Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Inneren EDI

SR 816.111
Ergänzung 1 zu Anhang 5 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier

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

National extensions to the IHE Technical Framework

Ausgabe 1: 22. März 2017
Inkrafttreten: 15. April 2017

1 National Extensions

Die in diesem Abschnitt dokumentierten nationalen Anpassungen der Integrationsprofile sollen in Verbindung mit den Definitionen von Integrationsprofilen, Aktoren und Transaktionen verwendet werden, die in den Bänden 1 bis 3 des IHE IT Infrastructure Technical Frameworks enthalten sind. Dieser Abschnitt umfasst Erweiterungen und Einschränkungen, um die regionale Praxis der Gesundheitsversorgung in der Schweiz wirksam zu unterstützen. Darüber hinaus werden einige englische Begriffe übersetzt, um eine korrekte Interpretation der Anforderungen des IT Infrastructure Technical Frameworks zu gewährleisten.

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 Technical Framework. This section includes extensions and restrictions to effectively support the regional practice of healthcare in Switzerland. It also translates a number of English terms to ensure correct interpretation of requirements of the IT Infrastructure Technical Framework.

This IT Infrastructure national extension document was authored under the supervision of the Federal Office of Public Health (FOPH), eHealth Suisse and IHE Suisse in order to fulfil the Swiss regulations. See also Ordinance on the Electronic Patient Record (EPRO), published in the Official Compilation of Federal Legislation[1] (available in German, French and Italian).

[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 Definitions of terms

1.1.1 Electronic Patient Record (EPR)

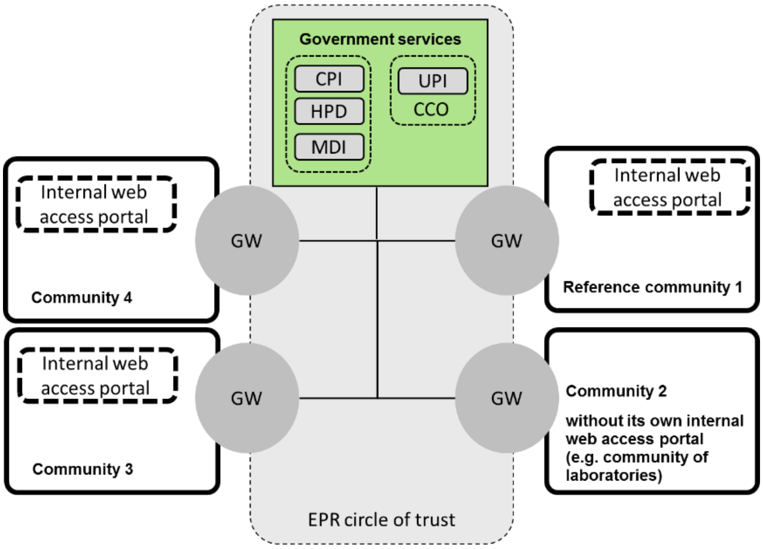
The object of the Federal Act on Electronic Patient Records (EPRA) is to define the conditions for processing data and documents relating to electronic health records. Using electronic health records, healthcare professionals can access data relevant to treatment of their patients that was compiled and decentral recorded by healthcare professionals involved in the treatment process. Healthcare professionals may save copies of this data if necessary in their practice and hospital information systems outside of the electronic health records. To access electronic health records, healthcare professionals must join a certified community, which is an association of healthcare professionals and their institutions, and their patients must grant them the necessary access rights. In addition, the electronic health record also allows patients to view their data, to make their own data accessible and to manage the allocation of access rights. Healthcare professionals may only process data in electronic health records with the consent of the patient. Patients have the option of granting individual and graded access rights.

Notation of this term in the following text: **EPR**

1.1.2 EPR circle of trust

From an organizational perspective and in terms of the EPRA, communities are an association of healthcare professionals and their institutions. Communities who want to participate in the Swiss EPR must 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 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.

Notation of this term in the following text: **EPR circle of trust**


Government services
CPI
HPD
MDI
UPI
CCO
Internal web access portal
Community 4
Internal web access portal
Community 3
GW
GW
GW
GW
Internal web access portal
Reference community 1
Community 2
without its own internal web access portal (e.g. community of laboratories)
EPR 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

1.1.3 Reference community

If a patient decides to open an EPR, she or he first chooses a community that manages all of his or her current consents and access right configurations to be used by other EPR users (in essence healthcare professionals) while accessing his personal EPR. Consents and access rights for one patient are managed by exactly one reference community in the EPR circle of trust.

Although the term home community is used by IHE in a slightly different way, the current specification states this consent and access right management community as reference community.

Accesses to documents within the EPR circle of trust are only permitted when the initiating user gets permission by the access rights defined by the patient. Although cross-community accesses may occur between each community within the EPR circle of trust regardless whether it is the patient's reference community or not, the responding community must always apply the current access right settings managed by the reference community. This is also valid for all accesses within the own community of the initiating user.

The patient may change his reference community at any time (for example, when moving to another residence).

Notation of this term in the following text: **referenceCommunity**

1.1.4 Patient Identifiers (EPR-PID, MPI-PID)

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

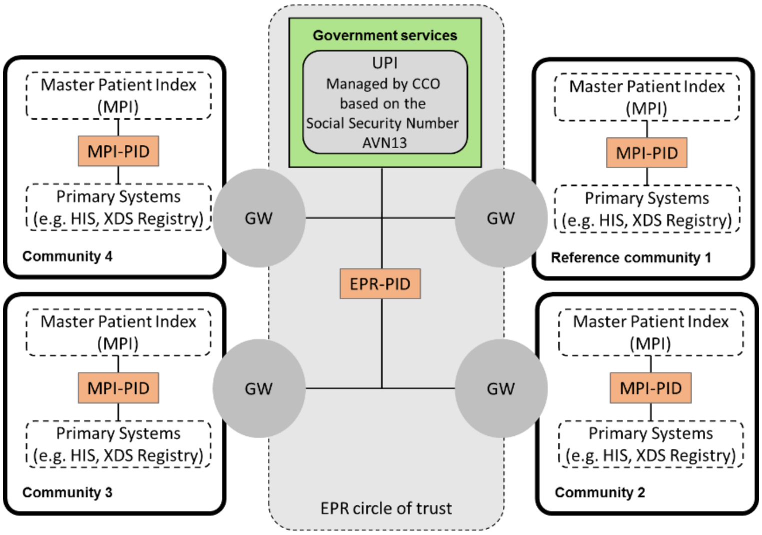


Figure 2 Swiss Patient Identifiers

1.2 Scope of precisions

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

[2] http://www.zas.admin.ch/index.html

- IT Infrastructure: Consistent Time (CT)
- IT Infrastructure: Audit Trail and Node Authentication (ATNA)
- IT Infrastructure: Cross-Community Access (XCA)
- IT Infrastructure: Cross-Enterprise User Assertion (XUA)
- IT Infrastructure: Patient Identifier Cross-Reference HL7 V3 (PIXv3)
- IT Infrastructure: Patient Demographic Query HL7 V3 (PDQv3)
- IT Infrastructure Technical Framework Supplement: Cross-Community Patient Discovery (XCPD)
- IT Infrastructure Technical Framework Supplement: Healthcare Provider Directory (HPD)

1.3 Requirements on CT Profile for Swiss Time Service

ITI TF-1 does not specify any NTP Servers. The following Time Service MUST be used by all actors in the Swiss EPR circle of trust.

- Maintain Time [ITI-1] ntp.metas.ch MUST be used as Time Service.

1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption

1.4.1 Introduction

The EPRA requires a patient access on the complete audit trail within the EPR circle of trust. The access to the audit trail will be provided by certified web access portals for patients.

The present national extension will use and precise the existing transactions and content profiles of the Audit Trail and Node Authentication (ATNA), Cross-Enterprise Document Sharing (XDS.b) and Cross-Community Access (XCA) integration profiles in order to achieve the Swiss regulation needs on the audit trail access by patients.

This figure shows all relevant actors and transactions for the present national extension:

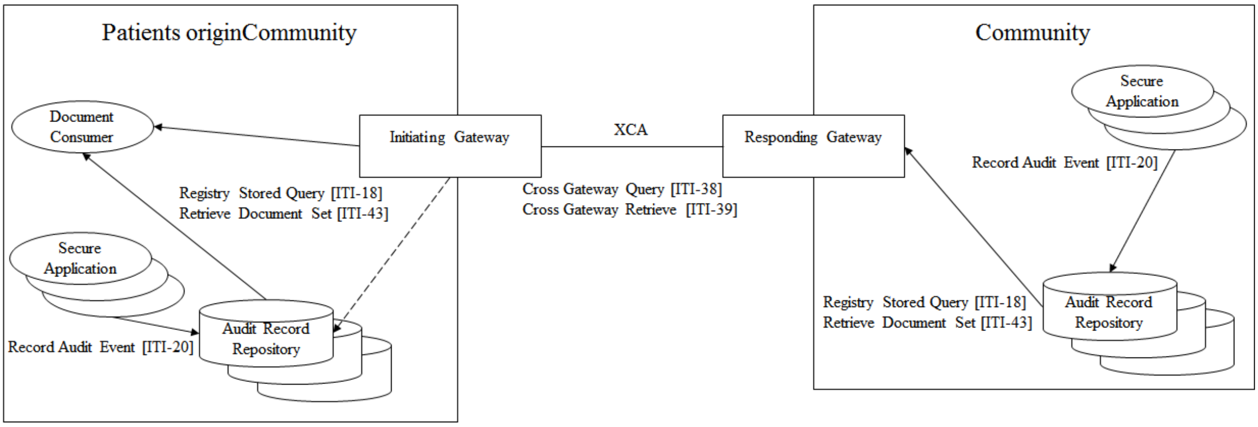

Patients originCommunity
Document Consumer
Initiating Gateway
Registry Stored Query [ITI-18]
Retrieve Document Set [ITI-43]
Secure Application
Record Audit Event [ITI-20]
Audit Record Repository
XCA
Cross Gateway Query [ITI-38]
Cross Gateway Retrieve [ITI-39]
Community
Responding Gateway
Secure Application
Record Audit Event [ITI-20]
Registry Stored Query [ITI-18]
Retrieve Document Set [ITI-43]
Audit Record Repository

Figure 3 Big picture – actors and transactions

This figure shows all relevant content profiles for the present national extension:

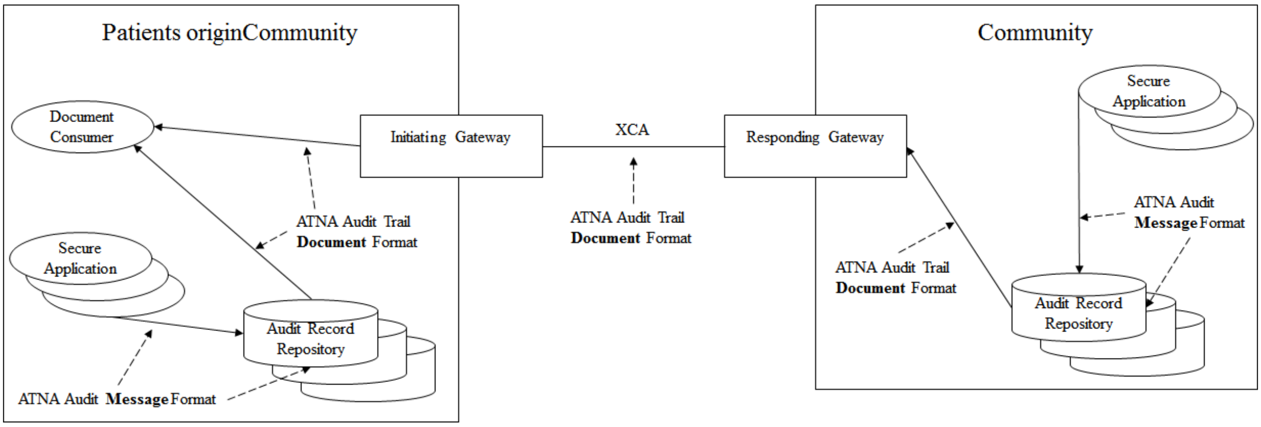


Figure 4 Big picture - content profiles

1.4.2 Actors

1.4.2.1 XDS.b Document Consumer

The following option MUST be implemented by all web access portal providers for patients in the Swiss EPR circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

These actors MUST:

- combine all Audit Trail Message entries of all Audit Trail Document entries into one single document of type ATNA Audit Trail Document Format (see chapter “1.4.4.2 ATNA Audit Trail Document Format” on page 19).
  Relevant transactions:
  - Registry Stored Query [ITI-18] transaction that uses the parameters described in chapter “1.4.3.1.1 Parameters for stored query FindDocuments” on page 9.
  - Retrieve Document Set [ITI-43] transaction performed against an Audit Record Repository using a document UUID received by a previously executed by a Registry Stored Query mentioned before.
- translate the coded information into the language preferred by the user when provide it to the user through the UI or other results like reports. Translations MUST fulfil the following requirements:
  - Translations in German, French and Italian MUST be supported. Other language translations are permitted but remain in the responsibility of the software vendor.
  - Translations for coded values from the Swiss Metadata Value-Set[3] must match the translations provided in the Swiss Metadata Value-Set.
  - Translations for coded values mentioned in the present national extensions MUST be used.
  - No translation is required for narrative text.

1.4.2.2 XCA Initiating Gateway

The following option MUST be implemented by all community gateways in the Swiss EPR circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

[3] See FDHA Ordinance on the Electronic Patient Record, Annex 3

These actors basically relay the XDS.b Registry Stored Query [ITI-18] and XDS.b Retrieve Document Set [ITI-43] transactions to the XCA Cross Gateway Query [ITI-38] and XCA Cross Gateway Retrieve [ITI-39] as described in IHE ITI TF-2.

If the homeCommunityId represents the local community and the parameter $XDSDocumentEntryTypeCode contains the value 60049 (Audit trail), these actors MUST initiate a Registry Stored Query to all local ATNA Audit Repositories. See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 9.

1.4.2.3 XCA Responding Gateway

The following option MUST be implemented by all community gateways in the Swiss EPR circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

These actors basically relay the XCA Cross Gateway Query [ITI-38] and XCA Cross Gateway Retrieve [ITI-39] to XDS.b Registry Stored Query [ITI-18] and XDS.b Retrieve Document Set [ITI-43] transactions as described in ITI TF-2. If the parameter $XDSDocumentEntryTypeCode contains the value 722160009 (Audit trail report), these actors MUST initiate a Registry Stored Query to all local ATNA Audit Repositories. See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 9 .

1.4.2.4 ATNA Secure Application

The following transactions are declared as optional in ITI TF-1 but are REQUIRED by the present national extension:

- Maintain Time [ITI-1]
  See chapter "1.3 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption" on page 6.
- Record Audit Event [ITI-20]
  The Audit Message Format described in chapter "1.4.4.1 ATNA Audit Message Format" on page 12 MUST be used.

This behaviour MUST be implemented by all applications in the Swiss EPR circle of trust that are requesting, consuming or producing health information of patients having an EPR.

1.4.2.4.1 Audit messages

All ATNA Secure Application actors are required to record the audit messages defined by the IHE actor they are grouped with as described in the IHE Technical Framework.

In case these audit messages do not fulfil the requirements described in chapter "1.4.4.1 ATNA Audit Message Format" on page 12 , ATNA Secure Application actors within the Swiss EPR circle of trust MUST record an additional audit message as described in chapter "1.4.4.1 ATNA Audit Message Format" on page 12 for each transaction concerning a patient having an EPR.

1.4.2.5 ATNA Audit Record Repository

ATNA Audit Record Repository actors within the Swiss EPR circle of trust MUST:

- support the following options and transactions:
  (see chapter "1.5.3 Transactions" on page 24 for detailed descriptions)
  - On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5).
  - XDS.b Registry Stored Query [ITI-18].
  - XDS.b Retrieve Document Set [ITI-43].

- be able to receive and store audit messages of Audit Message Format described in chapter “1.4.4.1 ATNA Audit Message Format” on page 12 by the Record Audit Event [ITI-20] which is based on the preferred Audit Message Format by IHE ATNA (see ITI TF-2a, chapter 3.20.7.1).
- be able to perform the Retrieve Document Set transaction for all On-Demand documents specified by document and repository UUIDs created by a previously Registry Stored Query transaction.
- have assigned a unique repository ID within the community (similar to XDS.b Document Repository actors).

1.4.3 Transactions

1.4.3.1 Registry Stored Query [ITI-18]

See ITI TF-2a, chapter “3.18.4.1.2.3 Query Request Parameters – Coding Style”. The query parameters described in the following chapter MUST be used for Audit Trail Consumption.

1.4.3.1.1 Parameters for stored query FindDocuments

ITI TF-2a specifies the query parameters for a stored query “FindDocuments” (see ITI TF-2a 3.18.4.1.2.3.7.1). The stored query “FindDocuments” MUST be used using the following parameters in order to retrieve Audit Trails within the Swiss EPR circle of trust.

The mentioned Swiss Metadata Value-Set can be found in appendix 3 of the FDHA Ordinance on the Electronic Patient Record (EPRO-FDHA).

Table 1 Parameters for stored query FindDocuments

Element Name **Attribute**	**Card.**	**Original descriptions**	**Swiss National Extension**
$XDSDocumentEntryPatientId XDSDocumentEntry.patientId	[1..1]	The format of the patientId value is CX. See also ITI TF-3, 4.2.3.2.16	No further refinement.
$XDSDocumentEntryClassCode XDSDocumentEntry.classCode	[0..*]	The code specifying the high-level use classification of the document type (e.g., Report, Summary, Images, Treatment Plan, Patient Preferences, Workflow). See also description 1 below and ITI TF-3, 4.2.3.2.3	This value MUST represent the following value from the Swiss Metadata Value-Set “xds-clasCod” (2.16.756.5.30.1.127.3.10.1.3)
$XDSDocumentEntryTypeCode XDSDocumentEntry.typeCode	[0..*]	The code specifying the precise type of document from the user perspective. See also description 1 below and ITI TF-3, 4.2.3.2.25	This value MUST represent the following value from the Swiss Metadata Value-Set “xds-typeCo” (2.16.756.5.30.1.127.3.10.1.27)
$XDSDocumentEntryPracticeSettingCode XDSDocumentEntry.practiceSettingCode	[0..*]	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g., Family Practice, Laboratory, Radiology).	When specified, this value MUST represent a value from the Swiss Metadata Value-Set “xds-pracSetCo” (2.16.756.5.30.1.127.3.10.1.18)

		See also description 1 below and ITI TF-3, 4.2.3.2.17	
$XDSDocumentEntryCreationTimeFrom Lower value of XDSDocumentEntry.creationTime	[0..1]	creationTime represents the time the author created the document. See also description 6 below and ITI TF-3,4.2.3.2.6	MUST NOT be specified ([0..0]).
$XDSDocumentEntryCreationTimeTo Upper value of XDSDocumentEntry.creationTime	[0..1]		
$XDSDocumentEntryServiceStartTimeFrom Lower value of XDSDocumentEntry.serviceStartTime	[0..1]	Represents the start time of the service being documented took place (clinically significant, but not necessarily when the document was produced or approved). See also ITI TF-3, 4.2.3.2.19	Used to specify the start time of the desired audit trail message to be returned. All audit trail messages having the @EventDateTime (AuditMessage/EventIdentification) equals or newer MUST be returned by the Audit Record Repository actor.
$XDSDocumentEntryServiceStartTimeTo Upper value of XDSDocumentEntry.serviceStartTime	[0..1]		MUST NOT be specified ([0..0]).
$XDSDocumentEntryServiceStopTimeFrom Lower value of XDSDocumentEntry.serviceStopTime	[0..1]	Represents the stop time of the service being documented took place (clinically significant, but not necessarily when the document was produced or approved). See also ITI TF-3, 4.2.3.2.20	MUST NOT be specified ([0..0]).
$XDSDocumentEntryServiceStopTimeTo Upper value of XDSDocumentEntry.serviceStopTime	[0..1]		Used to specify the stop time of the desired audit trail message to be returned. All audit trail messages having the @EventDateTime (AuditMessage/EventIdentification) equals or older MUST be returned by the Audit Record Repository actor.
$XDSDocumentEntryHealthcareFacilityTypeCode XDSDocumentEntry.healthcareFacilityTypeCode	[0..*]	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred. See also description 1 below and ITI TF-3, 4.2.3.2.11	When specified, this value MUST represent a value from the Swiss Metadata Value-Set “xds-hcFacTyCo” (2.16.756.5.30.1.127.3.10.1.11)
$XDSDocumentEntryEventCodeList XDSDocumentEntry.eventCodeList	[0..*]	This list of codes represents the main clinical acts, such as a colonoscopy or an appendectomy being documented. See also description 1, 3 below and ITI TF-3, 4.2.3.2.8	No further refinement.
$XDSDocumentEntryConfidentialityCode XDSDocumentEntry.confidentialityCode	[0..*]	The code specifying the security and privacy tags of the document.	This value MUST represent the following value from the Swiss Metadata Value-Set “xds-confCod” (2.16.756.5.30.1.127.3.10.1.5)

		See also description 1 below and ITI TF-3, 4.2.3.2.5	
$XDSDocumentEntryAuthorPerson XDSDocumentEntry.author	[0..*]	Represents the humans and/or machines that authored the document. See also description 4 below and ITI TF-3, 4.2.3.2.1	No further refinement.
$XDSDocumentEntryFormatCode XDSDocumentEntry.formatCode	[0..*]	The code specifying the detailed technical format of the document. See also description 1 below and ITI TF-3, 4.2.3.2.9	This value MUST represent the following value from the Swiss Metadata Value-Set “xds-formCo” (2.16.756.5.30.1.127.3.10.1.9)
$XDSDocumentEntryStatus XDSDocumentEntry.status	[1..*]	Represents the status of the DocumentEntry. A DocumentEntry shall have one of two availability statuses: Approved: The document is available for patient care. Deprecated: The document is obsolete. See also ITI TF-3, 4.2.3.2.2	While audit trail entries may not be deprecated, the following value MUST be used:urn:oasis:names:tc:ebxml-regrep:StatusType:Approved or urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecatd
$XDSDocumentEntryType XDSDocumentEntry.objectType	[0..*]	The objectType attribute reflects the type of DocumentEntry. As described in ITI TF-3, Section 4.1.1, there are two DocumentEntry types: Stable Document Entry and On-Demand Document Entry. See also description 5 below and ITI TF-3, 4.2.3.2.30	While queries to audit trails are On-Demand documents, the following value MUST be used: urn:uuid:34268e47-fdf5-41a6-ba33-82133c465248 (On-Demand)

Descriptions from ITI TF-2a, 3.18.4.1.2.3.7.1:

1. Shall be coded according to specification in Section 3.18.4.1.2.3.4 Coding of Code/Code-Scheme.
2. Supports AND/OR semantics as specified in Section 3.18.4.1.2.3.5.
3. The value for this parameter is a pattern compatible with the SQL keyword LIKE which allows the use of the following wildcard characters: % to match any (or no) characters and _ to match a single character. The match shall be applied to the text contained in the Value elements of the authorPerson Slot on the author Classification (value strings of the authorPerson sub-attribute)
4. See Section 3.18.4.1.2.3.6.2
5. CreationTimeFrom and CreationTimeTo are ignored when evaluating an On-Demand Document Entry’s selection for inclusion in the query response.

1.4.3.1.2 Response

ATNA Audit Record Repository actors within the Swiss EPR circle of trust MUST:

1. create a virtual document UUID and return it as one single document entry in the result (On-Demand Document) and
2. cache all audit messages matched by the filter parameters in order to provide them by the retrieve Document Set transaction using the corresponding document UUID in the ATNA Audit Trail Document Format. Caching is REQUIRED for 8 hours. Later accesses to the corresponding document UUID MUST fail.

1.4.3.2 Retrieve Document Set [ITI-43]

ATNA Audit Record Repository actors within the Swiss EPR circle of trust MUST return the audit messages matched by the filter parameters in the query of the corresponding document UUID. The contents of the document returned MUST exactly conform to the state at the point of time of the stored query FindDocuments execution.

1.4.3.3 Record Audit Event [ITI-20]

The ATNA Audit Message Format described in chapter “1.4.4.1 ATNA Audit Message Format” starting on page 13 MUST be used for all events for patients having an EPR.

1.4.4 Content profiles

1.4.4.1 ATNA Audit Message Format

IHE ITI TF-2a references to several Audit Message Formats (see ITI TF-2a, 3.20.7) and prefers use of the DICOM schema for audit records generated by all IHE actors (see ITI TF-2a, 3.20.7.1). ATNA Secure Application actors within the Swiss EPR circle of trust MUST record an audit message for each transaction concerning a patient having an EPR using the mentioned DICOM schema.

The schema can be found in the DICOM Standard, Part 15 Annex A.5 - Edition DICOM PS3.15 2016e (available from: http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html).

Detailed contents to be provided by all ATNA Secure Application actors within the Swiss EPR circle of trust are described in the following chapter.

1.4.4.1.1 Detailed AuditMessage definitions

The detailed specifications for IHE actor audit message requirements specified within the IHE integration profiles MUST be used with the following specification.

Table 2 Detailed AuditMessage definitions

Element Name	Card.	Original descriptions	Swiss National Extension
AuditMessage [1..1] (root element)			
AuditMessage/EventIdentification [1..1] (type: EventIdentificationContents)			

@EventActionCode
(type: xs:token)
	[0..1]	Indicator for type of action performed during the event that generated the audit.
		C= Create
		R= Read
		U= Update
		D= Delete
		E= Execute
			No further refinement.

@EventDateTime (type: xs:dateTime)	[1..1]	Universal coordinated time (UTC), i.e., a date/time specification that is unambiguous as to local time zones. The time at which the audited event occurred. See Section A.5.2.5	Date and time format following ISO 8601 MUST be used. Indication of the time zone in Switzerland during the daylight- savings time (summer): UTC +2 hours and during normal time (winter): UTC +1 hour. Sample daylight-savings time: 2016-08-10T20:29:10+02:00 Sample normal time: 2016-02-10T20:29:10+01:00
@EventOutcomeIndicator (type: xs:token)	[1..1]	Indicates whether the event succeeded or failed. When a particular event has some aspects that succeeded and some that failed, then one message shall be generated for successful actions and one message for the failed actions (i.e., not a single message with mixed results). 0= Nominal Success (use if status otherwise unknown or ambiguous) 4= Minor failure (per reporting application definition) 8= Serious failure (per reporting application definition) 12= Major failure (reporting application now unavailable)	No further refinement.
EventID (type: CodedValueType)	[1..1]	Identifier for a specific audited event. The identifier for the family of event. E.g., "User Authentication"; Extended by DICOM using DCID (400)	No further refinement.
EventTypeCode (type: CodedValueType)	[0..*]	Identifier for the category of event. The specific type(s) within the family applicable to the event, e.g. "User Login". Note: DICOM/IHE defines and uses this differently than RFC-3881. Extended by DICOM using DCID (401).	No further refinement.
EventOutcomeDescription	[0..1]	N/A	No further refinement.
AuditMessage/ActiveParticipant [1..1] (type: ActiveParticipantContents)			
@UserID (type: text)	[1..1]	Unique identifier for the user actively participating in the event. If the participant is a person, then the User ID shall be the identifier used for that person on this particular system, in the form of loginName@domain-name. If the participant is an identifiable process, the UserID selected shall be one of the identifiers used in the internal system logs. See also A.5.2.1	No further refinement.
@AlternativeUserID (type: text)	[0..1]	Alternative unique identifier for the user.	No further refinement.

		If the participant is a person, then Alternative User ID shall be the identifier used for that person within an enterprise for authentication purposes, for example, a Kerberos	
Username (user@realm)		If the participant is a DICOM application, then Alternative User ID shall be one or more of the AE Titles that participated in the event. See also A.5.2.2	
@UserName (type: text)	[0..1]	A human readable identification of the participant. If the participant is a person, the person's name shall be used. If the participant is a process, then the process name shall be used. See also A.5.2.3	If the participant is a person, the person's name MUST be specified as follows: [<title>]<family name> <given name>
@UserIsRequestor (type: xs:Boolean)	[1..1]	Indicator that the user is or is not the requestor, or initiator, for the event being audited. Used to identify which of the participants initiated the transaction being audited. If the audit source cannot determine which of the participants is the requestor, then the field shall be present with the value FALSE in all participants. The system shall not identify multiple participants as UserIsRequestor. If there are several known requestors, the reporting system shall pick only one as UserIsRequestor.	No further refinement.
@NetworkAccessPointID (type: xs:token)	[0..1]	An identifier for the network access point of the user device This could be a device id, IP address, or some other identifier associated with a device. See also A.5.2.4	No further refinement.
@NetworkAccessPointTypeCode	[0..1]	An identifier for the type of network access point. 1= Machine Name, including DNS name 2= IP Address 3= Telephone Number 4= Email address 5= URI (user directory, HTTP-PUT, ftp, etc.) See also A.5.2.4	No further refinement.
RoleIDCode (type: CodedValueType)	[0..*]	Specification of the role(s) the user plays when performing the event, as assigned in role-based access control security Extended by DICOM using DCID (402) Usage of this field is refined in the individual message descriptions below. Other additional roles may also	When describing a human user’s participation in an event, this value MUST represent a value from the Swiss Metadata Value-Set “epd_xds_authorRole” (2.16.756.5.30.1.127.3.10.1.1.3)
		be present, since this is a multi-valued field. 3.20.7.1.1 RoleIDCode with access control roles: When describing a human user’s participation in an event, the RoleIDCode value should represent the access control roles/permissions that authorized the event. RoleIDCode is a CodedValueType. Use of standards-	

		based roles/permissions is recommended, rather than use of site or application specific codes. Many older security systems are unable to produce this data, hence it is optional, but should be provided when known. For example: at a site "St Fraser" they have defined a functional role code "NURSEA" for attending nurse. This can be represented as EV("NURSEA", "St Fraser", "Attending Nurse") Candidate standards based structural/functional role codes can be found at ISO, HL7, ASTM, and various other sources.	
MediaIdentifier/MediaType (type: CodedValueType)	[0..1]	When importing or exporting data, e.g., by means of media, the UserID field is used both to identify people and to identify the media itself. See also A.5.2.1	When importing or exporting data, this value MUST represent either a unique media identifier or at least a unique media type (e.g., DVD, paper, film). Currently there is no Swiss Metadata Value-Set available for media types, but as soon as there is one, it MUST be used when describing media types.
AuditMessage/AuditSourceIdentification [1..1] (type: AuditSourceIdentificationContents)			
@code (type: xs:token)	[1..1]	1= End-user display device, diagnostic device 2= Data acquisition device or instrument 3= Web Server process or thread 4= Application Server process or thread 5= Database Server process or thread 6= Security server, e.g., a domain controller 7= ISO level 1-3 network component 8= ISO level 4-6 operating software 9= other Other values are allowed if a codeSystemName is present.	No further refinement.
other-csd-attributes	N/A	See descriptions for attribute group other-csd-attributes.	
@AuditEnterpriseSiteID	[0..1]	Logical source location within the healthcare enterprise network, e.g., a hospital or other provider location within a multi-entity provider group. Serves to further qualify the Audit Source ID, since Audit Source ID is not required to be globally unique.	[1..1] The OID of the audit source MUST be specified. Audit sources may apply for a GLN. When presenting to the user, the GLN details MUST be provided[4].
@AuditSourceID (type: xs:token)	[1..1]	Identifier of the source. The identification of the system that detected the auditable event and created this audit message. Although	A meaningful description of the audit source, comprehensible for the patient / citizen must be specified.

[4] There exists a Webservice at the Refdata foundation which might be used: http://refdatabase.refdata.ch/Service/Partner.asmx?WSDL (see also http://www.refdata.ch/content/page_1.aspx?Nid=60&Aid=636&ID=296)

		often the audit source is one of the participants, it could also be an external system that is monitoring the activities of the participants (e.g., an add-on audit-generating device).	
AuditSourceTypeCode (type: xs:token)	[0..*]	Code specifying the type of source Used as defined in RFC 3881: 1= End-user display device, diagnostic display 2= Data acquisition device or instrument 3= Web server process 4= Application server process 5= Database server process 6= Security server, e.g., a domain controller 7= ISO level 1-3 network component 8= ISO level 4-6 operating software 9= External source, other or unknown type E.g., an acquisition device might use "2" (data acquisition device), a PACS/RIS system might use "4 "(application server process).	No further refinement.
AuditMessage/ParticipantObjectIdentification [0..*] (type: ParticipantObjectIdentificationContents)			
@ParticipantObjectID (type: xs:token)	[1..1]	Describes the identifier that is contained in Participant Object ID. Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
@ParticipantObjectTypeCode (type: xs:token)	[0..1]	1= Person 2= System object 3= Organization 4= Other	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
@ParticipantObjectTypeCodeRole (type: xs:token)	[0..1]	1= Patient 2= Location 3= Report 4= Resource 5= Master File 6= User 7= List 8= Doctor 9= Subscriber 10= guarantor 11= Security User Entity 12= Security User Group 13= Security Resource 14= Security Granularity Definition 15= Provider 16= Report Destination 17= Report Library 18= Schedule 19= Customer 20= Job 21= Job Stream 22= Table 23= Routing Criteria 24= Query	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.

@ParticipantObjectDataLifeCycle (type: xs:token)	[0..1]	1= Origination, Creation 2= Import/ Copy 3= Amendment 4= Verification 5= Translation 6= Access/Use 7= De-identification 8= Aggregation, summarization, derivation 9= Report 10= Export 11= Disclosure 12= Receipt of Disclosure 13= Archiving 14= Logical deletion 15= Permanent erasure, physical destruction	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
@ParticipantObjectSensitivity (type: xs:token)	[0..1]	Denotes policy-defined sensitivity for the Participant Object ID such as VIP, HIV status, mental health status, or similar topics. Used as defined in RFC 3881.	The current confidentiality code of the object MUST be specified when the object is a document in the EPR. This value MUST represent a value from the Swiss Metadata Value-Set “xds-confCod” (2.16.756.5.30.1.127.3.10.1.5) in the HL7 CNE datatype format. The following sequences are required: CNE.1: Code national CNE.2: Text in ge, fr or it CNE.7: Publication date of the value-set in the format YYYYMMDD CNE.14: OID of the value-set Sample: 1051000195109^normal^^^^^ 20150702^^^^^^^ 2.16.756.5.30.1.127.3.10.1.5
ParticipantObjectIDTypeCode (type: CodedValueType)	[1..1]	Describes the identifier that is contained in Participant Object ID. Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
ParticipantObjectName (type: xs:token) Or ParticipantObjectQuery (type: xs:base64Binary)	[1..1]	An instance-specific descriptor of the Participant Object ID audited, such as a person's name. Or The actual query for a query-type participant object. Usage refined by individual message descriptions	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
ParticipantObjectDetail (type: ValuePair)	[0..*]	Implementation-defined data about specific details of the object accessed or used. Used as defined in RFC 3881. Note 1: The value field is xs:base64Binary encoded, making this attribute suitable for conveying binary data. Note 2: optional details, these can be extensive and large.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
ParticipantObjectDescription (type: xs:token)	[0..*]	Optional descriptive text	When used, it MUST be specified in the preferred language by the patient / citizen (see also chapter “1.4.2.1 XDS.b Document Consumer on page 7).
DICOMObjectDescriptionContents	[0..1]	These are extensions made by DICOM to RFC-3881 schema for use describing DICOM objects. See descriptions for group DICOMObjectDescriptionContents.	

CodedValueType			
@csd-code (type: xs:token)	[1..1]	N/A	The code MUST be unique within the OID specified with @codeSystemName.
other-csd-attributes	N/A	See descriptions for attribute group other-csd-attributes	
other-csd-attributes			
@codeSystemName (type: xs:token)	[1..1]	codeSystemName is either an OID or String. OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"	An OID MUST be used.
@displayName (type: xs:token)	[0..1]	N/A	The name of the code system specified by the OID must be specified in the patient's preferred language. It MUST be a valuable translation of the original OID description in the ISO/IEC 9834-1 registration authority.
@originalText (type: xs:token)	[0..1]	Note: this also corresponds to DICOM "Code Meaning"	The name of the element must be specified in the patient's preferred language. It MUST be a valuable translation of the element's original text.
DICOMObjectDescriptionContents			
MPPS	[0..*]	DICOM extension. An MPPS Instance UID(s) associated with this participant object.	No further refinement.
Accession	[0..*]	DICOM extension. An Accession Number(s) associated with this participant object.	No further refinement.
SOPClass	[1..1]	DICOM extension. The UIDs of SOP classes referred to in this participant object. Required if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") and any of the optional fields (AccessionNumber, ContainsMPPS, NumberOfInstances, ContainsSOPInstances, Encrypted, Anonymized) are present in this Participant Object. May be present if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") even though none of the optional fields are present.	No further refinement.
ParticipantObjectContainsStudy	[0..1]	ICOM extension. A Study Instance UID, which may be used when the ParticipantObjectIDTypeCode is not (110180, DCM, "Study Instance UID").	No further refinement.
Encrypted	[0..1]	DICOM extension.	No further refinement.

		A single value of True or False indicating whether or not the data was encrypted. Note: If there was a mix of encrypted and non-encrypted data, then create two event reports.	
Anonymized	[0..1]	DICOM extension. A single value of True or False indicating whether or not all patient identifying information was removed from the data.	No further refinement.

See also “Appendix A – AuditMessage schema (AuditMessage.xsd)” on page 52

1.4.4.2 ATNA Audit Trail Document Format

Following the Swiss regulations, any patient has the right to access the audit trail of his own EPR. While the audit trails are stored in multiple Audit Record Repositories in multiple communities, the purpose of the ATNA Audit Trail Document Format is to combine all Audit Trail entries of all Documents returned by Registry Stored Queries [ITI-18] that used the parameters described in chapter “1.4.3.1.1 Parameters for stored query FindDocuments” on page 9 into one single document. Detailed contents to be provided by all ATNA Audit Record Repository actors within the Swiss EPR circle of trust are described in the following chapter.

1.4.4.2.1 Detailed AuditTrail definitions

Table 3 Detailed AuditTrail definitions

Element Name	Card.	Description
AuditTrail [1..1] (root element)		
AuditMessage	[1..*]	An AuditTrail consist of one to many AuditMessage elements. See chapter “1.4.4.1.1 Detailed AuditMessage definitions” starting on page 12.

See also “Appendix B – AuditTrail schema (AuditTrail.xsd)” on page 52.

1.4.5 Translations

Translation of the codes listed in the following tables into the national languages will be published by eHealth Suisse. These translations MUST be while presenting the audit trail to the user. Other translations are optional (see also chapter “1.4.2.1 XDS.b Document Consumer” on page 7).

Table 4 EventActionCode

Code	English
C	Create
R	Read
U	Update
D	Delete
E	Execute

Table 5 EventOutcomeIndicator

Code	English

0	Nominal Success
4	Minor failure
8	Serious failure
12	Major failure

Table 6 NetworkAccessPointTypeCode

Code	English
1	Machine Name
2	IP Address
3	Telephone Number
4	Email address
5	URI

Table 7 AuditSourceIdentification code

Code	English
1	End-user display device, diagnostic device
2	Data acquisition device or instrument
3	Web Server process or thread
4	Application Server process or thread
5	Database Server process or thread
6	Security server, e.g., a domain controller
7	ISO level 1-3 network component
8	ISO level 4-6 operating software
9	Other

Table 8 AuditSourceTypeCode

Code	English
1	End-user display device, diagnostic display
2	Data acquisition device or instrument
3	Web server process
4	Application server process
5	Database server process
6	Security server, e.g.,
7	ISO level 1-3 network component
8	ISO level 4-6 operating software
9	External source, other or unknown type

Table 9 ParticipantObjectTypeCode

Code	English
1	Person
2	System object
3	Organization
4	Other

Table 10 ParticipantObjectTypeCodeRole

Code	English
1	Patient

2	Location
3	Report
4	Resource
5	Master File
6	User
7	List
8	Doctor
9	Subscriber
10	Guarantor
11	Security User Entity
12	Security User Group
13	Security Resource
14	Security Granularity Definition
15	Provider
16	Report Destination
17	Report Library
18	Schedule
19	Customer
20	Job
21	Job Stream
22	Table
23	Routing Criteria
24	Query

Table 11 ParticipantObjectDataLifeCycle

Code	English
1	Origination, Creation
2	Import/ Copy
3	Amendment
4	Verification
5	Translation
6	Access/Use
7	De-identification
8	Aggregation, summarization, derivation
9	Report
10	Export
11	Disclosure
12	Receipt of Disclosure
13	Archiving
14	Logical deletion
15	Permanent erasure, physical destruction

1.4.6 Implementation using RESTful ATNA

There exists an IHE Trial Implementation “Add RESTful Query to ATNA”. Communities are allowed to implement the requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption as described in the chapters before, if and only if they implement the same functionality in order to provide a patient access on the complete audit trail within the EPR circle of trust.

1.5 Requirements on XUA Profile for Authentication and User Assertion

1.5.1 Introduction

The EPRA requires a secure environment and therefore strong authentication and access control mechanisms within the EPR circle of trust. The present national extension will use the existing transaction Provide X-User Assertion [ITI-40] of the IHE Cross-Enterprise User Assertion (XUA) integration profile and precise the - in IHE ITI TF - not further specified transactions Authenticate User and Get X-User Assertion in order to achieve the Swiss regulation needs on the security of the system, especially to ensure that nobody can fake its identity for abusive accesses.

The following figures show all relevant actors and transactions for the present national extension:

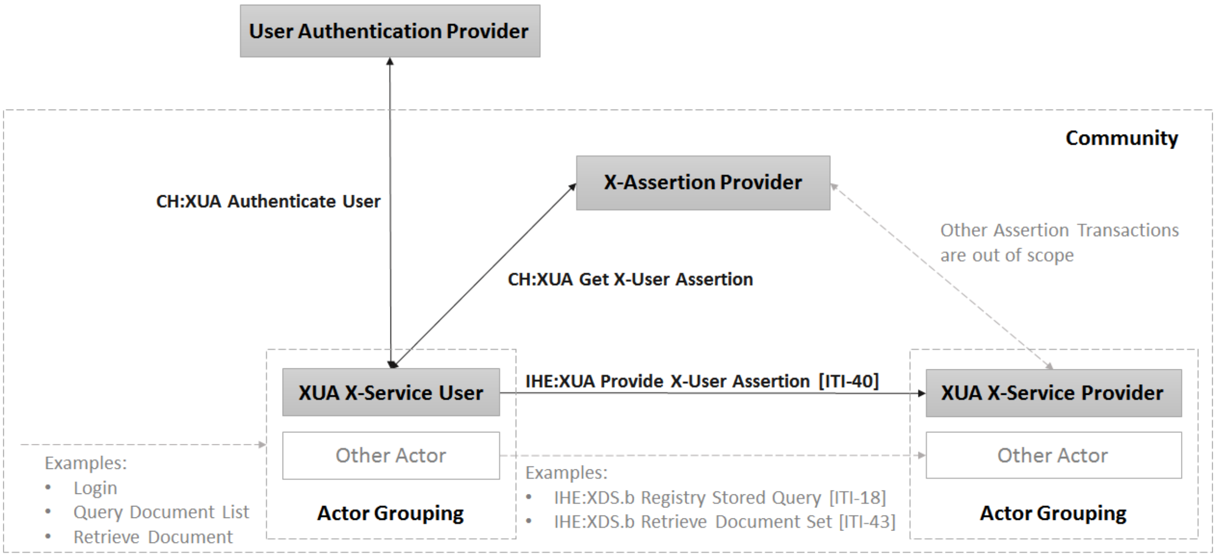

User Authentication Provider
Community
X-Assertion Provider
CH:XUA Authenticate User
Other Assertion Transactions are out of scope
CH:XUA Get X-User Assertion
XUA X-Service User
IHE:XUA Provide X-User Assertion [ITI-40]
XUA X-Service Provider
Other Actor
Other Actor
Examples:
Login
Query Document List
Retrieve Document
Actor Grouping
Examples:
IHE:XDS.b Registry Stored Query [ITI-18]
IHE:XDS.b Retrieve Document Set [ITI-43]
Actor Grouping

Figure 5 XUA Actors for the use within one community

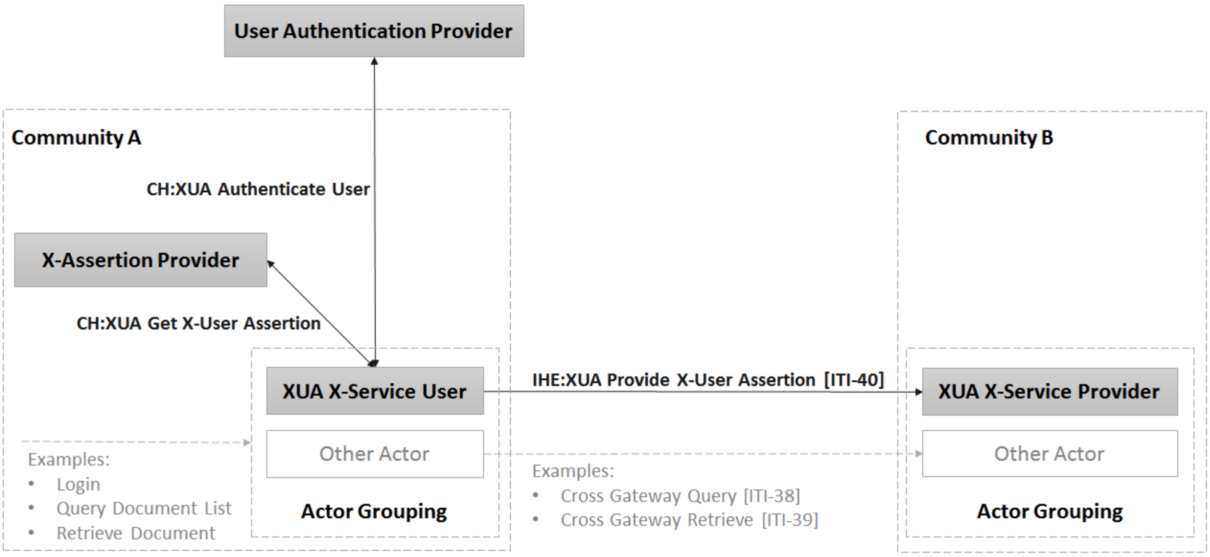


Figure 6: XUA Actors for the use in cross-community communications

1.5.2 Actors

1.5.2.1 User Authentication Provider

This actor is defined in IHE XUA, but not further specified. Its responsibility is to perform user authentication. In the context of this national extension, it’s understood as the Identity Provider (IdP).

In the context of this national extension, it’s required to use the transactions from the WS-Trust specification with SAML binding.

This actor MUST be implemented in any Identity Provider within the EPR circle of trust.

User Authentication Provider actors MUST:

- implement the SAML User Authentication Response specified in chapter “1.5.3.1 Authenticate User” on page 24.
- handover the public keys to the X-Service User actors. These keys allow the X-Service Users to digitally sign and encrypt their requests, as well as to decrypt and validate responses from the User Authentication Provider.
- support SAML http POST binding and SAML SOAP binding for user authentication.
- be able to decrypt SAML User Authentication Request objects and their assertions and check the signature.

1.5.2.2 X-Assertion Provider

This actor is defined in IHE XUA, but not further specified. Its responsibility is to create XUA compliant SAML User Assertions for access authorization.

In the context of this national extension, it’s required to use the transactions from the WS-Trust specification with SAML binding. Therefore, this actor is understood as a WS-Trust Secure Token Service (STS) with SAML binding.

This actor MUST be implemented in any community within the EPR circle of trust.

X-Assertion Provider actors MUST:

- implement the SAML User Assertion Response transaction specified in chapter “1.5.3.2 Get X-User Assertion” on page 28
- handover the public keys to the X-Service User actors. These keys allow the X-Service Users to digitally sign and encrypt their requests, as well as to decrypt and validate responses from the X-Assertion Provider using these keys.

1.5.2.3 X-Service User

This actor is defined and specified in IHE XUA. Its responsibility is to provide a valid SAML User Assertion using the IHE transaction Provide X-User Assertion [ITI-40]. The contents of the SAML User Assertion contain all information needed by the X-Service Provider actor to check the authorization of access to a specific resource.

This actor MUST be grouped with any application that uses any services of Document Registries, Repositories and Policy Repositories within the EPR circle of trust – within a community and across communities.

X-Service User actors MUST:

- implement the SAML User Authentication Request of the «Authenticate User» transaction specified in 1.5.3.1.
- implement the SAML User Assertion Request specified in 1.5.3.2.
- implement the Provide X-User Assertion [ITI-40] transaction specified by the IHE XUA integration profile.
- support either SAML http POST binding or SAML SOAP binding for user authentication.
- be able to create SAML User Authentication Request objects with encrypted and signed assertions according to the Identity Provider.

- be able to decrypt SAML User Authentication Response and User Assertion Response objects including their assertions and check the signature.
- be able to manage the certificates recognized in the EPR circle of trust.
- be able to send SAML attribute queries to the Identity Provider to query specific attributes according to the Identity Provider.
- implement the WS-Trust protocol for the request and validation of SAML assertions.
- be able to request SAML User Assertions from an X-Assertion Provider via a Web service call using WS-Trust Request Security Token Requests.

1.5.2.4 X-Service Provider

This actor is defined and specified in IHE XUA. Its responsibility is to receive SAML User Assertions according to the IHE transaction Provide X-User Assertion [ITI-40] and to delegate the authorization of access to a specific resource.

This actor MUST be grouped with the actor «Authorization Decision Provider» as defined in the CH:ADR integration profile, which itself is grouped with Document Registries, Repositories and Policy Repositories.

X-Service Provider actors MUST:

- implement the Provide X-User Assertion [ITI-40] specified by the IHE XUA integration profile.

1.5.3 Transactions

1.5.3.1 Authenticate User

1.5.3.1.1 Scope

Two procedures are defined for authenticating a user to an application:

1. Identity Provider initiated authentication: In the case of authentication initiated by the Identity Provider, the user first authenticates to the Identity Provider and, after successful authentication, selects the application to which it wishes to access.

2. Service Provider initiated authentication: In the case of authentication initiated by the Service Provider, the user first selects the application (service provider) and is forwarded to the Identity Provider for authentication.

For Web-based applications, service provider-initiated authentication with SAML 2.0 and POST binding is recommended. The Identity Provider-initiated variant for Web applications merely forms part of the service provider-initiated authentication and can be derived.

Rich client applications (Java, C#, or similar) currently use Identity Provider-initiated authentication with the SAML SOAP binding. The steps are virtually identical to Identity Provider-initiated authentication for Web applications, where the SAML SOAP binding is implemented instead of http POST binding.

1.5.3.1.2 Use Case Roles

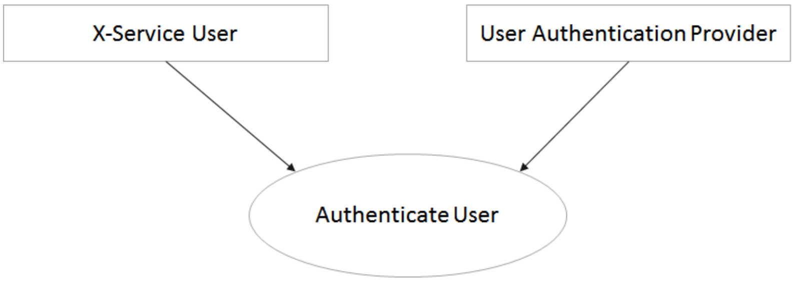


Figure 7: Use Case Roles for Authenticate User

Actors:

- X-Service User Role: Performs a SAML User Authentication Request
- User Authentication Provider Role: Returns a SAML User Authentication Response with the authenticated attributes of the authentication process

1.5.3.1.3 Referenced Standards

See ITI TF-2b, chapter “3.40.3 Referenced Standards”. In addition, the following standards are normative for this transaction:

- 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
- 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
- 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
- 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
- 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
- Web Services Security: SAML Token Profile 1.1
  https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf
- 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
- WS-Trust 1.4
  http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html
- OASIS eXtensible Access Control Markup Language (XACML) v2.0
  https://www.oasis-open.org/standards#xacmlv2.0
- 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
- 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

1.5.3.1.4 Interaction Diagram

The interactions UserAuthenticationRequest and UserAuthenticationResponse are normative for this national extension. Other shown interactions are informative and assist with understanding or implementing this transaction.

1.5.3.1.4.1 Service provider initiated authentication with SAML Post Binding

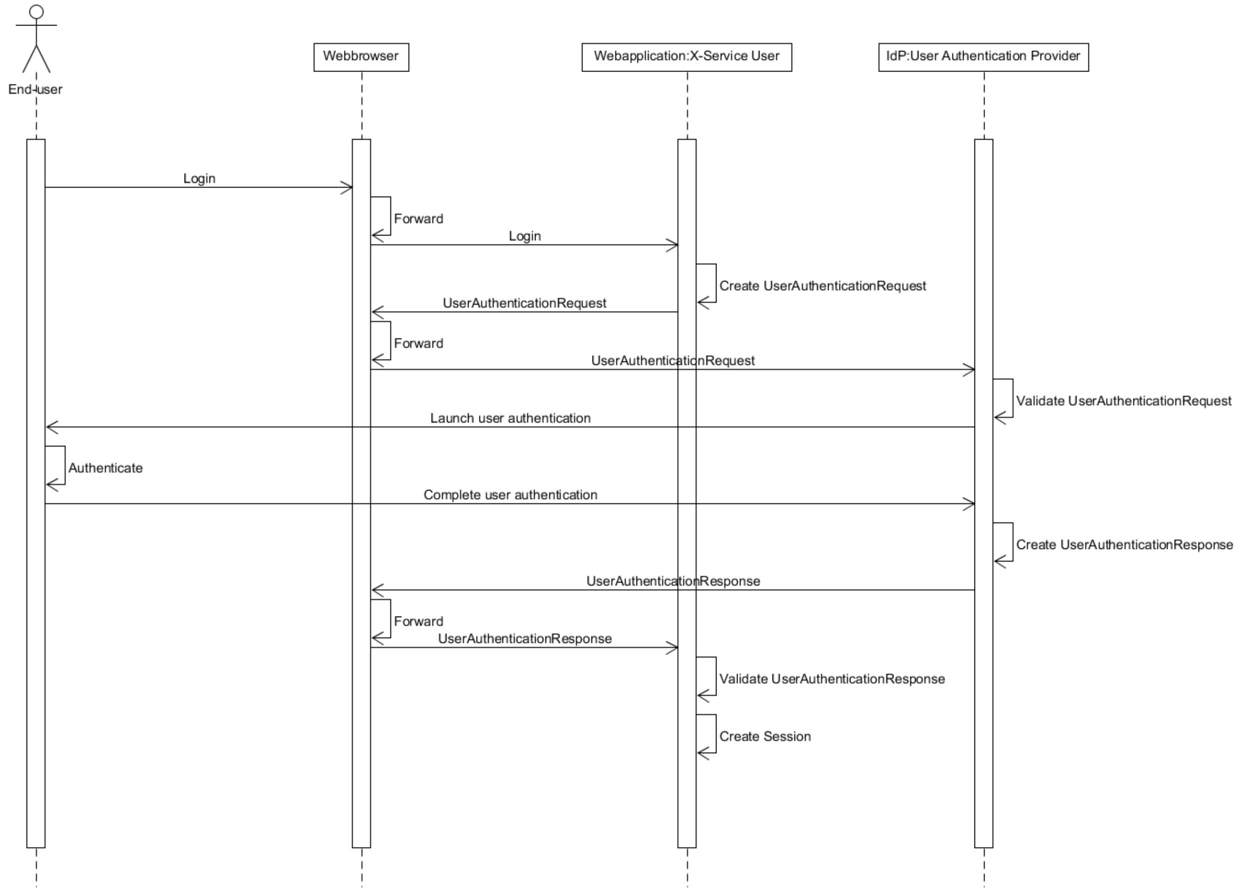

End-user
Webbrowser
Webapplication:X-Service User
IdP:User Authentication Provider
Login
Forward
Login
Create UserAuthenticationRequest
UserAuthenticationRequest
Forward
UserAuthenticationRequest
Validate UserAuthenticationRequest
Launch user authentication
Authenticate
Complete user authentication
Create UserAuthenticationResponse
UserAuthenticationResponse
Forward
UserAuthenticationResponse
Validate UserAuthenticationResponse
Create Session

Figure 8: Service provider initiated authentication with SAML Post Binding interaction diagram

1.5.3.1.4.2 Identity Provider initiated authentication with SAML SOAP Binding

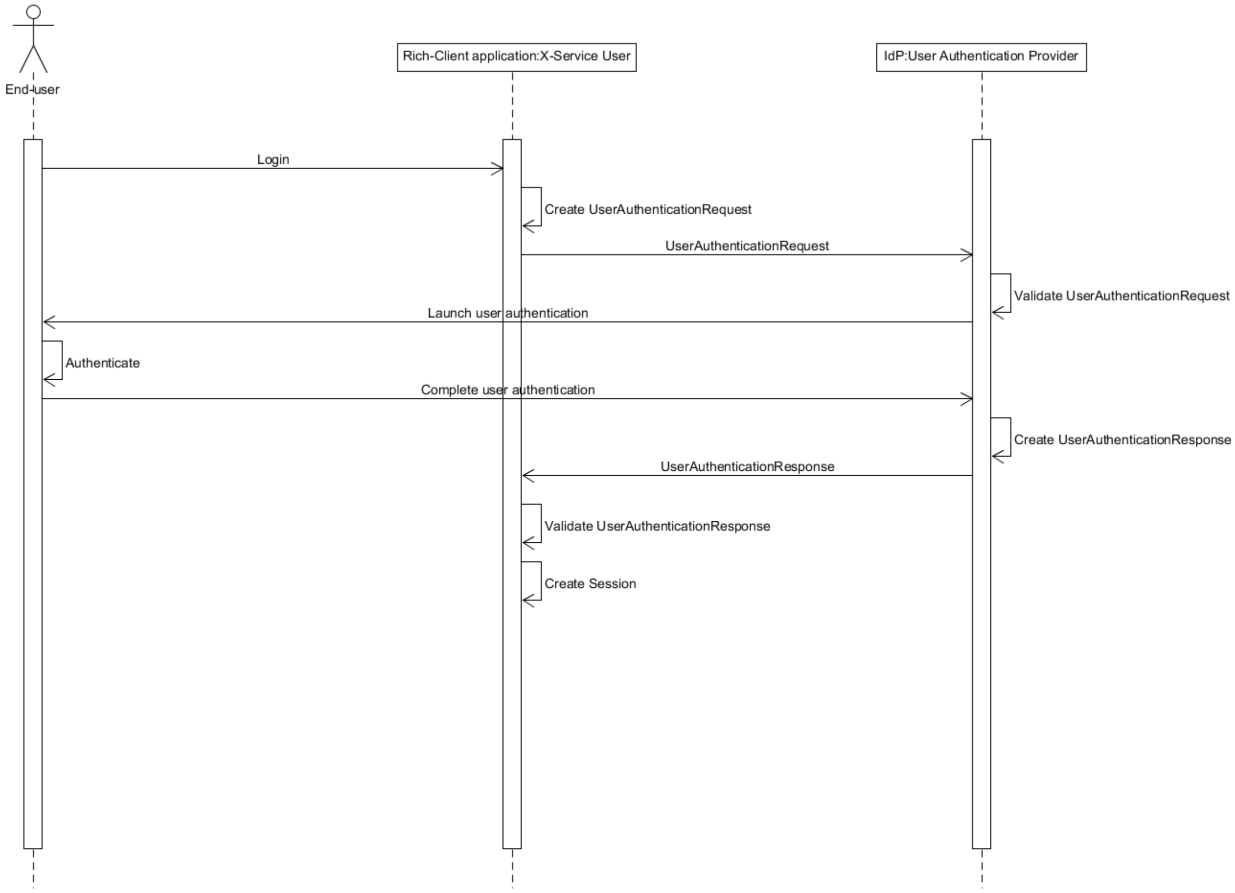

End-user
Rich-Client application:X-Service User
IdP:User Authentication Provider
Login
Create UserAuthenticationRequest
UserAuthenticationRequest
Validate UserAuthenticationRequest
Launch user authentication
Authenticate
Complete user authentication
Create UserAuthenticationResponse
UserAuthenticationResponse
Validate UserAuthenticationResponse
Create Session

Figure 9: Identity Provider initiated authentication with SAML SOAP Binding interaction diagram

1.5.3.1.4.3 Trigger

The Authenticate User transaction is necessary, when a user logs into an application that is grouped with the X-Service User actor.

1.5.3.1.4.4 Message Semantics

The SAML User Authentication Request and Response objects are not specified in this national extension. Their content and semantics MUST be implemented according to the specifications of the IdP.

1.5.3.1.4.5 Expected Actions

The X-Service User creates a SAML User Authentication Request and sends it to the User Authentication Provider.

The User Authentication Provider checks the validity of the SAML User Authentication Request.

When the SAML User Authentication Request is acknowledged to be valid, the User Authentication Provider triggers its own process to authenticate the user (e.g., RSA Secure ID).

The end-user authenticates with his personal identification means.

After successful authentication, the User Authentication Provider creates a SAML User Authentication Response with the authentication details and sends the SAML User Authentication Response to the X-Service User. In case the authentication fails, the User Authentication Provider sends a SAML User Authentication Response with status=failure to X-Service User, who is responsible for the according error message to the end-user.

The X-Service User checks the validity and completeness of the SAML User Authentication Response. Optionally, it can query further attributes from the User Authentication Provider, which are required for the correct identification. This can be done using SAML Attribute Query.

1.5.3.2 Get X-User Assertion

1.5.3.2.1 Scope

A user authenticated according to the «Authenticate User» transaction accesses a protected resource of a system within the EPR circle of trust.

Examples:

- Search for documents of a patient:
  - A healthcare professional has previously authenticated in his primary system according to the «Authenticate User» transaction, selects a patient from the list of his patients, and queries the patient's list of documents within its community (retrieving the document metadata for the existing documents using IHE XDS.b Registry Stored Query [ITI-18]).
  - A patient has previously authenticated in his access portal according to the «Authenticate User» transaction and queries the list of his documents within the EPR circle of trust (cross-community query of the document metadata for the existing documents using IHE XCA Cross Gateway Query [ITI-38]).
- Retrieve of a document:
  - A healthcare professional has performed the above-described search for documents. Then he uses the metadata to select a specific document and retrieves the document from the corresponding repository (download the document using the IHE XDS.b Retrieve Document Set [ITI-43]).
  - A patient has performed the above-described search for documents. Then he uses the metadata to select a specific document and retrieves the document from the corresponding repository (download the document using the IHE XCA Cross Gateway Retrieve [ITI-39]).
- Edit the policy configuration of an EPR:
  - A patient has previously authenticated in his access portal according to the Authenticate User transaction and queries the policy configuration with the definition of the access rights (CH:PPQ XACMLPolicyQuery), edits them in the access portal and saves the changes (CH:PPQ AddPolicyRequest, CH:PPQ UpdatePolicyRequest or CH:PPQ DeletePolicyRequest).

1.5.3.2.2 Use Case Roles

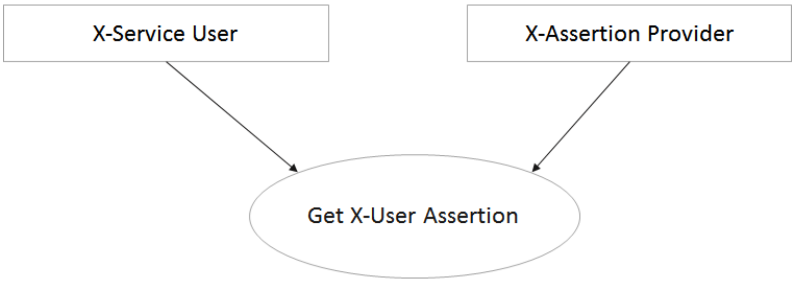


Figure 10: Use Case Roles for Get X-User Assertion

Actors:

- X-Service User
  Role: Performs a SAML User Assertion Request
- User X-Assertion Provider
  Role: Returns a SAML User Assertion Response with the verified attributes during the assertion process

1.5.3.2.3 Referenced Standards

The referenced standards are identical to 1.5.3.1.3.

1.5.3.2.4 Interaction Diagram

The interaction GetXUserAssertionRequest and GetXUserAssertionResponse are normative for this national extension. Other shown interactions are informative and assist with understanding or implementing this transaction.

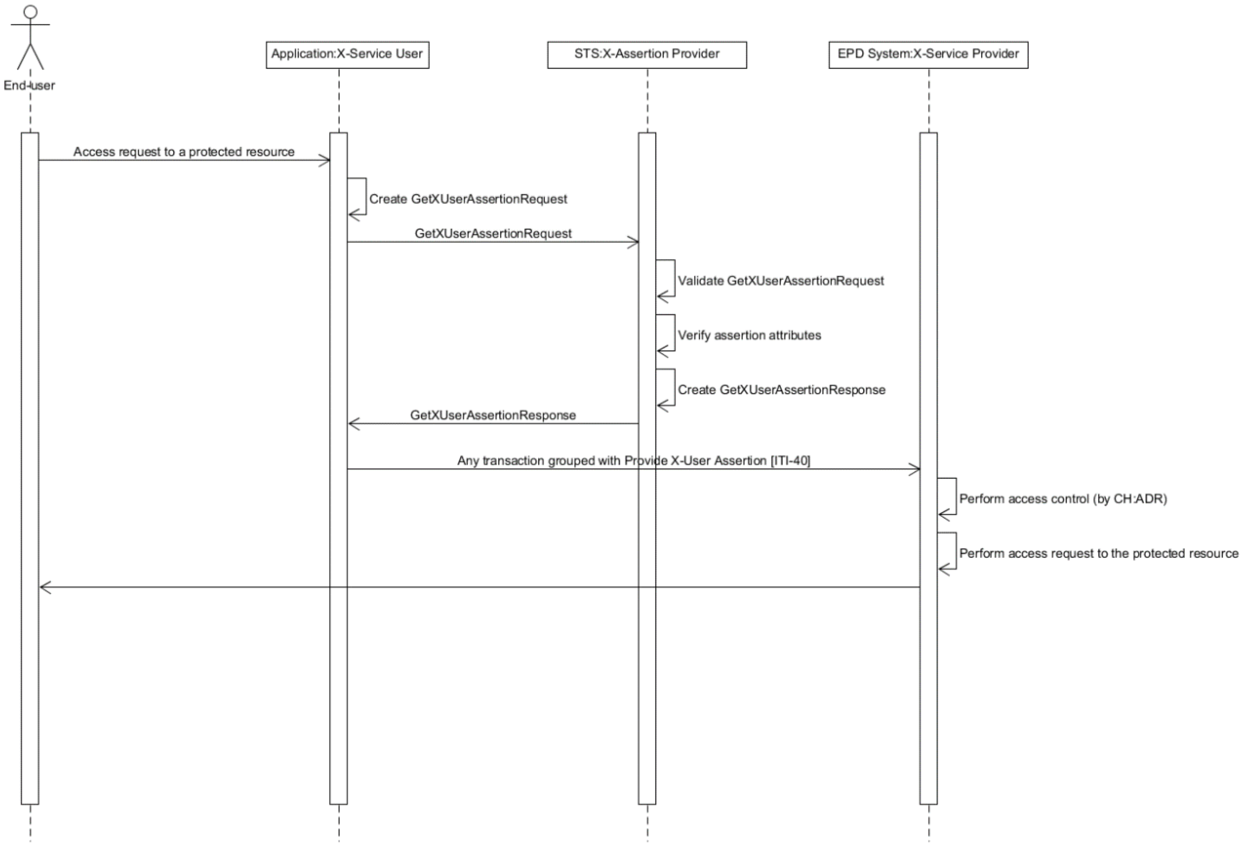

End-user
Application:X-Service User
STS:X-Assertion Provider
EPD System:X-Service Provider
Access request to a protected resource
Create GetXUserAssertionRequest
GetXUserAssertionRequest
Validate GetXUserAssertionRequest
Verify assertion attributes
Create GetXUserAssertionResponse
GetXUserAssertionResponse
Any transaction grouped with Provide X-User Assertion [ITI-40]
Perform access control (by CH:ADR)
Perform access request to the protected resource

Figure 11: Get X-User Assertion interaction diagram

1.5.3.2.4.1 Trigger

The «Get X-User Assertion» transaction is necessary, each time before the «Provide X-User Assertion» [ITI-40] transaction is executed by the X-Service User actor.

1.5.3.2.4.2 Message Semantics

Minimal list of SAML User Assertion attributes:

- **Id of the accessing person:**
  /SUBJECT/NameID: Unique identification of the user
  For healthcare professionals: GLN of the user
  For patients: EPR-PID of the patient

- **Name of the accessing person:**
  /AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"]/AttributeValue:
  Plain text of the users name (e.g., "John Doe")

- **Organization id of the accessing person:**
  /AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"]/AttributeValue:
  For healthcare professionals: GLN of an organization or a group from the Health Organization Index (HOI)
  For patients: empty

- **Organization name of the accessing person:**
  /AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:organization"]/AttributeValue
  For healthcare professionals: Plain text of the organizations name (e.g., "Good health hospital")
  For patients: empty

- **Role of the accessing person:**
  /AttributeStatement/Attribute[@name=”urn:oasis:names:tc:xacml:2.0:subject:role”]/AttributeValue:
  - PAT for patient
  - HCP for healthcare professional
  - ASS for Assistant
  - REP for Representative
- **Requested resource id:**
  /AttributeStatement/Attribute[@name=”urn:oasis:names:tc:xacml:2.0:resource:resource-id”]/AttributeValue:
  EPR-PID of the patient, to which the transaction refers.

- **Purpose of use:**
  /AttributeStatement/Attribute[@name=”urn:oasis:names:tc:xspa:1.0:subject:purposeofuse”]/AttributeValue:
  - NORM for standard access
  - EMER for access during a medical emergency

Request
The SAML User Assertion Request MUST contain the original SAML User Authentication Response and the requested SAML User Assertion Attributes according to the list above. For all other specification, see the referenced standards.

Response
The SAML User Assertion Response objects MUST contain the verified SAML User Assertion Attributes according to the list above. For all other specification, see the referenced standards.

1.5.3.2.4.3 Expected Actions

The X-Service User actor sends a request for a SAML User Assertion the X-Assertion Provider. The request reflects its current application context and provides therefore the desired attributes.

The X-Assertion Provider checks the validity of the SAML User Assertion Request.

When the SAML User Assertion Request is acknowledged to be valid, the X-Assertion Provider triggers its own verification process of the requested attributes.

The attribute verification process MUST ensure that:

- the following attributes (see 1.5.3.2.4.2 for more information about these attributes) correspond unambiguously to the person that was authenticated by the User Authentication Provider. Therefore, the original SAML User Authentication Response provided in the SAML User Assertion Request can be used.
  - Id of the accessing person
  - Name of the accessing person
  - Organization id of the accessing person
  - Organization name of the accessing person
  - Role of the accessing person
- All other requested attributes are copied without any changes from the request into the response, especially the following ones:
  - Requested resource id
  - Purpose of use

After successful verification of the requested attributes, the X-Assertion Provider creates a SAML User Assertion Response with the assertion details and sends the SAML User Assertion Response to the X-Service User. In case the verification fails, the X-Assertion Provider sends a SAML User Assertion Response with status=failure to X-Service User, who is responsible for the according error message to the end-user.

The X-Service User checks the validity and completeness of the SAML User Assertion Response and hands it over to the Provide X-User Assertion [ITI-40] transaction.

1.5.3.3 Provide X-User Assertion [ITI-40]

See ITI TF-2b, chapter “3.40 Provide X-User Assertion [ITI-40]”. The SAML User Assertion MUST be taken from the Get X-User Assertion transaction specified in 1.5.3.2.

1.6 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.

1.6.1 Message Semantics

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

PersonalRelationship
This is used for sending information pertaining to the mother’s maiden name. See also IHE ITI TF-2b, chapter 3.44.4.1.2.1. In Switzerland, the fathers and mothers name can be added here to.

Message Information Model
The Message Information Model for both the Patient Activate and Patient Revise messages, as it is

described in IHE ITI TF-2b, Table 3.44.4.1.2-1 is further restricted for use in an MPI within the EPR on the following attributes:

Table 12 Patient Active and Revise Model 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 [1..*] (M) Patient (SET<II>)	Identifiers designated by this patient identity source for the focal person.	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..*]	Telecommunication address(es) for communicating with this person.	No further refinement.

Person (BAG<TEL>)		
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.	MUST NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST 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.	If patient is already registered in a community, the MPI-PID MUST be provided here.

		The EPR-PID MAY be added here.
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.	Codes:
		FTH= Father
		MTH= Mother

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.	
classCode [1..1] (M)	Structural attribute; this is a 'nation' type of entity.	No further refinement.

Organization (CS) {CNE:NAT, fixed value= "NAT"}		
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..*]	A living subjecst's birth place represented by a unique identifier.	No further refinement.

Birthplace (SET<II>)		
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.
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.

1.7 Requirements on PIXv3 Profile 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-PID.

1.7.1 Message Semantics

1.7.1.1 Major Components of the Patient Registry Query by Identifier

DataSource Parameter

This parameter specifies the assigning authority/authorities of the Patient Identity Domain(s) whose identifiers need to be returned. The DataSource Parameter MUST be specified to the assigning authority/authorities of the MPI-PID in the affinity domain. See also ITI TF-2b, chapter 3.45.4.1.2.1

1.7.2 Return Corresponding Identifiers

1.7.2.1 Major Components of the Get Corresponding Identifiers Query Response

The otherId MUST contain the EPR-PID. See also ITI TF-2b, chapter 3.45.4.2.2.1

1.8 Requirements on PDQv3 Profile for Patient Demographics Query

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

1.8.1 Message Semantics

1.8.1.1 Major Components of the Patient Registry Query by Demographics

The PatientTelecom Query Parameter MUST NOT be used.

1.8.1.1.1 Additional components for the Swiss National Extension

MothersName Parameter

This optional parameter specifies the name of the mother of the person whose information is being queried. For this parameter item, a single person name (PN) data item shall be specified in the Person.value attribute. Within the PN data type, the given name and family name may be specified. If the sender needs to indicate that the name parts specified are not limited to an exact match, then the use attribute of the value element shall be set to "SRCH".

FathersName Parameter

This optional parameter specifies the name of the father of the person whose information is being queried. For this parameter item, a single person name (PN) data item shall be specified in the Person.value attribute. Within the PN data type, the given name and family name may be specified. If the sender needs to indicate that the name parts specified are not limited to an exact match, then the use attribute of the value element shall be set to "SRCH".

1.8.1.2 Message Information Model

The Message Information Model for both the Patient Activate and Patient Revise messages is described in IHE ITI TF-2b, Table 3.47.4.1.2-1. Within the Swiss national extensions the following sections MAY additionally be included:

Table 13 Patient Demographics Query – Swiss national extension sections

PRPA_HD201306IHE Patient Registry Query by Demographics	**This HMD extract defines the message used to query a patient registry for records matching a set of demographics information. Derived from Figure 3.47.4.1.2-1 (PRPA_RM201306IHE)**	**Swiss National Extension**
MothersName	N/A	Design Comments: This query parameter is the 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 name is the person name part of "family" for the person who is the player in a PersonalRelationship of type of "mother" to the focal person.
value [1..1] ParameterItem (PN)	N/A	Design Comments: A person name. In this case it may consist of only the given name part, the family name part, or both.
semanticsText [1..1] ParameterItem (ST) {default= "Person.MotherName"}	N/A	These static values MUST be used.

FathersName	N/A	Design Comments: This query parameter is the name of a focal person's father. 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 Father's name is the person name part of "family" for the person who is the player in a PersonalRelationship of type of "father" to the focal person.
value [1..1] ParameterItem (PN)	N/A	Design Comments: A person name. In this case it may consist of only the given name part, the family name part, or both.
semanticsText [1..1] ParameterItem (ST){default= "Person.Father.Name"}	N/A	These static values MUST be used.

1.8.2 Patient Demographics Query Response

1.8.2.1 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-2b, chapter 3.47.4.2.3.

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

Table 14 Message Information Model for Patient Registry Find Candidates

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. Note: The EPR-PID should be added in OtherIDs.id.
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 orPatient.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]	A value representing the domestic partnership status of this person.	No further refinement.

Person (CE) {CWE:MaritalStatus}		
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	The EPR-PID MAY be added here.
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.	
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.
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/	Structural attribute – this is an event.	No further refinement.

infrastructure/vocabulary/ActMood.htm - ActMood, default= "EVN"}		
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.

1.8.2.1.1 Special handling for more attributes requested

If there are more than 5 matches zero matches a special handling like in the XCPD transaction (see IHE ITI TF-2b, chapter 3.55.4.2.2.6) is necessary.

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 15. 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 codeSystem for these code elements is *<2.16.756.5.30.1.127.3.10.2.1>* instead of 1.3.6.1.4.1.19376.1.2.27.1 as described in IHE ITI TF-2b, Table 3.55.4.4.2-4.

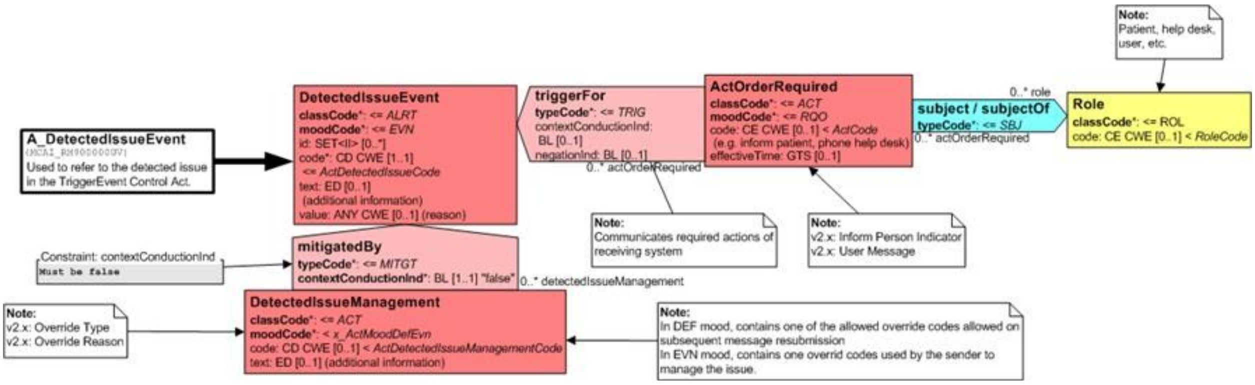

A_DetectedIssueEvent
(MCAI_RM900000UV)
Used to refer to the detected issue in the TriggerEvent Control Act.
DetectedIssueEvent
classCode*: <= ALRT
moodCode*: <= EVN
id: SET<II> [0..*]
code*: CD CWE [1..1] <= ActDetectedIssueCode
text: ED [0..1] (additional information)
value: ANY CWE [0..1] (reason)
triggerFor
typeCode*: <= TRIG
contextConductionInd: BL [0..1]
negationInd: BL [0..1]
0..* actOrderRequired
ActOrderRequired
classCode*: <= ACT
moodCode*: <= RQO
code: CE CWE [0..1] < ActCode (e.g. inform patient, phone help desk)
effectiveTime: GTS [0..1]
0..* role
subject / subjectOf
typeCode*: <= SBJ
0..* actOrderRequired
Role
classCode*: <= ROL
code: CE CWE [0..1] < RoleCode
Note: Patient, help desk, user, etc.
Note: Communicates required actions of receiving system
Note: v2.x: Inform Person Indicator v2.x: User Message
Constraint: contextConductionInd
Must be false
mitigatedBy
typeCode*: <= MITGT
contextConductionInd*: BL [1..1] "false"
0..* detectedIssueManagement
DetectedIssueManagement
classCode*: <= ACT
moodCode*: < x_ActMoodDefEvn
code: CD CWE [0..1] < ActDetectedIssueManagementCode
text: ED [0..1] (additional information)
Note: v2.x: Override Type v2.x: Override Reason
Note: In DEF mood, contains one of the allowed override codes allowed on subsequent message resubmission In EVN mood, contains one overrid codes used by the sender to manage the issue.

Figure 12 XCPD – RMIM for DetectedIssueEvent

Table 15 Coded Values for actOrderRequired code (codeSystem=2.16.756.5.30.1.127.3.10.2.1)

Value for code	Meaning of code
LivingSubjectAdministrativeGenderRequested	Requests the LivingSubjectAdministrativeGender attribute be specified
PatientAddressRequested	Requests the PatientAddress attribute be specified

LivingSubjectBirthPlaceNameRequested	Requests the LivingSubjectBirthPlaceName attribute be specified
BirthNameRequested	Requests the Birth Name attribute be specified
MothersNameRequested	Requests the Mothers Name attribute be specified
FahtersNameRequested	Requests the Fathers Name attribute be specified

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

```
<detectedIssueEvent classCode="ALRT" moodCode="EVN">

 <code code="ActAdministrativeDetectedIssueCode"
codeSystem="2.16.840.1.113883.5.4"/>

 <triggerFor typeCode="TRIG">

 <actOrderRequired classCode="ACT" moodCode="RQO">

  <code code="PatientAddressRequested” codeSystem="2.16.756.5.30.1.127.3.10.2.1" />

 </actOrderRequired>

 </triggerFor>

 <triggerFor typeCode="TRIG">

 <actOrderRequired classCode="ACT" moodCode="RQO">

  <code code=" LivingSubjectAdministrativeGenderRequested”
  codeSystem="2.16.756.5.30.1.127.3.10.2.1"/>

 </actOrderRequired>

 </triggerFor>

</detectedIssueEvent>
```

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

1.9 Requirements on XCPD Profile for Cross- Community Patient Discovery

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

1.9.1 Modes and Options

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

The Health Data Locator and Revoke Option of the Patient Location Query transaction [ITI-56] MUST NOT be used.[5]

1.9.2 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 values MUST NOT exceed 3 days. See also IHE ITI TF-2b, chapter 3.55.4.1.

1.9.2.1 Major Components of the Patient Registry Query by Demographics

LivingSubjectId Parameter is the only allowed query Parameter. All other parameter in IHE ITI TF-2b, chapter 3.55.4.1.2.1 MUST NOT be used.

The LivingSubjectId Parameter MUST contain the EPR-PID.

Reverse Cross-Gateway Queries
Reverse Cross-Gateway Queries MUST NOT be used (see IHE ITI TF-2b, chapter 3.55.4.1.2.4).

1.9.3 1.8.3 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 values MUST NOT exceed 3 days. See also IHE ITI TF-2b, chapter 3.55.4.2.

1.9.3.1 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 MUST state 100 for an exact match.

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

Table 16 Message Information Model for Patient Registry Find Candidates

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.
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	The MPI-PID MUST be returned if there is a match from the EPR-PID.

[5] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCPD_HDL_Revoke_Option.pdf

	shall be specified in the OtherIDs.id attribute.	
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.	MUST 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.	MUST NOT be used.
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>) {null, fixed value nullFlavor="NA"}	Name(s) for this person. Fixed to be null, <name nullFlavor="NA"/>, request contains only a patient identifier and no demographic data.	No further refinement.
telecom [0] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	MUST 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.	MUST NOT be used.
birthTime [0] Person (TS)	The date and time this person was born.	MUST NOT be used.
deceasedInd [0] Person (BL)	An indication that this person is dead.	MUST NOT be used.
deceasedTime [0] Person (TS)	The date and time this person died.	MUST NOT be used.
multipleBirthInd [0] Person (BL)	An indication that this person was part of a multiple birth.	MUST NOT be used.
multipleBirthOrderNumber [0] Person (INT)	The order in which this person was born if part of a multiple birth.	MUST NOT be used.
addr [0] Person (BAG<AD>)	Address(es) for corresponding with this person.	MUST NOT be used.

maritalStatusCode [0] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	MUST NOT be used.
religiousAffiliationCode [0] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	MUST NOT be used
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).	MUST NOT be used.
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.	MUST NOT be used.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	MUST NOT be used.
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.	MUST NOT be used.
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.	MUST NOT be used.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	MUST NOT be used.
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.	MUST NOT be used.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	MUST NOT be used.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	MUST NOT be used.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	MUST 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.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	MUST NOT be used.
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.	MUST NOT be used.
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.	MUST NOT be used.
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.	MUST NOT be used.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the local person for the associated mode.	MUST 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.
moodCode [1..1] (M)	Structural attribute – this is an event.	No further refinement.

Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infra structure/vocabulary/ActMood.htm - ActMood, default= "EVN"}		
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).	This value MUST state 100 for a match, 0 otherwise.

1.10 Requirements on HPD Profile for Replication

1.10.1 Introduction

The Healthcare Provider Directory (HPD) profile is extended to support the incremental replication of the entire directory or part 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 scarifying their operational independence.

This extension also defines some content profiles to ease the integration between communities, by limiting the value-set of several attributes, e.g. identifiers, organization types, provider types, etc.

1.10.2 Use-case: Provider information replication

Table 17 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.

1.10.3 Actors / Transactions

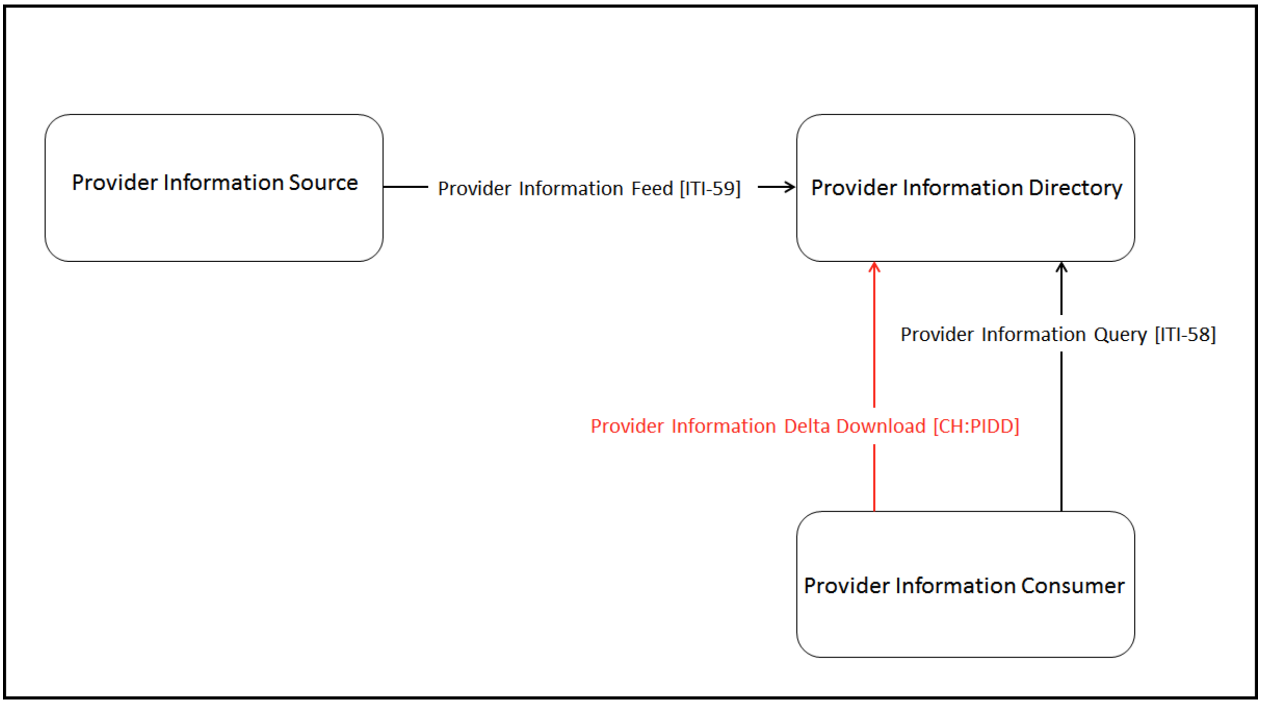

Provider Information Source
Provider Information Feed [ITI-59]
Provider Information Directory
Provider Information Query [ITI-58]
Provider Information Delta Download [CH:PIDD]
Provider Information Consumer

Figure 13 Swiss extended HPD Actors / Transactions

1.10.3.1 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.

1.10.3.2 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.

1.10.4 Transactions

1.10.4.1 Provider Information Delta Download (CH:PIDD)

This transaction schema extends the DSMLv2 interface by supporting an additional SOAP schema (see Appendix C – Provider Information Delta Download schema (PIDD.xsd) on page 52) and an additional wsdl operation:

```
<operation name="ProviderInformationDownloadRequest">

        <soap:operation soapAction="urn:ihe:iti:hpd:2010:ProviderInformationDownloadRequest" />

        <input>
```

```
            <soap:body use="literal" />
        </input>
        <output>
            <soap:body use="literal" />
        </output>
  </operation>
```

1.10.4.1.1 Interaction Diagram

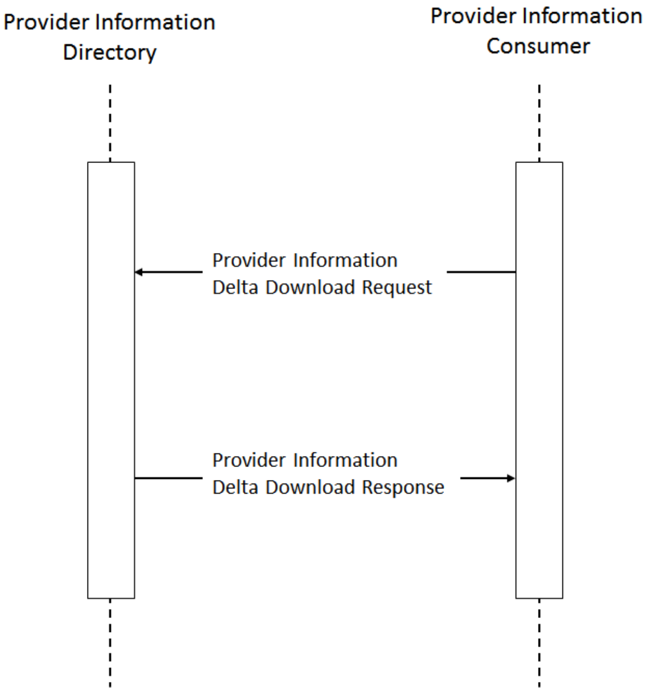

Provider Information Directory
Provider Information Consumer
Provider Information Delta Download Request
Provider Information Delta Download Response

Figure 14 Provider Information Delta Download (CH:PIDD) interaction diagram

1.10.4.1.2 Provider Information Delta Download Request

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

- A required **fromDate** parameter to define the inclusive range starting date of the requested transactions sequence;
- An optional **toDat** parameter to define the inclusive range ending date of the requested transactions sequence (default: now);
- An optional **filterMyTransactions** boolean parameter to manage the server side filtering of the author issued transactions (default: true);

1.10.4.1.3 Provider Information Delta Download Response

The response message contains a sequence of DSMLv2 batchRequest elements.

1.10.5 Message Semantics

1.10.5.1 HPD Schema Content

1.10.5.1.1.1 Identifiers

Organizational (e.g. hospitals) and Individual (health professionals) Providers are identified by Object Identifiers (OID). For Organizational Provider, the ID is equal to the OID for the healthcare facility that has been registered by the community in the national OID registry[6]. For Individual Provider, the ID consists of the OID for GS1 GLN (2.51.1.3) plus the GLN[7] of the Individual Provider as a suffix number.

Example for Individual Provider (2.51.1.3.<*gln individual provider*>)

```
2.51.1.3.7601003899986
```

1.10.5.1.2 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 both organizational and individual providers.

Conventions:

Optionality column (?): O=optional, R=required, R2=required if available; Cardinality column (#): S=Single-valued, M=Multi-valued;

Deviations from the HPD profile are **highlighted**.

Table 18 Swiss refined HPD Organizational provider attributes

HPD profile [1]			**Swiss National Extension**		
Attribute name	**?**	**#**	**?**	**#**	***Notes***
Unique Entity Identifier	R	S	R	S	*Auto-generated*
Org Identifiers	R	M	R	**S**	OID
Org Names	R	M	R	M	Legal name(s)
Org Known Names	R2	M	R2	M	Other name(s)
Org Type	O	M	**R**	M	HealthCareFacilityCode value [App. A-1]
Org Type description	O	M	O	M	HealthCareFacilityCode display name [App. A-1]
Org Status	O	S	O	S	Possible values: *Active, Inactive*
Org Supported Lang.	O	M	O	M	Encoded using ISO-639-1
Org Specialty	O	M	**R2**	M	PracticeSettingCode value [App. A-2]
Org Relationships	O	M	**R**	M	Reference to community or parent org.

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 HPD Supplement for Trial Implementation, Table 3.58.4.1.2.2.3-1: Organizational Provider Mapping applies.

Table 19 Swiss refined HPD Individual provider attributes

HPD profile [1]			**Swiss National Extension**		
Attribute name	**?**	**#**	**?**	**#**	***Notes***
Unique Entity Identifier	R	S	R	S	*Auto-generated*

[6] http://oid.refdata.ch/

[7] http://www.refdata.ch/content/partner_d.aspx?Nid=6&Aid=908&ID=412

Provider Identifiers	R	M	R	**S**	OID (GLN OID plus GLN)
Provider Type	R	M	R	M	IndProviderTypeCode value [App. A-3]
Provider Type descript.	R	M	R	M	IndProviderTypeCode display name [App. A-3]
Provider Status	O	S	O	S	Possible values: *Active, Inactive*
Provider Primary Name	R	S	R	S	i.e. provider display name
Provider First Name	R2	M	**R**	M	Actual first name
Provider Last Name	R	M	R	**S**	Actual last name
Provider Known Names	R	M	R	M	Composed name string (e.g. title, first name,...)
Provider Supported Lang.	O	M	O	M	Encoded using ISO-639-1
Provider Gender	O	S	O	S	RFC 2985
Provider Specialty	O	M	O	M	AuthorSpecialtyCode value [App. A-4]
Provider Relationships	O	M	**R**	**M**	Reference to community or parent org.

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 HPD Supplement for Trial Implementation, Table 3.58.4.1.2.2.2-1: Individual Provider Mapping applies.

2 Appendices

2.1 Appendix A – AuditMessage schema (AuditMessage.xsd)

This XML schema is identical to the DICOM A.5.1-1 Audit Message Schema, which is provided inRelax NG Compact format.

See https://www.bag.admin.ch/epra

2.2 Appendix B – AuditTrail schema (AuditTrail.xsd)

Includes the AuditMessage schema, introduced in chapter “1.4.4.1.1 Detailed AuditMessage definitions” starting on page 12.

See https://www.bag.admin.ch/epra

See also Appendix A – AuditMessage schema starting on page 45.

2.3 Appendix C – Provider Information Delta Download schema (PIDD.xsd)

See https://www.bag.admin.ch/epra

3 Glossary

The IHE Glossary can be found as an appendix to the IHE Technical Frameworks General Introduction[8]. See also chapter “1.1 Definitions of terms” on page 4.

[8] http://ihe.net/TF_Intro_Appendices.aspx

4 Illustrations

5 Tables