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.

Die XDS Metadaten gemäss Anhang 3 EPDV-EDI werden in ART-DECOR gepflegt und regelmässig in die Verordnung übernommen. Aktuell gilt die Version 201704.3-beta der Value Sets im Status final, 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:	1.6
Datum:	30. November 2018
Profile:	**ATNA, HPD, 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
1.5	1.1.4	EPD-248	Correction in figure 2: Text changed from *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.
1.5	1.2	EPD-193	Scope of Precisions: Added Profiles XDS, XCA, XCF.
1.5	1.3	EPD-193	Added chapter 1.3 Requirements on XDS, XCA, XCF.
1.2	1.4	EPD-10	New chapter "1.4 Requirements on XDS and XCA In Stored Queries (transactions ITI-18, ITI-38), the parameter $MetadataLevel, whenever provided, shall equal to 1 (one). Whenever a receiving actor (e.g. a Document Registry) discovers that this requirement is violated in an incoming request, it shall reject this request and return an error with the code XDSRegistryError (see section 1.4.1). Expected actions for receiving actors receiving unexpected parameters*"* added.
1.2	1.4.1	EPD-198	Typo: Section “2.4.2” corrected to “4.2.4 ".
1.3	1.4.1 1.4.2	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*~~	~~*0*~~	~~*EPD-246*~~	~~*Changed the title of chapter 0 to “Requirements on CT” and slightly the text, because for this profile, there is actually no Swiss extension.*~~
1.5	Former 1.5	EPD-246	Removed this chapter. For CT there is no national extension required. Annex 2 EPRO-DFI states in let. 2.9.34, that the official Swiss time according to METAS must be used.
~~*1.1*~~	~~*Former 1.4.2.2*~~	~~*EPD-75*~~	~~*Obsolete, because contained text has been removed. $XDSDocumentEntryTypeCode contains the value 722160009*~~
1.5	1.5	EPD-65, EPD-245	Reworked the whole chapter. Only minimal Swiss specific requirements on ATNA remain.
~~*1.4*~~	~~*Former 1.5.1*~~	~~*EPD-237*~~	~~*Replaced the complete text of the Introduction of the chapter “0 ” to address the requirements on the Swiss profile ATC.*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*EPD-65*~~	~~*At point “Maintain Time [ITI-1]” the wrong chapter was referenced. Correct: “0 ”.*~~

Version	Chapter	Ticket	Comment to changes
~~*1.1*~~	~~*Former 1.5.2.1*~~	~~*EPD-135*~~	~~*Duplicate Text like in 2.1 Appendix A – AuditMessage schema (AuditMessage.xsd) removed.*~~
~~*1.1*~~	~~*Former 1.5.2.1*~~	~~*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*~~	~~*Former 1.5.2.1*~~	~~*EPD-80*~~	~~*Table 1 (@ParticipantObjectSensitivity): The current confidentiality code of the object MUST be specified **IF KNOWN**, when …*~~
~~*1.1*~~	~~*Former 1.5.2.1*~~	~~*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*~~	~~*Former 1.5.2.1*~~	~~*EPD-190*~~	~~*Adjusted Swiss refinement of @EventDateTime.*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*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."*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*EPD-156*~~	~~*Mandate XUA: Attribute @UserID:Clarification added:*~~ ~~*"…as input to construct the @UserName attribute as defined in the IHE-XUA profile."*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*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*~~	~~*Former 1.5.2.1*~~	~~*EPD-226*~~	~~*Swiss Extension of "RoleIDCode" authorRole is not correct. The actor must be used: eprActor.*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*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*~~	~~*Former 1.5.2.1*~~	~~*EPD-223*~~	~~*Swiss Extension of "MediaType": Text updated for the now available Swiss Metadata value set "Media Type Code".*~~
~~*1.3*~~	~~*Former 1.5.2.1*~~	~~*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".

Version	Chapter	Ticket	Comment to changes
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.
1.3	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	1.6.2.2		Mandate XUA: X-Assertion Provider: Text reworked completely after "X-Service User actors MUST".
1.4	1.6.2.2	EPD-244	Added line: "*assistant: UAP Identifier – GLN*".
1.5	1.6.2.3	EPD-257	SAML Assertions should not be encrypted. Removed bullet point "*be able to create SAML User Authentication Request objects with encrypted and signed assertions according to the Identity Provider.*"
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.
1.4	1.6.2.4	EPD-244	In second paragraph corrected the actor "Authorization Decision Provider" to "Authorization Decision Consumer" and shortened the sentence.
~~*1.3*~~	~~*Former 1.6.2.1*~~	~~*EPD-153*~~	~~*Changed text for Artifact Binding.*~~
~~*1.2*~~	~~*Former 1.5.3.1.3*~~	~~*EPD-85*~~	~~*XUA: WS-Trust Version: Only v1.3 allowed*~~
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 annex 8.
1.3	1.6.3.2		Mandate XUA: ***Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.*** reworked completely.
1.5	1.6.3.2.1	EPD-321	Removed following sentence, because chapter 1.6.3.2.1.5 Get X-User Query has been deleted: "The X-Assertion Provider provides a query function to inquire possible on behalf transformation tar-gets."
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).
~~1.5~~	~~Former 1.6.3.2.1.5~~	~~EPD-230~~	~~Chapter 1.6.3.2.1.5 Get X-User Query removed. This should be solved by the vendors themselves.~~
1.5	1.6.3.2.3		In chapter X-Service Provider the specifications were dropped and there is a link to annex 8. shortened
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).

Version	Chapter	Ticket	Comment to changes
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.
1.5	1.6.3.2.4.2	EPD-283	Changed HOI to HPD.
1.5	1.6.3.2.4.2	EPD-315	Typo: Changed GLN to OID at “Organization id of the accessing person”.
1.3	1.6.4	EPD-224	Mandate XUA: ***1.6.4 EPR XUA Requirements for XDS and PPQ*** added.
1.5	1.6.4	EPD-224	Corrected and extended roles in text “*There are **six** roles to be distinguished within the EPR: Patient, Healthcare Professional, Assistant, **Representative, Technical User, Administrative User**.*”
1.5	1.6.4	EPD-283	Changed to HPD: Healthcare Provider Directory (~~aka HPI/HOI~~ **HPD**)
~~*1.3*~~	~~*Former 1.7.4.2*~~	~~*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.”
~~*1.1*~~	~~*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.*~~
1.5	1.9.2.1	EPD-309	EPR-SPID optional in patient class ID list. Must be identical to EPR-SPID in OtherIDs.
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 on LivingSubjectId for a Patient Registry Query.
1.5	1.10.2.1	EPD-95	Removed reference, which is no more working anyway.
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).***
1.4	1.11.5.1.2	EPD-106	Intregrate revised list of attributes for HPD.
1.5	1.11.1	EPD-249	Deleted last sentence in chapter.
1.2	1.11.4.1.2	EPD-15	Typo: "toDat" changed to "toDate"
~~*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.*~~
1.5	1.12.5.1.1.1 1.12.4.1.2 1.12.4.1	EPD-267 EPD-266 EPD-265	Formulation clarified/changed.
1.5	1.12.4.1.2	EPD-57	Additional formulation for filtermytransactions added.
1.5	1.12.5.1.2	EPD-279 EPDM-179 EPDM-180	Validation for Individual Provider hcIdentifier added; Value Set for Individual Provider hc Specialisation changed to EprAuthorSpeciality; Validation for Organizational Provider hcIdentifier modified (doublet check)
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

Version	Chapter	Ticket	Comment to changes
1.6	1.6	EPD-197, EPD-224, EPD-244, EPD-269, EPD-290, EPD-293, EPD-294, EPD-296, EPD-297, EPD-298, EPD-301, EPD-312, EPD-313, EPD-319, EPD-323, EPD-328, EPD-330, EPD-331, EPD-332, EPD-333, EPD-334, EPD-335, EPD-337, EPD-338, EPD-339, EPD-341, EPD-342, EPD-344, EPD-345, EPD-346, EPD-347, EPD-348, EPD-349, EPD-350, EPD-351, EPD-352, EPD-356, EPD-353, EPD-354, EPD-355, EPD-365, EPD-366, EPD-370, EPD-371, EPD-372, EPD-373, EPD-385, EPD-388	Refactored section 1.6 to precisely define the requirements on the message semantics and the expected actions of the CH:XUA national extension and improve the separation of concerns. Changes: • Changed the structure of the chapter according to the structure of IHE technical frameworks for a better readability. • Examples for Get X-User Assertion Request and Response have been elaborated for each role (separate files). • Role of the Administrator has been split into: - DADM: Document Administrator - PADM: Policy Administrator • Requirements for a technical user (TCU) have been refined. • Claim Validation of X-Assertion Provider. • Resolution of Goup Memberships.

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**

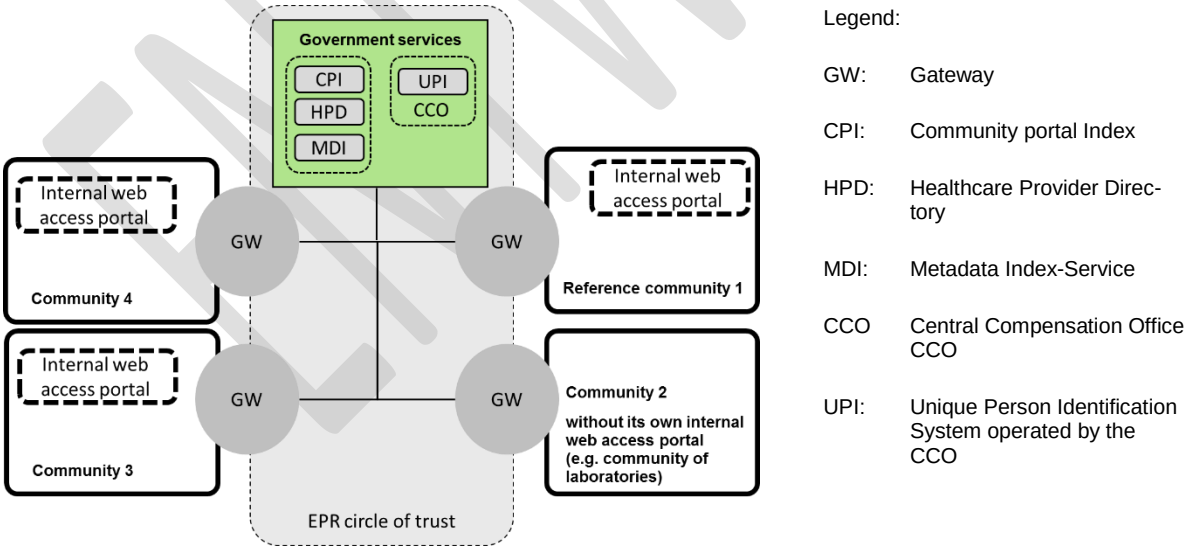

Figure 1 Swiss EPR circle of trust

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.

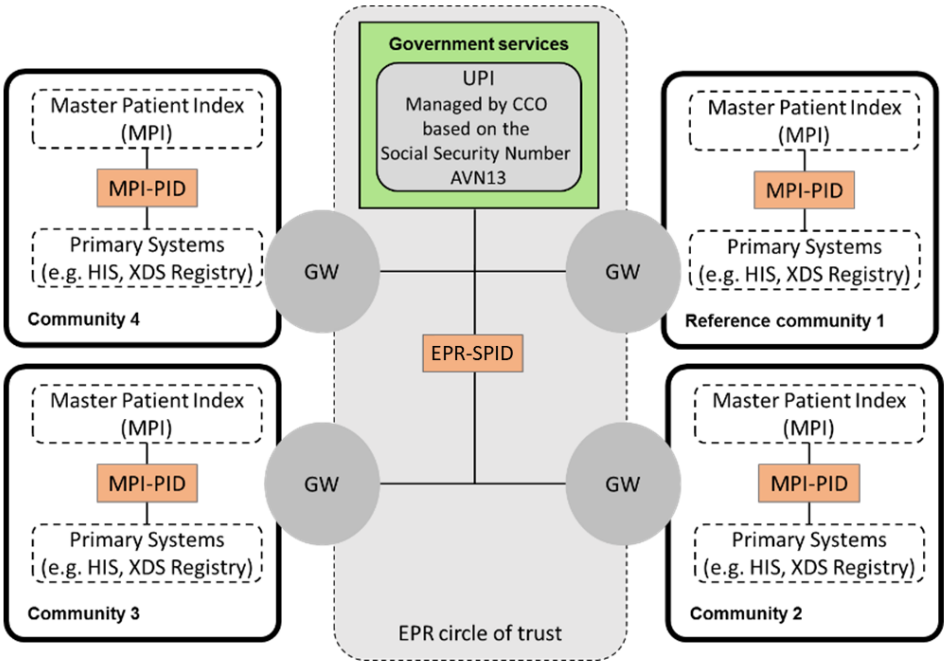

Figure 2 Swiss Patient Identifiers

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

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.

To support identifier transformations and On Behalf transformations, each community must manage community-local data sources for the X-Assertion Provider actor (1.6 Requirements on XUA Profile for Authentication and User Assertion). 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: Cross-Enterprise Document Sharing (XDS)
- IT Infrastructure: Cross-Community Access (XCA)
- 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 Requirements on XDS and XCA

In Stored Queries (transactions ITI-18, ITI-38), the parameter $MetadataLevel, whenever provided, shall equal to 1 (one). Whenever a receiving actor (e.g. a Document Registry) discovers that this requirement is violated in an incoming request, it shall reject this request and return an error with the code XDSRegistryError (see section 1.4.1).

1.4 Expected actions for receiving actors receiving unexpected parameters

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

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

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

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

1.5 Requirements on ATNA

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

- The attribute //AuditSourceIdentification/@AuditEnterpriseSiteID is required and shall contain the OID of the audit source.
- Whenever an element //PatrticipantObjectIdentification describes an XDS document, the attribute //PatrticipantObjectIdentification/@ParticipantObjectSensitivity shall contain the confidentiality code of this document (if known). The format if HL7v2 CE with the code system OID as the code system name, e.g. `1051000195109^normal^2.16.840.1.113883.6.96`.
- In all elements of the type CodedValueType: whenever the represented code belongs to the Swiss Metadata Value Set, the attribute @codeSystemName shall contain the OID of the corresponding code system instead of its symbolic name. For all other codes, this requirement is optional.

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

1.6 Requirements on XUA Profile for Authentication and User Assertion

1.6.1 Introduction

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

The XUA Profile in IHE Technical Framework Vol. 1 defines means to communicate claims about authenticated principals (user, applications, and systems) in transactions that cross enterprise boundaries. In the context of the EPR these claims are used for access control and to protocol information not available in the transaction messages.

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

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

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

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

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

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

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

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

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

1.6.2 Actors / Transactions

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

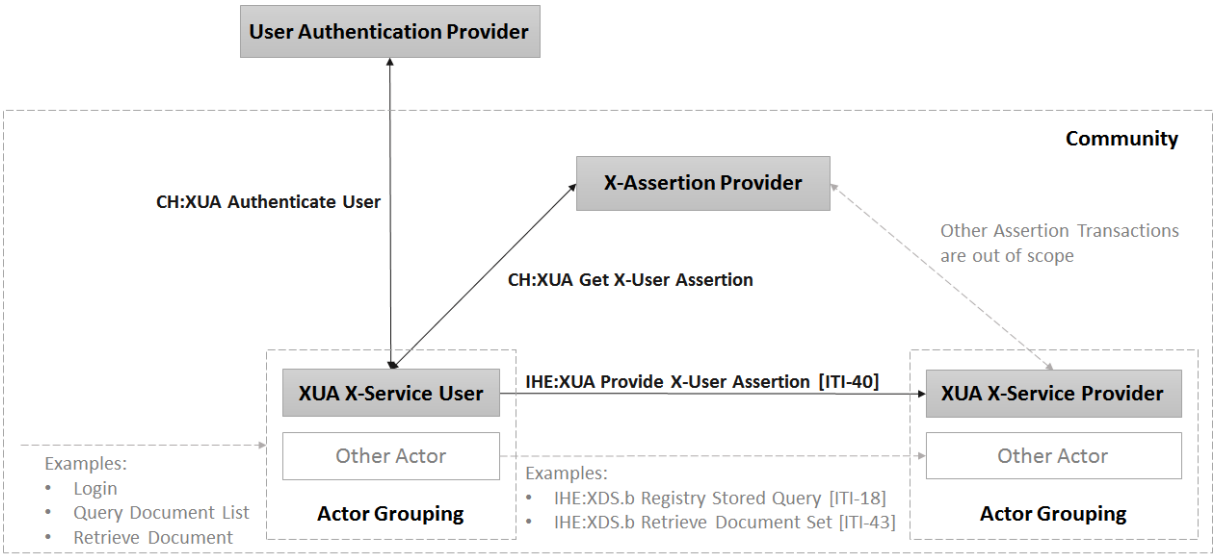

Figure 3 XUA Actors for the use within one community

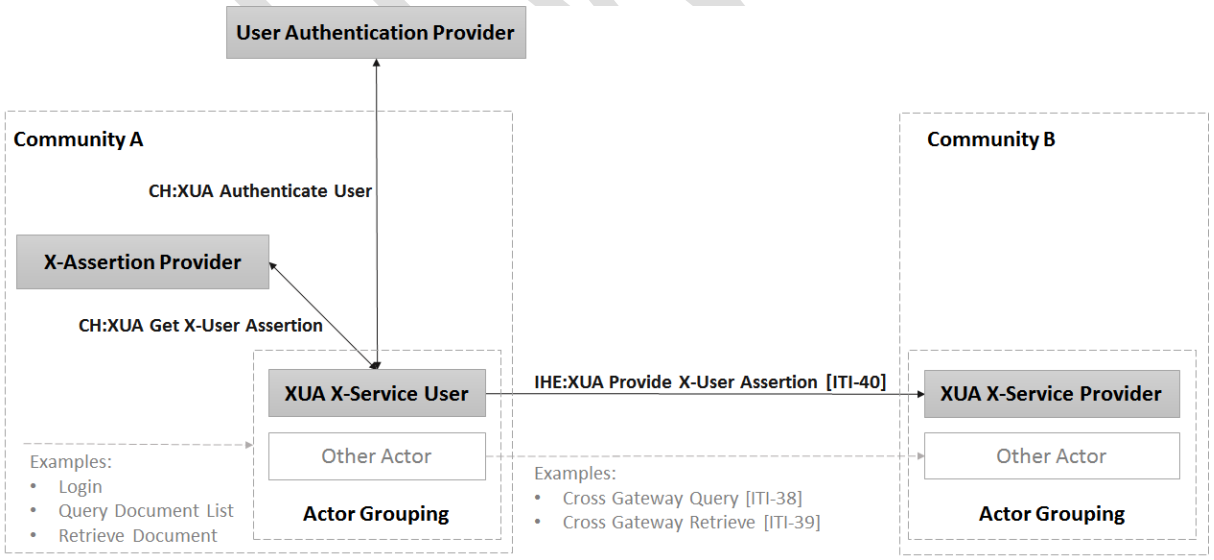

Figure 4: XUA Actors for the use in cross-community communications

In order to be compliant with this national extension, an implementation must perform the following required transactions (labelled “R”):

Table 1: CH:XUA actors and transactions.

Actor	Transaction	Optionality	Remark
X- Service User	Provide X-User Assertion [ITI-40]	R	see ITI TF-2b: 3.40
X-Service Provider	Provide X-User Assertion [ITI-40]	R	see ITI TF-2b: 3.40
X-Assertion Provider	Get X-User Assertion	R	
X-Service User	Get X-User Assertion	R	
User Authentication Provider	Authenticate User	R	
X-Service User	Authenticate User	R/O	

Here the Authenticate User transaction is labelled “R/O” for the X-Service User, since it is optional in the technical user extension only, while it is required in all other extensions.

1.6.3 Actor Groupings

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

EPR Actor	Optionality	Actor to be grouped with	Remark
X-Service User	R	CH:CT Time Client	
	R	CH:ATNA Secure Node	Indirect, via grouped actors
X-Service Provider	R	CH: CT Time Client	Indirect, via grouped actors
	R	CH:ATNA Secure Node	Indirect, via grouped actors
	R	CH:ADR Authorization Decision Consumer	Indirect, via grouped actors
X Assertion Provider	R	CH:CT Time Client	
	R	HPD Provider Information Consumer	
User Authentication Provider	R	CH:CT Time Client	

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

EPR Actor	Optionality	Actor to be grouped with	Remark
XDS.b Document Consumer	R	X-Service User	
XDS.b Document Source	R	X-Service User	
XDS-i.b Imaging Document Consumer	R	X-Service User	

EPR Actor	Optionality	Actor to be grouped with	Remark
XDS-i.b Imaging Document Source	R	X-Service Provider	
XDS MU Document Administrator	R	X-Service User	
RMU Update Initiator	R	X-Service User	
XCA(I) Initiating (Imaging) Gateway	R	X-Service User	
XCA(I) Responding (Imaging) Gateway	R	X-Service Provider	
CH:PPQ Policy Source	R	X-Service User	
CH:PPQ Policy Consumer	R	X-Service User	
CH:ADR Authorization Decision Consumer	R	X-Service User	
CH:ADR Authorization Decision Provider	R	X-Service Provider	
XDS.b Document Registry	R	X-Service Provider	By grouping with ADR Consumer
XDS.b Document Repository	R	X-Service Provider	
CH:PPQ Policy Repository	R	X-Service Provider	By grouping with ADR Consumer
RMU Update Responder	R	X-Service Provider	
CH:ATC Patient Audit Consumer	R	X-Service User	Via IUA with XUA option.
CH:ATC Patient Audit Record Repository	R	X-Service Provider	By grouping with ADR Consumer and IUA Resource Server.

1.6.4 Transactions

1.6.4.1 Authenticate User

1.6.4.1.1 Scope

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

1.6.4.1.2 Use Case Roles

Actor: User Authentication Provider

Role: Verifies the authentication information, creates a SAML Identity Assertion and sends it to the X Service User. This actor corresponds to the term “Identity Provider” as defined and specified in annex 8 EPRO-FDHA.

Actor: X Service User

Role: Communicates authentication information to the User Authentication Provider and receives a SAML Identity Assertion. Communicates authorization information to the X Assertion Provider and receives a SAML Authorization Assertion. Provides the SAML Authorization Assertion in the Provide X-User Assertion [ITI-40] transaction. This actor also corresponds to the term “Relying Party” as defined and specified in annex 8 EPRO-FDHA.

1.6.4.1.3 Referenced Standards

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

1.6.4.1.4 Interaction Diagram

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

1.6.4.2 Get X-User Assertion

1.6.4.2.1 Scope

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

1.6.4.2.2 Use Case Roles

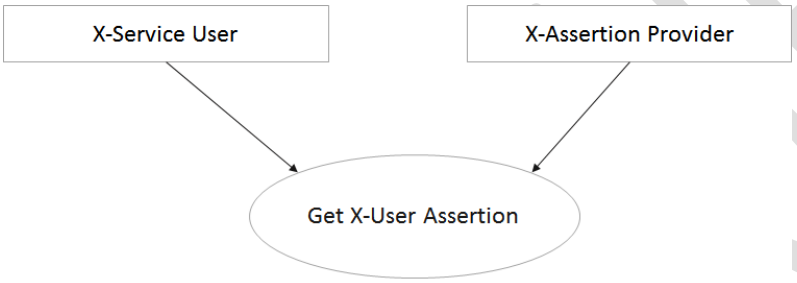

Figure 5: Use Case Roles for Get X-User Assertion

Actor: X Service User

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

Actor: X Assertion Provider

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

1.6.4.2.3 Referenced Standards

The following standards are normative for this transaction:

- Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
- Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

- Security Assertion Markup Language (SAML) V2.0 Technical Overview
  Committee Draft 02, 25 March 2008
  http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf
- Web Services Security: SAML Token Profile 1.1
  https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf
- Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
  https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
- WS-Trust 1.3
  http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html
- OASIS eXtensible Access Control Markup Language (XACML) v2.0
  https://www.oasis-open.org/standards#xacmlv2.0
- OASIS Multiple Resource Profile of XACML v2.0
  https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-mult-profile-spec-os.pdf
- OASIS SAML 2.0 profile of XACML v2.0
  http://docs.oasis-open.org/xacml/xacml-saml-profile/v2.0/xacml-saml-profile-v2.0.html

1.6.4.2.4 Interaction Diagram

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

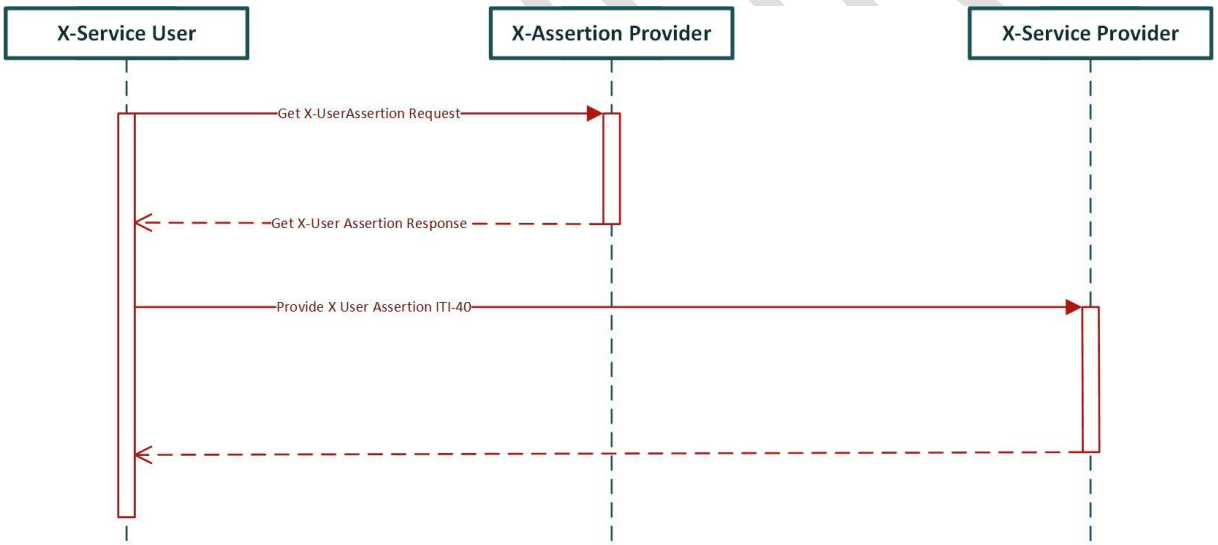

Figure 6: Get X-User Assertion interaction diagram

1.6.4.2.4.1 Trigger Events

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

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

1.6.4.2.4.2 Message Semantics

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

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

The Get X-User Assertion request message extends the <wst:RequestSecurityToken> message defined in WS-Trust 1.3. In addition to the elements defined in WS-Trust 1.3, the Get X-User Assertion request MUST contain a <wst:Claims> element with attribute claims described below.

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

- There MUST be an <Attribute> element with name "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse". The <AttributeValue> child element MUST convey a coded value of the current transaction's <PurposeOfUse>. There are three values to be distinguished within the EPR: Normal Access, Emergency Access and Technical User with the corresponding codes NORM, EMER and AUTO from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set..
- There MUST be one <Attribute> element with name "urn:oasis:names:tc:xacml:2.0:subject:role". The <AttributeValue> child element MUST convey a coded value of the subject's <Role>.
- There MUST be an <Attribute> element with name "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The <AttributeValue> child MUST convey the EPR-SPID identifier of the patient's record the current transaction is related to. For the EPR-SPID the syntax of the ITI-18 XDSDocumentEntryPatientId MUST be used.

1.6.4.2.4.2.1 Heathcare Professional Extension

For healthcare professionals the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

1.6.4.2.4.2.2 Assistant Extension

For assistants the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

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

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

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

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

1.6.4.2.4.2.3 Technical User Extension

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

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

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

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

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

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

1.6.4.2.4.2.4 Policy Administrator Extension

For policy administrators the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

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

1.6.4.2.4.2.5 Document Administrator Extension

For document administrators the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

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

1.6.4.2.4.2.6 Patient Extension

For patients the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

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

The following optional attributes MAY be added to the <wst:Claims> element of the Get X-User Assertion request in the patient extension[3]:

- There MAY be one <Attribute> element with name "urn:e-health-suisse:principal-id". If present, the <AttributeValue> child element MUST convey the EPR-SPID of the patient.
- There MAY be one <Attribute> element with the attribute name "urn:e-health-suisse:principal-name". If present, the <AttributeValue> child element MUST convey the name of the patient.

1.6.4.2.4.2.7 Representative Extension

For representatives the Get X-User Assertion request MUST convey the SAML 2 Identity Assertion retrieved from the Authenticate User transaction response described above. The SAML 2 Identity Assertion MUST be contained in the Web Service security header of the SOAP message.

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

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

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

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

1.6.4.2.4.3 Expected Actions X-Service User

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

1.6.4.2.4.4 Expected Actions X-Assertion Provider

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

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

Error that occurred (fault string)	Fault code (fault code)	Remark
The request was invalid or malformed	wst:InvalidRequest	MUST be used, if required claims are missing, wrong or if the claims are not according to the extensions defined below.
Authentication failed	wst:FailedAuthentication	MUST be used, if the signature of the SAML 2 Identity Assertion in the security header of the Get X User

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

Error that occurred (fault string)	Fault code (fault code)	Remark
		Assertion Request is not from a certified identity provider nor from a technical user registered in the community.

1.6.4.2.4.4.1 Healthcare Professional Extension

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

The SAML 2 Identity Assertion in the security header MAY convey the GLN of the authenticated healthcare professional. If present, the X-Assertion Provider MUST use the GLN from the SAML 2 Identity Assertion in the <NameID> of the subject in the <Assertion> returned with the Get X-User Assertion Response message. If not, the X-Assertion Provider actor MUST query the community data stores to resolve the Name ID of the <Subject> element to the GLN of the healthcare professional to be returned in the <Assertion> returned with the Get X-User Assertion response message.

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

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

1.6.4.2.4.4.2 Assistant Extension

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

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

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

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

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

1.6.4.2.4.4.3 Technical User Extension

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

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

The X-Assertion Provider actor MUST validate, that the Name ID of the <Subject> element of Get X-User Assertion request of the technical user is registered in the community data stores as authorized to act on behalf of the healthcare professional declared in the claim attribute "urn:e-health-suisse:principal-id" of the Get X-User Assertion request. In addition the X-Assertion Provider actor must check that the time interval defined in the <Condition> element of the SAML 2 Identity Assertion is neither exceeded nor below the limit.

1.6.4.2.4.4.4 Policy Administrator Extension

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

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

1.6.4.2.4.4.5 Document Administrator Extension

See 1.6.4.2.4.4.4.

1.6.4.2.4.4.6 Patient Extension

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

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

1.6.4.2.4.4.7 Representative Extension

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

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

1.6.4.2.4.5 Message Examples

For message examples see https://www.e-health-suisse.ch/specs.
[CAVE: Vor Inkraftsetzung auf BAG-Website verweisen]

1.6.4.2.5 Security Consideration

In the Swiss EPR all actors grouped with the X-Service User are required to be grouped must be grouped with ATNA Secure Node or Secure Application Actor. In addition the X-Assertion Provider MUST be grouped with the ATNA Secure Application Actor. This grouping forces the network transactions to utilize mutually authenticated and encrypted TLS or equivalent.

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

1.6.4.3 Provide X-User Assertion [ITI-40]

This section describes the national extension for the Swiss EPR of the ITI-40 Transaction defined in IHE TF 2.b.

1.6.4.3.1 Scope

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

1.6.4.3.2 Use Case Roles

Actor: X Service User

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

Actor: X-Service Provider

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

1.6.4.3.3 Referenced Standards

The following standards are normative for this national extension:

- Security Assertion Markup Language (SAML) V2.0 Technical Overview
  Committee Draft 02, 25 March 2008
  http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf
- Web Services Security: SAML Token Profile 1.1
  https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf
- Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
  https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
- OASIS SAML V2.0 Condition for Delegation Restriction Version 1.0
  http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation-cs-01.pdf

1.6.4.3.4 Interaction Diagrams

1.6.4.3.4.1 Trigger Events

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

1.6.4.3.4.2 Message Semantics

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

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

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

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

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

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

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

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

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

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

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

- There MUST be one <Attribute> element with the name attribute "urn:oasis:names:tc:xspa:1.0:subject:subject-id". The <AttributeValue> child element MUST convey the subject’s real world name as plain text as defined by IHE XUA in all extensions.
- There MUST be one <Attribute> element with the name attribute "urn:oasis:names:tc:xacml:2.0:subject:role". The <AttributeValue> child element MUST convey a coded value of the subject’s role.
- There MUST be one or more <Attribute> elements with the name attribute "urn:oasis:names:tc:xspa:1.0:subject:organization-id". The <AttributeValue> child element MUST convey the ID of the subject’s organization or group registered in the HPD or empty, if not known.
- There MUST be one or more <Attribute> elements with the name attribute: "urn:oasis:names:tc:xspa:1.0:subject:organization". The <AttributeValue> child element MUST convey a plain text the subject’s organization name as registered in the HPD or empty, if not known.
- There MUST be one <Attribute> element with the name attribute: "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The <AttributeValue> child MUST

convey the EPR-SPID identifier of the patient's record the current transaction rrequires access to in all extensions. The syntax MUST be as used in XDSDocumentEntryPatientId attribute of the ITI-18 transaction.
- There MUST be one <Attribute> element with the name attribute: "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse". The <AttributeValue> child element MUST convey a coded value of the current transaction's purpose of use.

1.6.4.3.4.2.1 Heathcare Professional Extension

In the healthcare professional extension the following requirements hold for the <Subject> element of the <Assertion>:
- The <NameID> child element of the <Subject> MUST contain the GLN of the subject with name qualifier name qualifier attribute set to "urn:gs1:gln".

In the healthcare professional extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:
- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") must be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") MUST convey the identifiers of the organizations or groups the subject is assigned to. The identifiers MUST be OID in the format of URN as registered in the healthcare provider directory.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") of the <AttributeStatement> MUST convey the name of the organizations or groups the subject is a member of.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") of the <AttributeStatement> MUST be either code NORM or EMER from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.2 Assistant Extension

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

In the assistant extension the following requirements hold for the <Subject> element of the <Assertion>:
- The <NameID> child element of the <Subject> element MUST contain the GLN of the subject (responsible healthcare professional) with name qualifier name qualifier attribute set to "urn:gs1:gln".
- The <SubjectConfirmation> element MUST contain a <NameID> child element. The <NameID> element must convey the GLN of the assistant with name qualifier name qualifier attribute set to "urn:gs1:gln".
- The <SubjectConfirmation> element MUST contain a <SubjectConfirmationData> child element with one <AttributeStatement> which conveys the assistant real name as plain text in an <Attribute> with name "urn:oasis:names:tc:xspa:1.0:subject:subject-id".

In the assistant extension the <Assertion> must contain a <Conditions> element conveying the relation of the assistant to the healthcare professional the assistant is acting on behalf of. The following requirements hold for the <Conditions> element:
- The NotBefore and NotOnOrAfter attributes of the <Conditions> element MUST define a valid time interval.
- The <Conditions> element MUST contain a <AudienceRestriction> element coveying a single <Audience> child element with the value set to "urn:e-health-suisse:token-audience:all-communities".
- The <Conditions> element MUST contain a single <Condition> element with a <NameID> child element with Format "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" and NameQualifier "urn:gs1:gln" conveying the GLN of the assistant.

In the assistant extension the following requirements hold for the <AttributeStatement> element of the <Assertion>:
- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") of the <AttributeStatement> must be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") of the <AttributeStatement> MUST convey the identifiers of the organizations or groups the subject is assigned to. The identifier MUST be OID in the format of URN as registered in the healthcare provider directory.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") of the <AttributeStatement> MUST convey the name of the organizations or groups the subject is assigned to.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") of the <AttributeStatement> MUST be either code NORM or EMER from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.3 Technical User Extension

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

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

- The <NameID> child element of the <Subject> element MUST contain the GLN of the subject (responsible healthcare professional) with name qualifier attribute set to ”urn:gs1:gln”.
- The <SubjectConfirmation> element MUST contain a <NameID> child element. The <NameID> element must convey the unique ID the technical user is registered within the community and NameQualifier "urn:e-health-suisse:technical-user-id".

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

- The NotBefore and NotOnOrAfter attributes of the <Conditions> element MUST define a valid time interval.
- The <Conditions> element MUST contain a <AudienceRestriction> element coveying a single <Audience> child element with the value set to "urn:e-health-suisse:token-audience:all-communities".
- The <Conditions> element MUST contain a single <Condition> element with a <NameID> child element with Format "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" and NameQualifier "urn:e-health-suisse:technical-user-id" conveying the unique ID the technical user is registered with in the community.

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

- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") of the <AttributeStatement> must be code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") MUST convey the identifiers of the organizations or groups the subject (i.e. the responsible healthcare professional) is assigned to. The identifier MUST be OID in the format of URN as registered in the healthcare provider directory.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") MUST convey the names of the organizations or groups the subject is assigned to.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") MUST be code Normal Access from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.4 Policy Administrator Extension

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

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

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

- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") must be code PADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element MUST be empty.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element MUST be empty.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute MUST be code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.5 Document Administrator Extension

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

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

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

- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") must be code DADM from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element MUST be empty.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element MUST be empty.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") attribute MUST be code Normal Access from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.6 Patient Extension

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

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

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

- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") must be code PAT from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element MUST be empty.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element MUST be empty.
- The purpose of use attribute ("urn:oasis:names:tc:xspa:1.0:subject:purposeofuse") MUST be code Normal Access from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

1.6.4.3.4.2.7 Representative Extension

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

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

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

- The role attribute ("urn:oasis:names:tc:xacml:2.0:subject:role") must be code REP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.
- The organization ID attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization-id") element MUST be empty.
- The organization attribute ("urn:oasis:names:tc:xspa:1.0:subject:organization") element MUST be empty.

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

1.6.4.3.4.3 Expected Actions X-Service User

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

1.6.4.3.4.4 Expected Actions X-Service Provider

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

1.6.4.3.4.5 Message Examples

For message examples see https://www.e-health-suisse.ch/specs.
[CAVE: Vor Inkraftsetzung auf BAG-Website verweisen]

1.6.4.3.5 Security Consideration

The SAML 2 Authorization Assertion must be protected against confidentiality risks. In the Swiss EPR all actors grouped with the X-Service User and X-Service Provider are required to be grouped with ATNA Secure Node or Secure Application Actor. This grouping forces the network transactions to utilize mutually authenticated and encrypted TLS or equivalent.

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

1.6.4.3.5.1 Specifying ActiveParticipants in ATNA records

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

- The first element MUST be built according to IHE XUA requirements described in ITI TF-2b:3.40.4.2 (with or without subject role specification).
- The second element describes the main user (the subject of the XUA assertion) and MUST have the following contents:

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

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

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

Examples for various combinations of human users:

HCP, identified by GLN:

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

ASS representing HCP, both identified by GLN:

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

PAT, identified by EPR-SPID:

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

REP representing PAT, PAT identified by EPR-SPID, REP identified by e-mail address:

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

```
</ActiveParticipant>
<ActiveParticipant UserID="mutter@priv-email-provider.org" UserName="Maria Patientin">
   <RoleIDCode csd-code="REP" codeSystemName="2.16.756.5.30.1.127.3.10.6"
               originalText="Representative" />
</ActiveParticipant>
```

PADM, identified by GLN:

```
<ActiveParticipant UserID="alias2&lt;7601000000000@demo.org&gt;"
                   UserName="alias2&lt; 7601000000000@demo.org&gt;"/>
<ActiveParticipant UserID="7601000000000" UserName="Dr. Hans Muster">
   <RoleIDCode csd-code="PADM" codeSystemName="2.16.756.5.30.1.127.3.10.6"
               originalText="Policy Administrator" />
</ActiveParticipant>
```

DADM, identified by GLN:

```
<ActiveParticipant UserID="alias2&lt;7601000000000@demo.org&gt;"
                   UserName="alias2&lt; 7601000000000@demo.org&gt;"/>
<ActiveParticipant UserID="7601000000000" UserName="Dr. Hans Muster">
   <RoleIDCode csd-code="DADM" codeSystemName="2.16.756.5.30.1.127.3.10.6"
               originalText="Document Administrator" />
</ActiveParticipant>
```

Example for a technical user:

TCU, identified by software ID:

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

1.7 Requirements on PIXv3 for Patient Identity Feed

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

1.7.1 Message Semantics

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

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

Table 2 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) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number. Please see notes above in the Major Components section on the use of OtherIDs.	If patient is already registered in a community, the MPI-PID MUST be provided here. The EPR-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]	A non-unique textual identifier or moniker for this nation.	No further refinement.

Organization (ON)		
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

In this transaction, however, the Patient Identity Cross-Reference Manager has also the option to send all identifiers in the id attributes of the Patient class. If the EPR-SPID is present in the Patient class, the following requirement is imposed on the Patient.id attribute:

Patient.id containing the EPR-SPID SHALL be identical to the EPR-SPID in OtherIDs.id.

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 3 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..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	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) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	No further refinement.

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 4. 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.

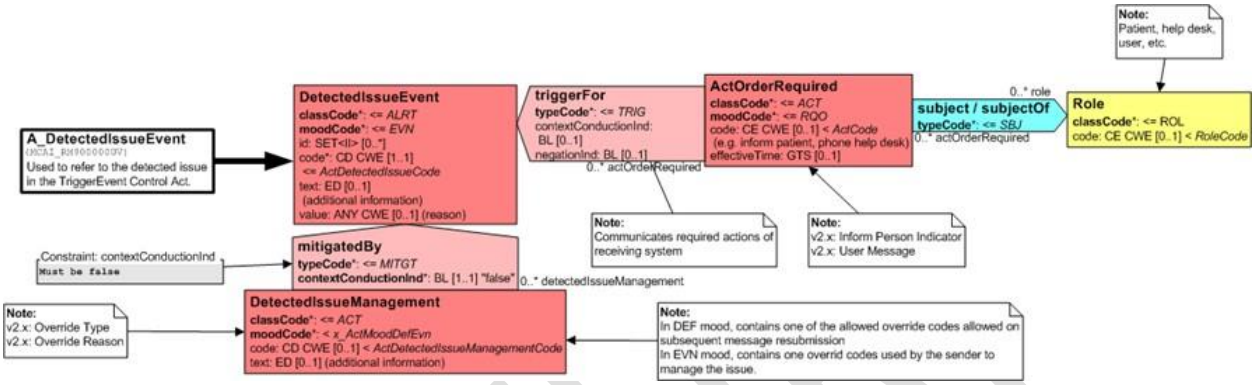

Figure 7 RMIM for DetectedIssueEvent

Table 4 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.[4]

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:

- 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.

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

Table 5: 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.
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 birth-place represented as an address	MUST NOT be used.
value [1..*] ParameterItem (SET<AD>)		MUST NOT be used.
semanticsText [1..1] ParameterItem (ST){default= "LivingSubject.Birth-Place.Addr"}		MUST NOT be used.
LivingSubjectBirthPlaceName	This query parameter is a patient's birth-place 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.Birth-Place.Place.Name"}		MUST NOT be used.
PrincipalCareProviderId	This query parameter is the care provider identifier of a person who has been as-signed as the principal care provider of this patient. The requestor may specify multiple PrincipalCareProviderId elements which responder shall consider as possi-ble 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= "As-signedProvider.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 per-sons in some registries. This parameter does not map to a single RIM attribute, in-stead, 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 Per-sonalRelationship 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.Moth-ersMaidenName"}		MUST NOT be used.
PatientTelecom	This query parameter is a telecommunica-tions address for communicating with a living subject in the context of the target	MUST NOT be used.

	patient registry. It could be a telephone number, fax number or even an email address. There shall be only a single PatientTelecom element.	
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 6: 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]	A value specifying the state of this record in a patient registry (based on the RIM	No further refinement.

Patient (CS) {CNE:active, fixed value= "active"}	role class state-machine). This record is active.	
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]	A value representing the domestic partnership status of this person.	MUST NOT be used.

Person (CE) {CWE:MaritalStatus}		
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 type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	This node with its attributes MUST NOT be used
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	A numeric value between 0 (excluded) and 100 (0 < percentage

	to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	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.

1.11.2 Use-case: Provider information replication

Table 7 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

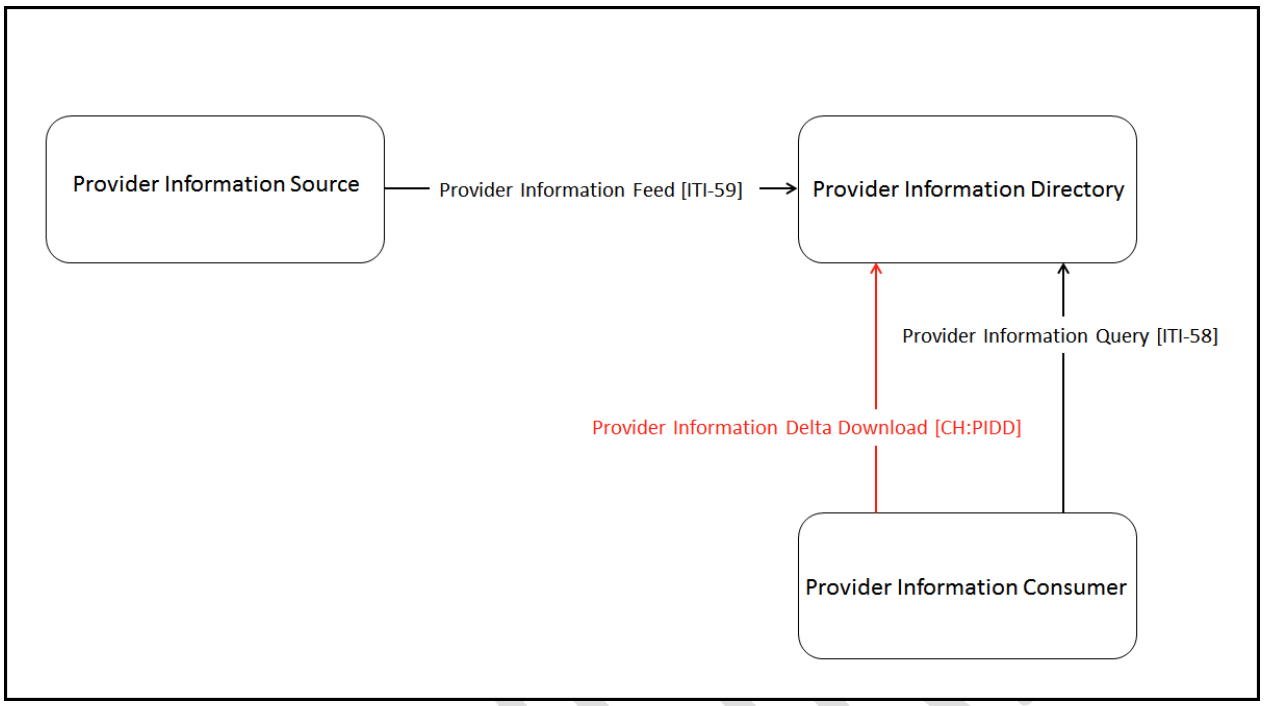

Figure 8 Swiss extended HPD Actors / Transactions

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 60) and an additional wsdl operation:

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

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

1.11.4.1.1 Interaction Diagram

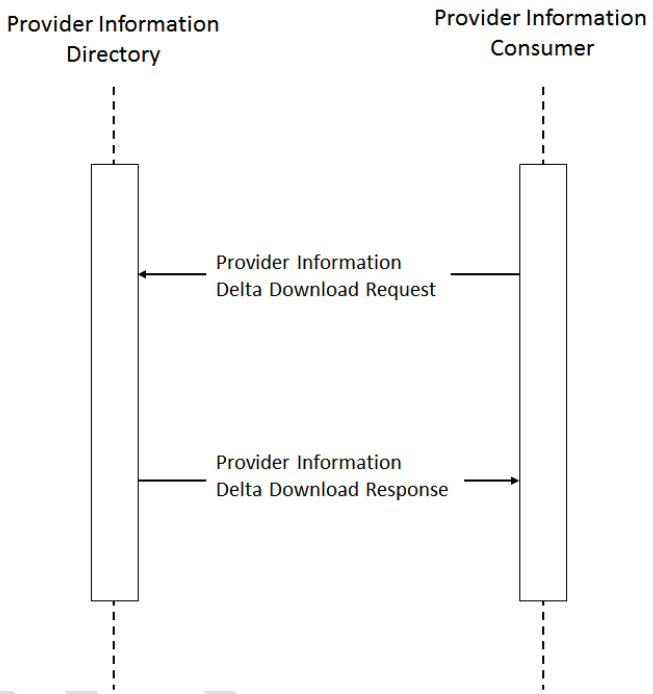

Figure 9 Provider Information Delta Download (CH:PIDD) interaction diagram

1.11.4.1.2 Provider Information Delta Download Request

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

- A 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: current time on the central query service server);
- An optional **filterMyTransactions** boolean parameter to manage the server side filtering of the author issued transactions (default: true);

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

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

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

1.11.4.1.3 Provider Information Delta Download Response

The response message contains a sequence of DSMLv2 batchRequest elements.

1.11.5 Message Semantics

1.11.5.1 HPD Schema Content

1.11.5.1.1.1 Identifiers

Organizational (e.g. hospitals) and Individual (health professionals) Providers are identified by Object Identifiers (OID). For Individual Provider, the ID is equal to the GLN[5] of the Individual Provider.

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

- If an Organizational Provider possesses an OID that is registered with a national OID register for health care OIDs, this OID has to be used.
- If an Organizational Provider does not possess an OID that is registered in a national OID register, the OID for this Organizational Provider has to comply with ISO/IEC 9834.
- For Swiss Organizational Providers that do not possess an unique OID registered in the Swiss health care OID register (RefData)[6], the OID consists of the RefData-registered OID for the higher-level healthcare facility this organization belongs to, plus an extension of this OID that is issued and maintained by the responsible healthcare facility.

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

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

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 8 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	validated	1	256	Issuing Authority:Type:ID:Status (where ID = GLN and Status = "active" or "inactive" or "revoked" or "suspended") Example: RefData:GLN:7601001064577:active Validation: It is validated whether at least one values that begins with *RefData:GLN:* is present. It is validated if the number after RefData:GLN: consists of thirteen digits.	
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)	

HPD Concept	Object class	Attribute name	Data type	Car-dinal-ity	Op-tion-ality	Techn. Re-marks	Min L.	Max L.	Comments	Swiss National Extension
Provider Type description	**person**	**description**	DString	M	R		1	1024	DisplayName in English corresponding to code in attribute hcPro-fession	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		
Provider Title	**Organization-alPerson**	**title**	DString	S	O		1	128		object class "organizationalPerson" instead of "inet-OrgPerson"
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 Sup-ported	**HPDProvider**	**hpdProviderLan-guageSupported**	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**	**hpdMedi-calRecordsDeliver-yEmailAddress**	DString	S	O		1	256		
Provider e-mail address	**inetOrgPerson**	**mail**	DString	M	O		1	256		
S-MIME Certificate	**inetOrgPerson**	**userSMIMECertifi-cate**	OString	M	O		1	32768		
Signing Certificate	**HCProfessional**	**hcSigningCertifi-cate**	OString	M	O		1	32768		
User Certificate	**inetOrgPerson**	**userCertificate**	OString	M	O		1	32768		
Creation Date	**System**	**createTimestamp**	GTime	S	System	read-only / opera-tional			Timestamp when the value was created	
Last Update date	**System**	**modifyTimestamp**	GTime	S	System	read-only / opera-tional			Timestamp when the value was modified	
Provider facility name	**Organization-alPerson**	**physicalDelivery-OfficeName**	DString	M	O		1	128		- object class: "organizationalPerson" instead of "inet-OrgPerson" - Optionality: O instead of R2
Provider Mailing Addresse	**HPDProvider**	**hpdProviderMail-ingAddress**	DString	M	O		1	4096		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 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
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 EprAuthorSpeciality (Id 2.16.756.5.30.1.127.3.10.1.1.4) 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 9 HPD Organizational Provider Attributes

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	techn Remarks	Min L.	Max L.	Comments	Swiss National Extension
Unique Entity Identifier	**uidObject**	**uid**	DString	S	R	validated	DN restriction	DN restriction	No further restrictions except for the technically given maximum length of 255 characters for the complete «distinguished name» (DN), including the uid. Validation if prefix correlates with currently logged-in community: "uid=<shcIssuerName>:"	UID RDN = prefix:id Prefix issued by FOPH. ID chosen by community.
Org Identifiers	**HCRegulatedOrganization**	**hcIdentifier**	DString	M	R	validated	1	256	Issuing Authority:Type:ID:Status (ID = OID or BUR number If ID = OID, status = "active" or "inactive" or "revoked" or "suspended" If ID = BUR number, status = "active" or "inactive" or " deleted" or "unknown" Example with OID: RefData:OID:2.99:active Example with BUR number: BFS:BUR:94763827:active Validation: Validation whether there is at least one value which starts with "RefData:OID:" Validation whether the OID is unique in the whole directory in HCRegulatedOrganization.hcIdentifier.	
Organization known names	**Organization**	**O**	DString	M	R		1	128	other name(s)	Optionality: R instead of R2
Organization Name	**HCRegulatedOrganization**	**HcRegisteredName**	DString	M	R		1	128	legal name(s)	
Org Type	**Organization**	**businessCategory**	DString	M	R	validated	1	128	Only valid MDI codes according to value set EprHealthcareFacilityTypeCode (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 businessCategory	
Org Status	**HPDProvider**	**hpdProviderStatus**	DString	S	O	validated	1	64	Allowed values: Active, Inactive (Case insensitive validation)	
Org Contact	**HCRegulatedOrganization**	**ClinicalInformationContact**	DN	M	O	validated	DN restriction	DN restriction	Only references to valid DNs and elements from the currently logged-in community are allowed. I.e the referenced element must have the same community prefix as the currently logged-in community.	
Org Practice Address	**HPDProvider**	**hpdProviderPracticeAddress**	DString	M	O		1	4096	Necessary for the clear identification of an organisation by the patient. It is highly recommended to provide values for this attribute if possible.	Optionality: O instead of R2
Org Billing Address	**HPDProvider**	**hpdProviderBillingAddress**	DString	M	O		1	4096		
Org Mailing Address	**HPDProvider**	**hpdProviderMailingAddress**	DString	M	O		1	4096		Optionality: O instead of R2
Provider Language Supported	**HPDProvider**	**hpdProviderLanguageSupported**	DString	M	O		1	64		Encoded using ISO-639-1

HPD Concept	Object class	Attribute name	Data type	Cardinality	Optionality	techn Remarks	Min L.	Max L.	Comments	Swiss National Extension
Org Speciality	**HCRegulatedOrganization**	**HcSpecialisation**	DString	M	O	validated	1	256	Only valid MDI codes according to value set 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 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 10 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=HCRegu-latedOrganization or owner OU=CHCommunity. Member HP is allowed if owner OU=HCRegulatedOr-ganization.	
	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[7]. See also chapter “1.1 Definitions of terms” on page 10.

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

4 Illustrations

5 Tables