-User Assertion [ITI-40] transaction beyond those defined in the IHE XUA Profile.

1.6.4.3.4.4 Expected Actions X-Service Provider

There are no further requirements defined for the X-Service Provider in the Provide X-User Assertion [ITI-40] transaction beyond those defined in the IHE XUA Profile.

1.6.4.3.5 Security Consideration

The SAML 2 Authorization Assertion SHALL be protected against confidentiality risks. In the Swiss EPR all actors grouped with the X-Service User and X-Service Provider are required to be grouped with ATNA Secure Node or Secure Application Actor implementing the "STX: TLS 1.2 floor using BCP195 Option" defined in the IHE ITI TF-2[13], chapter 3.19.6.2.3.

There are no requirements on the audit trail of the Provide X-User Assertion [ITI-40] transaction in this national extension. Instead there might be inherited requirements from actors grouped with the X-Service User or X-Service Provider to protocol information from the XUA Assertion in ATNA logs of the transactions.

1.6.4.3.5.1 Specifying ActiveParticipants in ATNA records

Whenever a transaction was secured by XUA, the corresponding ATNA record SHALL include the following set of <ActiveParticipant> elements related to involved users:

a. The first element SHALL be built according to IHE XUA requirements described in IHE ITI TF-2[13], chapter 3.40.4.2 (with or without subject role specification).

b. The second element describes the main user (the subject of the XUA assertion) and SHALL have the following contents:

Attribute	Sub-element	Description	Source of data in the XUA assertion
`@UserID`		ID of the user: GLN for a HCP, EPR-SPID for the patient, or the ID of the representative.	Text contents of the element `/Assertion/Subject/NameID`
`@UserName`		Real-world name of the user	Text contents of the element `/Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"]/AttributeValue`
`RoleIDCode`		Role of the user	
	`@csd-code`	Role code	Contents of the attribute `/Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xacml:2.0:subject:role"]/AttributeValue/Role/@code`
	`@codeSystemName`	Coding system OID of the role code	Contents of the attribute `/Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xacml:2.0:subject:role"]/AttributeValue/Role/@codeSystem`
	`@originalText`	Description of the role	Contents of the attribute `/Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xacml:2.0:subject:role"]/AttributeValue/Role/@displayName`

Table 9: Required attributes of the second <ActiveParticipant> element of the ATNA record

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

The third element is required, if some other person acted on behalf of the main user, and SHALL have the following contents:

Attribute	Sub-element	Description	Source of data in the XUA assertion / data derivation rule
`@UserID`		ID of the assistant or technical user	Text contents of the element `/Assertion/Subject/SubjectConfirmation/NameID`
`@UserName`		Real-world name of the assistant or technical user	Text contents of the element `/Assertion/Subject/SubjectConfirmation/SubjectConfirmationData/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"]/AttributeValue`
`RoleIDCode`		Role of the assistant or technical user	
	`@csd-code`	Role code	• ASS, if the role of the main user is HCP and //SubjectConfirmation/NameId/@NameQualifier is "urn:gs1:gln". • TCU, if the role of the main user is HCP and //SubjectConfirmation/NameId/@NameQualifier is "urn:e-health-suisse:technical-user-id".
	`@codeSystemName`	Coding system OID of the role code	Fixed value `2.16.756.5.30.1.127.3.10.6`
	`@originalText`	Description of the role	According to the role code

Table 10: Attributes of the third <ActiveParticipant> element of the ATNA Record

Examples for various combinations of human users:

HCP, identified by GLN:

```
<ActiveParticipant UserID="alias2&l601000000000@hcportal.demo.org&gt;"
          UserName="alias2&lt; 7601000000000@hcportal.demo.org&gt;"/>
<ActiveParticipant UserID="7601000000000" UserName="Dr. Hans Muster">
  <RoleIDCode csd-code="HCP"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
originalText="Healthcare Professional" />
</ActiveParticipant>
```

ASS representing HCP, both identified by GLN:

```
<ActiveParticipant
UserID="alias2&lt;7601000000000@hcpportal.demo.org&gt;"
          UserName="alias2&lt;7601000000000@hcpportal.demo.org&gt;">
  <RoleIDCode csd-code="HCP"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Healthcare Professional" />
</ActiveParticipant>
<ActiveParticipant UserID="7601000000000" UserName="Dr. Hans Muster">
  <RoleIDCode csd-code="HCP"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Healthcare Professional" />
</ActiveParticipant>
<ActiveParticipant UserID="7601000000001" UserName="Hannelore
Fleissig">
```

```
  <RoleIDCode csd-code="ASS"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Assistant" />
</ActiveParticipant>
```

PAT, identified by EPR-SPID:

```
<ActiveParticipant Use-
rID="&lt;761337611234567897@patientportal.demo.org&gt;"
          UserName="&lt;24524352435234@patientportal.demo.org&gt;"/>
<ActiveParticipant UserID="761337611234567897" UserName="Patricia
Patientin">
  <RoleIDCode csd-code="PAT"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Patient" />
</ActiveParticipant>
```

REP representing PAT, REP identified by uuid:

```
<ActiveParticipant Use-
rID="&lt;761337611234567897@patientportal.demo.org&gt;"

UserName="&lt;761337611234567897@patientportal.demo.org&gt;"/>
<ActiveParticipant UserID="uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
UserName="Peter Representative">
  <RoleIDCode csd-code="REP"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Representative" />
</ActiveParticipant>
```

PADM, identified by uuid:

```
<ActiveParticipant UserID="alias2&lt;7601000000000@demo.org&gt;"
          UserName="alias2&lt; 7601000000000@demo.org&gt;"/>
<ActiveParticipant UserID="uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
UserName="Alice P. Admin">
  <RoleIDCode csd-code="PADM"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
originalText="Policy Administrator" />
</ActiveParticipant>
```

DADM, identified by uuid:

```
<ActiveParticipant UserID="alias2&lt;7601000000000@demo.org&gt;"
          UserName="alias2&lt; 7601000000000@demo.org&gt;"/>
<ActiveParticipant UserID="uuid:7edca82f-054d-47f2-a032-9b2a5b5186c"
UserName="Bob D. Admin">
  <RoleIDCode csd-code="DADM"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
originalText="Document Administrator" />
</ActiveParticipant>
Example for a technical user:
```

TCU identified by software ID, HCP identified by GLN:

```
<ActiveParticipant UserID="&lt;image-archive-
demohospital@demo.org&gt;"
          UserName="&lt;image-archive-demohospital@demo.org&gt;">
  <RoleIDCode csd-code="TCU"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Technical User" />
</ActiveParticipant>
<ActiveParticipant UserID="7601000000000" UserName="Dr. Hans Muster">
  <RoleIDCode csd-code="HCP"
codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Healthcare Professional" />
</ActiveParticipant>
<ActiveParticipant UserID="image-archive-demohospital" UserName="Image
Archive Demo Hospital">
<RoleIDCode csd-code="TCU" codeSystemName="2.16.756.5.30.1.127.3.10.6"
        originalText="Technical User" />
</ActiveParticipant>
```

1.7 Requirements on PIXV3 for Patient Identity Feed

This section corresponds to the transaction Patient Identity Feed HL7 V3 [ITI-44] of the IHE IT Infrastructure Technical Framework. This transaction is used by the Patient Identity Source, Patient Identifier Cross-reference Manager and Document Registry Actors. With the PIXV3 Patient Identity Feed a primary system can register a local identifier within the MPI.

1.7.1 Message Semantics

1.7.1.1 Major Components of the Patient Registry Record Added/Revised Messages

Message Information Model

The Message Information Model for both the Patient Activate and Patient Revise messages, as it is described in IHE ITI TF-2[14], Table 3.44.4.1.2.2-1 is further restricted for use in an MPI within the EPR on the following attributes:

PRPA_HD201301IHE Patient Activate/Revise	This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)	Swiss National Extension
Patient	The primary record for the focal person in a Patient Identity Source.	
classCode [1..1] (M) Patient (CS) {CNE:PAT}	Structural attribute; this is a "patient" role.	No further refinement.
id [2..2] (M) Patient (SET<II>)	Identifiers designated by this patient identity source for the focal person.	SHALL convey the patient's local ID and the EPR-SPID.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0..*] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	No further refinement.

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

PRPA_HD201301IHE Patient Activate/Revise	This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)	Swiss National Extension
veryImportantPersonCode [0..1] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	No further refinement.
Person	A subtype of LivingSubject representing a human being. At least Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/infrastructure/ datatypes_r2/datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	SHALL NOT be used.

PRPA_HD201301IHE Patient Activate/Revise	This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)	Swiss National Extension
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	SHALL NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	SHALL NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number. Please see notes above in the Major Components section on the use of OtherIDs.	No further refinement.
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	No further refinement.
id [1..*] (M) Role (SET<II>)	One or more identifiers issued to the focal person by the associated scopingOrganization (e.g., a Driver's License number issued by a DMV).	No further refinement.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	
classCode [1..1] (M) Role (CS) {CNE:PRS, fixed value= "PRS"}	Structural attribute; this is a "personal relationship" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	No further refinement.
code [1..1] (M) Role (CE) {CWE:PersonalRelationshipRoleType}	A required value specifying the type of personal relationship between the relationshipHolder and the scoping living subject drawn from the PersonalRelationshipRoleType domain, for example, spouse, parent, unrelated friend.	SHALL NOT be used.
statusCode [0..1] Role (CE) {CWE:RoleStatus}	A value specifying the state of this personal relationship (based on the RIM Role class state-machine), for example, following divorce a spouse relationship would be "terminated".	No further refinement.
effectiveTime [0..1] Role (IVL<TS>)	An interval of time specifying the period during which this personal relationship is in effect, if such time is applicable and known.	No further refinement.
Citizen	Used to capture person information relating to citizenship.	
classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.
Nation	A politically organized body of people bonded by territory and known as a nation.	

PRPA_HD201301IHE Patient Activate/Revise	This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)	Swiss National Extension
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	No further refinement.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	No further refinement.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	No further refinement.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	No further refinement.
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.
occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	No further refinement.
BirthPlace	The birthplace of the focal living subject.	
classCode [1..1] (M) Birthplace (CS) {CNE:BIRTHPL}	Structural attribute; this is a "birthplace" role.	No further refinement.
id [0..*] Birthplace (SET<II>)	A living subject's birth place represented by a unique identifier.	No further refinement.
addr [0..*] Patient (BAG<AD>)	A living subject's birth place represented as an address. Note: Either BirthPlace.addr or an associated Place.name must be valued.	No further refinement.

PRPA_HD201301IHE Patient Activate/Revise	This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)	Swiss National Extension
classCode [1..1] (M) Birthplace (CS) {CNE:BIRTHPL}	Structural attribute; this is a "birthplace" role	No further refinement.
LanguageCommunication	A language communication capability of the focal person	
languageCode [1..1] (M) LanguageCommunication (CE) {CWE:HumanLanguage}	A value representing a language for which the focal person has some level of proficiency for written or spoken communication. Examples: Spanish, Italian, German, English, American Sign.	No further refinement.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the focal person for the associated mode.	No further refinement.

Table 11: Patient Active and Revise Model Attributes

1.8 Requirements on PIXV3 for Patient Identifier Cross-reference Query

This section corresponds to transaction PIXV3 Query [ITI-45] of the IHE IT Infrastructure Technical Framework. This transaction is used by the Patient Identifier Cross-reference Consumer and Patient Identifier Cross-reference Manager Actors. With the PIXV3 Query a primary system can query with the local identifier the MPI and get the corresponding MPI-PID and the EPR-SPID.

1.8.1 Message Semantics

1.8.1.1 Major Components of the Patient Registry Query by Identifier

The Data Source parameter specifies the assigning authority/authorities of the Patient Identity Domain(s) whose identifiers SHALL be returned. The Data Source parameter SHALL be specified to the assigning authorities of the EPR-SPID and the MPI-PID in the affinity domain. Other assigning authorities SHALL not be used.

1.9 Requirements on PDQV3 for Patient Demographics Query

This section corresponds to Patient Demographics Query HL7 V3 [ITI-47] of the IHE Technical Framework. This transaction is used by the Patient Demographics Consumer and Patient Demographics Supplier Actors.

1.9.1 Message Semantics

1.9.1.1 Major Components of the Patient Registry Query by Demographics

The PatientTelecom Query Parameter SHALL NOT be used.

1.9.2 Patient Demographics Query Response

1.9.2.1 Expected Actions

The Patient Demographics Supplier shall perform the matching of patient data based on the query parameter values it receives. The information provided by the Patient Demographics Supplier to Patient Demographics Consumers is a list of possible matching patients from the patient information source associated with the value that the Consumer sent in the Device class of the transmission wrapper of the query message. See also IHE ITI TF-2[15], chapter 3.47.4.2.3.

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

The Message Information Model for both the Patient Registry Find Candidates Response messages, as it is described in IHE ITI TF-2[15], Table 3.47.4.2.2-8 is further restricted for use in an MPI within the EPR on the following attributes:

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
Patient	The primary record for the focal person in a Patient Demographics Supplier.	
classCode [1..1] (M) Patient (CS) {CNE:PAT}	Structural attribute; this is a "patient" role.	No further refinement.
id [1..*] (M) Patient (SET<II>)	Patient identifiers. Patient Identifiers from different Identity Domains may be contained either here, or in the OtherIDs.id attributes, but not in both places. At least one Patient Identifier shall be present in this attribute.	No further refinement.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0..*] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	No further refinement.
veryImportantPersonCode [0..1] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	No further refinement.
Person	A subtype of LivingSubject representing a human being either Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/ infrastructure/datatypes_r2/ datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	SHALL NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	SHALL NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	SHALL NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	No further refinement.
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	No further refinement.
id [1..*] (M) Role (SET<II>)	One or more identifiers issued to the focal person by the associated scopingOrganization (e.g., identifiers from a different Patient Identity Domain).	No further refinement.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	
classCode [1..1] (M) Role (CS) {CNE:PRS, fixed value= "PRS"}	Structural attribute; this is a "personal relationship" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	No further refinement.
code [1..1] (M) Role (CE) {CWE:PersonalRelationshipRoleType}	A required value specifying the type of personal relationship between the relationshipHolder and the scoping living subject drawn from the PersonalRelationshipRoleType domain, for example, spouse, parent, unrelated friend.	Codes: FTH= Father MTH= Mother
Citizen	Used to capture person information relating to citizenship.	

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	No further refinement.
Nation	**A politically organized body of people bonded by territory and known as a nation.**	
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	No further refinement.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	No further refinement.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	No further refinement.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	No further refinement.
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	No further refinement.
LanguageCommunication	A language communication capability of the focal person.	
languageCode [1..1] (M) LanguageCommunication (CE) {CWE:HumanLanguage}	A value representing a language for which the focal person has some level of proficiency for written or spoken communication. Examples: Spanish, Italian, German, English, American Sign.	No further refinement.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the focal person for the associated mode.	No further refinement.

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
QueryMatchObservation	Used to convey information about the quality of the match for each record.	
classCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActClass.htm - ActClass, default= "OBS"}	Structural attribute – this is an observation.	No further refinement.
moodCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	No further refinement.

Table 12: Message Information Model for Patient Registry Find Candidates

1.9.2.1.1 Special handling for more attributes requested

If there are more than 5 matches, there shall be a special handling like in the XCPD transaction (see IHE ITI TF-2[16], chapter 3.55.4.2.2.6).

The Responding Gateway has the option of informing the Initiating Gateway when additional demographic attributes may result in a match. This would most often be used in cases where the security and privacy policies do not allow release of patient data unless and until there is a level of assurance that the same patient is referenced. In this case the Responding Gateway cannot return a matching patient or patients because the level of assurance is not great enough. If the Initiating Gateway was able to specify further demographic attributes the Responding Gateway might have greater assurance of the match and thus be able to return the match information.

To indicate this situation in its response the Responding Gateway codes a DetectedIssueEvent within the controlActProcess element, where the code in the actOrderRequired element references one of the coded elements described in Table 11. There may be as many triggerFor elements, each of them containing an actOrderRequired element, as needed to code the attributes which would increase the assurance of the match. The value set for these code elements is <2.16.756.5.30.1.127.3.10.16.1> instead of 1.3.6.1.4.1.19376.1.2.27.1 as described in IHE ITI TF-2[16], Table 3.55.4.2.2.6-1.

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

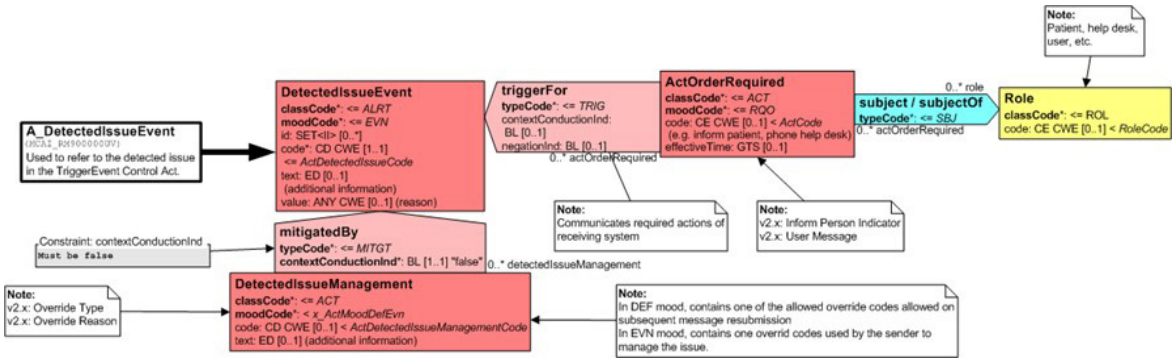


Figure 7: RIMM for DetectedIssueEvent

Value set: PDQ.actOrderRequired (OID: 2.16.756.5.30.1.127.3.10.16.1)

Value for Code	Meaning of Code	codeSystem
`LivingSubjectAdministrativeGenderRequested`	Requests the LivingSubjectAdministrativeGender attribute be specified	1.3.6.1.4.1.19376.1.2.27.1
`PatientAddressRequested`	Requests the PatientAddress attribute be specified	1.3.6.1.4.1.19376.1.2.27.1
`LivingSubjectBirthPlaceNameRequested`	Requests the LivingSubjectBirthPlaceName attribute be specified	1.3.6.1.4.1.19376.1.2.27.1
`BirthNameRequested`	Requests the Birth Name attribute be specified	2.16.756.5.30.1.127.3.10.17

Table 13: Coded Values for actOrderRequired code

The following example shows part of a response requesting the PatientAddress and the LivingSubjectAdministrativeGender attributes.

```
<detectedIssueEvent classCode="ALRT" moodCode="EVN">
<code code="ActAdministrativeDetectedIssueCode" codeSys-
tem="2.16.840.1.113883.5.4"/>
<triggerFor typeCode="TRIG">
<actOrderRequired classCode="ACT" moodCode="RQO">
<code code="PatientAddressRequested" codeSys-
tem="1.3.6.1.4.1.19376.1.2.27.1"/>
</actOrderRequired>
</triggerFor>
<triggerFor typeCode="TRIG">
<actOrderRequired classCode="ACT" moodCode="RQO">
<code code=" LivingSubjectAdministrativeGenderRequested" codeSys-
tem="1.3.6.1.4.1.19376.1.2.27.1"/>
</actOrderRequired>
</triggerFor>
</detectedIssueEvent>
```

The different return cases should be handled equivalent to the XCPD cases in IHE ITI TF-2[17], chapter 3.55.4.2.3 "Expected Actions".

1.10 Requirements on XCPD for Cross-Community Patient Discovery

XCPD is used in Switzerland for resolving the national patient identifier (EPR-SPID) into the community identifiers (MPI-PID) in another affinity domain/community. The Query can either return an exact match or no match.

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

1.10.1 Modes and Options

The Cross Gateway Patient Discovery [ITI-55] has several modes. For the EPR only the Shared/National Patient Identifier Query mode or Demographic Query and Feed mode SHALL be used. Other modes as defined in this transaction (see also IHE ITI TF-2[17], chapter 3.55.1) SHALL NOT be used.

The Patient Location Query [ITI-56] according to the Health Data Locator and Revoke Option[18] SHALL NOT be used.

1.10.2 Cross Gateway Patient Discovery Request

Caching

The Initiating Gateway may specify a duration value in the SOAP Header element of the request. This value suggests to the Responding Gateway a length of time that the Initiating Gateway recommends caching any correlation resulting from the interaction. This value SHALL NOT exceed 3 days. See also IHE ITI TF-2[17], chapter 3.55.4.1.

1.10.2.1 Major Components of the Patient Registry Query by Demographics

LivingSubjectId Parameter is the only required query Parameter. The following parameters of IHE ITI TF-2[17], chapter 3.55.4.1.2.1 MAY be used:

LivingSubjectAdministrativeGender:

value [1..1] ParameterItem (CE) {CWE:AdministrativeGender}

LivingSubjectBirthTime:

value [1..1] ParameterItem (IVL<TS>)

LivingSubjectName:

value [1..1] ParameterItem (PN)

The LivingSubjectId parameter SHALL contain the EPR-SPID.

PRPA_HD201306IHE Patient Registry Query by Demographics	**This HMD extract defines the message used to query a community for patients matching a set of demographics information. Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)**	**Swiss National Extension**
QueryByParameter	The entry point for the domain content in this query.	
`queryId [1..1] QueryByParameter (II)`	Unique identifier for the query	No further refinement.
`statusCode [1..1] (M) QueryByParameter (CS) {CNE:QueryStatusCode, fixed value="new"}`	The status of the query, shall be "new"	No further refinement.
`responseModalityCode [1..1] QueryByParameter (CS) {CNE:ResponseModality, fixed value="R"}`	The mode of the response – always real-time.	No further refinement.

[18] IHE IT Infrastructure Technical Framework Supplement, Cross-Community Patient Discovery (XCPD) Health Data Locator and Revoke Option, Revision 2.10, July 2, 2021.

PRPA_HD201306IHE Patient Registry Query by Demographics	This HMD extract defines the message used to query a community for patients matching a set of demographics information. Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)	Swiss National Extension
responsePriorityCode [1..1] QueryByParameter (CS) {CNE:QueryPriority}	Either "I" or "D" shall be specified. "I" (Immediate) indicates that the Responding Gateway is required to send an immediate response. "D" (Deferred) indicates the Responding Gateway is required to send a deferred response, see Section 3.55.6.2.	"I" shall be specified.
initialQuantity [0..1] QueryByParameter (INT)	Not supported, any value will be ignored by responder.	No further refinement.
initialQuantityCode [0..1]	Not supported, any value will be ignored by responder.	No further refinement.
QueryByParameter (CE) {CWE:QueryRequestLimit, default="RD"}		No further refinement.
MatchAlgorithm	This parameter conveys instructions to the Responding Gateway specifying the preferred matching algorithm to use and may be ignored.	
value [1..1] ParameterItem (ST)	The name of the algorithm	No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "MatchAlgorithm"}		No further refinement.
MinimumDegreeMatch	This parameter conveys instructions to the Responding Gateway specifying minimum degree of match to use in filtering results and may be ignored.	
value [1..1] ParameterItem (INT)	The numeric value of the degree of match. Shall be value between 0 and 100 .	No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "MinimumDegreeMatch"}		No further refinement.
LivingSubjectAdministrativeGender	This query parameter is a code representing the administrative gender of a person in a patient registry.	
value [1..1] ParameterItem (CE) {CWE:AdministrativeGender}		No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.administrativeGender"}		No further refinement.
LivingSubjectBirthTime	This query parameter is the birth date of a living subject.	
value [1..1] ParameterItem (IVL<TS>)	A date or date range. This parameter can convey an exact moment (e.g., January 1, 1960 @ 03:00:00 EST), an approximate date (e.g., January 1960), or even a range of dates (e.g., December 1, 1959 through March 31, 1960).	A birthdate (YYYYMMDD).

PRPA_HD201306IHE Patient Registry Query by Demographics	This HMD extract defines the message used to query a community for patients matching a set of demographics information. Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)	Swiss National Extension
`semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.birthTime"}`		No further refinement.
LivingSubjectId		
`value [1..*] (M) ParameterItem (II)`	A patient identifier, used to assist in finding a match for the query and, when so designated by the Initiating Gateway, used by the Responding Gateway in a XCA Cross Gateway Query directed to the Community designated by the homeCommunityId value specified in the Control Act Wrapper – see Section 3.55.4.1.2.4.	SHALL contain only the EPR-SPID.
`semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.id"}`		No further refinement.
LivingSubjectName	This query parameter is the name of a person. If multiple instances of LivingSubjectName are provided, the receiver must consider them as possible alternatives, logically connected with an "or".	
`value [1..1] ParameterItem (PN)`	Only one instance of the value element is allowed. Only some of the name parts may be populated. If, for example, only the family and given name parts of a person's name are sent, then the query would match all persons with that family name and given name regardless of their initials. The use attribute of the value element shall not be set to "SRCH".	No further refinement.
`semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.name"}`		No further refinement.
PatientAddress	This query parameter is a postal address for corresponding with a patient. There shall be only a single PatientAddress element.	SHALL NOT be used.
`value [1..*] ParameterItem (AD)`	Multiple instances of the value element within a Patient Address may be specified and are combined with OR logic.	SHALL NOT be used.
`semanticsText [1..1] ParameterItem (ST){default= "Patient.addr"}`		SHALL NOT be used.
LivingSubjectBirthPlaceAddress	This query parameter is a patient's birthplace represented as an address.	SHALL NOT be used.
`value [1..*] ParameterItem (SET<AD>)`		SHALL NOT be used.

PRPA_HD201306IHE Patient Registry Query by Demographics	This HMD extract defines the message used to query a community for patients matching a set of demographics information. Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)	Swiss National Extension
`semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.BirthPlace.Addr"}`		SHALL NOT be used.
LivingSubjectBirthPlaceName	This query parameter is a patient's birthplace represented as a place name.	SHALL NOT be used.
`value [1..*] ParameterItem (SET<EN>)`		SHALL NOT be used.
`semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.BirthPlace.Place.Name"}`		SHALL NOT be used.
PrincipalCareProviderId	This query parameter is the care provider identifier of a person who has been assigned as the principal care provider of this patient. The requestor may specify multiple PrincipalCareProviderId elements which responder shall consider as possible alternatives, logically connected with an "or".	SHALL NOT be used.
`value [1..1] ParameterItem (II)`	There shall have only one id in the "value" attribute.	SHALL NOT be used.
`semanticsText [1..1] ParameterItem (ST){default= "AssignedProvider.id"}`		SHALL NOT be used.
MothersMaidenName	This query parameter is the maiden name of a focal person's mother. It is included as a parameter because it is a common attribute for confirming the identity of persons in some registries. This parameter does not map to a single RIM attribute, instead, in RIM terms Mother's maiden name is the person name part of "family" with an EntityNamePartQualifier of "birth" for the person who is the player in a PersonalRelationship of type of "mother" to the focal person.	SHALL NOT be used.
`value [1..1] ParameterItem (PN)`	A person name. In this case it may consist of only the given name part, the family name part, or both.	SHALL NOT be used.
`semanticsText [1..1]`		SHALL NOT be used.
`ParameterItem (ST){default= "Person.MothersMaidenName"}`		SHALL NOT be used.

PRPA_HD201306IHE Patient Registry Query by Demographics	This HMD extract defines the message used to query a community for patients matching a set of demographics information. Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)	Swiss National Extension
PatientTelecom	This query parameter is a telecommunication address for communicating with a living subject in the context of the target patient registry. It could be a telephone number, fax number or even an email address. There shall be only a single PatientTelecom element.	SHALL NOT be used.
`value [1..*] ParameterItem (TEL)`	A telecommunication address. The scheme attribute specifies whether this is a telephone number, fax number, email address, etc. Multiple instances of the value element within a PatientTelecom may be specified and are combined with OR logic.	SHALL NOT be used.
`semanticsText [1..1] ParameterItem (ST){default= "Patient.telecom"}`		SHALL NOT be used.

Table 14: Message Information Model for the Patient Registry Query by Demographics Message

Reverse Cross Gateway Queries

Reverse Cross Gateway Queries SHALL NOT be used (see IHE ITI TF-2[19], chapter 3.55.4.1.2.4).

1.10.3 Cross Gateway Patient Discovery Response Caching

The Responding Gateway may specify a duration value in the SOAP Header element of the response. This value suggests to the Initiating Gateway a length of time that the Responding Gateway recommends caching any correlation resulting from the interaction. This value SHALL NOT exceed 3 days. See also IHE ITI TF-2[19], chapter 3.55.4.2.

1.10.3.1 Major Components of the Patient Registry Find Candidates Response Message

The QueryMatchObservation class is used to convey information about the quality of the match for the record returned by the query response. This value SHALL contain a numeric value greater 0 (0 is excluded because subjectOf element is not present if there is no match) and below or equal 100 (for an exact match) indicating the confidence in the match for this record (0 < percentage value <= 100).

The Message Information Model for the Patient Registry Find Candidates Response message is further restricted within the EPR:

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
Patient	The primary record for the focal person.	
`classCode [1..1] (M) Patient (CS) {CNE:PAT}`	Structural attribute; this is a "patient" role.	No further refinement.

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

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
id [1..1] (M) Patient (SET<II>)	The Patient Identifier to be used in subsequent XCA Cross Gateway Query transactions related to this patient when sent to the Responding Gateway sending the response. All other patient identifiers shall be specified in the OtherIDs.id attribute.	The MPI-PID SHALL be returned, if there is a match from the EPR-SPID.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	SHALL NOT be used.
veryImportantPersonCode [0] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	SHALL NOT be used.
Person	A subtype of LivingSubject representing a human being either Person.name or Patient.id must be non-null.	The Patient.id SHALL be non-null.
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1] Person (BAG<PN>) {null, fixed value nullFlavor="NA"}	Name(s) for this person. May be null i.e., <name nullFlavor="NA"/> only if the request contained only a patient identifier and no demographic data.	No further refinement.
telecom [0] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	SHALL NOT be used.
administrativeGenderCode [0] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0] Person (BL)	An indication that this person is dead.	SHALL NOT be used.
deceasedTime [0] Person (TS)	The date and time this person died.	SHALL NOT be used.

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
multipleBirthInd [0] Person (BL)	An indication that this person was part of a multiple birth.	SHALL NOT be used.
multipleBirthOrderNumber [0] Person (INT)	The order in which this person was born if part of a multiple birth.	SHALL NOT be used.
addr [0] Person (BAG<AD>)	Address(es) for corresponding with this person.	SHALL NOT be used.
maritalStatusCode [0] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	SHALL NOT be used.
religiousAffiliationCode [0] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	SHALL NOT be used.
raceCode [0] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	SHALL NOT be used.
ethnicGroupCode [0] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	SHALL NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	This node with its attributes SHALL NOT be used.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	This node with its attributes SHALL NOT be used.
Citizen	Used to capture person information relating to citizenship.	This node with its attributes SHALL NOT be used.
Nation	A politically organized body of people bonded by territory and known as a nation.	This node with its attributes SHALL NOT be used.
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	This node with its attributes SHALL NOT be used.
LanguageCommunication	A language communication capability of the focal person.	This node with its attributes SHALL NOT be used.
QueryMatchObservation	Used to convey information about the quality of the match for each record.	
classCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infra structure/vocabulary/ActClass.htm - ActClass, default= "OBS"}	Structural attribute – this is an observation.	No further refinement.

PRPA_HD201310IHE Patient Registry Find Candidates Response	This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)	Swiss National Extension
moodCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infra structure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	A numeric value between 0 (excluded) and 100 (0 < percentage value <= 100) SHALL be used (100 for an exact match).

Table 15: Message Information Model for Patient Registry Find Candidates

1.11 Requirements on HPD for Replication

1.11.1 Introduction

The Healthcare Provider Directory (HPD) profile is extended to support the incremental replication of the entire directory or parts of it to a second directory (across organizational boundaries). This extension will support the integration of multiple Swiss organizations with a single national HPD service, providing them with the support for the asynchronous synchronization of the directory content, without sacrificing their operational independence.

1.11.2 Use-case: Provider information replication

Scenario	A Provider Information Consumer is used to feed a second directory based on changes applied.
Triggering event	A new provider is published to the Provider Information Directory.
Involved actors	Provider Information Directory Provider Information Consumer
Short description	The Provider Information Consumer issues a Provider Information Delta Download transaction to retrieve valid mutations from the Provider Information Directory.
Pre-conditions	The actor is authenticated and authorized to communicate with the Provider Information Directory.
Post-conditions	The content of the Provider Information Directory is unchanged and the replication at the Provider Information Consumer is updated.
Activities flow	1. Based on a timer (or on a notification), the Provider Information Consumer issues a Provider Information Delta Download transaction to download all delta changes since the last successful transaction; 2. Optionally, some filtering criteria are processed.

Table 16: Use-case – Provider information replication

1.11.3 Actors / Transactions

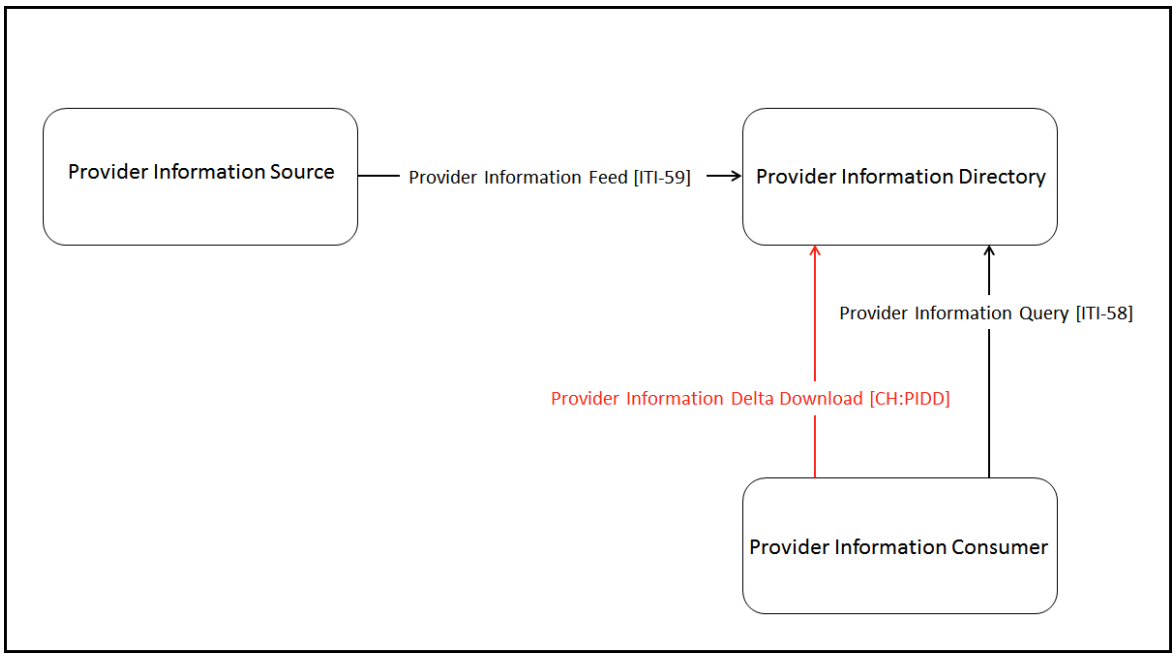


Figure 8: Swiss extended HPD Actors / Transactions

1.11.3.1 Provider Information Directory

The Provider Information Directory is extended with the following option:

`Provider Information Delta Download Option`

This option requires the implementation of the Swiss Provider Information Delta Download [CH:PIDD] transaction.

1.11.3.2 Provider Information Consumer

The Provider Information Consumer is extended with the following option:

`Provider Information Delta Download Option`

This option requires the implementation of the Swiss Provider Information Delta Download [CH:PIDD] transaction.

1.11.4 Transactions

1.11.4.1 Provider Information Delta Download [CH:PIDD]

This transaction schema extends the DSMLv2 interface by supporting an additional SOAP schema (Provider Information Delta Download schema (PIDD.xsd) and an additional wsdl operation:

```
<operation name="ProviderInformationDownloadRequest">
        <soap:operation soapAction="urn:ihe:iti:2010:ProviderInformationDownload" />
        <input>
                <soap:body use="literal" />
        </input>
        <output>
                <soap:body use="literal" />
        </output>
</operation>
```

1.11.4.1.1 Interaction Diagram

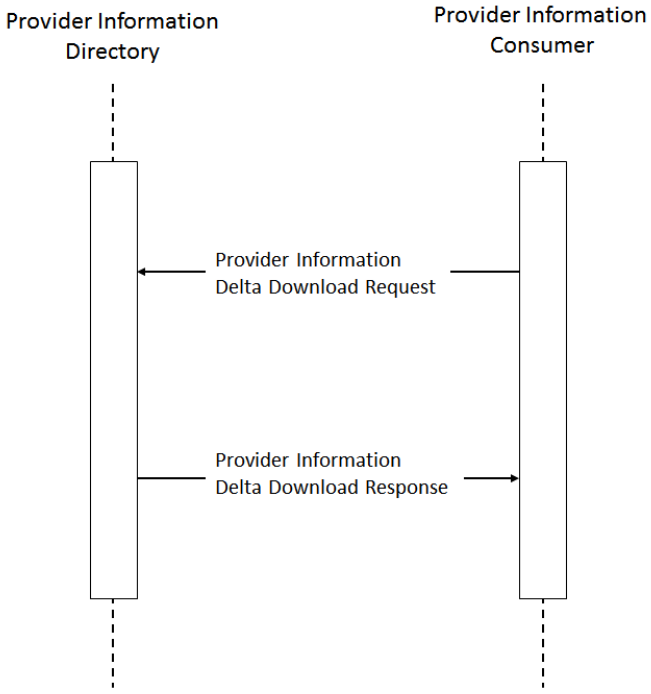


Figure 9: Provider Information Delta Download (CH:PIDD) Interaction diagram

1.11.4.1.2 Provider Information Delta Download Request

Provider Information Consumer initiates a Provider Information Delta Download Request to the Provider Information Directory. This request includes:

a. A required fromDate parameter to define the inclusive range starting date of the requested transactions sequence;

b. An optional toDate parameter to define the inclusive range ending date of the requested transactions sequence (default: current time on the central query service server);

c. An optional filterMyTransactions boolean parameter to manage the server side filtering of the author issued transactions (default: true).

The attribute "filter my transaction" in the HPD request will work as follows:

`true`: Returns the records (according to query) except those of the requesting community.

`false`: Returns all records including the ones of the requesting community.

1.11.4.1.3 Provider Information Delta Download Response

The response message contains a sequence of DSMLv2 batchRequest elements.

1.11.5 Message Semantics

1.11.5.1 HPD Schema Content

1.11.5.1.1 Identifiers

Organizational (e.g. hospitals) and Individual (healthcare professionals) Providers are identified by Object Identifiers (OID). For Individual Provider, the ID is equal to the GLN of the Individual Provider.

For IDs of Organizational Providers the following requirements shall be met:

a. If an Organizational Provider possesses an OID that is registered with a national OID register for health care OIDs, this OID has to be used.

b. If an Organizational Provider does not possess an OID that is registered in a national OID register, the OID for this Organizational Provider has to comply with ISO/IEC 9834.

c. For Swiss Organizational Providers that do not possess a unique OID registered in the Swiss healthcare OID register (RefData) , the OID consists of the RefData-registered OID for the higher-level healthcare facility this organization belongs to, plus an extension of this OID that is issued and maintained by the responsible healthcare facility.

1.11.5.1.2 Attribute

Some additional restrictions apply to the Swiss national extension of the IHE ITI HPD Profile to ensure a better quality of the data. The following sections report the list of attributes supported, together with some indications on the deviations from the original HPD profile and ISO standard for organizational providers, individual providers and the relations between the two.

Conventions:

Optionality column: O = Optional; R = Required; S = System;

Cardinality column: S = Single-valued, M = Multi-valued.

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Unique Entry Identifier	**inetOrgPerson**	**uid**	DString	S	R	validated	DN restriction	DN restriction	No further restrictions except for the technically given maximum length of 255 characters for the complete "distinguished name" (DN), including the uid. Validation if prefix correlates with currently logged-in community: "uid=<shclssuerName>:"	uid RDN = prefix:id The prefix is the name of the community (Issuing Authority) defined by the FOPH. The id SHALL be chosen by the community. The uid SHALL only contain one colon (:). Only the following characters are allowed in the DN: - Alphanumeric - Minus "-" - Colon ":" - Exclamation mark "!" - Pipe symbol "|" - Underscore "_" - Full stop "."
Provider "Identifiers"	**HCProfessional**	**hcIdentifier**	DString	M	R	validated	1	256	Issuing Authority:Type:ID:Status (where ID = GLN and Status = "active" or "inactive" or "revoked" or "suspended") Example: RefData:GLN:7601001064577:active Validation: It is validated whether at least one values that begins with *RefData:GLN:* is present. It is validated if the number after RefData:GLN: consists of thirteen digits.	

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Provider Type	**HCProfessional**	**hcProfession**	DString	M	R	validated	1	256	Only valid MDI codes according to value set HCProfessional.hcProfession (Id 2.16.756.5.30.1.127.3.10.8.1) are allowed. Format = IssuingAuthority:Code System:Code[:DisplayName] (where IssuingAuthority = BAG, CodeSystem = OID of the code system and Code = code of the respective concept) The suffix :DisplayName is optional and will not be validated against the DisplayName stored in the MDI. Thus, only the part "IssuingAuthority:Code System:Code" is validated.	
Provider Status	**HPDProvider**	**hpdProviderStatus**	DString	S	O	validated	1	64	valid values: Active, Inactive, Retired, Deceased (case insensitive validation)	
Provider Primary Name	**inetOrgPerson**	**displayName**	DString	S	R		1	256		
Provider Title	**OrganizationalPerson**	**title**	DString	S	O		1	128		object class "organizationalPerson" instead of "inetOrgPerson"
Provider First Name	**inetOrgPerson**	**givenName**	DString	M	O		1	128	contains the first name by which someone is known	Optionality: O instead of R2
Provider Middle Name	**inetOrgPerson**	**initials**	DString	M	O		1	6	contains all other first and middle names	
Provider Last Name	**person**	**sn**	DString	S	R		1	128	contains the last name	- Cardinality: S instead of M - object class: "person" instead of "inetOrgPerson"
Provider Known Names	**person**	**cn**	DString	M	R	validated	1	128	Validation: Values structured according to ISO 21091 (2013) "9.2.2.3 General name". However, the discrete structural elements are not validated. Thus validation according to: '[string], [string], [string]'. The attribute shall be filled by the communities according to ISO 21091 (2013) "9.2.2.3 Common Name". i.e.: Surname, Given Names, UID	object class: "person" instead of "inetOrgPerson"
Provider Language Supported	**HPDProvider**	**hpdProviderLanguageSupported**	DString	M	O		1	64		Encoded using ISO-639-1
Provider Gender	**Natural Person**	**gender**	PString	S	O	validated	1	64	valid values according to RFC 2985: Male ("m"|"M") or female ("f"|"F"). Values will not be validated against the MDI value set EprGender.	
Provider medical records deliver email address	**HPDProvider**	**hpdMedicalRecordsDeliveryEmailAddress**	DString	S	O		1	256		
Provider e-mail address	**inetOrgPerson**	**mail**	DString	M	O		1	256		
S-MIME Certificate	**inetOrgPerson**	**userSMIMECertificate**	OString	M	O		1	32768		
Signing Certificate	**HCProfessional**	**hcSigningCertificate**	OString	M	O		1	32768		

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
User Certificate	**inetOrgPerson**	**userCertificate**	OString	M	O		1	32768		
Creation Date	**System**	**createTimestamp**	GTime	S	System	read-only / operational			Timestamp when the value was created	
Last Update date	**System**	**modifyTimestamp**	GTime	S	System	read-only / operational			Timestamp when the value was modified	
Provider facility name	**OrganizationalPerson**	**physicalDeliveryOfficeName**	DString	M	O		1	128		- object class: "organizationalPerson" instead of "inetOrgPerson" - Optionality: O instead of R2
Provider Mailing Addresse	**HPDProvider**	**hpdProviderMailingAddress**	DString	M	O		1	4096		Optionality: O instead of R2
Provider Billing address	**HPDProvider**	**hpdProviderBillingAddress**	DString	M	O		1	4096		
Provider Practice Address	**HPDProvider**	**hpdProviderPracticeAddress**	DString	M	O		1	4096	Necessary for clear identification of the healthcare professional by the patient. The communities are urged to fill the attribute if possible.	Optionality: O instead of R2
Provider Practice Organization	**HCProfessional**	**hcPracticeLocation**	DN	M	O	validated	DN restriction	DN restriction	Only references to valid DNs and members from the same community are allowed. I.e. the referenced item must have the same community prefix as the currently logged-in community.	
Provider Business Phone	**person, organizationalPerson**	**telephoneNumber**	DString	M	O		1	64		- object class: "person" and "organizationalPerson" instead of " inetOrgPerson - Optionality: O instead of R2
Provider Mobile phone	**inetOrgPerson**	**mobile**	DString	M	O		1	64		Optionality: O instead of R2
Provider Pager	**inetOrgPerson**	**pager**	DString	M	O		1	64		Optionality: O instead of R2
Provider Fax	**OrganizationalPerson**	**facsimileTelephoneNumber**	DString	M	O		1	64		- object class: "organizationalPerson" instead of "inetOrgPerson" - Optionality: O instead of R2
Provider Specialty	**HCProfessional**	**hcSpecialisation**	DString	M	O	validated	1	256	Only valid MDI codes according to value set HCProfessional.hcSpecialisation (Id 2.16.756.5.30.1.127.3.10.8.2) are allowed. Format = IssuingAuthority:Code System:Code[:DisplayName] The suffix :DisplayName is optional and will not be validated against the DisplayName stored in the MDI. Thus, only the part "IssuingAuthority:Code System:Code" is validated.	
Provider Relationship	**HPDProvider**	**memberOf**	DN	M	O	read-only / calculated			This attribute is calculated and can only be edited indirectly via the other side groupOfNames.member	

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Legal Address	**HPDProvider**	**hpdProviderLegalAddress**	DString	S	O		1	4096		
	HCProfessional	**HcRegistrationStatus**	DString	M	R	validated	1	64	Only valid value is "Unknown" (case-insensitive)	Attribute is not listed explicitly in IHE HPD Trial Implementation of August 31, 2015, but was introduced as a mandatory field due to the specification in ISO 21091: 2013 (which is referenced in IHE HPD Trial Implementation).
	top	**objectClass**	OID	M	Rt	validated	Object identifier	Object identifier	Only defined objectClasses are allowed.	

Table 17: HPD Individual Provider Attributes

NOTE: HPD profile or ISO standard format restrictions are not reported here; more information on these restrictions and on additional attributes are available in the IHE ITI Supplement HPD[20], Table 3.58.4.1.2.2.2-1: Individual Provider Mapping applies.

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	techn Remarks	Min L.	Max L.	Comments	Swiss National Extension
Unique Entity Identifier	**uidObject**	**uid**	DString	S	R	validated	DN restriction	DN restriction	No further restrictions except for the technically given maximum length of 255 characters for the complete "distinguished name" (DN), including the uid. Validation if prefix correlates with currently logged-in community: "uid=<shclssuerName>:"	uid RDN = prefix:id The prefix is the name of the community (Issuing Authority) defined by the FOPH. The id SHALL be chosen by the community. The uid SHALL only contain one colon (:). Only the following characters are allowed in the DN: - Alphanumeric - Minus "-" - Colon ":" - Exclamation mark "!" - Pipe symbol "|" - Underscore "_" - Full stop "."

[20] IHE IT Infrastructure Technical Framework Supplement Healthcare Provider Directory (HPD), Revision 1.8, August 28, 2020.

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	techn Remarks	Min L.	Max L.	Comments	Swiss National Extension
Org Identifiers	**HCRegulatedOrganization**	**hcIdentifier**	DString	M	R	validated	1	256	Issuing Authority:Type:ID:Status (ID = OID or BUR number If ID = OID, status = "active" or "inactive" or "revoked" or "suspended" If ID = BUR number, status = "active" or "inactive" or " deleted" or "unknown" Example with OID: RefData:OID:2.99:active Example with BUR number: BFS:BUR:94763827:active Validation: Validation whether there is at least one value which starts with "RefData:OID:" Validation whether the OID is unique in the whole directory in HCRegulatedOrganization.hcIdentifier.	
Organization known names	**Organization**	**O**	DString	M	R		1	128	other name(s)	Optionality: R instead of R2
Organization Name	**HCRegulatedOrganization**	**HcRegisteredName**	DString	M	R		1	128	legal name(s)	
Org Type	**Organization**	**businessCategory**	DString	M	R	validated	1	128	Only valid MDI codes according to value set DocumentEntry.healthcareFacilityTypeCode (Id 2.16.756.5.30.1.127.3.10.1.11) are allowed. Format = IssuingAuthority:Code System:Code[:DisplayName] The suffix :DisplayName is optional and will not be validated against the DisplayName stored in the MDI. Thus, only the part "IssuingAuthority:Code System:Code" is validated.	Optionality: R instead of O
Org Status	**HPDProvider**	**hpdProviderStatus**	DString	S	O	validated	1	64	Allowed values: Active, Inactive (Case insensitive validation)	
Org Contact	**HCRegulatedOrganization**	**ClinicalInformationContact**	DN	M	O	validated	DN restriction	DN restriction	Only references to valid DNs and elements from the currently logged-in community are allowed. I.e the referenced element must have the same community prefix as the currently logged-in community.	
Org Practice Address	**HPDProvider**	**hpdProviderPracticeAddress**	DString	M	O		1	4096	Necessary for the clear identification of an organisation by the patient. It is highly recommended to provide values for this attribute if possible.	Optionality: O instead of R2
Org Billing Address	**HPDProvider**	**hpdProviderBillingAddress**	DString	M	O		1	4096		
Org Mailing Address	**HPDProvider**	**hpdProviderMailingAddress**	DString	M	O		1	4096		Optionality: O instead of R2
Provider Language Supported	**HPDProvider**	**hpdProviderLanguageSupported**	DString	M	O		1	64		Encoded using ISO-639-1

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	techn Remarks	Min L.	Max L.	Comments	Swiss National Extension
Org Speciality	**HCRegulatedOrganization**	**HcSpecialisation**	DString	M	O	validated	1	256	Only valid MDI codes according to value set DocumentEntry.practiceSettingCode (Id 2.16.756.5.30.1.127.3.10.1.18) are allowed. Format = IssuingAuthority:Code System:Code[:DisplayName] The suffix :DisplayName is optional and thus is not validated against the DisplayName stored in the MDI.Thus, only the part "IssuingAuthority:Code System:Code" is validated.	
Signing Certificates	**HCRegulatedOrganization**	**HcSigningCertificate**	OString	M	O		1	32768		
Organization Certificate	**HCRegulatedOrganization**	**HcOrganizationCertificates**	OString	M	O		1	32768		
Org Business Phone	**Organization**	**telephoneNumber**	DString	M	O		1	64		Optionality: O instead of R2
Org Fax	**Organization**	**facsimileTelephoneNumber**	DString	M	O		1	64		Optionality: O instead of R2
Provider Relationship	**HPDProvider**	**memberOf**	DN	M	O	read-only / calculated			Reference to community or parent org The value of this attribute is calculated and can only be modified indirectly by modifying the counterpart element groupOfNames.member.	
Creation Date	**System**	**createTimestamp**	GTime	S	System	read-only / operational			Timestamp when the object was created.	
Last Update Date	**System**	**modifyTimestamp**	GTime	S	System	read-only / operational			Timestamp, when the object was modified.	
Legal Address	**HPDProvider**	**hpdProviderLegalAddress**	DString	S	O		1	4096		
	HPDProvider	**hpdMedicalRecordsDeliveryEmailAddress**	DString	S	O		1	256		This attribute is missing in the IHE HPD Trial Implementation of August 31, 2015. Since it belongs to object class HPDProvider we regard it not only as part of object class HCProfessional but also as part of HCRegulatedOrganization.
	top	**objectClass**	OID	M	R	validated	Object identifier	Object identifier	Only defined objectClasses are allowed.	

Table 18: HPD Organizational Provider Attributes

NOTE: HPD profile or ISO standard format restrictions are not reported here; more information on these restrictions and on additional attributes are available in the IHE ITI Supplement HPD[21], Table 3.58.4.1.2.2.3-1: Organizational Provider Mapping applies

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	technical Remarks	Min L.	Max L.	Comments	Swiss National Extension
Relationship Name	**groupOfNames**	**cn**	Dstring	S	R		1	128	CN RDN = prefix:id Prefix issued by FOPH. ID chosen by community. No further restrictions except for the maximum length of 128 characters. This attribute is used as RDN in groupOfNames as well as in InetOrgPerson.cn Validation if prefix correlates with currently logged-in community: "uid=<shcIssuerName>:"	
Owning organization	**groupOfNames**	**owner**	DN	S	R	validated	DN restriction	DN restriction	Only references to valid DNs and elements from the currently logged-in community are allowed. I.e. the referenced element must have the same community prefix as the currently logged-in community. Validation: Only OU=HCRegulatedOrganization or OU=CHCommunity are allowed.	Optionality: R instead of R2
Member providers	**HPDProvider**	**member**	DN	M	O	validated	DN restriction	DN restriction	Only references to valid DNs and elements from the currently logged-in community are allowed. I.e. the referenced element must have the same community prefix as the currently logged-in community. Member HO is allowed if owner OU=HCRegulatedOrganization or owner OU=CHCommunity. Member HP is allowed if owner OU=HCRegulatedOrganization.	
	top	**objectClass**	OID	M	R	validated	Object identifier	Object identifier	Only defined objectClasses are allowed.	

Table 19: HPD Relationship Attributes

[21] IHE IT Infrastructure Technical Framework Supplement Healthcare Provider Directory (HPD), Revision 1.8, August 28, 2020.

1.12 Requirements on XDS Metadata Update and Restricted Metadata Update

The community SHALL describe policies defining which metadata, if any, may be updated by which role.

Following restrictions SHALL be applied:

a. Healthcare professionals and assistants SHALL be able to update metadata of documents published by healthcare professionals, assistants or technical users in their home community, but not the confidentialityCode and deletionStatus.

b. Patients and representatives SHALL be able to update metadata of documents published by the patient or the representative.

c. Patients and representatives SHALL be able to change the confidentialityCode and deletionStatus of documents published by healthcare professionals, assistants, technical users and document administrators published in any community.

d. Document administrators SHALL be able to change metadata of documents within their home community.

e. Metadata listed in the list of immutable attributes (see section 1.12.1)

1.12.1 Immutable Metadata Attributes

The following attributes SHALL NOT be updated by actors of the Profiles XDS Metadata Update or Restricted Metadata Update:

a. creationTime

b. documentAvailability

c. entryUUID

d. hash

e. homeCommunityId

f. limitedMetadata

g. logicalId

h. objectType

i. repositoryUniqueId

j. size

k. sourcePatientId

l. uniqueId

m. version

n. originalProviderRole

The following attribute SHALL be updated only by a user acting in the role of a document administrator (DADM):

o. patientId

1.13 Requirements on exchange formats

1.13.1 Introduction

Exchange formats permit the simple exchange of data between different health information systems without the need for any special agreement. The specifications of the exchange formats define the technical, syntactic and semantic standards required for the interoperable exchange of information. The objective is to standardize data exchange in the healthcare sector. The following requirements apply to the display and validation of the exchange formats within the Swiss EPR.

1.13.2 Use-case Roles

Actor	Role
Content Creator	Create document to be exchanged between two actors
Content Consumer	Consume document that has been exchanged between two actors

Table 20: Use-case Roles for Exchange Formats

1.13.3 Actors / Transaction

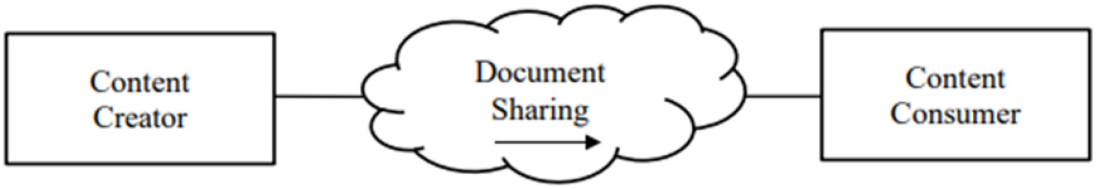


Figure 10: Document Sharing Actors / Transaction

Actor		Reference
Content Creator	*No options defined*	-
Content Consumer	View Option	IHE PCC TF-2[22], chapter 3.1.1
	Document Import Option	IHE PCC TF-2[22], chapter 3.1.2
	Discrete Data Option	IHE PCC TF-2[22], chapter 3.1.4

Table 21: Document Sharing Actors / Transaction

1.13.3.1 View Option

When a FHIR Document is used, in addition to the content of the document, information about the document itself, such as the unique identification, language, author, type of document and the patient of the subject resource should be displayed in a human-readable form. This information facilitates the retrieval of the documents. When using stylesheets to display the documents, the minimum elements to use are the elements defined in the XSLT-Stylesheets for the exchange formats. It is allowed to use a different Stylesheet or view option, as long as the minimal elements for the XSLT-Stylesheet are provided and guaranteed.

1.13.3.2 Document Import Option

The Content Consumer that supports the Document Import Option shall support the View Option. The Content Consumer may offer means to store documents to view the documents without the need to retrieve it again. When viewed after it was imported, a Content Consumer shall query the Document Registry to verify if the document displayed is the latest version.

1.13.3.3 Discrete Data Import Option

This option does not require support for the view option and the document import option. The content consumer that supports the Discrete Data Import option shall be able to support the storage of structured content in a document. This option requires that the user be able to select clinically relevant entries from the specific structured content sections for import into their primary system as part of the local patient record and present them in a system-specific view.

1.13.4 Validation of FHIR resources

The Content Consumer should validate a FHIR resource based on the following aspects:

a. *Structure*: Checks that all the content in the resource is described by the specification, and nothing extra is present.

[22] IHE Patient Care Coordination (PCC) Technical Framework, Volume 2, Revision 11.1, April 14, 2021.

b. *Cardinality*: Checks that the cardinality of all properties is correct (min and max).

c. *Value Domains*: Checks that the values of all properties conform to the rules for the specified types.

d. *Coding bindings*: Checks that codes/displays provided in the Coding types are valid.

e. *Constraints*: Checks that the constraints have been followed correctly.

f. *Profiles*: Checks that any rules in profiles have been followed.

g. *Business Rules*: Business rules are made outside the specification, such as checking for duplicates, checking that references resolve, checking that a user is authorized to do what they want to do.

1.14 Requirements on Medication Card document

1.14.1 Introduction

The Medication Card document gives a complete overview of the current medication of a patient. It serves as an overview of the medications that a patient is taking or should be taking, facilitates the preparation of the medications, and is the basis for a medication history and interaction control. For the patient, the Medication Card document gives an overview of when he should take which medication.

The Medication Card document conforms to the IHE Community Medication List Content Profile (PML), which defines the content and format of a medication list created during a process in which a healthcare professional requests this information (e.g., to support his prescription). The Community Medication List Content Profile is used as part of the Community Medication Prescription and Dispense (CMPD) integration profile.

1.14.2 Representation of the document

For the display of Medication Card document, it is necessary to ensure that the receiver can recognize all information that the sender has sent. Furthermore, the order of the content (e.g., the order of the sections in the text) shall not be changed. Changing the order may change the medical context.

The Presentation of the Medication Card document shall use the PDF original representation. The narrative part in the resources shall not be used.

The original representation of the Medication Card document shall be embedded in a Base 64 encoded as a PDF in PDF/A-1 or PDF/A-2 format. This means that a new Medication Card document is created each time the medication is updated.

For the FHIR format the original representation shall be specified in the resource "Binary":

```
{
  "resourceType": "Binary",
  "id": "2-7-pdf",
  "language": "de-CH",
  "contentType": "application/pdf",
  "data": "JVBERi0xLjQKMSAwIG9iago8PAovVGl0bGU..."
}
```

2 Appendix

2.1 Appendix A – AuditMessage schema (AuditMessage.xsd)

The IHE schema is based on the DICOM Standard, Part 15, Annex A.5 Audit Trail Message Format Profile (see http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html). The required IHE modifications of DICOM PS3.15 2017c are available at: https://gazelle.ihe.net/XSD/IHE/ATNA/dicom_ihe_ps3.15_a.5.1_2017c.xsd).

List of figures

List of tables