eHealth platform – G19 report
Hub service “getTransaction” – functional description

Version	Date	Description
1.0	30/07/2010	First release hub – metahub system.
1.1	04/10/2018	Proposition BCP - Add ETK via ‘ID-ENCRYPTION-KEY’

Introduction

This document aims to provide the *functional description* of the service ‘getTransaction‘, that should be provided by one hub to other hubs.

The description is limited to functional elements: purpose, business XML messages. Pragmatic considerations such as security and WSDL descriptions are out-of-scope of this document. The description does not include the overall usage conditions to be implemented by the hubs (e.g. regarding the legal aspects).

This document is a part of KMEHR specification. (***https://www.ehealth.fgov.be/standards/kmehr/*** *)*.

We first provide a ‘functional description’ of the service (purpose, input, and output parameters independently of their XML representation …).

We then translate this functional description into a KMEHR service (i.e. we describe the excepted input and output messages)

This document does not contain any XML example. Those examples are available on the KMEHR site.

1. Functional description

Service name	getTransaction
Purpose	This service should be used by a hub to retrieve a transaction (given a transaction identifier) within another hub. This service should be called by a hub only to 'propagate' a request from one of its clients. This service does not allow a hub to retrieve a document outside of the network covered by the target hub.
Input parameters	- the identifier of a transaction (as provided by the target hub in a preliminary 'getTransactionList' exchange) - the owner of T (with at least the hub owner that must be the target hub) - the identifier of a patient P - the sender S of the request, i.e. the hub and the healthcare party that performs the operation call This element also contains the information indicating the encryption end-point (hub or healthcare party) and the information needed to retrieve the Encryption Token Key for this encryption end-point from the eHealth ETK depot (1) - information about the request (id/date/time)
Output parameters	- the initial request - an acknowledge indicating the completion of the request - the encrypted transaction
Usage Conditions (to be checked by the caller hub)	- a national consent exists for P - a therapeutic link exists between S and P - S is allowed to perform the operation (according to the caller rules)
Post-condition	
Possible exceptions	- Technical error - Invalid data • Invalid sender • Invalid transaction identifier • Invalid patient identifier • Invalid transaction owner - Unrecognized sender

[1] See document ''*Système de cryptage end-to-end, Destinaire connu* » or "*Systeem voor end- to-end vercijfering: Bekende bestemmeling*" at ***https://www.ehealth/.fgov.be/ehealthplatform***

	- Owner outside of network - No transaction found with the provided identifier - The transaction T is not associated with P - T is not available for S according to the transaction access rights
Comments	About the “Sender”: the sender must at least identify the organization responsible of the caller system. For this specific operation that is a consultation operation, it should also identify the healthcare party corresponding to the end-user.

2. Message description

2.1 Syntax: XSchema

Operation name	GetTransaction
Input data	request x select
Output data	response x acknowledge x kmehrmessage

2.2 Semantics: rules and interpretation

2.2.1 Input data

The ‘request’ parameter gathers the elements relative to

- the information about the request (id, date, time),
- the sender of the request.

The ‘select’ parameter gathers the elements relative to

- the identifier of the transaction
- the owner of the transaction
- the identifier of the patient

Parameter	**Attributes**		**Comments**
request	id [1]	Identification of the request within the caller system.	
	author [1]	The sender of the request represented as a sequence of *hcparty* elements. It must at least contain the hub requester and the healthcare party corresponding to the sender of the initial request (e.g. hospital).	This information must be coherent with the information provided in the technical identification and authentication system (e.g. SAML token).

		For a specific operation that is a consultation operation, it should also identify the healthcare party corresponding to the end-user.		This element also contains the information indicating the encryption end-point (hub or healthcare party) and the information needed to retrieve the Encryption Token Key for this encryption end-point from the eHealth ETK depot (see below).
	date [1]	Date of request		
	time [1]	Time of request		
select	patient [1]	Identifier of the patient		Must contain the INSS number.
	transaction [1]	id [1]	Local identifier of the transaction	
		author [1]	The owner of the transaction	This field must at least contain the hub owner of the transaction.

Sender encryption elements

The use of the ETK depot requires identifying two concepts:

- the ‘encryption actor’ that corresponds, roughly, to the organization or physical person to which the encrypted data is addressed ,
- the ‘encryption application’ that corresponds, very roughly, to a particular IT system or sub-organization acting for this encryption actor. Encryption application is optional. In this case, it is assumed that there exists at most one token/key for the encryption actor.

Within an HCParty chain, an HCParty is marked as an encryption actor or as an encryption application by using the following elements.

ETK concept	**Hcparty elements**		
Encryption actor	id	Attribute S set to ‘ID-ENCRYPTION-ACTOR’	Identifies the encryption actor within the ETK depot (according to the type of encryption actor)
	id	Attribute S set to ‘ID-ENCRYPTION-KEY’	Allows providing the ETK of the encryption actor, only if no

			encryption application is specified.
	cd	Attribute S set to ‘CD-ENCRYPTION-ACTOR’	Specifies the type of encryption actor within the ETK depot. Allowed values : NIHII, NIHII-HOSPITAL, NIHII-PHARMACY, CBE, SSIN, EHP[1]
Encryption application	id	Attribute S set to ID-ENCRYPTION-APPLICATION This element should be used only with hcparty elements representing applications.	Specifies a particular IT system within the encryption actor identified using the ID-ENCRYPTION-ACTOR and CD-ENCRYPTION-ACTOR schemes. Corresponds with the ApplicationID as used by the ETK Depot service of the eHealth ETEE system.
	id	Attribute S set to ‘ID-ENCRYPTION-KEY’	Allows to provide the ETK of the encryption application

2.2.2 Output data

The ‘response’ parameter gathers the elements relative to the

- information about the response (id, date, time),
- the initial request,
- the sender of the response.

The ‘acknowledge’ parameter gathers the element relative to the

- service completion,
- errors or exceptions that occurred during the service execution (only if the service completion is set to ‘false’).

The ‘kmehrmessage’ parameter corresponds to the payload.The medical content is encrypted at the ‘folder’ level.

[1] Excact value : to be confirmed.

Parameter	Attributes		Comments
response [1]	id [1]	Identifier of the response within the target hub.	
	author [1]	Sender of the response: the target hub and the target hospital	
	date [1]	Date of response	
	time [1]	Time of response	
	request [1]	Initial request	
acknowledge [1]	iscomplete [1]	Indicates if the execution has been successfully completed	The execution is successful if the transaction is returned.
	error [0-*]	Indicates the error/exceptions description	
kmehrmessage [0-1]		The kmehr message that includes the transaction details. This element is defined by the kmehr message standard.	The medical content is encrypted at the 'folder' level.