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 each hub to its clients (hospitals, GP server, etc.).

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 that have 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

This service is particular in the sense that it should be provided by each hub but also by the hospitals (or other organizations taking part, as provider, in a hub).

The interface should be the same for both purposes; however, the usage conditions could differ. We describe here only the service provided by the hub.

Service name	getTransaction
Purpose	This service should be used to retrieve a transaction (given a transaction identifier) within a hub. This service must take into account the overall access rules required for a consultation. This service should support to get transaction within the current hub but also external transaction stored in the others hubs.
Input parameters	- the identifier of a transaction T - the identifier of the hub owner of T (required for an inter-hub consultation) - the identifier of a patient P - the sender S of the request, i.e. the healthcare party that performs the operation call If the caller is the end-point for the encryption mechanism, S contains the elements needed to retrieve its Encryption Token Key from the eHealth ETK depot1 - information about the request (id/date/time)
Output parameters	- the initial request - an acknowledge indicating the completion of the request - the transaction If the caller is the end-point for the encryption mechanism, the medical content is encrypted.
Post-condition	
Possible exceptions	- Technical error - Invalid data - Invalid sender (according to the rules of the hub) - Invalid transaction identifier - Invalid patient identifier - Invalid hub owner

[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***

	- S is not accredited within the hub - S is not allowed to perform the operation according to the hub rules - No consent found of the required type for P - No therapeutic link between S and P - External hub unavailable - No transaction found in the owner hub with the provided identifier - The transaction T is not associated with P - T is not available for S according to the transaction access rights - No valid ETK found
Comments	- About the “Sender”: the sender must at least identify the organization responsible of the caller system. For a specific operation that is a consultation operation, it should also identify the healthcare party corresponding to the end-user. - About external transaction: if the transaction comes from another hub, the verification of the rules that justify the consultation (patient consent, therapeutic link) is under the responsibility of the requestor hub.

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 identifier of the hub owner
- 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 healthcare party corresponding to the organization responsible of the system. For a specific operation that is a consultation operation, it should also identify the healthcare party corresponding to the end-user.		This information must be coherent with the information provided in the technical identification and authentication system (e.g. certificate). If the caller is the end-point for the encryption mechanism, S contains the elements needed to retrieve its Encryption Token Key from the eHealth ETK depot.
	date [1]	Date of request		
	time [1]	Time of request		
select	patient [1]	Patient concerned by the transaction.		Contains only the identifiers of the patient. All interhub exchanges will exclusively rely on the INSS number.
	transaction [1]	id [1]	Local identifier of the transaction.	
		author [0-1]	The owner(s) of the transaction	In interhub exchanges, the field is mandatory and must at least contain the hub owner of the transaction. If the field is not present, the transaction is supposed to belong to the current hub.

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,

[1] Exact value : to be confirmed.

- 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. If the caller is the encryption end-point, the folder of this ‘kmehrmessage’ is encrypted

Parameter	Attributes		Comments
response	id [1]	Identifier of the response within the target hub	The response is supposed to be built by the last hub before the hospital owner. The sender will thus be composed of the hub and hospital owner of the transaction.
	author [1]	Sender of the response	
	date [1]	Date of response	
	time [1]	Time of response	
	request [1]	Initial request	
acknowledge	iscomplete [1]	Indicates if the execution has been successfully completed	The execution is successful if the transaction is returned.
	error [0-*]	Indicates the error/exception descriptions	
kmehrmessage [0-1]		The KMEHR message that includes the transaction details. This element is defined by the KMEHR message standard.	