SR 816.111

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

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

National extensions to the IHE Technical Framework

Ausgabe 1:	dd. mm YYYY
Inkrafttreten:	dd. mm YYYY

1 Introduction

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.

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

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 document with national extensions of IHE integration profiles was authored in order to fulfil the Swiss regulations of the Ordinance on the Electronic Patient Record (EPRO, SR 816.11). The EPRO and the EPRO-DFI are published in Official Compilation of Federal Legislation[1] (AS) (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 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119][2].

1.1.2 Scope of precisions

The extensions, restrictions and translations specified apply to the following IHE IT Infrastructure (ITI) Integration profiles: SMART on FHIR, IUA, PIXm, MHD, RESTful ATNA

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

2 Overview

2.1 Introduction

This national extension is motivated by the intention to ease integration of mobile applications to the Swiss EPR by extending the IHE FHIR based mobile profiles. This national extension to IHE profiles is intended for mobile applications running on mobile devices, but not limited to. The IHE FHIR based mobile profiles use technologies (REST, OAuth, etc.) which are widely spread in the developer community and may be used for native applications and Web Applications, for example in web based primary systems.

The scope of this extension covers the following use cases:

1. Client authentication and authorization;
2. User Authentication;
3. Read documents from the EPR;
4. Write documents to the EPR;
5. Write logs to the EPR ATNA Audit Record Repository.

This extension covers two options:

1. Generic mHealth option – This option adresses primary systems or mobile applications using the basic EPR flows but replace the XDS.b related and PIX V3 profiles with the FHIR based profiles;
2. SMART on FHIR – This option adresses mobile apps or modular primary systems that want to connect to the Swiss EPR using SMART on FHIR.

2.2 Profiles, actors and transactions

The following figure shows the profiles, actors and transactions specified or referenced in this national extension:

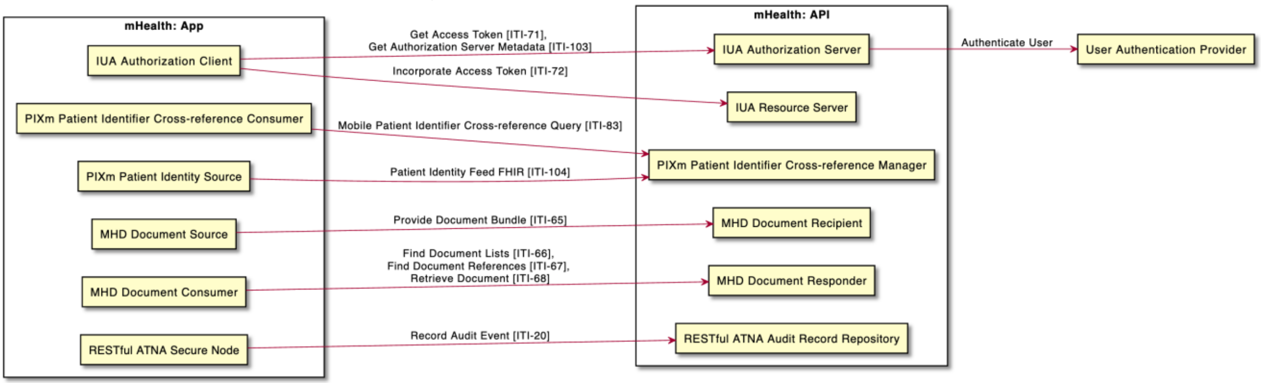
mHealth: App
IUA Authorization Client
PIXm Patient Identifier Cross-reference Consumer
PIXm Patient Identity Source
MHD Document Source
MHD Document Consumer
RESTful ATNA Secure Node
Get Access Token [ITI-71],
Get Authorization Server Metadata [ITI-103]
Incorporate Access Token [ITI-72]
Mobile Patient Identifier Cross-reference Query [ITI-83]
Patient Identity Feed FHIR [ITI-104]
Provide Document Bundle [ITI-65]
Find Document Lists [ITI-66],
Find Document References [ITI-67],
Retrieve Document [ITI-68]
Record Audit Event [ITI-20]
mHealth: API
IUA Authorization Server
IUA Resource Server
PIXm Patient Identifier Cross-reference Manager
MHD Document Recipient
MHD Document Responder
RESTful ATNA Audit Record Repository
Authenticate User
User Authentication Provider

Figure 1: Profiles, actors and transactions covered in this national extension.

2.3 Integration Profiles

2.3.1 Internet User Authorization (IUA)

This section specifies Swiss national extensions to Internet User Authorization (IUA) Profile, which is published as an IHE ITI Trial Implementation profile.

2.3.1.1 Scope

There is no extension or restriction of the profile scope defined in this national extension.

As described in the IUA Trial Implementation the profile is intended to provide means to retrieve EPR conformal access token (SAML or JWT) and to incorporate the access token to transactions which access protected resources.

2.3.1.2 Use Cases

No extensions or restrictions to the use cases defined in the IUA profile are specified in the Swiss in national extension.

2.3.1.3 Actors and Transactions

No extensions or restrictions to the IUA actors and transactions are specified in the Swiss national extension.

2.3.1.4 Actor Options

This national extension restricts the IUA options to the Authorization Server Metadata, JWT Token and SAML Token option. The Token Introspection option of the IUA profile SHALL not be used.

2.3.1.5 Grouping

The Swiss national extension does not define requirements on the grouping of actors in this profile, which extend or restrict the grouping required from the IUA profile.

2.3.1.6 Process Flow

For the process flow of this profile and its interplay with the other mHealth profiles see sequence diagrams.

2.3.1.7 Security Consideration

The IUA Authorization Server SHALL enforce authentication of the user by redirecting the mHealth App to the User Authentication Provider (Identity Provider) as described in Section 3.2.8.

2.3.2 Patient Identifier Cross-referencing for mobile (PIXm)

This section specifies Swiss national extensions to Patient Identifier Cross-referencing for mobile (PIXm) profile. PIXm is published as an IHE ITI Trial Implementation profile.

2.3.2.1 Scope

In the Swiss EPR, the PIXm profile ensures that different systems can correlate the local identity with the MPI-PID (and EPR-SPID) for the community and that the initial demographics data can be feeded to the MPI. The profile supports creation, update and deprecation of patient master identity information about a subject of care using the HL7 FHIR standard resources and RESTful transactions.

2.3.2.2 Use Cases

A mHealth App wants to get data from the EPR. The mHealth App needs to know the MPI-PID in the community. With the local identifier the mHealth App can query the MPI-PID (and EPR-SPID) for the community. The local identifier with the initial demographics data needs to be setup initially in the community that the correlation is possible.

2.3.2.3 Actors and Transactions, Content Specifications

This national extension adds restrictions to the correlation to other local identifiers, to the query results and a specific patient content profile is defined. Otherwise there are no extensions or restrictions to the profile actors and the transaction.

2.3.2.4 Actor Options

No extensions or restrictions to the profile actor options are specified in the Swiss national extension.

2.3.2.5 Required Actor Grouping

This national extension enforces authentication and authorization for access control. Therefore actors of this profile must be grouped with actors of other profiles according to the following table:

Actor	Required Grouping	Optionality
Patient Identifier Cross-reference Manager	IUA Resource Server	R
Patient Identity Source	IUA Authorization Client	R
Patient Identifier Cross-reference Consumer	IUA Authorization Client	R

Table 1: Grouping of PIXm actors required by this national extension.

2.3.2.6 Process Flow

For the process flow of this profile and its interplay with the other mHealth profiles see sequence diagrams.

2.3.2.7 Security Consideration

This national extension enforces authentication and authorization of access to the Patient Identifier Cross-reference Manager using the IUA profile with basic access token as described in Section 3.2.

2.3.3 Mobile Access to Health Documents (MHD) with XDS on FHIR

This section specifies Swiss national extensions to the Mobile Access to Health Documents (MHD) with XDS on FHIR Profile, which is published as an IHE ITI Trial Implementation profile.

2.3.3.1 Scope

A mHealth App can query, retrieve or publish data to EPR communities using the transaction of the MHD profile.

2.3.3.2 Use Cases

No extensions or restrictions to the profile use cases are specified in the Swiss in national extension.

2.3.3.3 Actors and Transactions

No extensions or restrictions to the actors and transactions are specified in the Swiss national extension.

2.3.3.4 Actor options

For all actors the Comprehensive Metadata Option and the XDS on FHIR Option SHALL be supported. For all actors the Metadata as defined in Annex 3 SHALL be supported.

2.3.3.5 Required Actor Groupings

The Actors Document Recipient and Document Responder MUST be grouped according to the XDS on FHIR grouping condition see Table 33.3-1: MHD - Actors Required Grouping.

This national extension enforces authentication and authorization for access control. Therefore actors of this profile must be grouped with actors of other profiles according to the following table:

Actor	Required Grouping	Optionality
Document Recipient	IUA Resource Server	R
Document Responder	IUA Resource Server	R
Document Source	IUA Authorization Client	R
Document Consumer	IUA Authorization Client	R

Table 2: Grouping of MHD actors required by this national extension.

2.3.3.6 Process Flow

For the process flow of this profile and its interplay with the other mHealth profiles see sequence diagrams.

2.3.3.7 Security Consideration

This national extension enforces authentication and authorization of access to the Patient Identity Manager using the IUA profile with extended access token as described in Section 3.2.

2.3.4 RESTful ATNA

This section specifies Swiss national extensions to the Add RESTful ATNA (Query and Feed) supplement, which is published as an IHE ITI Trial Implementation profile.

2.3.4.1 Scope

A mHealth App needs to submit audit records according to the IHE ITI profiles. The Add RESTful ATNA (Query and Feed) supplement allows an mHealth App to add audit events through a RESTful Feed to the Audit Record Repository.

2.3.4.2 Use Cases

No extensions or restrictions to the profile use cases are specified in the Swiss in national extension.

2.3.4.3 Actors and Transactions

No extensions or restrictions to the actors and transactions are specified in the Swiss national extension.

2.3.4.4 ATNA Actor Options

The Audit Record Repository SHALL support the ATX: FHIR Feed Option.

2.3.4.5 Grouping

The Swiss national extension does not define requirements on the grouping of actors in this profile, which extend or restrict the grouping required from the ATNA profile.

2.3.4.6 Process Flow

For the process flow of this profile and its interplay with the other mHealth profiles see sequence diagrams.

2.3.4.7 Security Consideration

The Swiss national extension does not define additional requirements on ATNA Security Considerations.

3 Transactions

This sections describes the new transactions required for mHealth and the Swiss national extensions to existing transactions.

3.1 Get Authorization Server Metadata [ITI-103]

3.1.1 Scope

At launch time the app may connect to the Authorization Server to retrieve the configuration data. The Authorization Server responds with the configuration data and the Authorization Server endpoint the app shall direct the User Agent to.

3.1.2 Actor Roles

Actor: Authorization Client or Resource Server

Role: Sends a request to the Authorization Server to retrieve configuration data and the server endpoint to redirect the User Agent to.

Actor: Authorization Server

Role: Responds with the FHIR Server configuration data.

3.1.3 Referenced Standards

- IHE ITI Technical Framework Supplement Internet User Authorization (IUA) Revision 2.1
- SMART Application Launch Framework Implementation Guide Release 1.0.0

3.1.4 Messages

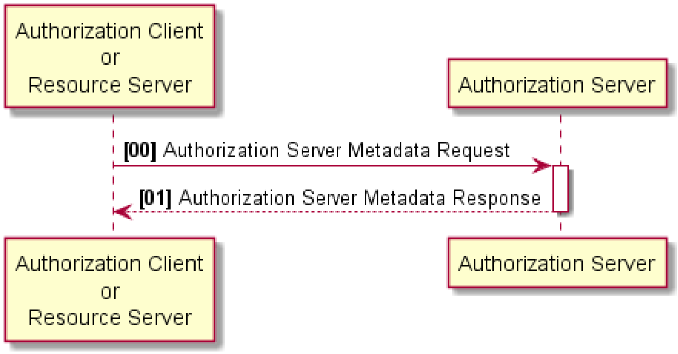
Authorization Client or Resource Server
Authorization Server
[00] Authorization Server Metadata Request
[01] Authorization Server Metadata Response
Authorization Client or Resource Server
Authorization Server

Figure 2: Interaction diagram of the Get SMART on FHIR Metadata transaction.

3.1.5 Trigger Events

A mHealth App or a Resource server wants to retrieve the Authorization Server configuration data. A mHealth App is launched in a SMART on FHIR launch sequence.

3.1.6 Message Semantics

3.1.6.1.1 Request

The Authorization Client or Resource Server performs a HTTP GET request to the Authorization Server Well-Known URI. The request SHALL neither use parameter nor body data.

3.1.6.1.2 Response

The Authorization Server SHALL response with a HTTP response conveying a JSON formatted object as HTTP body element. The JSON object SHALL convey the following attributes:

Attribute	Option-ality	Reference	Description
authorization_endpoint	R	SMART on FHIR/IUA	URL to the IUA Authorization Server endpoint.
token_endpoint	R	SMART on FHIR /IUA	Authorization Server's Authorization token endpoint location.
token_endpoint_auth_methods	O	SMART on FHIR	Client authentication methods supported by the token endpoint. The options are “client_secret_post” and “client_secret_basic”.
registration_endpoint	O	SMART on FHIR	URL to the OAuth2 dynamic registration endpoint for this FHIR server.
scopes_supported	O	SMART on FHIR /IUA	Recommended: Supported scopes.
response_types_supported	O	SMART on FHIR /IUA	Recommended: Supported OAuth2.1 response_type values.
grant_types_supported	R	IUA	SHALL be “authorization_code”.
management_endpoint	O	SMART on FHIR	URL an end-user can view which applications currently have access to data and can make adjustments to these access rights.
revocation_endpoint	O	SMART on FHIR	Recommended: URL to a server’s revoke endpoint that can be used to revoke a token.
capabilities	R	SMART on FHIR	SMART capabilities (e.g., single-sign-on or launch-standalone) that the server supports.
issuer	R	IUA	The Authorization Server's issuer identifier.
jwks_uri	R	IUA	URL of the Authorization Server's JWK Set [RFC7517, Section 5] document.
access_token_format	O	IUA	JSON string defining the format of the access token as provided by the Authorization Server. Values are “ihe_jwt” or “ihe_saml”.

Table 3: Attributes of the Get metadata transaction

3.1.7 Expected Actions Authorization Client or Resource Server

The Authorization Client or Resource Server MAY read the URL of the IUA Authorization Server and redirect the User Agent to the Authorization Server.

3.1.8 Expected Actions Authorization Server

There are no further requirements beyond those defined in the SMART on FHIR specification.

3.1.9 Message Example

3.1.9.1.1.1 Request

```
GET {URL-SMART-FHIR-Server}/.well-known/smart-configuration  HTTP/1.1
```

3.1.9.1.1.2 Response

Example

3.1.10 Security Consideration

There are no special security requirements for this transaction.

3.2 IUA: Get Access Token [ITI-71]

This section describes the national extension for the Swiss EPR to the Get Access Token [ITI-71] transaction defined in the IUA profile published in the IHE IT Infrastructure Technical Framework Trial Implementation **“**Internet User Authorization”.

In this transaction, the OAuth Authorization Code grant type option is enforced for security reasons.

3.2.1 Scope

The transaction is used by an mHealth App to pass claims to the IUA Authorization Server and to retrieve access token to be used for authorization of the apps access to write data to and retrieve data from the Swiss EPR.

Depending on the claims made by the mHealth App, two different flavors of access tokens are provided by the IUA Authorization Server:

- Basic Access Token – IUA conformal access token authorizing access to the EPR endpoints which are NOT protected by the EPR role and attribute based authorization (i.e. for the PIXm endpoints).
- Extended Access Token – IUA conformal access token for the EPR endpoints which are protected by the EPR role and attribute based authorization (i.e. for the MHD endpoints).

A mHealth App in the SMART Standalone Launch sequence SHALL perform the transaction first to get basic access to the Swiss EPR. This requires user authentication as well as the user consent, allowing the mHealth App to access the Swiss EPR and perform transactions on behalf of the user. The IUA Authorization Server SHALL present a User Interface for the user to authenticate and provide user consent, or by validating against data stored at app registration time.

Once the mHealth App is authorized, it may launch other embedded mHealth Apps (or views) using the SMART EHR Launch Sequence. In this case, the embedded app inherits the basic access authorization from the launching app[3] and may retrieve extended access token for EPR endpoints protected by the EPR role and attribute based authorization (e.g. to retrieve documents).

3.2.2 Actor Roles

Actor: IUA Authorization Client

Role: Communicates launch information and claims to the IUA Authorization Server and receives JWT access token or XUA Authorization Assertion.

Actor: IUA Authorization Server

Role: Verifies claims and authentication information, retrieves and validates the user consent for the mHealth App to act on behalf of the user[4] and responds a JWT or XUA compliant access token to the IUA Authorization Client.

3.2.3 Referenced Standards

This national extension does not reference additional standards to the standards referenced in the Get Access Token [ITI-71] transaction of the IUA Trial Implementation.

[3] By claiming a launch indicator, the launch is indicated as a SMART EHR Launch, initiated from an app, which has already been authorized before.

[4] E.g. by presenting a screen for the user to give consent.

3.2.4 Messages

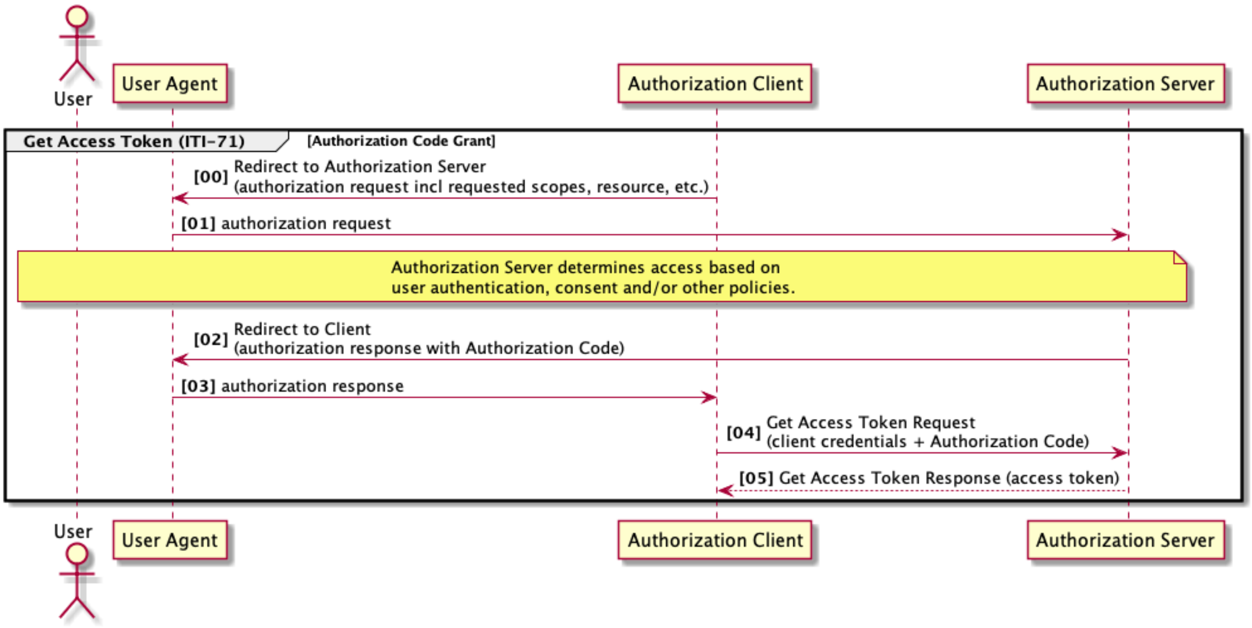
User
User Agent
Authorization Client
Authorization Server
Get Access Token (ITI-71)
[Authorization Code Grant]
[00] Redirect to Authorization Server
(authorization request incl requested scopes, resource, etc.)
[01] authorization request
Authorization Server determines access based on
user authentication, consent and/or other policies.
[02] Redirect to Client
(authorization response with Authorization Code)
[03] authorization response
[04] Get Access Token Request
(client credentials + Authorization Code)
[05] Get Access Token Response (access token)
User
User Agent
Authorization Client
Authorization Server

Figure 3: OAuth 2.1 authorization code grant flow of the of the IUA Get Access Token transaction.

Step	Parameter	Opt (Basic/ Extended).	Reference	Remark
The mHealth App sends a HTTP GET request to the IUA Authorization Server endpoint.	response_type	R	IUA	The value must be *code*.
	client_id	R	IUA	The ID, the client is registered at the IUA Authorization Server.
	redirect_uri	R	IUA SMART on FHIR	Used as callback URL, the IUA Authorization Server will send the authorization code to.The URL SHALL match one of the client's pre-registered redirect URIs.
	state	R	IUA	An unguessable value used by the client to track the state between the authorization request and the callback.
	scope	R	IUA SMART on FHIR	Attributes the app claims (see detailed description below).
	aud	R	SMART on FHIR	The audience URL the token will be used for.
	launch	O/R	SMART on FHIR	If present, the launch parameter indicates that the app (or the view) was launched from an EHR or mHealth App context which has already been authorized to access the Swiss EPR (e.g. SMART on FHIR based primary system).
	code_challenge	R	IUA	Transformed version of code_verifier with code_challenge_method.
	code_challenge_method	R	IUA	SHALL be “S256”.

The Authorization Server performs a HTTP GET on the callback URL (redirect_uri) conveying the authorization code.	code	R	IUA	The authorization code generated by the Authorization Server.
	state	R	IUA	The unguessable value used by the client to track the state between the authorization request and the callback.
The app performs an HTTP POST with parameter as a form-encoded HTTP entity body, passing its client_id and client_secret as an HTTP Basic authorization header.	client_id	R	IUA	The ID the client is registered at the IUA Authorization Server.
	redirect_uri	R	IUA	The URI to redirect the apps user agent to.
	grant_type	R	IUA	Value shall be "authorization_code".
	code	R	IUA	The authorization code.
	code_verifier	R	IUA	The original code verifier string.
The Authorization Server responds with the access token in the HTML body element.	access_token	R	IUA	A string containing the access token which may either be a JWT or a XUA Authorization Assertion.
	token_type	R	IUA	The value of the parameter shall be Bearer.
	scope	R	IUA	The scope granted by the Authorization Server.
	expires_in	R	IUA	Maximum duration of 5 minutes.
	refresh_token	O	IUA	how to handle refresh tokens

Table 4: Description of the HTTP conversation of the transaction.

3.2.5 Trigger Events

A user launches an mHealth App or a specific application view to access data and documents from the Swiss EPR.

3.2.6 Message Semantics

3.2.6.1 Request

The following table summarizes the requirements on the scope parameter used to convey the claims:

Scope	Optionality (Basic/ Extended)	Type	Reference	Remark
launch	O/R		SMART on FHIR	Permission to obtain launch context when the app is launched from an EHR. Required for apps or views launched from an EHR or a mHealth App which was authorized before.
purpose_of_use	O/R	token[5]	See sections below.	Value taken from code system 2.16.756.5.30.1.127.3.10.5 of the CH: EPR value set.

[5] Token format according FHIR token type: https://www.hl7.org/fhir/search.html#token

subject_role	O/R	token	See sections below.	Only the values for the Role of Healthcare Professionals, Assistants, Patients and Representatives are allowed.
person_id	O/R	string, CX	See sections below.	EPR-SPID identifier of the patient's record-and the patient assigning authority formatted in CX syntax.
principal	O/O	token	See sections below.	Name of the healthcare professional an assistant is acting on behalf of.
principal_id	O/O	token	See sections below.	GLN of the healthcare professional an assistant is acting on behalf of.
group	O/O	string	See sections below.	Name of the organization or group an assistant is acting on behalf of.
group_id	O/O	string	See sections below.	OID of the organization or group an assistant is acting on behalf of.
access_token_format	O/O	string		Either ihe-jwt or ihe-saml as value. Will return this token_flavor. If scope is not provided defaults to ihe-jwt.

Table 5: Overview of the request's scope parameter. For the explanation see the following sections.

The scope parameter of the request MAY claim the following attributes:

- There may be a scope with name "launch". If present, it indicates the permission to obtain launch context for apps (or views) launched in SMART EHR Launch mode. The scope SHALL be used by all apps (or views) launched from a mHealth App which was authorized before.
- There MAY be a scope with name "purpose_of_use=token". If present, the token SHALL convey the coded value of the current transaction's purpose of use. Allowed values are NORM (normal access) and EMER (emergency access) from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set. e.g. purpose_of_use=urn:oid:2.16.756.5.30.1.127.3.10.5|NORM
- There MAY be a scope with name "subject_role=token". If present, the token SHALL convey the coded value of the subject's role. The value SHALL be either HCP (healthcare professional), ASS (assistant), REP (representative) or PAT (patient) from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set. e.g.: subject_role=urn:oid:2.16.756.5.30.1.127.3.10.6|HCP
- There MAY be a scope with name "person_id=value". If present, the value SHALL convey the EPR-SPID identifier of the patient's record and the patient assigning authority formatted in CX syntax. e.g: person_id=761337610435209810^^^&amp;2.16.756.5.30.1.109.6.5.3.1.1&amp;ISO

Depending on the value of the role scope additional scopes are required, as described in the following sections.

3.2.6.1.1 Heathcare Professional Extension

In the healthcare professional extension, the scope subject_role SHALL be the code HCP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set.

3.2.6.1.2 Assistant Extension

In the assistant extension, the scope subject_role SHALL be the code ASS from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set. There SHALL be a scope with name principal_id=value. The value SHALL convey the GLN of the healthcare professional an assistant is acting on behalf of. There SHALL be a scope with name principal=value. The value SHALL convey the name of the healthcare professional an assistant is acting on behalf of.

There MAY be one or more scopes with name group_id=value and corresponding group=value. If present each value SHALL convey the ID and name of the subject's organization or group as registered in the EPR HPD. The ID MUST be an OID in the format of an URN.

3.2.6.1.3 Patient Extension

In the patient extension, the scope subject_role SHALL be the code PAT from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set. The value of the purpose of use scope SHALL be the code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

3.2.6.1.4 Representative Extension

In the representative extension, the scope subject_role SHALL be the code REP from code system 2.16.756.5.30.1.127.3.10.6 of the CH:EPR value set. The token of the purpose_of_use scope SHALL be the code NORM from code system 2.16.756.5.30.1.127.3.10.5 of the CH:EPR value set.

3.2.6.2 Response

The response SHALL either convey a basic acces token in JWT format, granting basic access to the EPR (i.e. to access patient data), or an extended access token (see section 3.2.1) to access resources protected by the role and attribute based EPR authorization (i.e. read and write documents).

3.2.6.2.1 JSON Web Token Option

The access token SHALL have the same required attributes as defined in the IUA 3.71.4.2.2.1 JSON Web Token Option.

3.2.6.2.1.1 JWT IUA extension

The Authorization Server and Resource Server SHALL support the 3.71.4.2.2.1.1 JWT IUA extension with the following claims as defined in Table todo.

The claim content for the JWT IUA extensions SHALL correspond to the content defined in the XUA specification (see 1.6.4.2 Get X-User Assertion, A5E1).

JWT Claim (Extension)	Optionality	XUA Attribute EPR	Remark
subject_name	O/R	urn:oasis:names:tc:xspa:1.0:subject:subject-id	Plain text’s user name.
subject_role	O/R	urn:oasis:names:tc:xacml:2.0:subject:role	Code indicating the user role. In the Swiss EPR the value SHALL be taken from the EPR Role Code Value Set.
purpose_of_use	O/R	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	Code indicating the purpose of use. In the Swiss EPR the value SHALL be taken from the EPR Purpose Of Use Value Set.
person_id	O/R	urn:oasis:names:tc:xacml:2.0:resource:resource-id	SHALL be the EPR-SPID of the patients EPR.

Table 6: Attributes of the IUA Get Access Token response in the JWT extension ihe_iua.

3.2.6.2.1.2 The JWT ch_epr extension

The Authorization Server and Resource Server SHALL support the following extensions to the JWT access token for an EPR user:

- user_id: subject identifier according to Annex 5 E1 1.6.4.3.4.2 Message Semantics

JWT Claim (Extension)	Optionality	XUA Attribute EPR	Remark
user_id	R	<NameID> child element of the <Subject>	Depending on the Annex 5 E1 Extension
user_id_qualifier	R	Name qualifier attribute of <NameID>	Depending on the Annex 5 E1 Extension

Table 7: Attributes of the IUA Get Access Token response in the JWT extension ch_epr.

3.2.6.2.1.3 The JWT ch_group extension

The Authorization Server and Resource Server SHALL support the following extensions to the JWT access token for a list of groups a subject is member of:

- name: Name of the organization/group. The name MUST be a string.
- id: The id of the organization/group.The id MUST be an OID in the format of an URN

The ch_group extension claims shall be wrapped in an "extensions" object with key 'ch_group' and a JSON array containing the JSON objects with properties name and id. The id MUST be an OID in the format of an URN.

ch_group array element	Optionality	XUA Attribute EPR	Remark
name	O/R	urn:oasis:names:tc:xspa:1.0:subject:organization	In XUA it is an array of text description of the groups/organizations, in the JWT extension it is an array of groups with properties name, id.
id	O/R	urn:oasis:names:tc:xspa:1.0:subject:organization-id	In XUA it is an array of ids of the groups/organizations, in the JWT extension it is an array of group name, group id.

Table 8: Attributes of the IUA Get Access Token response in the JWT extension ch_group.

3.2.6.2.1.4 The JWT ch_delegation extension

The Authorization Server and Resource Server shall support the following extensions to the JWT access token:

- principal (optional) Name of the healthcare professional an assistant is acting on behalf of.
- principal_id (optional) GLN of the healthcare professional an assistant is acting on behalf of.

The ch_delegation extension claims shall be wrapped in an "extensions" object with key 'ch_delegation' and a JSON value object containing the claims.

The claim content for the JWT CH:EPR extensions shall correspond to the content defined in the XUA specification (see 1.6.4.2 Get X-User Assertion, A5E1).

JWT Claim (Extension)	Optionality	XUA Attribute EPR	Remark
principal	O/R	urn:e-health-suisse:principal-name	Name of the healthcare professional an assistant is acting on behalf of.
principal_id	O/R	urn:e-health-suisse:principal-id	GLN of the healthcare professional an assistant is acting on behalf of.

Table 9: Attributes of the IUA Get Access Token response in the JWT extension ch_delegation.

3.2.7 Expected Actions IUA Authorization Client

The IUA Authorization Client SHALL support the HTTP conversation of the OAuth 2.1 Authorization Code grant as follows:

When launched, the IUA Authorization Client SHALL perform HTTP GET request with the URL query parameter as defined in Table 4 and with the scope claims described in Table 5.

If the IUA Authorization Client receives the request from the IUA Authorization Server on the callback URL conveying the authorization code, it SHALL perform the HTTP POST request with the client_id and client_secret in the HTTP authorization header to resolve the authorization code to the access token.

The IUA Authorization Client SHALL use the access token as defined in IUA Incorporate Access Token transaction, when performing requests to resources of the Swiss EPR[6].

3.2.8 Expected Actions IUA Authorization Server

The IUA Authorization Server SHALL support the HTTP conversation of the OAuth 2.1 Authorization Code grant as follows:

If the IUA Authorization Server receives a request, it SHALL authenticate the user by redirecting the request to a XUA Authentication Provider[7]. The XUA Authentication provider authenticates the user based on its internal session management (i.e. by checking the requests cookies or other methods) or by validating the user authentication means and returns the identity token to the IUA Authorization Server.

In case of authentication failure, the IUA Authorization Server must respond with HTTP error code 401 ‘Not authorized’.

The IUA Authorization Server SHALL verify the user consent for the mHealth App either by presenting the user a dialog to confirm the required consent, or by validating preregistered contracts.

If the app (or view) is launched as an SMART EHR Launch, the IUA Authorization Server SHALL validate the launch scope parameter, by verifying that the user consent is registered with this launch parameter value. In case of failure, it SHALL respond with HTTP error code 401 ‘Not authorized’.

Depending on the scope claimed, the IUA Authorization Server SHALL either build a basic access authorization token allowing basic access to the EPR (i.e. to access patient data), or an extended access to access resources protected by the role and attribute based EPR authorization (i.e. read and write documents).

The business rules for the IUA Authorization Server for the Healthcare Professional, Assistant, Patient and Representative Extension SHALL be the same as for Annex 5E1 1.6.4.2.4.4 Expected Actions X-Assertion Provider Extensions.

[6] This covers all possible EPR transaction, with the exception of the ITI-103.

[7] The XUA Authentication Provider currently only supports SAML 2 based authentication as defined in Annex 8 of the EPDV-EDI, but will be extended to Open ID Connect in the future. Currently SMART on FHIR does not have a SAML 2 option.

If successful the IUA Authorization Server SHALL generate an OAuth 2.1 authorization code and perform a callback to the URL defined in the request, using the OAuth authorization code as URL query parameter with key ‘code’.

The IUA Authorization Server SHALL store the access token and the assigned authorization code and respond the access token on request to the Authorization Client.

3.2.9 Message Examples

Examples

3.3 Patient Identity Feed FHIR [ITI-104]

3.3.1 Scope

This transaction communicates patient information, including corroborating demographic data, after a patient's identity is established, modified or merged or after the key corroborating demographic data has been modified.

3.3.2 Actor Roles

Actor: Patient Identity Source

Role: Provides notification to the Patient Identifier Cross-reference Manager for any patient identification related events including: creation, updates, merges, etc.

Actor: Patient Identifier Cross-reference Manager

Role: Serves a well-defined set of Patient Identification Domains. Based on information provided in each Patient Identification Domain by a Patient Identity Source Actor, it manages the cross-referencing of patient identifiers across Patient Identification Domains.

3.3.3 Referenced Standards

Patient Identifier Cross-referencing for mobile (PIXm) – Rev. 3.0.0 – November 8, 2021

3.3.4 Messages

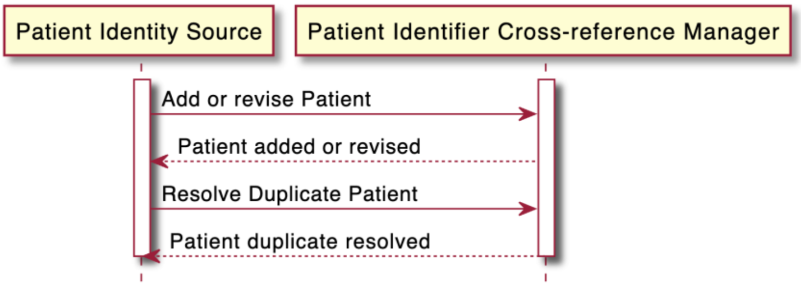
Patient Identity Source
Patient Identifier Cross-reference Manager
Add or revise Patient
Patient added or revised
Resolve Duplicate Patient
Patient duplicate resolved

Figure 4: Interaction diagram for [ITI-93]

3.3.5 Trigger Events

The Add Patient message is triggered when a new patient is added to a Patient Identity Source.

The Revise Patient message is triggered when the patient information is revised within a Patient Identity Source (e.g., change in patient name, patient address, etc.).

A Resolve Duplicate Patient message is triggered when the Patient Identity Source does a merge within its Patient Identification Domain.

3.3.6 Message Semantics

The same message semantic apply as in 2:3.104.4.1.2 and 2:3.104.4.2.2 Message Semantics.

The patient data SHALL be conform to the PIXm Patient profile with the canonical url http://fhir.ch/ig/ch-epr-mhealth/StructureDefinition/ch-pixm-patient. The Patient Identifier Cross-reference Manager SHALL reference the PIXm Patient profile or a derived constrained profile as a supportedProfile in the CapabilityStatement.

If the patient is already registered in a community, the MPI-PID SHALL be provided as an identifier. The EPR-SPID as an identifier MAY be added. The birthname can be added with the ISO 21090 qualifier extension, the religion SHALL not be added.

3.3.7 Expected Actions Consumer played by Patient Identifier Cross-reference Manager

If the MPI-PID is provided as an identifier Patient Identifier Cross-reference Manager SHALL use the MPI-PID to correlate the patient in the community.

3.3.8 Message Example

Example

3.3.9 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Patient Identifier Cross-reference Manager using the IUA profile with basic access token as decribed in Section 3.2. Consequently the Patient Identity Feed FHIR [ITI-104] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.4 Mobile Patient Identifier Cross-reference Query [ITI-83]

This section documents additional requirements in the Swiss EPR context on the Mobile Patient Identifier Cross-reference Query.

3.4.1 Scope

The Mobile Patient Identifier Cross-reference Query is used by an app in the Swiss EPR to query with the local identifier the MPI and get the corresponding MPI-PID and the EPR-SPID identifier for the patient.

3.4.2 Actor Roles

Actor: Patient Identifier Cross-reference Consumer

Role: Queries the Patient Identifier Cross-reference Manager for the MPI-PID and EPR-SPID.

Actor: Patient Identifier Cross-reference Manager

Role: Resolves the local ID sent with the request to the MPI-PID and EPR-SPID.

3.4.3 Referenced Standards

Patient Identifier Cross-referencing for mobile (PIXm) – Rev. 3.0.0 – November 8, 2021

This PIXm profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.4.4 Messages

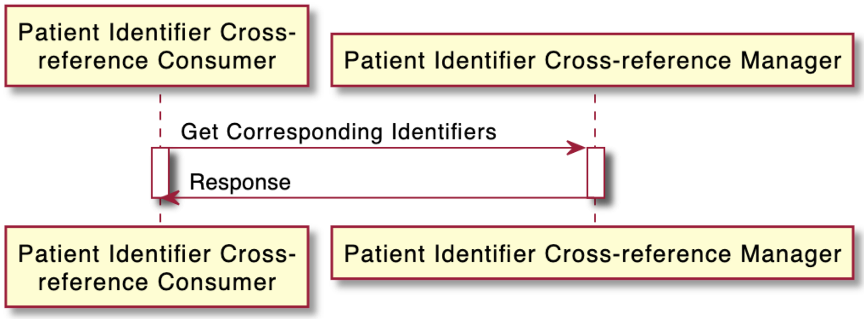
Patient Identifier Cross-reference Consumer
Patient Identifier Cross-reference Manager
Get Corresponding Identifiers
Response
Patient Identifier Cross-reference Consumer
Patient Identifier Cross-reference Manager

Figure 5: Interaction diagram for [ITI-83]

3.4.5 Trigger Events

A mobile app wants to access (read or write) documents, which requires the MPI-PID of the patient.

3.4.6 Message Semantics

The message semantics is the same as defined in 3.83.4.1.2 with a restriction on the targetSystem query Parameter:

```
GET [base]/Patient/$ihe-pix?sourceIdentifier=[token]{&targetSystem=[uri]}{&_format=[token]}
```

Table 3.83.4.1.2-1: $ihe-pix Message HTTP query Parameters

Query parameter Name	Cardinality	Search Type	Description	Swiss National Extension
Input Parameters				
sourceIdentifier	[1..1]	token	The Patient identifier search parameter that will be used by the Patient Identifier	No further refinement.

			Cross-reference Manager to find cross matching identifiers associated with the Patient Resource. See Section 2:3.83.4.1.2.1.	
targetSystem	**[1..2]**	uri	The Assigning Authorities for the Patient Identity Domains from which the returned identifiers shall be selected. See Section 2:3.83.4.1.2.2.	SHALL be Restricted to the Assigning authority of the community and/or the EPR-SPID.
_format	[0..1]	token	The requested format of the response from the mime-type value set. See ITI TF-2: Appendix Z.6	No further refinement.

Table 3.83.4.2.2-1: $ihe-pix Message Response

Parameter	Card.	Data Type	Description
FHIR Parameters Resource			
targetIdentifier	**[0..2]**	Identifier	The identifier found. Constraints to include the assigning authority as specified in ITI TF-2: Appendix E.3
targetId	**[0..1]**	Reference(Patient)	The URL of the Patient Resource

If the targetSystem is not restricted to the Assigning authority of the community and/or the EPR-SPID the error `Target Domain not recognized` (2:3.83.4.2.2.4) SHALL be returned.

3.4.7 Message Example

Example

3.4.8 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Patient Identifier Cross-reference Manager using the IUA profile with basic access token as decribed in Section 3.2. Consequently the Mobile Patient Identifier Cross-reference Query [ITI-83] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.5 MHD: Provide Document Bundle [ITI-65]

This section describes the additional requirements for the Swiss EPR of the Provide Document Bundle [ITI-65] transaction defined in the MHD profile published in the IHE ITI Trial Implementation “Mobile Access to Health Documents”.

3.5.1 Scope

In the Swiss EPR the transaction is used by the MHD Document Source to store documents in the EPR.

3.5.2 Actor Case Roles

Actor: Document Source

Role: Sends documents and metadata to the Document Recipient

Actor: Document Recipient

Role: Accepts the document and metadata sent from the Document Source.

3.5.3 Referenced Standards

Mobile access to Health Documents (MHD), Rev. 4.0.2 – November 8, 2021

This MHD profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.5.4 Messages

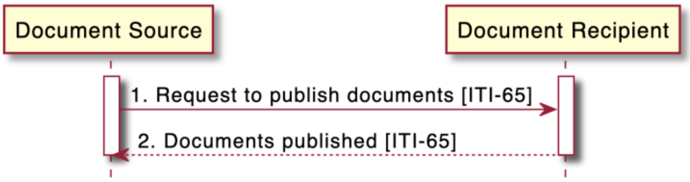
Document Source
Document Recipient
1. Request to publish documents [ITI-65]
2. Documents published [ITI-65]

Figure 6: Interaction diagram for [ITI-65]

3.5.5 Trigger Events

This method is invoked when the Document Source needs to submit one or more documents to a Document Recipient.

3.5.6 Message Semantics

The same message semantics as for 2:3.65.4.1.2 Message Semantics applies. The FHIR Bundle.meta.profile shall have the following value:

http://profiles.ihe.net/ITI/MHD/StructureDefinition/IHE.MHD.Comprehensive.ProvideBundle

The additional Swiss EPR metadata is defined with:

- DeletionStatus (Annex 5.1 1.2.4.1)
- SubmissionSet.Author.AuthorRole (Annex 5.1 1.2.4.3)
- DocumentEntry.originalProviderRole (Annex 5.1 1.2.4.4)

3.5.6.1 DeletionStatus

The optional metadata about the DeletionStatus of the document is represented in the DocumentReference using the extension with the URL http://fhir.ch/ig/ch-epr-mhealth/StructureDefinition/ch-ext-deletionstatus. The values are defined in the ValueSet ch-ehealth-valueset-deletionstatus.

3.5.6.2 SubmissionSet.Author.AuthorRole

The SubmissionSet.Author element MAY be used to track the user who made the latest changes to the document metadata. If present, the value of the AuthorRole attribute SHALL be taken from the SubmissionSet.Author.AuthorRole value set with the OID 2.16.756.5.30.1.127.3.10.1.41. The required metadata about the AuthorRole of the Author is represented in the List for the SubmissionSet using the extension with the URL http://fhir.ch/ig/ch-epr-mhealth/StructureDefinition/ch-ext-author-authorrole. The values are defined in the ValueSet SubmissionSet.Author.AuthorRole.

3.5.6.3 DocumentEntry.originalProviderRole

An extra metadata attribute SHALL be used to distinguish document originally provided by patients or their representatives from documents originally provided by healthcare professionals, assistants, technical users or document administrators. The extra metadata attribute SHALL be set by the Document Source actor to the role value of the current user and SHALL NOT be updated by Update Initiator or Document Administrator actors. The required metadata about the originalProviderRole of the Author is represented in the Document Reference using the extension with the URL http://fhir.ch/ig/ch-epr-mhealth/StructureDefinition/ch-ext-author-authorrole. The values are defined in the ValueSet DocumentEntry.originalProviderRole.

3.5.7 Message Example

Examples

3.5.8 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Document Recipient using the IUA profile with extended access token as decribed in Section 3.2. Consequently the Provide Document Bundle [ITI-65] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.6 MHD: Find Document Lists [ITI-66]

There are no additional requirements for the Swiss EPR of the Find Document Lists [ITI-66] transaction defined in the MHD profile published in the IHE ITI Trial Implementation “Mobile Access to Health Documents”. The SubmissionSet.Author.AuthorRole mapping to DocumentManifest has to be supported. The Document Responder does not need to support the FindFolders Query from the XDS on FHIR Option.

3.6.1 Scope

The Find Document Lists [ITI-66] transaction is used to find List Resources that satisfy a set of parameters. It is equivalent to the FindSubmissionSets query in the Registry Stored Query [ITI-18] transaction, as documented in ITI TF-2: 3.18.4.1.2.3.7.2. The result of the query is a Bundle containing List Resources that match the query parameters.

3.6.2 Actor Roles

Actor: Document Consumer

Role: Requests List Resources, matching the supplied set of criteria, from the Document Responder

Actor: Document Responder

Role: Returns List Resources that match the search criteria provided by the Document Consumer,

3.6.3 Referenced Standards

Mobile access to Health Documents (MHD), Rev. 4.0.2 – November 8, 2021

This MHD profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.6.4 Messages

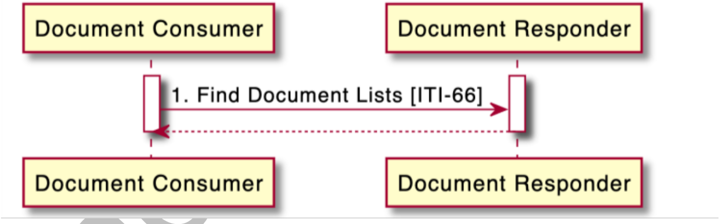

Figure 7 Interaction diagram for [ITI-66]

3.6.5 Trigger Events

When the Document Consumer needs to discover List Resources matching various metadata parameters it issues a Find Document Lists message.

3.6.6 Message Example

Examples

3.6.7 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Document Responder using the IUA profile with extended access token as decribed in Section 3.2. Consequently the Find Document Lists [ITI-66] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.7 MHD: Find Document References [ITI-67]

There are no additional requirements for the Swiss EPR extension of the Find Document References [ITI-67] transaction defined in the MHD profile published in the IHE ITI Trial Implementation “Mobile Access to Health Documents”.

3.7.1 Scope

The Find Document References transaction is used to find DocumentReference Resources that satisfy a set of parameters. It is equivalent to the FindDocuments and FindDocumentsByReferenceId queries from the Registry Stored Query [ITI-18] transaction. The result of the query is a FHIR Bundle containing Document Reference Resources that match the query parameters.

3.7.2 Actor Roles

Actor: Document Consumer

Role: Requests a list of DocumentReference Resources, matching the supplied set of criteria, from the Document Responder.

Actor: Document Responder

Role: Returns DocumentReference Resources that match the search criteria provided by the Document Consumer.

3.7.3 Referenced Standards

Mobile access to Health Documents (MHD), Rev. 4.0.2 – November 8, 2021

This MHD profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.7.4 Messages

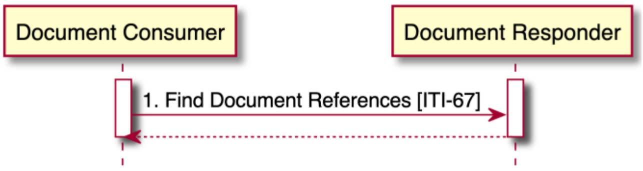

Figure 8 Interaction diagram for [ITI-67]

3.7.5 Trigger Events

When the Document Consumer needs to discover DocumentReference Resources matching various metadata parameters, it issues a Find Document References message.

3.7.6 Message Example

Examples

3.7.7 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Document Responder using the IUA profile with extended access token as decribed in Section 3.2. Consequently the Find Document References [ITI-67] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.8 MHD: Retrieve Document [ITI-68]

There are no additional requirements for the Swiss EPR extension of the Retrieve Document [ITI-68] transaction defined in the MHD profile which is published in the IHE ITI Trial Implementation “Mobile Access to Health Documents”.

3.8.1 Actor Roles

Actor: Document Consumer

Role: Requests a document from the Document Responder.

Actor: Document Responder

Role: Serves the document to the Document Consumer.

3.8.2 Referenced Standards

Mobile access to Health Documents (MHD), Rev. 4.0.2 – November 8, 2021

This MHD profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.8.3 Messages

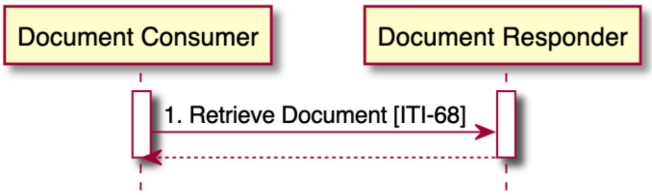

Figure 9 Interaction diagram for [ITI-68]

3.8.4 Trigger Events

The Document Consumer wants to obtain a document.

3.8.5 Message Semantics

The Document Consumer sends a HTTP GET request to the server.

3.8.6 Security Consideration

TLS SHALL be used. This national extension enforces authentication and authorization of access to the Document Responder using the IUA profile with extended access token as decribed in Section 3.2. Consequently the Retrieve Document [ITI-68] request must authorize using the Incorporate Access Token [ITI-72] transaction of the IUA profile.

3.9 RESTful ATNA: Send Audit Resource Request Message – RESTful interaction [ITI-20]

This section describes the national extension for the Swiss EPR of the Send Audit Resource Request Message – RESTful interaction [ITI-20] transaction defined in the RESTful ATNA profile which is currently prepared as IHE Trial Implementation with the working title ”Add RESTful ATNA (Query and Feed)”.

3.9.1 Referenced Standards

Add RESTful ATNA (Query and Feed), Rev. 3.3 – Trial Implementation, July 2, 2021

This RESTful ATNA profile is based on Release 4 of the emerging HL7® FHIR® standard.

3.9.2 Messages

The “Send Audit Resource Request Message – FHIR Feed Interaction” is used for auditing the FHIR Audit Event Resource using the RESTful protocol.

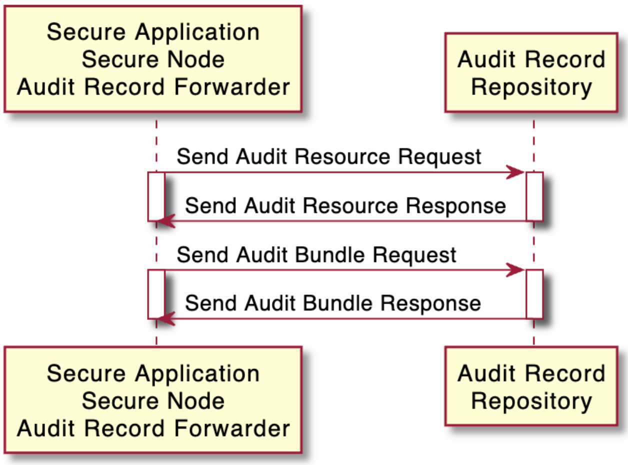

Figure 10: Interaction diagram for FHIR Feed Interaction

3.9.3 Trigger Events

This message is sent when an actor that is grouped with Secure Node or Secure Application or an Audit Record Forwarder needs to post a single or multiple AuditEvent Resource to the Audit Record Repository.

3.9.4 Message Semantics & Expected Actions

Same Message Semantics apply as described in the ITI-20 transaction.

3.9.5 Expected Actions

TLS SHALL be used.

4 Appendix

All examples and conformance profiles can be found in the Implementation guide CH EPR mHealth: http://build.fhir.org/ig/ehealthsuisse/ch-epr-mhealth.

4.1 Appendix A – Extension to XUA Authenticate User

The SMART Application Launch Framework Implementation Guide Release 1.0.0 requires Open ID Connect authentication. Authentication for the Swiss EPR is defined in Annex 8 of the ordinances. This section defines the changes necessary changes. Add Open ID Connect authentication specification for Swiss EPR

4.2 XUA

Currently the national extension E1A5 only supports SAML 2 Assertions for document and policy access (read and write). We need to extend it to also support the SAML option in the IUA Get Access Token transaction for basic access token. At first glance the assertion could look like currently defined assertion, but without the Purpose of Use and the resource ID (EPR-SPID) attributes. This extension is also driven by an open EPR issue to secure the access to the MPI and HPD, which was raised independently.

4.3 Appendix B – Open Issues

See current list of issues on https://github.com/ehealthsuisse/ch-epr-mhealth/issues

4.3.1 IUA: handling of client authentication

How is client authentication is handled with the Authorization Server? Should the token_endpoint_auth_methods be further defined?

4.3.2 IUA: Refresh token handling

Refresh token handling needs to be defined if allowed or not (refresh without authentication possible).

4.3.3 IUA: ihe_saml token option supported for the generic mHealth Option

Open discussion if the ihe_saml token option shall be supported for the generic mHealth Option requesting an ihe_saml token and incorporate it in the MHD transactions.

4.3.4 IUA: ihe-jwt token option handling in XDS environment

If an ihe-jwt token is incorporated in the MHD transactions how can this token be used with the IHE XDS transactions?

4.3.5 MHD extension for RMU

Updating the document with the new DeletionStatus is currently not specified in IHE MHD, this would need a new additional transaction corresponding to the IHE RMU transaction.

4.3.6 RESTful ATNA

Is the described mapping in 3.20.4.2.2.1 Mapping between DICOM Audit Message definitions and FHIR AuditEvent Resource for the FHIR Feed interactions specific enough or do we need additional mappings?

5 Figures

6 Tables