Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Inneren EDI

‘

Revisionsentwurf zur 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

Änderungsnachweis seit Inkrafttreten am 15. April 2017

Die Anpassungen der Anhänge zur EPDV-EDI vom 22. März 2017 werden durch das BAG laufend vorgenommen und die Zwischenstände durch eHealth Suisse der Öffentlichkeit zugänglich gemacht. Der Nachweis ermöglicht eine Vorschau auf eine mögliche künftige Version der normativen Spezifikationen. Bis zur Inkraftsetzung der revidierten Verordnung gilt formell die Ausgabe, welche am 15. April 2017 in Kraft getreten ist.

Bezüglich der zu verwendenden Metadaten gilt aktuell die Version 1.2 des Revisionsentwurfs zum Anhang 3 der EPDV-EDI. Dieser entspricht den publizierten Value Sets der Version 201704.2-beta auf ART-DECOR, abrufbar unter: http://art-decor.org/art-decor/decor-project--ch-epr-

Die von eHealth Suisse publizierte Programmierhilfe enthält die aktuellen Verweise auf die Stable/Beta-Versionen: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/180131_Anleitung_Zugang_Metadaten_und_Synonymen_v1.2_d.pdf

Version:	1.4
Datum:	29. Juni 2018
Profile:	**ATNA, PDQv3, PIXv3, XCPD und XUA**

Changes:

Version	Chapter	Ticket	Comment to changes
1.1	Front page	EPD-3	Version DE: No changes; Version FR: „5“ missing on front page.
1.1	All	EPD-62	Changed EPR-PID to EPR-SPID
1.3	1.2	EPD-234	For XCA there is no national extension. Removed point: “*IT Infrastructure: Cross-Community Access (XCA)*”
1.4	1.2	EPD-246	The profile Consistent Time is not a national extension. Therefore the line “IT Infrastructure: Consistent Time (CT)” was removed. The precision on the time server is made in annex 2 only.
1.2	1.3	EPD-10	New chapter "*1.3 Expected actions for receiving actors receiving unexpected parameters*" added.
1.2	1.3	EPD-198	Typo: Section “2.4.2” corrected to “4.2.4 ".
1.3	1.3.1 1.3.2	EPD-236	Made this chapter dynamic. Changed: "1.3.1 For ebXML-based profiles (XDS.b, XCA, XCMU, …):" to "1.3.1 For ebXML-based profiles **(e.g. XDS.b)**:" And: "1.3.2 For HL7v3-based profiles (PIXv3, PDQv3, XCPD):" to "1.3.2 For HL7v3-based profiles **(e.g. PIXv3)**:"
1.4	1.4	EPD-246	Changed the title of chapter 1.4 to “*Requirements on CT*” and slightly the text, because for this profile, there is actually no Swiss extension.
~~*1.1*~~	~~*Former 1.4.2.2*~~	~~*EPD-75*~~	~~*Obsolete, because contained text has been removed. $XDSDocumentEntryTypeCode contains the value 722160009*~~
1.1	1.5	EPD-65	Audit Trail Consumption is deprecated, because there is a new Swiss specific profile CH:ATC. Chapter reduced to “Requirements on ATNA”.
1.4	1.5.1	EPD-237	Replaced the complete text of the Introduction of the chapter “1.5 Requirements on ATNA” to address the requirements on the Swiss profile ATC.
1.3	1.5.2.1	EPD-65	At point “Maintain Time [ITI-1]” the wrong chapter was referenced. Correct: “1.4 Requirements on ”.
1.1	1.5.4.1	EPD-135	Duplicate Text like in *2.1 Appendix A – AuditMessage schema (AuditMessage.xsd)* removed.
1.1	1.5.4.1.1	EPD-46	Table 1: When describing a human user’s participation in an event, this value MUST represent a value from the Swiss Metadata Value-Set “epr_xds_authorRole” (2.16.756.5.30.1.127.3.10.1.1.3)
1.1	1.5.4.1.1	EPD-80	Table 1 (@ParticipantObjectSensitivity): The current confidentiality code of the object MUST be specified **IF KNOWN**, when …
1.1	1.5.4.1.1	EPD-78	Table 1 (@codeSystemName): “If this value represents a value from the Swiss Metadata Value-Set, an OID MUST be used. Otherwise either an OID or a String MUST be used.”
1.3	1.5.4.1.1	EPD-190	Adjusted Swiss refinement of @EventDateTime.
1.3	1.5.4.1.1	EPD-156	Mandate XUA: Attribute @UserID: Revised definition: “*If a XUA SAML User Assertion Response has been provided, the /SUBJECT/NameID from the XUA SAML User Assertion Response MUST be used.*”

Version	Chapter	Ticket	Comment to changes
1.3	1.5.4.1.1	EPD-156	Mandate XUA: Attribute @UserID:Clarification added: *"…as input to construct the @UserName attribute as defined in the IHE-XUA profile."*
1.3	1.5.4.1.1	EPD-156	Mandate XUA: Attribute @UserName: Revised definition: "*If a XUA SAML User Assertion Response has been provided, the subject-id attribute value from the XUA SAML User Assertion Response MUST be used.*"
1.3	1.5.4.1.1	EPD-226	Swiss Extension of "RoleIDCode" authorRole is not correct. The actor must be used: eprActor.
1.3	1.5.4.1.1	EPD-225	@ParticipantObjectSensitivity: CNE.2 and CNE.7 removed, because with CH:ATC no language support in CH:ATNA is required and the date of the version of the value set is not necessary, because there is not expected a lot of change the next years for this value set.
1.3	1.5.4.1.1	EPD-223	Swiss Extension of "MediaType": Text updated for the now available Swiss Metadata value set "Media Type Code".
1.3	1.5.4.1.1	EPD-156	Requirements on ATNA: Attribute @UserName: "If a XUA SAML User Assertion Response has been provided, the subject-id attribute value from the XUA SAML User Assertion Response MUST be used."
~~*1.3*~~	~~*Former 1.5.5*~~	~~*EPD-65*~~	~~*Translations are still being provided by eHealth Suisse, but not legally required any more (reason: CH:ATC). This parts therefore has been removed.*~~
1.3	1.6.1		Mandate XUA: Actors and transactions added.
1.3	1.6.2.1	EPD-153	Mandate XUA: Sentence "support SAML http POST binding and SAML SOAP binding for user authentication." resplaced with "support POST/Artifact Binding".
1.3	1.6.2.2		Mandate XUA: X-Assertion Provider: Text reworked completely after "X-Service User actors MUST".
1.3	1.6.2.2	EPD-156	Mandate XUA: X-Assertion Provider: Last point changed: "*To ensure meaningful data in the ATNA logs, the X-Assertion Provider MUST be grouped with Patient Identifier Cross-reference Consumer and Provider Information Consumer actors to resolve names of healthcare professionals and patients.*"
1.3	1.6.2.3		Mandate XUA: Typo: "*Get X*-User Assertion Request" instead of "*SAML* User Assertion Request."
1.3	1.6.2.3	EPD-153	At X-Services User, the sentence "*support either SAML http POST binding or SAML SOAP binding for user authentication.*" is removed according to decision in AG TSI of 06.06.2018. The regulations in Ausgabe 2 zu Anhang 8 are to be followed.
1.3	1.1.1.1	EPD-153	Changed text for Artifact Binding.
1.2	1.1.1.1	EPD-85	XUA: WS-Trust Version: Only v1.3 allowed
1.3	1.6.3.2		Mandate XUA: *1.6.3.2 Get X-User Assertion* reworked completely.
1.3	1.6.3.2.1.4		Mandate XUA: Paragraph added at the end describing the semantic grouping of organization-id and organization (text).

Version	Chapter	Ticket	Comment to changes
1.2	1.6.3.2.4.2	EPD-83	Typo: Some SAML attributes names are wrongly spelled @name instead of @Name (role, resource-id and purpose of use).
1.3	1.6.3.2.4.2	EPD-156	Name of the accessing Person: Changed second part of the paragraph: "*Name of the accessing person is a text string. Contents depends on the Role of the accessing person, see section "Response" below.*"
1.3	1.6.3.2.4.2	EPD-156	X-Assertion Provider: 1.6.3.2.4.2 Message Semantics: Added the name attributes from the sources to the responses according to the role. Added “(name)” to patient and representative from MPI. Added “(Provider Primary Name)” to healthcare professional and assistant from HPD.
1.3	1.6.4		Mandate XUA: *1.6.4 EPR XUA Requirements for XDS and PPQ* added.
1.3	1.6.4.2	EPD-156	Specified the format in attribute @UserName: “*…human user* ***in the format alias"<"user"@"issuer">"”*** and the element *… difference* **that the "user" element *of*** *its attribute…*
~~*1.3*~~	~~*Former 1.6*~~	~~*EPD-231*~~	~~*Typo corrected: Correct: "In Switzerland, the father**'s** and mother**'s** name can be added here."*~~ ~~*Meanwhile this sentence has been removed.*~~ ~~*Mother and Father Name should not be used.*~~
1.4	1.7.1.1	EPD-232	Because mother and father name should not be used, removed paragraph *PersonalRelationship*.
1.4	1.7.1.1	EPD-232	Because mother and father name should not be used, changed attribute *Role* in section *PersonalRelationship* of the table to “MUST NOT be used.”
1.1	1.7.1.1	EPD-39	PIXv3: Attribute Person: “**At least** Person.name or Patient.id must be non-null.”
1.4	1.6.2.1	EPD-244	Because the specifications are already defined in version 2 of annex 8, removed the text and added a reference to annext 8.
1.4	1.6.2.2	EPD-244	Added line: “*assistant: UAP Identifier – GLN*”.
1.4	1.6.2.4	EPD-244	In second paragraph corrected the actor “Authorization Decision Provider” to “Authorization Decision Consumer” and shortened the sentence.
1.4	1.6.3.1	EPD-244	Because the specifications are already defined in version 2 of annex 8, removed the text and added a reference to annext 8.
~~*1.1*~~	~~*1.8.1*~~	~~*EPD-8*~~	~~*PDQv3: Inconsistency Person.MotherName vs Person.Father.Name solved: Person.FatherName.*~~ ~~*Meanwhile these element have been removed.*~~
~~*1.1*~~	~~*Former 1.8.2.1.1*~~	~~*EPD-9*~~	~~*Typo corrected: FahtersNameRequested instead of FathersNameRequested.*~~ ~~*This part has been removed.*~~
1.1	1.9.2.1.1	EPD-147	XCPD is not correct in that place. Correct: "Figure 10 RMIM for DetectedIssueEvent".

Version	Chapter	Ticket	Comment to changes
1.1	1.10.1	EPD-95, EPD-146	"*For the EPR only the Shared/National Patient Identifier Query mode* ***or Demographic Query and Feed*** *mode MUST be used.*" Added as a consequence of allowing additional attributes according to EPD-95/EPD-146.
1.1	1.10.2.1	EPD-95	XCPD: Restriction relaxed: LivingSubjectId Parameter is the only required query Parameter. All other parameter in IHE ITI TF-2b, chapter 3.55.4.1.2.1 MAY be used.
1.1	1.10.3.1	EPD-45	XCPD: Attribute Person: Swiss specific specification that, Patient.id MUST NOT be Null.
1.1	1.10.3.1	EPD-42	XCPD: Whole nodes are forbidden instead of all its attributes.
1.1	1.10.3.1	EPD-43	XCPD: Attribute QueryMatchObservation: "*A numeric value between 0 (excluded) and 100 (0 < percentage value <= 100) MUST be used (100 for an exact match).*"
1.2	1.10.3.1	EPD-43	Refined: *"This value MUST contain a numeric value greater 0 (0 is excluded because subjectOf element is not present if there is no match) and 100 (for an exact match) indicating the confidence in the match for this record (0 < percentage value <= 100)."* Table 16: ***A numeric value between 0 (excluded) and 100 (0 < percentage value <= 100) MUST be used (100 for an exact match).***
1.2	1.11.4.1.2	EPD-15	Typo: "toDat" changed to "toDate"
1.3	2.1	EPD-135	Upgraded to schema DICOM Standard, Part 15 Annex A.5 - Edition DICOM PS3.15 **2017c.** Change of DICOM message scheme (→ 2017c): Just the Version change was not sufficient. IHE required the use of the 2017c Edition but with IHE Modifications. see: https://gazelle.ihe.net/content/atna-testing-connectathon-digital-certificates#ATNALogging
~~*1.3*~~	~~*Former 2.2*~~	~~EPD-135~~	~~*Removed "2.2 Appendix B – AuditTrail schema (AuditTrail.xsd)", because the exchange of audit messages is covered by the CH:ATC profile.*~~
1.4	1.11.5.1.2 Attribute	EPD-106	Intregrate revised list of attributes for HPD

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)

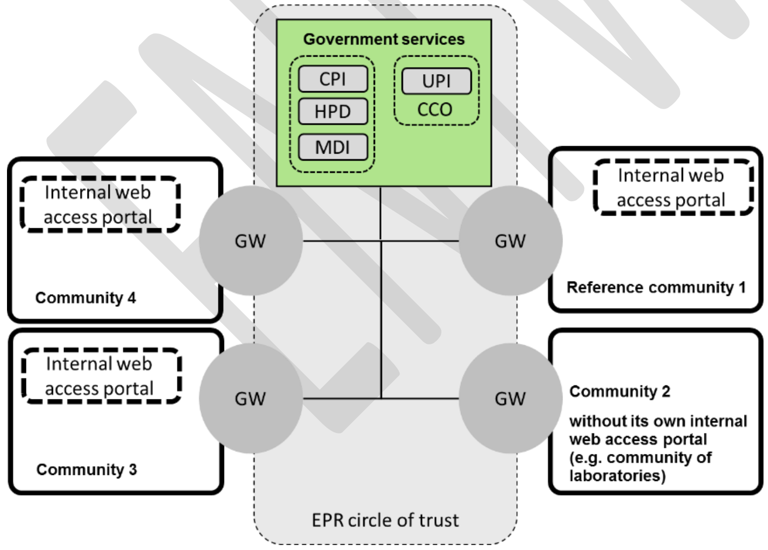
The object of the Federal Act on Electronic Patient Records (EPRA) is to define the conditions for processing data and documents relating to electronic health records. Using electronic health records, healthcare professionals can access data relevant to treatment of their patients that was compiled and 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
GW
GW
Internal web access portal
Reference community 1
Internal web access portal
Community 3
GW
GW
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-SPID, MPI-PID)

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

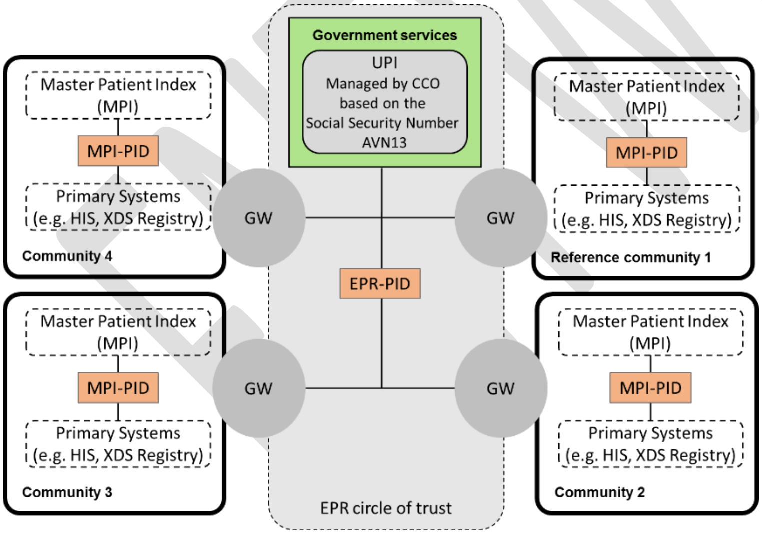


Figure 2 Swiss Patient Identifiers

1.1.5 Management of Identifiers and On Behalf Relationships

A relationship is called "On Behalf Relationship", if an authorized person or system acts on behalf of a subject that is registered in the community.

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

To support identifier transformations and On Behalf transformations, each community must manage community-local data sources for the X-Assertion Provider actor (1.6.2.2 X-Assertion Provider). Annex 2 EPRO-FDHA (subparagraphs 1.4.2, 1.6 and 8.2) defines operational certification requirements on these data sources.

Access rights can only be managed for authorized persons or a systems. Subjects acting on behalf of authorized persons or systems have the same access rights as their responsible and therefore their access rights cannot be managed separately.

1.2 Scope of precisions

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

- IT Infrastructure: Audit Trail and Node Authentication (ATNA)
- 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 Expected actions for receiving actors receiving unexpected parameters

1.3.1 For ebXML-based profiles (e.g. XDS.b):

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

The response message MUST specify the corresponding status code and provide information about each discovered error as prescribed in Section 4.2.4 " Success and Error Reporting" of ITI TF-3.

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

1.3.2 For HL7v3-based profiles (e.g. PIXv3):

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

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

- typeCode – fixed value "E" (error).
- code – error code, preferably from the HL7 code system 2.16.840.1.113883.12.357 or 2.16.840.1.113883.5.1100.

- text – description of the error in one or more natural languages.

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

1.4 Requirements on CT

Consistent Time (CT) 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.

1.5 Requirements on ATNA

BECAUSE OF THE PROFILE CH:ATC, ONLY MINIMAL SWISS REGULATIONS ON ATNA NEED TO BE MADE. THE UPDATE OF THIS CHAPTER WILL BE DELIVERED AS SOON AS POSSIBLE.

1.5.1 Introduction

The EPRA explicitly grants the patient to be informed about any data processing in his or her EPR upon request. For this reason, all IHE actors in Switzerland must write Swiss specific Audit Trail and Node Authentication (ATNA) logs. The Swiss precisions on the integration profile IHE ATNA are provided in this chapter.

The patient portal must display log data that is easier to understand for patients and their representatives. These requirements are described in the national profile Audit Trail Consumption (ATC).

As ATC concentrates on the most relevant information for display to the patient, the creation of ATNA logs is still essential to be able to provide all important data on events according to an EPR.

1.5.2 Actors

1.5.2.1 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 “1.4 Requirements on CT Profile for Swiss Time Service” on page 11.
- Record Audit Event [ITI-20]
  The Audit Message Format described in chapter “1.5.4.1 ATNA Audit Trail 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.

1.5.2.1.1 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 “1.5.4.1 ATNA Audit Trail 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 “1.5.4.1 ATNA Audit Trail Message Format” on page 12 for each transaction concerning a patient having an EPR.

1.5.3 Transactions

1.5.3.1 Record Audit Event [ITI-20]

The ATNA Audit Message Format described in chapter “1.5.4.1 ATNA Audit Trail Message Format” starting on page 12 MUST be used for all events for patients having an EPR.

1.5.4 Content profiles

1.5.4.1 ATNA Audit Trail Message Format

IHE ITI TF-2a references to several Audit Message Formats (see ITI TF-2a, 3.20.7) and prefers the 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 schema (see 2.1 Appendix A – AuditMessage schema (AuditMessage.xsd)).

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

1.5.4.1.1 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 1 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. Samples daylight-savings time Switzerland:~~ ~~2016-08-10T20:29:10+02:00~~ ~~2016-08-10T18:29:10+02:00~~ ~~Samples normal time Switzerland:~~ ~~2016-02-10T20:29:10+01:00~~ ~~2016-02-10T19:29:10Z~~
@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).	No further refinement.

		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)	
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	~~If a XUA SAML User Assertion Response has been provided, the /SUBJECT/NameID from the XUA SAML User Assertion Response MUST be used as input to construct the @UserName attribute as defined in the IHE-XUA profile.~~ No further refinement.
@AlternativeUserID (type: text)	[0..1]	Alternative unique identifier for the user. 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	No further refinement.
@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 a XUA SAML User Assertion Response has been provided, the subject-id attribute value from the XUA SAML User Assertion Response MUST be used.~~
@UserIsRequestor (type: xs:Boolean)	[1..1]	Indicator that the user is or is not the requestor, or initiator, for the event being audited.	No further refinement.

		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.	
@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 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.	~~This value MUST represent a value from the Swiss Metadata Value-Set "eprActor" (2.16.756.5.30.1.127.77.10.11.6).~~
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.5.2.1a	~~When importing or exporting data, this value MUST represent one of the media types in the Value-Set "MediaTypeCode" (2.16.840.1.113883.4.642.3.458):~~ ~~1= USB Disk Emulation~~ ~~2= Email~~ ~~3= CD~~ ~~4= DVD~~ ~~5= Compact Flash~~ ~~6= Multi-media Card~~

			~~7= Secure Digital Card~~ ~~8= URI~~ ~~9= Film~~ ~~10= Paper Document~~
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.**
@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 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).	No further refinement.
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	No further refinement.

		PACS/RIS system might use "4 "(aplication server process).	
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 IF KNOWN, 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.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	No further refinement.
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]*))*"	**If this value represents a value from the Swiss Metadata Value-Set, an OID MUST be used. Otherwise either an OID or a String MUST be used.**
@displayName (type: xs:token)	[0..1]	N/A	No further refinement.
@originalText (type: xs:token)	[0..1]	Note: this also corresponds to DICOM "Code Meaning"	No further refinement.
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. 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.	No further refinement.
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.

1.6 Requirements on XUA Profile for Authentication and User Assertion

THE PROFILES XUA, ADR AND PPQ HABE BEEN REWORKED. OPEN ISSUES ARE BEING SOLVED WITH A HIGH PRIORITY. THE STABLE VERSION OF THE SPECIFICATIONS FOR THE PAT2018 ARE PUBLISHED AS SOON AS POSSIBLE.

1.6.1 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 actors and transactions will support the following use cases:

- Asserting the authenticity of a user: 1.6.3.1 Authenticate User
- Transforming identifiers for use within the community: 1.6.3.2 Get X-User Assertion
- Transforming assertions for On Behalf use cases: 1.6.3.2 Get X-User Assertion
- Resolving Group Memberships: 1.6.3.2 Get X-User Assertion
- Asserting declarative attributes: 1.6.3.2 Get X-User Assertion
- Querying the identifier mapping and on behalf data sources: 1.6.3.2 Get X-User Assertion

- Providing assertions to X-Service Providers: 1.6.3.3 Provide X-User Assertion [ITI-40]

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

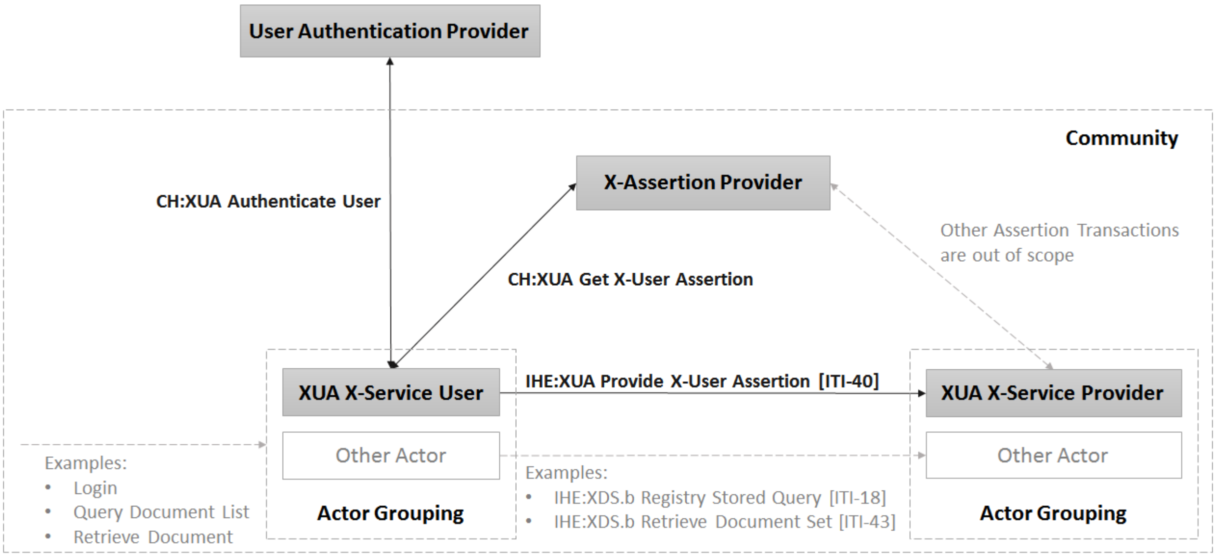

User Authentication Provider
Community
X-Assertion Provider
CH:XUA Authenticate User
Other Assertion Transactions are out of scope
CH:XUA Get X-User Assertion
XUA X-Service User
IHE:XUA Provide X-User Assertion [ITI-40]
XUA X-Service Provider
Other Actor
Other Actor
Examples:
• Login
• Query Document 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 3 XUA Actors for the use within one community

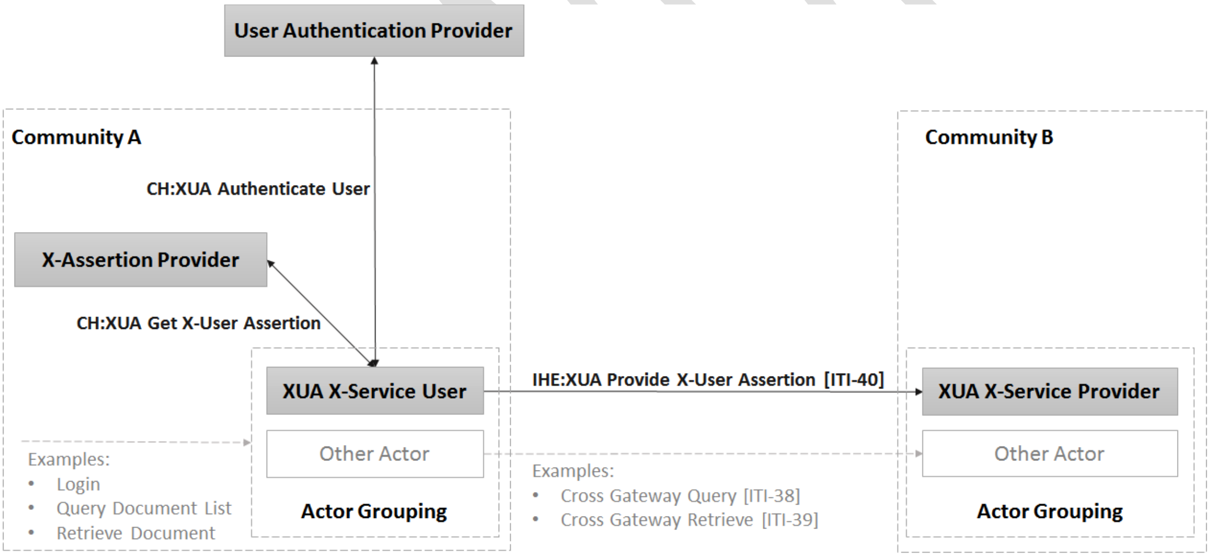


Figure 4: XUA Actors for the use in cross-community communications

1.6.2 Actors

1.6.2.1 User Authentication Provider

This actor is defined in IHE XUA profile of the IHE Technical Framework, but without detailing the specification of the transactions. This actor must be implemented as described in annex 8 EPRO-DFI.

1.6.2.2 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 "1.6.3.2 Get X-User Assertion" on page 21.
- Maintain a list of issuer certificates for trusted User Authentication Providers to validate assertions issued by these providers.
- Have their public keys published in the Community Portal Index (see article 40 EPRO) so that other actors (X-Service User, Authorization Devision Provider, etc.) may validate the authenticity of the signed SAML User Assertions.
- To ensure meaningful data in the ATNA logs, the X-Assertion Provider MUST be grouped with Patient Identifier Cross-reference Consumer and Provider Information Consumer actors to resolve names of healthcare professionals and patients.

To implement its transformation functionality, the X-Assertion Provider requires the following data sources:

• patient authentication:	UAP Identifier	– MPI-ID
• healthcare professional:	UAP Identifier	– GLN (HPD)
• assistant:	UAP Identifier	– GLN
• assistant:	GLN	– GLN (HPD)
• technical users:	machine identifier	– GLN (HPD)

A technical user is a system or application that is authorized to publish documents in an automated fashion. To authenticate itself, the technical user may use a SAML assertion signed with its own ATNA node authentication certificate. The X-Assertion Provider MUST add this certificate to the list of issuer certificates for trusted User Authentication Providers.

1.6.2.3 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 1.6.3.1.
- implement the Get X-User Assertion Request specified in 1.6.3.2.
- implement the Provide X-User Assertion [ITI-40] transaction specified by the IHE XUA integration profile.
- 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.

1.6.2.4 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 Consumer» as defined in the CH:ADR integration profile.

X-Service Provider actors MUST:

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

1.6.3 Transactions

1.6.3.1 Authenticate User

This transaction is defined in IHE XUA profile of the IHE Technical Framework, but without detailing the specification of the transactions. This actor must be implemented as described in annex 8 EPRO-DFI.

1.6.3.2 Get X-User Assertion

1.6.3.2.1 Scope

A user authenticated according to the «Authenticate User» transaction accesses a protected resource of a system within the EPR circle of trust. This includes but is not limited to the following transactions:

- search for documents of a patient
- retrieve a document
- publish a document
- edit the policy configuration of an EPR

The X-Assertion Provider provides support for declarative claims

- resource-id claims
- purposeofuse claims

The X-Assertion Provider provides the following functions:

- Identifier transformations
- On behalf transformations
- resolve group memberships

The X-Assertion Provider provides a query function to inquire possible on behalf transformation targets.

1.6.3.2.1.1 Declarative Claims

The X-Assertion Provider will handle declarative claims to add attributes to SAML User Assertions used by grouped IHE actors.

1.6.3.2.1.2 Identifier Transformation

If the assertion has been issued by a User Authentication Provider (e.g. IdP) then the NameID identifier provided by the User Authentication Provider must be replaced with the correctidentifier linked to that same person that is valid within the community. To this end the X-Assertion Provider uses the data sources provided with mappings for both patients, healthcare professionals and assistants.

During a replacement of the NameID the X-Assertion Provider MUST replace the subject-id information with the content retrieved from MPI (role PAT) or HPD (role HCP) as well. This ensures that the assertion contains the same display name as the rest of the community uses and avoids issues due to the different life cycle management requirements of the IdP and the community.

1.6.3.2.1.3 On Behalf Transformation

If the Get X-User Assertion request contains a claim for a role ASS or TCU then the X-Assertion Provider handles this request as an On Behalf transformation. The X-Assertion Provider requires a data source to determine if the authenticated identity is permitted to act on behalf of the claimed identity.

To validate the claim, the X-Assertion Provider queries the data sources as provided and maintained by the community.

The resulting assertion asserts and therefore must have the following contents:

- Subject information asserts the identity of the person being represented.
- Role is asserted as requested in the claim.
- Delegate and SubjectConfirmation information asserts the identity of the authenticated person or technical user.

1.6.3.2.1.4 Group Information

Every time an X-Assertion Provider performs an identifier transformation, the X-Assertion Provider MUST also resolve group memberships for the represented healthcare professional if the claimed role is one of HCP, ASS or TCU. The X-Assertion Provider will consider the following cases:

- If the SAML User Assertion request contains one or more claims for group memberships, the X-Assertion Provider will validate the correctness of the claim using HPD-data as an authoritative source. Semantically this allows a healthcare professional to authorize himself or an assistant to act only within the context of a particular list of groups.
- If the SAML User Assertion request does not supply any claims for group memberships, the X-Assertion Provider will retrieve all possible group memberships for the subject from HPD and treat them as having been claimed.

For each validated group membership, the X-Assertion Provider will add the group itself and all superior groups up to the root level. By adding this information to the assertion all subsequent actors can rely on the completeness of this information and do not need to query HPD again.

Each group membership is defined as an ordered tuple of first organization-id (OID) and second organization (text). Multiple group memberships are organized as a simple sequence of tuples. This leads to an ordered sequence of attributes (id1, name1, id2, name2, ...) in the SAML User Assertion Response.

~~1.6.3.2.1.5 Get X-User Query~~

~~The X-Service User may use the Get X-User Query transaction to retrieve all the potential transformation targets for a given UAP identifier and the desired role as follows:~~

- ~~Identifier transformation~~
  - ~~Request: UAP Identifier, Role~~
  - ~~Response: the transaction will return the GLN or MPI-ID of the user.~~
- ~~On Behalf transformations:~~
  - ~~Request: UAP Identifier, Role~~

- ~~Response: the transaction will return a list of zero or more GLN that the owner of the UAP identifier may act on behalf of.~~
  ~~Note: this query may be used with both UAP and GLN as query parameter.~~

1.6.3.2.2 Use Case Roles

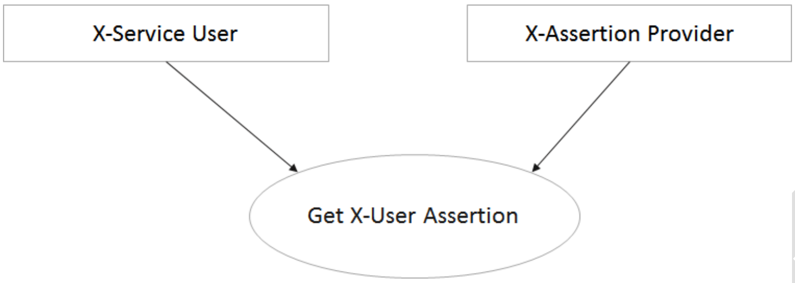


Figure 5: Use Case Roles for Get X-User Assertion

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

1.6.3.2.3 Referenced Standards

The referenced standards are identical to 1.1.1.1.

1.6.3.2.4 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.

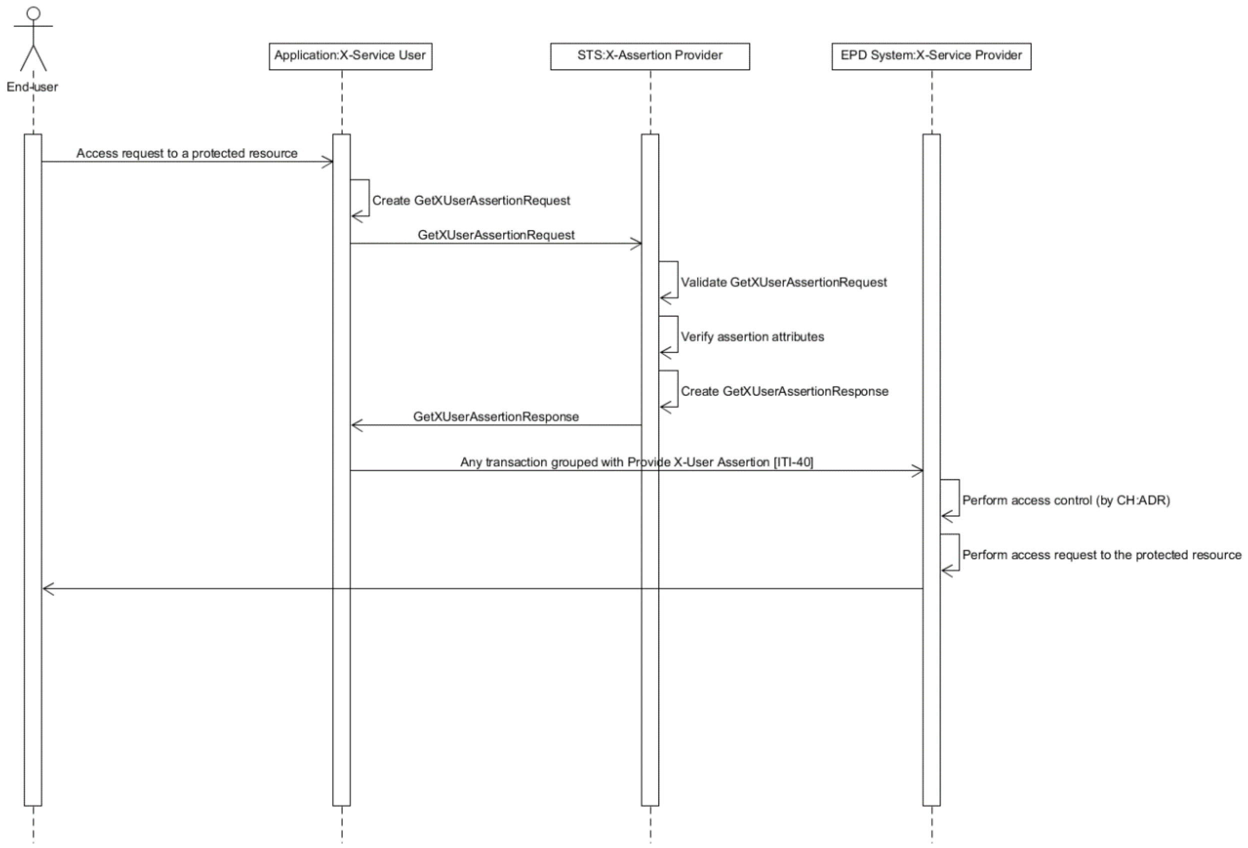

End-user
Application:X-Service User
STS:X-Assertion Provider
EPD System:X-Service Provider
Access request to a protected resource
Create GetXUserAssertionRequest
GetXUserAssertionRequest
Validate GetXUserAssertionRequest
Verify assertion attributes
Create GetXUserAssertionResponse
GetXUserAssertionResponse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

Figure 6: Get X-User Assertion interaction diagram

1.6.3.2.4.1 Trigger

The «Get X-User Assertion» transaction MUST be executed at least once to ensure identifier transformation or whenever a new or changed claim is to be added as an attribute to the SAML User Assertion.

1.6.3.2.4.2 Message Semantics

It is the responsibility of the X-Service User to ensure that every transaction grouped with XUA MUST always contain a complete SAML User Assertion. The X-Assertion Provider SHALL not enforce the list of mandatory attributes. This feature allows an X-Service Users to execute multiple calls to the X-Assertion Provider to assemble a complete SAML User Assertion in multiple steps.

List of mandatory 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-SPID of the patient

- **Name of the accessing person:**
  /AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"]/AttributeValue:

Name of the accessing person is a text string. Contents depends on the Role of the accessing person, see section "Response" below.

- **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 patients that use the XUA token themselves
  - HCP for healthcare professionals that use the XUA token themselves
  - ASS for assistants that use the XUA token to act on behalf of a healthcare professional
  - REP for representatives that use the XUA token on behalf of a patient they represent
  - TCU for technical users that use XUA token to on behalf of a healthcare professional
  - ADM for administrative users that needs privileged authorizations to initialize and administer the EPR

- **Requested resource id:**
  /AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id"]/AttributeValue:
  EPR-SPID 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

List of optional SAML User Assertion Elements

- **SubjectConfirmation**
- **delegate**

Both SubjectConfirmation and delegate elements of the SAML User Assertion are specified in full detail in chapter 1.6.4 EPR XUA Requirements for XDS and PPQ.

List of optional SAML User Assertion Elements

- **SubjectConfirmation**
- **delegate**

Both SubjectConfirmation and delegate elements of the SAML User Assertion are specified in full detail in chapter 1.6.4 EPR XUA Requirements for XDS and PPQ.

Request
The SAML User Assertion Request MUST contain a valid SAML User Assertion Response or a valid User Authentication Response combined with a list of claims. For all other specifications, see the referenced standards.

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

The following list details how the role attribute defines requirements on both request and response of the X-Get User Assertion transaction.

- patient:
    - request
        - provided assertion
        - role: PAT
    - response
        - EPR-SPID as NameID
        - Name from MPI (name) as subject-id
- health professional
    - request
        - provided assertion
        - role: HCP
        - claimed organization (optional)
    - response
        - GLN as NameID
        - Name from HPD (Provider Primary Name) as subject-id
        - claimed or retrieved group memberships
        - Organization ID from HPD as organization
        - Organization name from HPD as organization-id
- representative
    - request
        - provided assertion
        - claimed role: REP
    - response
        - if available, EPR-SPID of authenticated user as NameID, UAP ID otherwise
        - if available, name from MPI (name) as subject-id, UAP provided information otherwise
        - role: REP
- assistant
    - request
        - provided assertion
        - claimed role: ASS
        - claimed represented HCP with optional organization as
            - principal-id (Name="urn:e-health-suisse:principal-id")
            - principal-name (Name="urn:e-health-suisse:principal-name")
            - one or more organization-id
            - one or more organization
    - response
        - GLN of represented HCP as NameID
        - Name of represented HCP from HPD (Provider Primary Name) as subject-id
        - claimed or retrieved group memberships
        - IF provided assertion is from UAP
            - GLN transformed from identifier provided in assertion as NameID in SubjectConfirmation and delegate
            - Name from HPD (Provider Primary Name) as SubjectConfirmation
        - IF provided assertion is from X-Assertion Provider or XAP
            - Copy SubjectConfirmation and delegate statements
    - Note: this function can be used multiple times if the assistant wishes to assist different health professionals.

- technical user
  - request
    - self issued assertion
    - claimed role: TCU
    - claimed represented HCP with organization
      - principal-id (Name="urn:e-health-suisse:principal-id")
      - principal-name (Name="urn:e-health-suisse:principal-name")
      - organization-id
      - organization
  - response
    - GLN of represented HCP as NameID
    - Name of represented HCP from HPD as subject-id
    - IF provided assertion is from UAP
      - principal-id as NameID in SubjectConfirmation and delegate
      - principal-name as SubjectConfirmation
    - IF provided assertion is from X-Assertion Provider or XAP
      - Copy SubjectConfirmation and delegate statements
  - Note: this function can be used multiple times if the assistant wishes to assist different health professionals.
- administrative users
  - request
    - provided assertion
    - role: ADM[5]
  - response
    - UAP-ID as NameID
    - Name from UAP assertion as subject-id

The following example demonstrates how an X-Service User can use multiple steps to assemble a complete SAML User Assertion. In this example the authenticated user Hannelore Fleissig claims an assistant SAML User Assertion for Dr. Hans Müller in step 1. In step 2 the resource-id and purpose of use claims are added to the SAML User Assertion.

	User Authentication Assertion	**SAML User Assertion Step 1**	**SAML User Assertion Step 2**
NameId	1300-1234-2345-3456	7601000000000	7601000000000
LastName	Fleissig		
FirstName	Hannelore		
subject-id (AttributerStatement)		Dr. Hans Muster	Dr. Hans Muster
role (AttributeStatement)		ASS	ASS
NameId (SubjectConfirmation, delegate)		7601000000001	7601000000001
subject-id (SubjectConfirmation)		Hannelore Fleissig	Hannelore Fleissig
organization		Kantonsspital Aarau	Kantonsspital Aarau
organization-id		urn:oid:2.999	urn:oid:2.999

[5] Anhang 2 EPDV does allow the definition of additional roles to build and operate the EPR system. The definition here is to be considered exemplary for additional roles.

	User Authentication Assertion	SAML User Assertion Step 1	SAML User Assertion Step 2
resource-id			8901^^^&amp;2.16.756.5.30.1.127.3.10.3&amp;ISO
purposeofuse			NORM

Table 2 Example X-Service User uses 2 steps to obtain a SAML User Assertion

The following assertion fragment shows the claim submitted by an assistant (role is ASS) that requests to act on behalf of principal identified in the claims.

```
   <wst:Claims Dialect="http://bag.admin.ch/epr/2017/annex/5/addendum/2">
     <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:e-health-suisse:principal-id">
       <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">7601000000000</saml2:AttributeValue>
     </saml2:Attribute>
     <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:e-health-suisse:principal-name">
       <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Dr. Hans Muster</saml2:AttributeValue>
     </saml2:Attribute>
   </wst:Claims>
```

The following assertion fragment shows a declarative claim for resource-id and purposeofuse:

```
   <wst:Claims Dialect="http://bag.admin.ch/epr/2017/annex/5/addendum/2">
     <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
       <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">8901^^^&amp;2.16.756.5.30.1.127.3.10.3&amp;ISO </saml2:AttributeValue>
     </saml2:Attribute>
     <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
       <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:anyType">
         <PurposeOfUse xmlns="urn:hl7-org:v3" code="NORM" codeSystem="2.16.756.5.30.1.127.3.10.5" codeSystemName="eHealth Suisse Verwendungszweck" displayName="Normalzugriff" xsi:type="CE"/>
       </saml2:AttributeValue>
     </saml2:Attribute>
   </wst:Claims>
```

1.6.3.2.4.3 Expected Actions

The X-Service User actor executes a Get X-User Assertion transaction to the X-Assertion Provider. This transaction contains a request for a SAML User Assertion.

The SAML User Assertion request must contain:

- A valid and signed assertion issued by a User Authentication Provider or an X-Assertion Provider.
- A set of claims for the X-Assertion Provider to process.

The X-Assertion Provider checks the validity of the SAML User Assertion Request as follows:

- The User Authentication Assertion or the SAML User Assertion provided in the request is validated for its integrity
- The issuer of the User Authentication Assertion or the SAML User Assertion provided in the request is validated against the list of trusted assertion providers configured in the X-Assertion Provider.

When the SAML User Assertion Request is acknowledged to be valid, the X-Assertion Provider triggers the validation process of the requested claims as detailed in chapter 1.6.3.2.4.5 Claim Validation Requirements.

After successful validation of the requested attributes, the X-Assertion Provider creates a SAML User Assertion Response with the assertion details. In particular the X-Assertion Provider will execute the actions outlined in these chapters:

- 1.6.3.2.1.1 Declarative Claims

1.6.3.2.4.4 Declarative Claims

The X-Assertion Provider will handle declarative claims to add attributes to SAML User Assertions used by grouped IHE actors.

- Identifier Transformation

0 If the assertion has been issued by a User Authentication Provider (e.g. IdP) then the NameID identifier provided by the User Authentication Provider must be replaced with the correctidentifier linked to that same person that is valid within the community. To this end the X-Assertion Provider uses the data sources provided with mappings for both patients, healthcare professionals and assistants.

During a replacement of the NameID the X-Assertion Provider MUST replace the subject-id information with the content retrieved from MPI (role PAT) or HPD (role HCP) as well. This ensures that the assertion contains the same display name as the rest of the community uses and avoids issues due to the different life cycle management requirements of the IdP and the community.

- On Behalf Transformation
- 1.6.3.2.1.4 Group Information

The X-Assertion Provider SHOULD copy all the unchanged attributes from the assertion supplied in the SAML User Assertion request the newly created SAML User Assertion Response.

The X-Assertion Provider then signs the SAML User Assertion Response and sends it to the X-Service User.

In case the validation fails, the X-Assertion Provider sends a SAML User Assertion Response with status=failure to X-Service User, who is then 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.

1.6.3.2.4.5 Claim Validation Requirements

The following validations must be executed during the processing of claims and before the issuance of a new assertion:

Attribute	Validation	Data Source
Id of the accessing person	The ID must be provided in a valid, signed assertion issued by a trusted provider	• UAP Assertion • SAML User assertion • Identifier Mapping Data Source
Name of the accessing person	The name is replaced with the information available in the community. If the resolution to HPD or MPI fails, a REP, ASS or TCU claim MUST be included in the request.	• Patient: MPI • Healthcare Professional: HPD • assistant, representative, technical users: Identifier Mapping Data Source
Organization id of the accessing person	The validation searches HPD and MUST find a relationship between healthcare professional and group.	• Patient: none • Healthcare Professional: HPD
Organization name of the accessing person	No validation is required. The name is replaced with the information from HPD.	• Patient: none • Healthcare Professional: HPD
Role of the accessing person	This attribute determines how the request is to be validated. See chapter 1.1.1.1	None
Requested resource id	This attribute is not validated by the X-Assertion Provider	None
Purpose of use	This attribute is not validated by the X-Assertion Provider	None

Table 3 validation requirements for XAP transactions

1.6.3.3 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 1.6.3.2.

1.6.4 EPR XUA Requirements for XDS and PPQ

A SAML 2.0 **<Assertion>** is to be added as a WS-Security SOAP Header in each transaction request message to communicate entities (user identities) that initiated those transactions. This is a pre-requisite for subsequent Authorization Decision Query Requests.

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
  <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_37d8092df99f08cd8435ac29a7062092"
    IssueInstant="2014-04-09T19:10:00.294Z" Version="2.0">
     <!--Identity Claims-->
  </saml2:Assertion>
</wsse:Security>
```

Listing 1: The WS-Security SOAP header with the SAML2 Assertion element. For simplicity, the identity claims are not shown.

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

The EPR requires the following details to be claimed within the assertion:

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

```
<saml2:Issuer>urn:e-health-suisse:xua:community:ksa</saml2:Issuer>
```

<Signature> an X.509 signature by a trusted entity (XUA Assertion Provider) to guaranty the confidentiality of the claims being made and unaltered content of the assertion. For further details see [SAML 2.0].

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#_37d8092df99f08cd8435ac29a7062092">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
             <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>NRrlqwGn8o9tO0DIkYbOaXNqlM0=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo> <ds:SignatureValue>dbBafjF2NPY0WztQvRpda5DOV8BrPYL5KlCx8yvnEBZ9TQrKnjwhcE=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
        <!-- X.509 Certificate -->
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

Listing 2: The Signature Element of the WS Security context providing the details of signature algorithm used. For simplicity the X.509 certificate is not shown.

<Subject> identifies the Requester Entity (Who is asking for access?) and covers also cases where an assistant is acting on behalf of a professional. This element SHALL have the following SAML 2.0 **<NameID>** child element with the following attributes:

@Format=”urn:oasis:names:tc:SAML:2.0:nameid-format:persistent” and **@NameQualifier=”urn:e-health-suisse:2015:epr-spid”** in case of a patient or **@NameQualifier=”urn:gs1:gln”** in case of a professional

When an assistant is acting on behalf of a professional, the @NameQualifier attribute SHALL contain the GLN of this professional, while the identity of the assistant SHALL be provided in elements **<SubjectConfirmation>** and **<Conditions>** as explained below.

<Subject> SHALL have a second child element **<SubjectConfirmation>** with the following attribute: **@Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"**

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent“
                        NameQualifier="urn:gs1:gln">7601000000000</saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</saml2:Subject>
```

Listing 3: Subject element of the SAML assertion providing the ID and the name qualifier of the requesting subject.

When an assistant is acting on behalf of a professional, the element <SubjectConfirmation> SHALL contain the following additional child elements:

- <NameID> containing the GLN of the assistant as well as attributes @NameQualifier="urn:gs1:gln" and @Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent".
- <SubjectConfirmationData> containing a single element <AttributeStatement>. There SHALL be one <Attribute> element with the attribute @Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"

The **<AttributeValue>** child element SHALL convey the assistant's real world name in plain text.

```
<saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent“
                        NameQualifier="urn:gs1:gln">7601000000000</saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                        NameQualifier="urn:gs1:gln">7601000000001</saml2:NameID>
            <saml2:SubjectConfirmationData>
                  <saml2:AttributeStatement>
                        <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
                              <saml2:AttributeValue>Hannelore Fleissig</saml2:AttributeValue>
                        </saml2:Attribute>
                  </saml2:AttributeStatement>
            </saml2:SubjectConfirmationData>
      <saml2:SubjectConfirmation>
</saml2:Subject>
```

Listing 4: Subject element of the SAML assertion identifying an assistant which represents a professional.

<Conditions> specifying a validity period (time stamps) to prevent “replay” of the assertion while attributes MAY have changed. The time period MUST be defined between a minimum of 5 seconds and a maximum of 10 minutes.

An audience restriction (urn:e-health-suisse:token-audience:all-communities) specifies the intended recipient or system the assertion SHALL be valid for.

The reuse of the token (signed SAML identity assertion) MAY be denied by setting a <OneTimeUse> element. For further details see [SAML 2.0].

```
<saml2:Conditions NotBefore="2016-02-09T19:10:00.294Z" NotOnOrAfter="2016-02-09T19:15:00.294Z">
  <saml2:AudienceRestriction>
    <saml2:Audience>urn:e-health-suisse:token-audience:all-communities</saml2:Audience>
  </saml2:AudienceRestriction>
</saml2:Conditions>
```

Listing 5: The condition element of the SAML 2 assertion defining the assertion life time.

When an assistant is acting on behalf of a professional, the element <Conditions> SHALL contain a child element **<Condition>** of the type **<DelegationRestrictionType>** as defined in [SAML 2.0 Delegation]. The content of the element <Condition> SHALL be a single element **<Delegate>** holding the same child element **<NameID>** as in <SubjectConfirmationData> (cf. Listing 4)[6]. Example:

```
<saml2:Conditions NotBefore="2016-02-09T19:10:00.294Z" NotOnOrAfter="2016-02-09T19:15:00.294Z">
    <saml2:AudienceRestriction>
        <saml2:Audience>urn:e-health-suisse:token-audience:all-communities</saml2:Audience>
    </saml2:AudienceRestriction>
    <saml2:Condition xsi:type="del:DelegationRestrictionType"
                          xmlns:del="urn:oasis:names:tc:SAML:2.0:conditions:delegation">
         <del:Delegate>
              <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                              NameQualifier="urn:gs1:gln">7601000000001</saml2:NameID>
         </del:Delegate>
     </saml2:Condition>
</saml2:Conditions>
```

Listing 6: The condition element of the SAML 2 assertion defining the assertion life time and identifying an assistant which represents a professional.

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

```
<saml2:AuthnStatement AuthnInstant="2016-02-09T19:10:00.294Z">
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

Listing 7: The authentication statement providing the authentication procedure used by the requesting system.

[6] The reason of creating the seemingly redundant element <Condition> in parallel to <SubjectConfirmation> is explained in Section 1 of [SAML 2.0 Delegation]: "*Existing mechanisms designed for this purpose, such as the element definition in the SAML V2.0 core specification […], suffer from the drawback that they have advisory semantics for a relying party and are likey to be ignored by delegation-unaware SAML processing. While backward compatibility can be an advantage, ignoring security-relevant details that might impact upon a relying party's policy is unacceptable in some scenarios.*"

<AttributeStatement> identifies the Requester Entity’s attributes / identity claims. There are six mandatory **<Attribute>** child elements as follows.

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

@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"
The **<AttributeValue>** child element SHALL convey the subject’s real world name as plain text as defined by IHE XUA.

There SHALL be one <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xacml:2.0:subject:role"
The **<AttributeValue>** child element SHALL convey a coded value of the subject’s **<Role>**. There are four roles to be distinguished within the EPR: Patient, Healthcare Professional, Assistant and Delegate. Within the boundariies of a community it is possible to define additional roles.

There SHALL be one or more <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xspa:1.0:subject:organization"
The **<AttributeValue>** child element SHALL convey a plain text the subject’s organization is named by.

There SHALL be one or more <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
The **<AttributeValue>** child element SHALL convey the ID of the subject’s organization or group. That ID MUST be an OID in the format of an URN. The OIDs of organizations or groups are stored within the EPR’s Healthcare Provider Directory (aka HPI/HOI).

There SHALL be an <Attribute> element with the attribute:
@Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id"
The **<AttributeValue>** child SHALL convey the EPR-SPID identifier of the patient’s record the current transaction is related to.
(syntax as used in iti-18 XDSDocumentEntryPatientId)

There SHALL be an <Attribute> element with the attribute:
@Name=" urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
The **<AttributeValue>** child element SHALL convey a coded value of the current transaction’s **<PurposeOfUse>**. There are two values to be distinguished within the EPR: Normal Access and Emergency Access.

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
    <saml2:AttributeValue>Hans Muster</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
    <saml2:AttributeValue>
      <Role xmlns="urn:hl7-org:v3" xs:type="CE“
             code=“PAT"
             codeSystem="2.16.756.5.30.1.127.3.10.6"
             codeSystemName="eHealth Suisse EPR Actors"
             displayName=“Patient"/>
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
    <saml2:AttributeValue>Kantonspital Aarau</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
    <saml2:AttributeValue>urn:oid:2.999</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
   <saml2:AttributeValue>8901^^^&amp;2.16.756.5.30.1.127.3.10.3&amp;ISO</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
    <saml2:AttributeValue>
      <PurposeOfUse xmlns="urn:hl7-org:v3" xs:type="CE"
                    code=“NORM"
                    codeSystem="2.16.756.5.30.1.127.3.10.5"
                    codeSystemName="eHealth Suisse Verwendungszweck"
                    displayName=“Normalzugriff"/>
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Listing 8: The SAML 2 attribute statement with the IHE XUA attribute claims.

1.6.4.1 Referenced Standards

Besides all other spefications referenced in the given document, the folloging ones are especially relevant for the EPR XUA Requirements:

[SAML 2.0 Delegation]

OASIS SAML V2.0 Condition for Delegation Restriction Version 1.0,

Committee Specification 01, 15 November 2009.
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation-cs-01.pdf

1.6.4.2 Representing delegation in ATNA records

As defined in the IHE XUA specification, the ID of the "main" assertion subject (e.g. a practitioner) must be stored in the attribute @UserName of the first element <ActiveParticipant> representing the human user in the format alias"<"user"@"issuer">".

When an assistant is acting on behalf of the professional, a second repetition of the <ActiveParticipant> element SHALL be created and filled in the same way, with the difference that the "user" element of that its attribute @UserName SHALL be populated with the GLN of the assistant, i.e. with the value of the element <NameID> contained in the element <Delegate> (cf. Listing 6).

The order of the elements <ActiveParticipant> related to the practitioner and the assistant is important, because these are no special markers (e.g. role codes) for distinguishing between them, and therefore audit record consumers have no other means for the differentiation of the human participants' roles.

1.7 Requirements on PIXv3 for Patient Identity Feed

This section corresponds to the transaction Patient Identity Feed HL7 V3 [ITI-44] of the IHE IT Infrastructure Technical Framework. This transaction is used by the Patient Identity Source, Patient Identifier Cross-reference Manager and Document Registry Actors. With the PIXv3 Patient Identity Feed a primary system can register a local identifier within the MPI.

1.7.1 Message Semantics

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

Message Information Model
The Message Information Model for both the Patient Activate and Patient Revise messages, as it is described in IHE ITI TF-2b, Table 3.44.4.1.2-1 is further restricted for use in an MPI within the EPR on the following attributes:

Table 4 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. At least Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/infrastructure/datatypes_r2/datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE)	A value representing the domestic partnership status of this person.	No further refinement.

{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. 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-SPID 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.	MUST NOT be used.
statusCode [0..1] Role (CE) {CWE:RoleStatus}	A value specifying the state of this personal relationship (based on the RIM Role class state- machine), for example, following divorce a spouse relationship would be "terminated".	No further refinement.
effectiveTime [0..1] Role (IVL<TS>)	An interval of time specifying the period during which this personal relationship is in effect, if such time is applicable and known.	No further refinement.
Citizen	Used to capture person information relating to citizenship.	

classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.
Nation	A politically organized body of people bonded by territory and known as a nation.	
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	No further refinement.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	No further refinement.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	No further refinement.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	No further refinement.
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.

occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	No further refinement.
BirthPlace	The birthplace of the focal living subject.	
classCode [1..1] (M) Birthplace (CS) {CNE:BIRTHPL}	Structural attribute; this is a "birthplace" role.	No further refinement.
id [0..*] Birthplace (SET<II>)	A living subjecst's birth place represented by a unique identifier.	No further refinement.
addr [0..*] Patient (BAG<AD>)	A living subject's birth place represented as an address. Note: Either BirthPlace.addr or an associated Place.name must be valued.	No further refinement.
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.

1.8 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-SPID.

1.8.1 Message Semantics

1.8.1.1 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

1.8.2 Return Corresponding Identifiers

1.8.2.1 Major Components of the Get Corresponding Identifiers Query Response

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

1.9 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.

1.9.1 Message Semantics

1.9.1.1 Major Components of the Patient Registry Query by Demographics

The PatientTelecom Query Parameter MUST NOT be used.

1.9.2 Patient Demographics Query Response

1.9.2.1 Expected Actions

The Patient Demographics Supplier shall perform the matching of patient data based on the query parameter values it receives. The information provided by the Patient Demographics Supplier to Patient Demographics Consumers is a list of possible matching patients from the patient information source associated with the value that the Consumer sent in the Device class of the transmission wrapper of the query message. See also IHE ITI TF-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 5 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-SPID 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 or-Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/ infrastructure/datatypes_r2/ datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*]	Address(es) for corresponding with this person.	No further refinement.

Person (BAG<AD>)		
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.	The EPR-SPID 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)	Structural attribute – this is an event.	No further refinement.

Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/ 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.

1.9.2.1.1 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 6. 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.

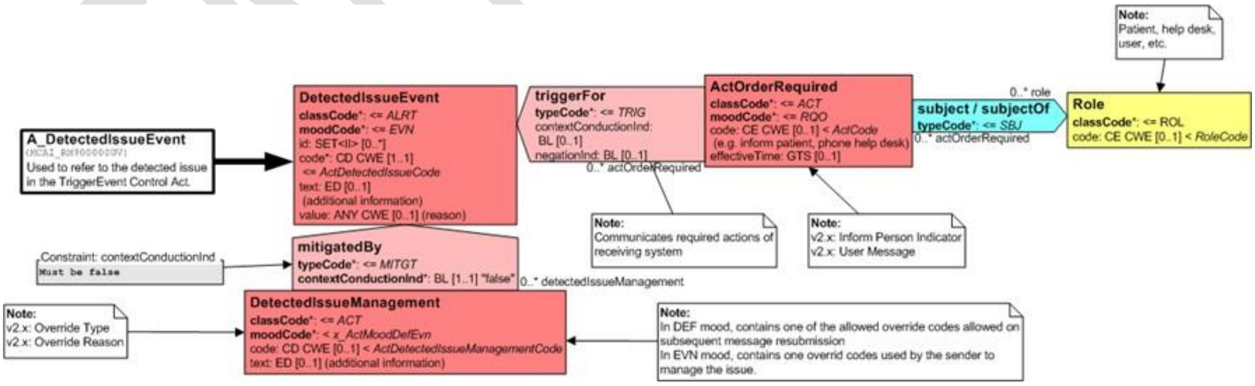

A_DetectedIssueEvent
(MCAI_RM900000UV)
Used to refer to the detected issue in the TriggerEvent Control Act.
DetectedIssueEvent
classCode*: <= ALRT
moodCode*: <= EVN
id: SET<II> [0..*]
code*: CD CWE [1..1] <= ActDetectedIssueCode
text: ED [0..1] (additional information)
value: ANY CWE [0..1] (reason)
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 7 RMIM for DetectedIssueEvent

Table 6 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

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

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

 <code code="ActAdministrativeDetectedIssueCode" codeSys-
tem="2.16.840.1.113883.5.4"/>

 <triggerFor typeCode="TRIG">

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

  <code code="PatientAddressRequested” 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” codeSys-
  tem="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.

1.10 Requirements on XCPD Profile for Cross- Community Patient Discovery

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

1.10.1 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 or Demographic Query and Feed 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.[7]

1.10.2 Cross Gateway Patient Discovery Request

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

1.10.2.1 Major Components of the Patient Registry Query by Demographics

LivingSubjectId Parameter is the only required query Parameter. The following parameters of IHE ITI TF-2b, chapter 3.55.4.1.2.1 MAY be used (see also):

- LivingSubjectAdministrativeGender
    - value [1..1] ParameterItem (CE) {CWE:AdministrativeGender}
- LivingSubjectBirthTime
    - value [1..1] ParameterItem (IVL<TS>)
- LivingSubjectName
    - value [1..1] ParameterItem (PN)

The LivingSubjectId Parameter MUST contain the EPR-SPID.

Table 7: Message Information Model for the Patient Registry Query by Demographics Message

PRPA_HD201306IHE **Patient Registry Query by Demographics**	**This HMD extract defines the message used to query a community for patients matching a set of demographics information.** **Derived from Figure 3.55.4.1.2-1 (PRPA_RM201306IHEXCPD)**	**Swiss National Extension**
QueryByParameter	The entry point for the domain content in this query	
queryId [1..1] QueryByParameter (II)	Unique identifier for the query	No further refinement.
statusCode [1..1] (M) QueryByParameter (CS) {CNE:QueryStatusCode, fixed value="new"}	The status of the query, shall be "new"	No further refinement.
responseModalityCode [1..1] QueryByParameter (CS) {CNE:ResponseModality, fixed value="R"}	The mode of the response – always real-time.	No further refinement.
responsePriorityCode [1..1] QueryByParameter (CS) {CNE:QueryPriority}	Either “I” or “D” shall be specified. “I” (Immediate) indicates that the Responding Gateway is required to send an immediate response. “D” (Deferred) indicates the Responding Gateway is required to send a deferred response, see Section 3.55.6.2.	“I” shall be specified.
initialQuantity [0..1] QueryByParameter (INT)	Not supported, any value will be ignored by responder.	No further refinement.

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

initialQuantityCode [0..1]	Not supported, any value will be ignored by responder.	No further refinement.
QueryByParameter (CE) {CWE:QueryRequestLimit, default="RD"}		No further refinement.
MatchAlgorithm	This parameter conveys instructions to the Responding Gateway specifying the preferred matching algorithm to use and may be ignored	
value [1..1] ParameterItem (ST)	The name of the algorithm	No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "MatchAlgorithm"}		No further refinement.
MinimumDegreeMatch	This parameter conveys instructions to the Responding Gateway specifying minimum degree of match to use in filtering results and may be ignored	
value [1..1] ParameterItem (INT)	The numeric value of the degree of match. Shall be value between 0 and 100 .	No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "MinimumDegreeMatch"}		No further refinement.
LivingSubjectAdministrativeGender	This query parameter is a code representing the administrative gender of a person in a patient registry.	
value [1..1] ParameterItem (CE) {CWE:AdministrativeGender}		No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.administrativeGender"}		No further refinement.
LivingSubjectBirthTime	This query parameter is the birth date of a living subject.	
value [1..1] ParameterItem (IVL<TS>)	A date or date range. This parameter can convey an exact moment (e.g., January 1, 1960 @ 03:00:00 EST), an approximate date (e.g., January 1960), or even a range of dates (e.g., December 1, 1959 through March 31, 1960).	A birthdate (YYYYMMDD).
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.birthTime"}		No further refinement.
LivingSubjectId		
value [1..*] (M) ParameterItem (II)	A patient identifier, used to assist in finding a match for the query and, when so designated by the Initiating Gateway, used by the Responding Gateway in a XCA Cross Gateway Query directed to the Community designated by the homeCommunityId value specified in the Control Act Wrapper – see Section 3.55.4.1.2.4.	MUST contain only the EPR-SPID.

semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.id"}		No further refinement.
LivingSubjectName	This query parameter is the name of a person. If multiple instances of LivingSubjectName are provided, the receiver must consider them as possible alternatives, logically connected with an "or".	
value [1..1] ParameterItem (PN)	Only one instance of the value element is allowed. Only some of the name parts may be populated. If, for example, only the family and given name parts of a person's name are sent, then the query would match all persons with that family name and given name regardless of their initials. The use attribute of the value element shall not be set to "SRCH".	No further refinement.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.name"}		No further refinement.
PatientAddress	This query parameter is a postal address for corresponding with a patient. There shall be only a single PatientAddress element.	MUST NOT be used.
value [1..*] ParameterItem (AD)	Multiple instances of the value element within a Patient Address may be specified and are combined with OR logic.	MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "Patient.addr"}		MUST NOT be used.
LivingSubjectBirthPlaceAddress	This query parameter is a patient's birthplace represented as an address	MUST NOT be used.
value [1..*] ParameterItem (SET<AD>)		MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.BirthPlace.Addr"}		MUST NOT be used.
LivingSubjectBirthPlaceName	This query parameter is a patient's birthplace represented as a place name	MUST NOT be used.
value [1..*] ParameterItem (SET<EN>)		MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.BirthPlace.Place.Name"}		MUST NOT be used.
PrincipalCareProviderId	This query parameter is the care provider identifier of a person who has been assigned as the principal care provider of this patient. The requestor may specify multiple PrincipalCareProviderId elements which responder shall consider as possible alternatives, logically connected with an "or".	MUST NOT be used.

value [1..1] ParameterItem (II)	There shall have only one id in the “value” attribute.	MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "AssignedProvider.id"}		MUST NOT be used.
MothersMaidenName	This query parameter is the maiden name of a focal person's mother. It is included as a parameter because it is a common attribute for confirming the identity of persons in some registries. This parameter does not map to a single RIM attribute, instead, in RIM terms Mother's maiden name is the person name part of "family" with an EntityNamePartQualifier of "birth" for the person who is the player in a PersonalRelationship of type of "mother" to the focal person.	MUST NOT be used.
value [1..1] ParameterItem (PN)	A person name. In this case it may consist of only the given name part, the family name part, or both.	MUST NOT be used.
semanticsText [1..1]		MUST NOT be used.
ParameterItem (ST){default= "Person.MothersMaidenName"}		MUST NOT be used.
PatientTelecom	This query parameter is a telecommunications address for communicating with a living subject in the context of the target patient registry. It could be a telephone number, fax number or even an email address. There shall be only a single PatientTelecom element.	MUST NOT be used.
value [1..*] ParameterItem (TEL)	A telecommunications address. The scheme attribute specifies whether this is a telephone number, fax number, email address, etc. Multiple instances of the value element within a PatientTelecom may be specified and are combined with OR logic.	MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "Patient.telecom"}		MUST NOT be used.

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

1.10.3 Cross Gateway Patient Discovery Response Caching

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

1.10.3.1 Major Components of the Patient Registry Find Candidates Response Message

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

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

Table 8: 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 shall be specified in the OtherIDs.id attribute.	The MPI-PID MUST be returned if there is a match from the EPR-SPID.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	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.	The 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. May be null i.e., <name nullFlavor=”NA”/> only if the request contained only a patient identifier and no demographic data.	No further refinement.

telecom [0] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	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.	No further refinement.
birthTime [0] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0] Person (BL)	An indication that this person is dead.	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.	This node with its attributes MUST NOT be used
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	This node with its attributes MUST NOT be used
Citizen	Used to capture person information relating to citizenship.	This node with its attributes MUST NOT be used
Nation	A politically organized body of people bonded by territory and known as a nation.	This node with its attributes 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	This node with its attributes MUST NOT be used

	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.	
LanguageCommunication	A language communication capability of the focal person.	This node with its attributes 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) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infra structure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	A numeric value between 0 (excluded) and 100 (0 < percentage value <= 100) MUST be used (100 for an exact match).

1.11 Requirements on HPD Profile for Replication

1.11.1 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 sacrificing 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.

1.11.2 Use-case: Provider information replication

Table 9 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.

1.11.3 Actors / Transactions

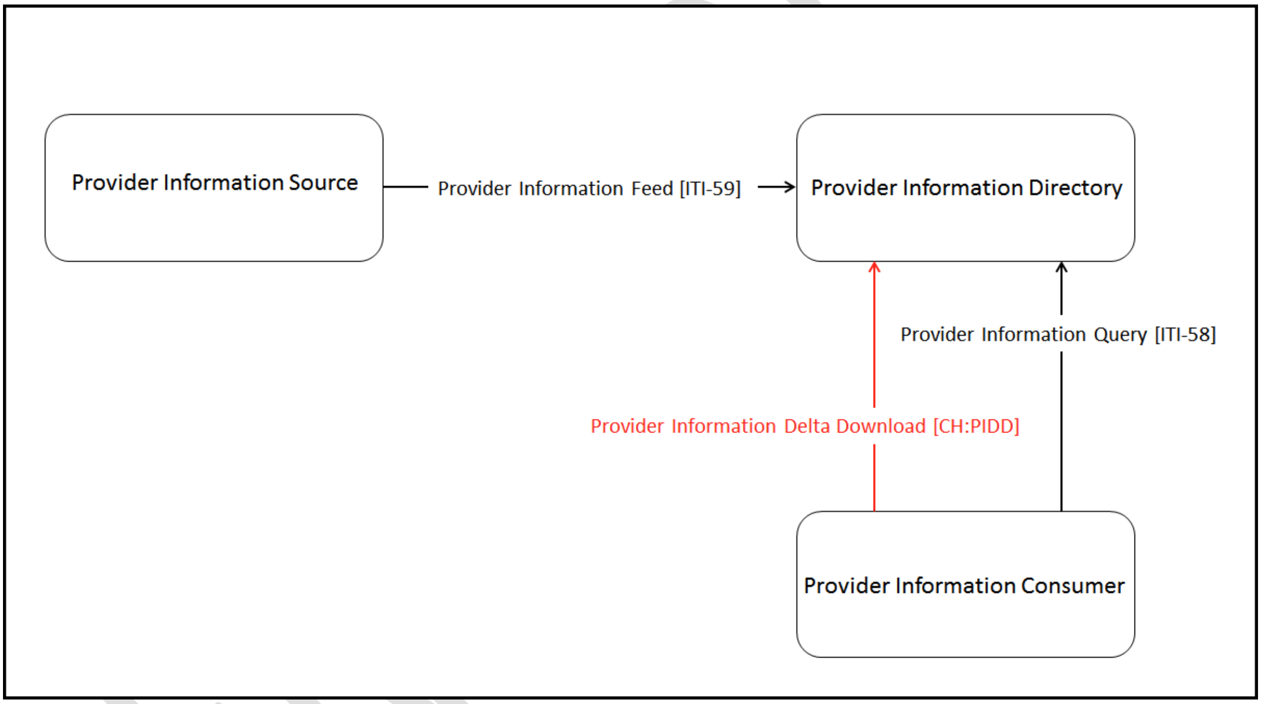

Provider Information Source
Provider Information Feed [ITI-59]
Provider Information Directory
Provider Information Query [ITI-58]
Provider Information Delta Download [CH:PIDD]
Provider Information Consumer

Figure 8 Swiss extended HPD Actors / Transactions

1.11.3.1 Provider Information Directory

The Provider Information Directory is extended with the following option:

- Provider Information Delta Download Option

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

1.11.3.2 Provider Information Consumer

The Provider Information Consumer is extended with the following option:

- Provider Information Delta Download Option

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

1.11.4 Transactions

1.11.4.1 Provider Information Delta Download (CH:PIDD)

This transaction schema extends the DSMLv2 interface by supporting an additional SOAP schema (see Appendix B – Provider Information Delta Download schema (PIDD.xsd) on page 63) 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>
```

1.11.4.1.1 Interaction Diagram

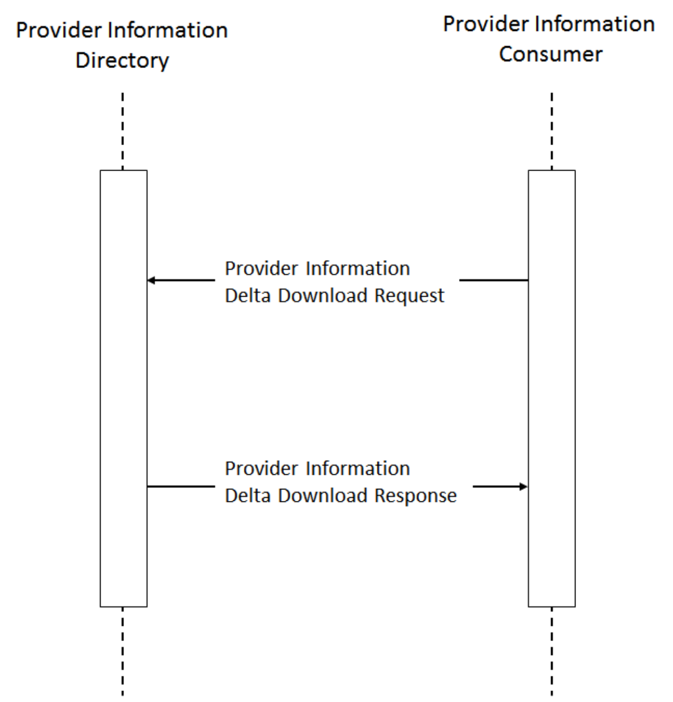

Provider Information Directory
Provider Information Consumer
Provider Information Delta Download Request
Provider Information Delta Download Response

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

1.11.4.1.2 Provider Information Delta Download Request

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

- A required **fromDate** parameter to define the inclusive range starting date of the requested transactions sequence;
- An optional **toDate** 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);

1.11.4.1.3 Provider Information Delta Download Response

The response message contains a sequence of DSMLv2 batchRequest elements.

1.11.5 Message Semantics

1.11.5.1 HPD Schema Content

1.11.5.1.1.1 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[8]. For Individual Provider, the ID is equal to the GLN[9] of the Individual Provider.

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

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

1.11.5.1.2 Attribute

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

Conventions:

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

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

Table 10 HPD Individual Provider Attributes

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Unique Entry Identifier	**inetOrgPerson**	**uid**	DString	S	R	validated	DN restriction	DN restriction	No further restrictions except for the technically given maximum length of 255 characters for the complete «distinguished name» (DN), including the uid. Validation if prefix correlates with currently logged-in community: "uid=<shcIssuerName>:"	UID RDN = prefix:id Prefix issued by FOPH. ID chosen by community.
Provider "Identifiers"	**HCProfessional**	**hcIdentifier**	DString	M	R		1	256	Issuing Authority:Type:ID:Status (where ID = GLN and Status = "active" or "inactive" or "revoked" or "suspended") Example: RefData:GLN:7601001064577:active	
Provider Type	**HCProfessional**	**hcProfession**	DString	M	R	validated	1	256	Only valid MDI codes according to value set EprAuthorRole (Id 2.16.756.5.30.1.127.3.10.1.1.3) are allowed. Format = IssuingAuthority:Code System:Code (where IssuingAuthority = BAG, CodeSystem = ID of the value set and Code = code of the respective concept)	
Provider Type description	**person**	**description**	DString	M	R		1	1024	DisplayName in English corresponding to code in attribute hcProfession	object class "person" instead of "inetOrgPerson"
Provider Status	**HPDProvider**	**hpdProviderStatus**	DString	S	O	validated	1	64	valid values: Active, Inactive, Retired, Deceased (case insensitive validation)	
Provider Primary Name	**inetOrgPerson**	**displayName**	DString	S	R		1	256		

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Provider Title	**OrganizationalPerson**	**title**	DString	S	O		1	128		object class "organizationalPerson" instead of "inetOrgPerson"
Provider First Name	**inetOrgPerson**	**givenName**	DString	M	O		1	128	contains the first name by which someone is known	Optionality: O instead of R2
Provider Middle Name	**inetOrgPerson**	**initials**	DString	M	O		1	6	contains all other first and middle names	
Provider Last Name	**person**	**sn**	DString	S	R		1	128	contains the last name	- Cardinality: S instead of M - object class: "person" instead of "inetOrgPerson"
Provider Known Names	**person**	**cn**	DString	M	R	validated	1	128	Validation: Values structured according to ISO 21091 (2013) "9.2.2.3 General name". However, the discrete structural elements are not validated. Thus validation according to: '[string], [string], [string]'. The attribute shall be filled by the communities according to ISO 21091 (2013) "9.2.2.3 Common Name". i.e.: Surname, Given Names, UID	object class: "person" instead of "inetOrgPerson"
Provider Language Supported	**HPDProvider**	**hpdProviderLanguageSupported**	DString	M	O		1	64		Encoded using ISO-639-1
Provider Gender	**Natural Person**	**gender**	PString	S	O	validated	1	64	valid values according to RFC 2985: Male ("m"|"M") or female ("f"|"F"). Values will not be validated against the MDI value set EprGender.	
Provider medical records deliver email address	**HPDProvider**	**hpdMedicalRecordsDeliveryEmailAddress**	DString	S	O		1	256		
Provider e-mail address	**inetOrgPerson**	**mail**	DString	M	O		1	256		
S-MIME Certificate	**inetOrgPerson**	**userSMIMECertificate**	OString	M	O		1	32768		
Signing Certificate	**HCProfessional**	**hcSigningCertificate**	OString	M	O		1	32768		
User Certificate	**inetOrgPerson**	**userCertificate**	OString	M	O		1	32768		
Creation Date	**System**	**createTimestamp**	GTime	S	System	read-only / operational			Timestamp when the value was created	
Last Update date	**System**	**modifyTimestamp**	GTime	S	System	read-only / operational			Timestamp when the value was modified	
Provider facility name	**OrganizationalPerson**	**physicalDeliveryOfficeName**	DString	M	O		1	128		- object class: "organizationalPerson" instead of "inetOrgPerson" - Optionality: O instead of R2
Provider Mailing Addresse	**HPDProvider**	**hpdProviderMailingAddress**	DString	M	O		1	4096		Optionality: O instead of R2
Provider Billing address	**HPDProvider**	**hpdProviderBillingAddress**	DString	M	O		1	4096		
Provider Practice Address	**HPDProvider**	**hpdProviderPracticeAddress**	DString	M	O		1	4096	Necessary for clear identification of the health professional by the patient. The communities are urged to fill the attribute if possible.	Optionality: O instead of R2

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	Techn. Remarks	Min L.	Max L.	Comments	Swiss National Extension
Provider Practice Organization	**HCProfessional**	**hcPracticeLocation**	DN	M	O	validated	DN restriction	DN restriction	Only references to valid DNs and members from the same community are allowed. I.e. the referenced item must have the same community prefix as the currently logged-in community.	
Provider Business Phone	**person, organizationalPerson**	**telephoneNumber**	DString	M	O		1	64		- object class: "person" and "organizationalPerson" instead of " inetOrgPerson - Optionality: O instead of R2
Provider Mobile phone	**inetOrgPerson**	**mobile**	DString	M	O		1	64		Optionality: O instead of R2
Provider Pager	**inetOrgPerson**	**pager**	DString	M	O		1	64		Optionality: O instead of R2
Provider Fax	**OrganizationalPerson**	**facsimileTelephoneNumber**	DString	M	O		1	64		- object class: "organizationalPerson" instead of "inetOrgPerson" - Optionality: O instead of R2
Provider Specialty	**HCProfessional**	**hcSpecialisation**	DString	M	O	validated	1	256	Only valid MDI codes according to value set EprDocumentPracticeSettingCode (Id 2.16.756.5.30.1.127.3.10.1.18) are allowed. Format = IssuingAuthority:Code System:Code[: DisplayName] The suffix :DisplayName is optional and will not be validated against the DisplayName stored in the MDI. Thus, only the part "IssuingAuthority:Code System:Code" is validated. Duplicates with the same code but with different DisplayName are not allowed.	
Provider Relationship	**HPDProvider**	**memberOf**	DN	M	O	read-only / calculated			This attribute is calculated and can only be edited indirectly via the other side groupOfNames.member	
Legal Address	**HPDProvider**	**hpdProviderLegalAddress**	DString	S	O		1	4096		
	HCProfessional	**HcRegistrationStatus**	DString	M	R	validated	1	64	Only valid value is "Unknown" (case-insensitive)	Attribute is not listed explicitly in IHE HPD Trial Implementation of August 31, 2015, but was introduced as a mandatory field due to the specification in ISO 21091: 2013 (which is referenced in IHE HPD Trial Implementation).
	top	**objectClass**	OID	M	Must	validated	Object identifier	Object identifier	Only defined objectClasses are allowed.	

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.

Table 11 HPD Organizational Provider Attributes

HPD Concept	Object class	Attribute name	Data type	Car-dinality	Op-tion-ality	techn Re-marks	Min L.	Max L.	Comments	Swiss National Extension
Unique Entity Identifier	**uidObject**	**uid**	DString	S	R	validated	DN re-striction	DN re-striction	No further restrictions except for the technically given maximum length of 255 characters for the complete «distinguished name» (DN), including the uid. Validation if prefix correlates with currently logged-in community: "uid=<shcIssuerName>:"	UID RDN = prefix:id Prefix issued by FOPH. ID chosen by community.
Org Identifiers	**HCRegulatedOrgani-zation**	**hcIdentifier**	DString	M	R	validated	1	256	Issuing Authority:Type:ID:Status (ID = OID or BUR number If ID = OID, status = "active" or "inactive" or "revoked" or "sus-pended" If ID = BUR number, status = "active" or "inactive" or " deleted" or "unknown" Example with OID: RefData:OID:2.99:active Example with BUR number: BFS:BUR:94763827:active Validation if there is at least one value which starts with "RefData:OID:"	
Organization known names	**Organization**	**O**	DString	M	R		1	128	other name(s)	Optionality: R instead of R2
Organization Name	**HCRegulatedOrgani-zation**	**HcRegisteredName**	DString	M	R		1	128	legal name(s)	
Org Type	**Organization**	**businessCategory**	DString	M	R	validated	1	128	Only valid MDI codes according to value set EprHealthcareFacili-tyTypeCode (Id 2.16.756.5.30.1.127.3.10.1.11) are allowed. Format = IssuingAuthority:Code System:Code	Optionality: R instead of O
Org Type Description	**Organization**	**description**	DString	M	O		1	1024	DisplayName in English corresponding to code in attribute busi-nessCategory	
Org Status	**HPDProvider**	**hpdProviderStatus**	DString	S	O	validated	1	64	Allowed values: Active, Inactive (Case insensitive validation)	
Org Contact	**HCRegulatedOrgani-zation**	**ClinicalInfor-mationContact**	DN	M	O	validated	DN re-striction	DN re-striction	Only references to valid DNs and elements from the currently logged-in community are allowed. I.e the referenced element must have the same community prefix as the currently logged-in com-munity.	
Org Practice Address	**HPDProvider**	**hpdProviderPrac-ticeAddress**	DString	M	O		1	4096	Necessary for the clear identification of an organisation by the pa-tient. It is highly recommended to provide values for this attribute if possible.	Optionality: O instead of R2
Org Billing Address	**HPDProvider**	**hpdProviderBillin-gAddress**	DString	M	O		1	4096		
Org Mailing Address	**HPDProvider**	**hpdProviderMail-ingAddress**	DString	M	O		1	4096		Optionality: O instead of R2
Provider Language Sup-ported	**HPDProvider**	**hpdProviderLan-guageSupported**	DString	M	O		1	64		Encoded using ISO-639-1
Org Speciality	**HCRegulatedOrgani-zation**	**HcSpecialisation**	DString	M	O	validated	1	256	Only valid MDI codes according to value set EprDocumentPrac-ticeSettingCode (Id 2.16.756.5.30.1.127.3.10.1.18) are allowed. Format = IssuingAuthority:Code System:Code[:DisplayName]	

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

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 12 HPD Relationship Attributes

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

2 Appendices

2.1 Appendix A – AuditMessage schema (AuditMessage.xsd)

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

2.2 Appendix B – 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[10]. See also chapter “1.1 Definitions of terms” on page 8.

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

4 Illustrations

5 Tables