1056-FAP 901 0481 Uen Rev B

G2 System Requirements

Requirement Specification

ERICSSON

Contents

1 Scope

The scope of this document is to describe different types of requirements that G2-System has to fulfil in order to be allowed and capable of using G1 services. These requirements includes:

- HL7 related requirements – refers to HL7 v3 – HR [1] application roles that have to be implemented in G2 in order to use services offered by G1. These requirements along with HRN ENV 13606 related requirements will in fact constitute G1 interface description,
- HRN ENV 13606 related requirements – refers to requirements that G2 must obey in order to exchange one specific part of information with G1. This is primarily related to patients' medical information,
- Other requirements – refers to all other requirements that is required from G2 in order to be allowed to become PHCIS user.

Any other requirements on G2 (including functionality requirements) that don't originate from G1 is out of the scope of this document.

2 Terminology

2.1 Abbreviations

EHCR	Electronic Health Record
HL7	Health Level 7
HZJZ	Public Health Institution ("Hrvatski Zavod za Javno Zdravstvo")
HZZO	National Health Insurance Company ("Hrvatski Zavod za Zdravstveno Osiguranje")
IS	Information System
PHC	Primary HealthCare
PHCIS	Primary HealthCare Information System
PZZ	Primary HealthCare ("Primarna Zdravstvena Zaštita»)
MPI	Master Patient Index

2.2 Definitions

HRN ENV 13606	Standard defining electronic healthcare record structure and communication
G1 (G1 System)	System used for interconnection of all PHCIS users (GP, Nurse, Paediatrician, Gynaecologist, HZZO, HZJZ) and access PHCIS databases (EHCR)
G2 (G2 Application)	Client end application used by PHC Providers (GP, Nurse, Paediatrician, Gynaecologist) to access PHCIS
G2-System	This is set comprised of G2 Application, hardware (computer) that G2 Application runs on and operating system (OS) installed on aforementioned computer
HL7 v3 - HR	HL7 version 3 with extensions needed for Croatian specific PHC business model (additional health insurance, reports to HZZO…)

2.3 Key words for requirements

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 IETF RFC 2119.

3 G1-G2 interface description

3.1 Introduction

This interface description will comprise list of all HL7 v3 - HR application roles that have to be implemented in G2. In order to get clearer picture appropriate roles required on G1 end will be listed too.

Due to the structure of HL7 v3 message i.e. it's composite nature (Figure 1)

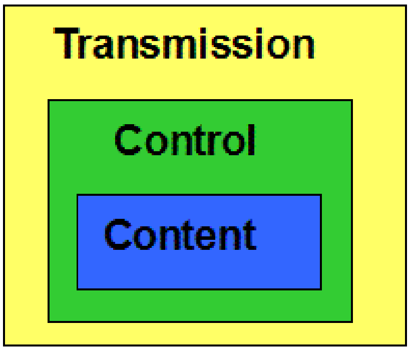

Figure 1 HL7 v3 message structure

there will be two types of roles described in this document:

- HL7 Communication roles – related with an outer "HL7 v3 Transmission wrapper" (see Figure 1)
- Domain specific application roles – related to the message content (Figure 1)

3.2 HL7 communication roles

3.2.1 Notification Message Sender – No Acknowledgements

HL7 v3 – HR ID	MCCI_AR000001
Description	Send HL7 v3 composite message payloads. Require accept-level acknowledgements (see Figure 3).
Implemented in	**G1, G2**

3.2.2 Notification Message Receiver – No Acknowledgements

HL7 v3 – HR ID	MCCI_AR000002
Description	Send HL7 composite message payloads. Expects no acknowledgement messages. (see Figure 3).
Implemented in	**G1**

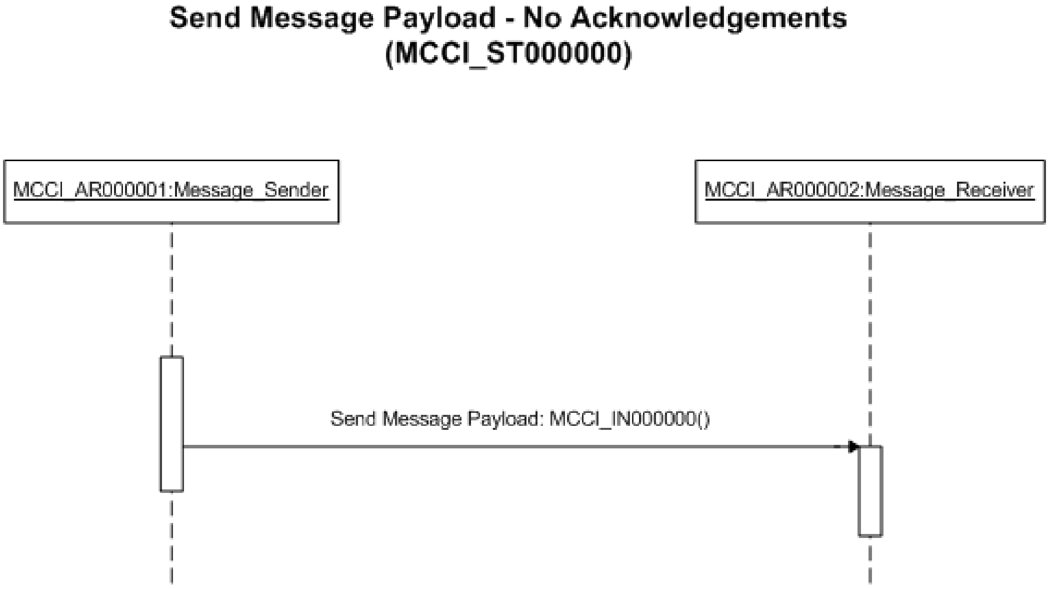
Send Message Payload - No Acknowledgements
(MCCI_ST000000)
MCCI_AR000001:Message_Sender
MCCI_AR000002:Message_Receiver
Send Message Payload: MCCI_IN000000()

Figure 2: Send message payload - no acknowledgement

3.2.3 Notification Message Sender with Accept Acks

HL7 v3 – HR ID	MCCI_AR000003
Description	Send HL7 v3 composite message payloads. Require accept-level acknowledgements (see Figure 3).
Implemented in	**G1, G2**

3.2.4 Notification Message Receiver with Accept Acks

HL7 v3 – HR ID	MCCI_AR000004
Description	Receive HL7 v3 composite message payloads. Send accept-level acknowledgements (see Figure 3).
Implemented in	**G1**

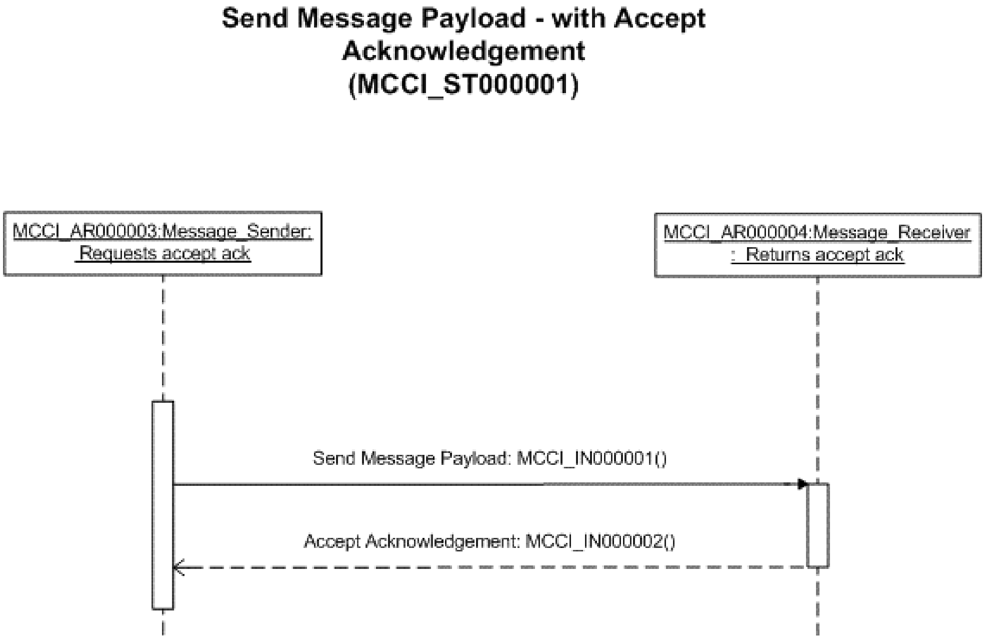
Send Message Payload - with Accept Acknowledgement (MCCI_ST000001)
MCCI_AR000003:Message_Sender: Requests accept ack
MCCI_AR000004:Message_Receiver : Returns accept ack
Send Message Payload: MCCI_IN000001()
Accept Acknowledgement: MCCI_IN000002()

Figure 3 Send message payload - with accept acknowledgement

3.2.5 Request Message Sender with App Acks (Immediate)

HL7 v3 – HR ID	MCCI_AR000005
Description	Send application request HL7 v3 composite message payloads. Require immediate application-level acknowledgements (see Figure 4).
Implemented in	**G2**

3.2.6 Request Message Receiver with App Acks (Immediate)

HL7 v3 – HR ID	MCCI_AR000006
Description	Receive application request HL7 v3 composite message payloads. Send immediate application-level acknowledgements (see Figure 4).
Implemented in	**G1**

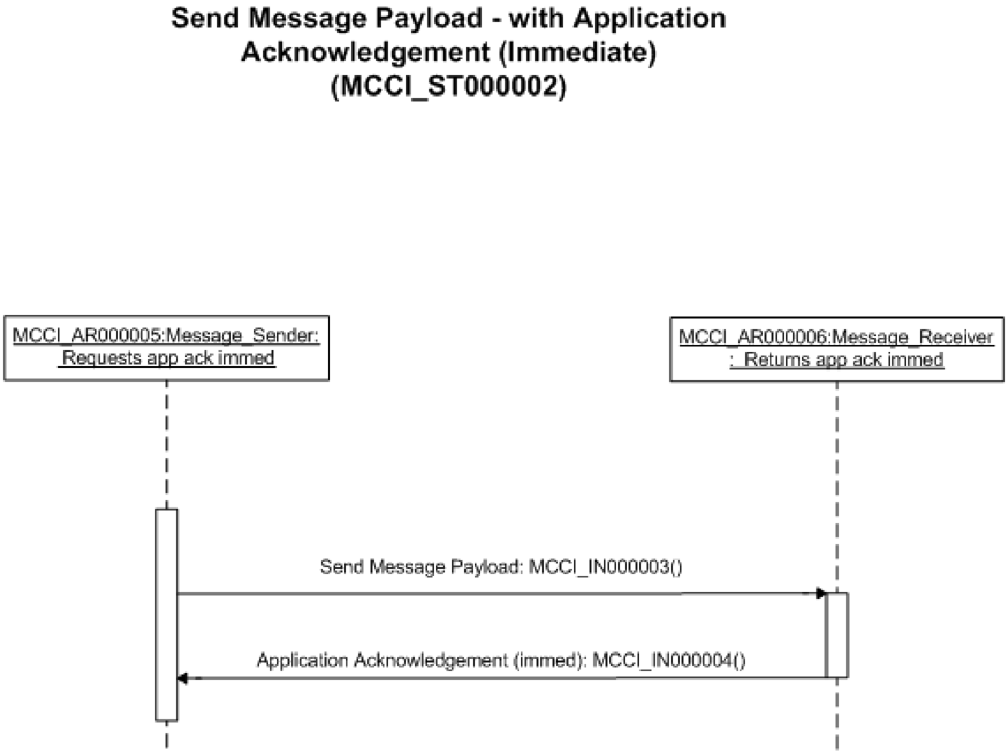
Send Message Payload - with Application Acknowledgement (Immediate) (MCCI_ST000002)
MCCI_AR000005:Message_Sender: Requests app ack immed
MCCI_AR000006:Message_Receiver : Returns app ack immed
Send Message Payload: MCCI_IN000003()
Application Acknowledgement (immed): MCCI_IN000004()

Figure 4 Send message payload - with application acknowledgement (immediate)

3.2.7 Request Message Sender with App Acks (with Accept Acks Deferred)

HL7 v3 – HR ID	MCCI_AR000007
Description	Send application request HL7 v3 composite message payloads. Require deferred application-level acknowledgements with accept-level acknowledgements for initial message sends (see Figure 5).
Implemented in	**G2**

3.2.8 Request Message Receiver with App Acks (with Accept Acks Deferred)

HL7 v3 – HR ID	MCCI_AR000008
Description	Receive application request HL7 v3 composite message payloads. Send deferred application-level acknowledgements. Accept-level acknowledgements required for initial message sends (see Figure 5).
Implemented in	**G1**

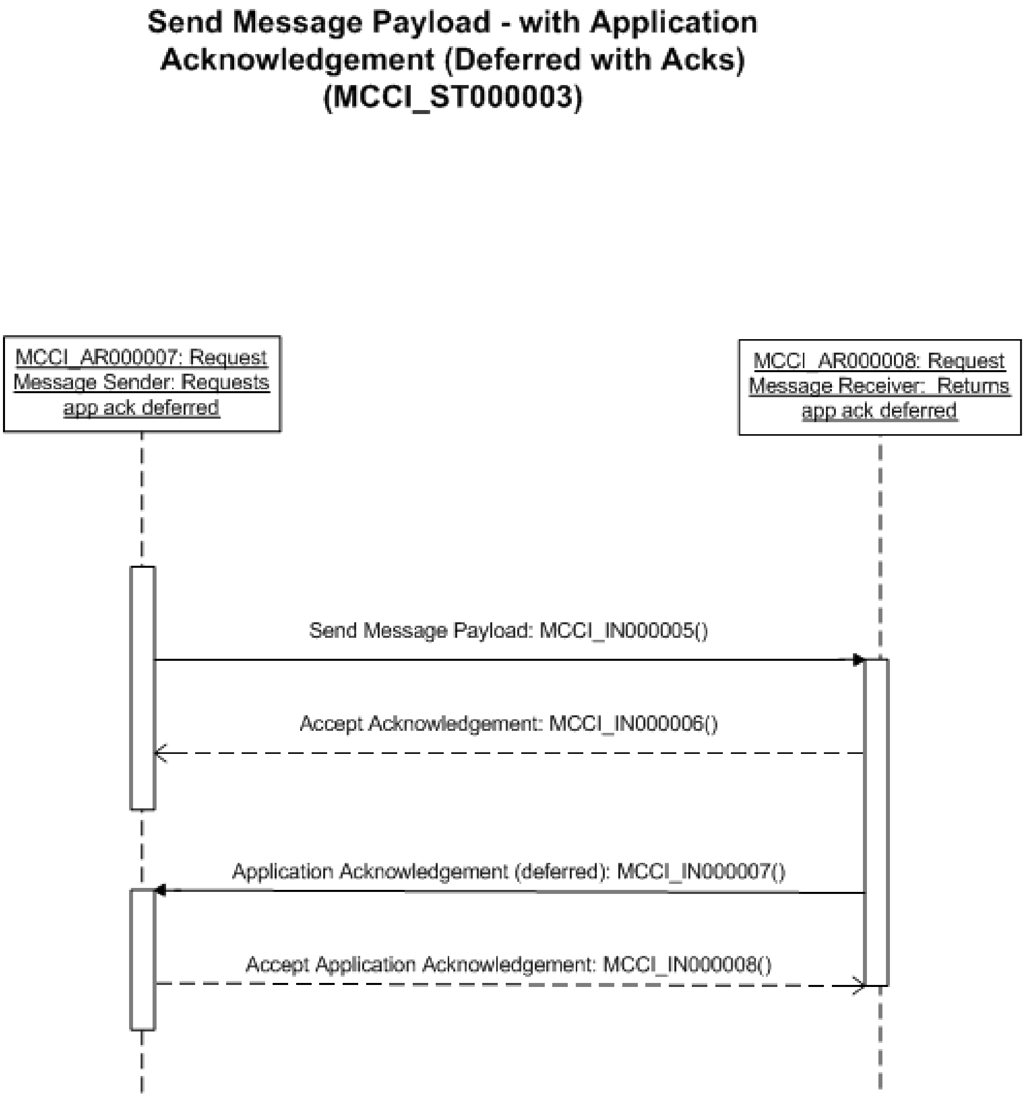
Send Message Payload - with Application Acknowledgement (Deferred with Acks) (MCCI_ST000003)
MCCI_AR000007: Request Message Sender: Requests app ack deferred
MCCI_AR000008: Request Message Receiver: Returns app ack deferred
Send Message Payload: MCCI_IN000005()
Accept Acknowledgement: MCCI_IN000006()
Application Acknowledgement (deferred): MCCI_IN000007()
Accept Application Acknowledgement: MCCI_IN000008()

Figure 5 Send message payload - with application acknowledgement (deffered with acks)

3.2.9 Message Queue Manager

HL7 v3 – HR ID	MCCI_AR100002
Description	Responds to HL7 poll request control message with next HL7 message in queue or a message queue poll error message. Requires an accept-level acknowledgement on all HL7 message payloads sent. May accept an embedded poll for next message in an accept-level message acknowledgement. Does not allow the send of an HL7 message payload that requires a deferred application level response (example interaction on Figure 6).
Implemented in	**G1**

3.2.10 Message Queue Poller

HL7 v3 – HR ID	MCCI_AR100001
Description	Sends HL7 poll request control message to an HL7 message queue manager. Can handle poll message errors returned by remote queue manager. Only able to handle notification HL7 message payloads or message payloads that do not require a deferred application level response (example interaction on Figure 6).
Implemented in	**G2**

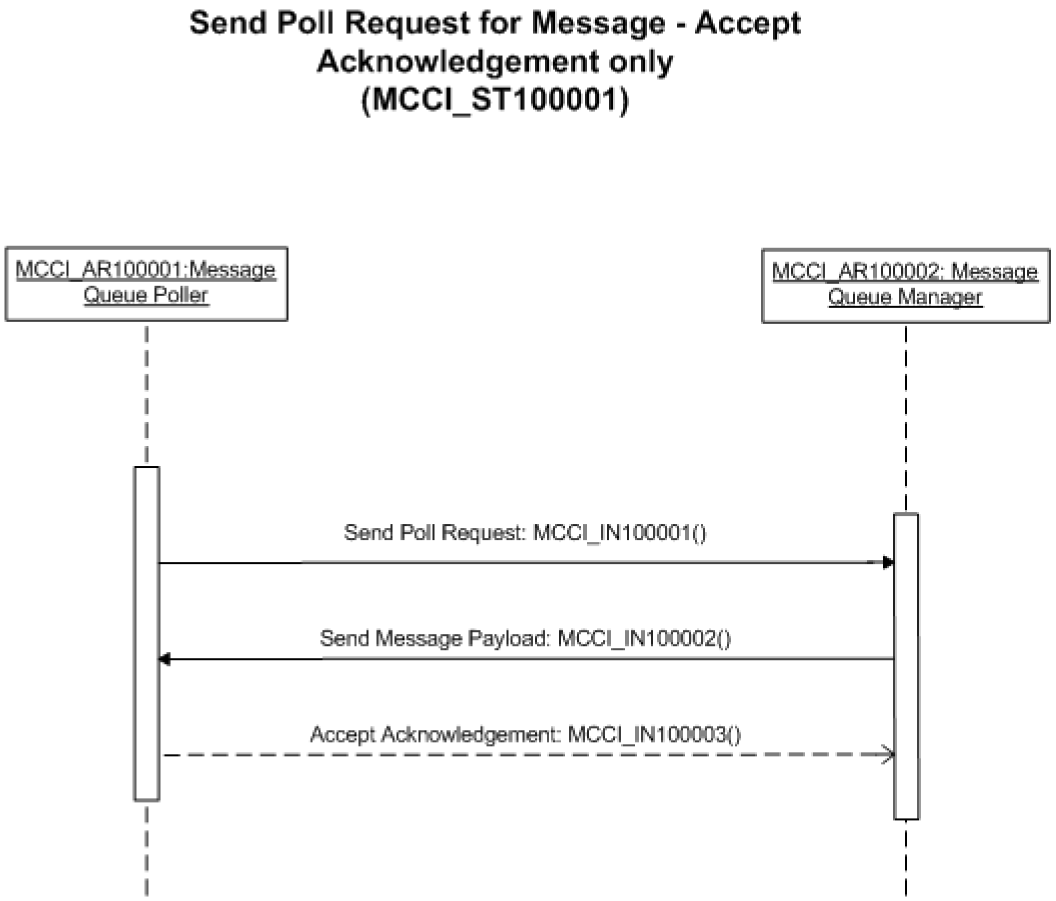
Send Poll Request for Message - Accept Acknowledgement only (MCCI_ST100001)
MCCI_AR100001:Message Queue Poller
MCCI_AR100002: Message Queue Manager
Send Poll Request: MCCI_IN100001()
Send Message Payload: MCCI_IN100002()
Accept Acknowledgement: MCCI_IN100003()

Figure 6 Send Poll Request for Message – Accept Acknowledgement/Poll next

3.2.11 Communication roles placement

Communication role	Implemented on **G1** side	Implemented on **G2** side
Notification Message Sender no Acks (MCCI_AR000001)	YES	YES
Notification Message Receiver no Acks (MCCI_AR000002)	YES	NO
Notification Message Sender with Accept Acks (MCCI_AR000003)	YES	YES
Notification Message Receiver with Accept Acks (MCCI_AR000004)	YES	NO
Request Message Sender with App Acks (Immediate) (MCCI_AR000005)	NO	YES
Request Message Receiver with App Acks (Immediate) (MCCI_AR000006)	YES	NO
Request Message Sender with App Acks (with Accept Acks Deferred) (MCCI_AR000007)	NO	YES
Request Message Receiver with App Acks (with Accept Acks Deferred) (MCCI_AR000008)	YES	NO
Message Queue Manager (MCCI_AR100002)	YES	NO
Message Queue Poller (MCCI_AR100001)	NO	YES

3.3 Domain specific application roles

3.3.1 Eligibility Event Generic Query Placer

HL7 v3 – HR ID	FICR_AR021001
Description	An application responsible for requesting information from public or private healthcare insurers concerning whether a person's insurance coverage is in effect for generic benefits coverage (see Figure 7). The request is for validating whether the patient's insurance policy (coverage) is in effect for a specified date. The response to this query may impact which products or services will be rendered to the patient and who will pay for them.
Implemented in	**G1, G2**

3.3.2 Eligibility Event No Policy Generic Query Placer

HL7 v3 – HR ID	FICR_AR022001
Description	An application responsible for requesting information from public or private healthcare insurers concerning whether a person's insurance coverage is in effect without the specification of an insurance policy (coverage). This request is for validating whether a patient has general healthcare benefits coverage in effect for a specified date, without the specification of a particular insurance policy (coverage).
Implemented in	**G1, G2**

3.3.3 Eligibility Event Generic Query Fulfiller

HL7 v3 – HR ID	FICR_AR023001
Description	An application that provides information about whether a patient's benefits coverage is in effect (see Figure 7). Typical responses for an Eligibility Request are Yes, the patient's insurance policy is in effect on the specified date or No, the patient does not have insurance coverage on the specified date. This response does not necessarily imply that a specific service or product will be covered for payment. It simply informs the Eligibility Requestor (Provider) that the patient has coverage and is qualified to receive benefits on a specified date. An Authorization Request or Pre-Determination Invoice must be submitted if a Provider is seeking commitment from the Authorization Manager (Payor) for payment of a specific service or product. The Eligibility Requestor (Provider) may use Eligibility Results to determine what services to render and how to collect payment for services.
Implemented in	**G1, (HI_IS)**

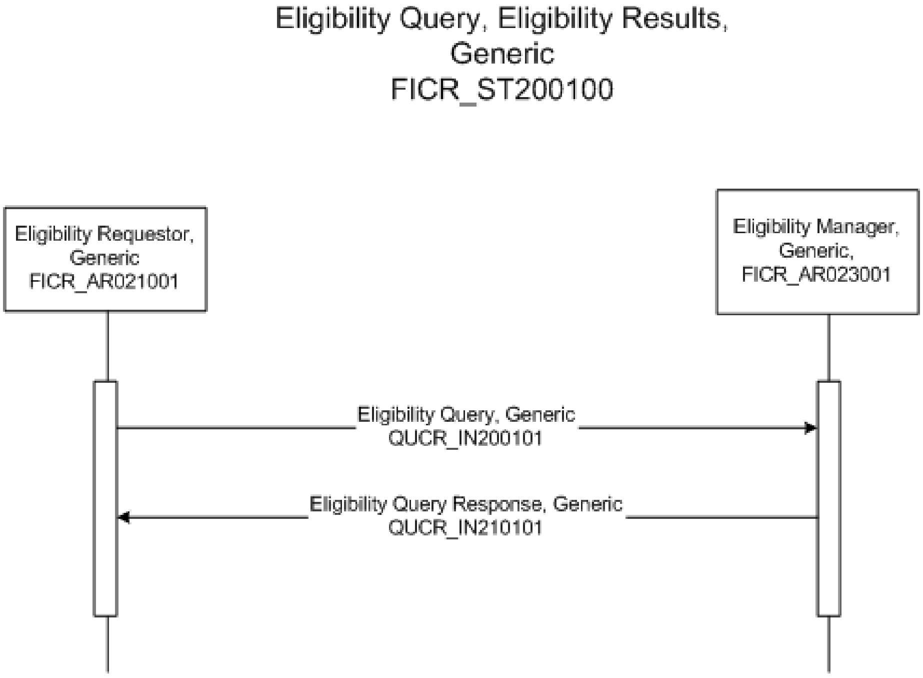
Eligibility Query, Eligibility Results, Generic FICR_ST200100
Eligibility Requestor, Generic FICR_AR021001
Eligibility Manager, Generic, FICR_AR023001
Eligibility Query, Generic QUCR_IN200101
Eligibility Query Response, Generic QUCR_IN210101

Figure 7 Eligibility Query, Eligibility Result, Generic

3.3.4 Medical Record Update Request Placer

HL7 v3 – HR ID	RCMR_AR990001
Description	An application role that is responsible for the submission of new medical data that have to be added to patient medical record (see Figure 8).
Implemented in	**G2**

3.3.5 Medical Record Update Request Fulfiller

HL7 v3 – HR ID	RCMR_AR990002
Description	A Medical Record Update Request Fulfiller processes the request for updating patients medical record and responds to that request (see Figure 8).
Implemented in	**G1**

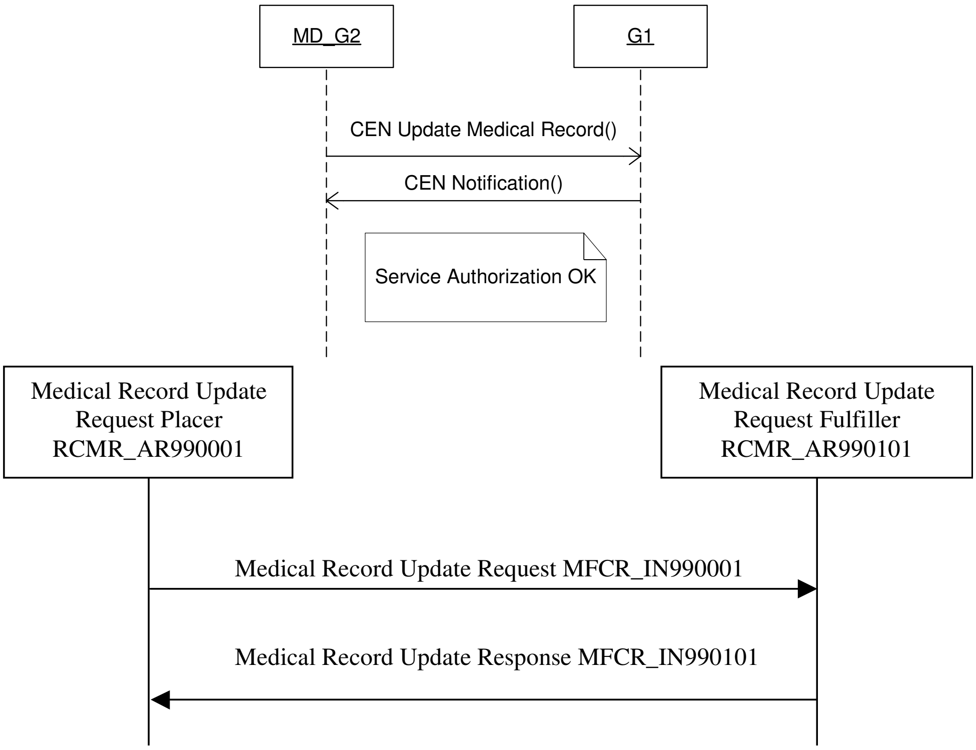
MD_G2
G1
CEN Update Medical Record()
CEN Notification()
Service Authorization OK
Medical Record Update Request Placer RCMR_AR990001
Medical Record Update Request Fulfiller RCMR_AR990101
Medical Record Update Request MFCR_IN990001
Medical Record Update Response MFCR_IN990101

Figure 8 Update Patient Medical Record Sequence Diagram

3.3.6 Medical Record Retrieve Request Placer

HL7 v3 – HR ID	RCMR_AR990003
Description	An application responsible for requesting medical information about particular patient (see Figure 9).
Implemented in	**G2**

3.3.7 Medical Record Retrieve Request Fulfiller

HL7 v3 – HR ID	RCMR_AR990004
Description	An application that provides patients medical data to the requestor (see Figure 9).
Implemented in	**G1**

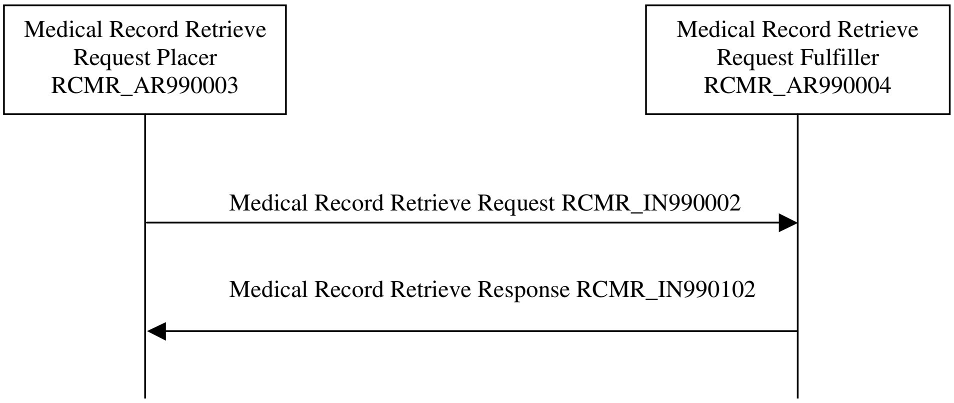

Figure 9 Retrieve Patinet Medical Data Sequece Diagram

3.3.8 Infection Notification Sender

HL7 v3 – HR ID	PORR_AR990001
Description	An application responsible for sending medical and non-medical information regarding infectious diseases (see Figure 10).
Implemented in	**G2**

3.3.9 Infection Notification Receiver

HL7 v3 – HR ID	PORR_AR990002
Description	An application responsible for receiving and processing medical and non-medical information regarding infectious diseases (see Figure 10).
Implemented in	**HZJZ**

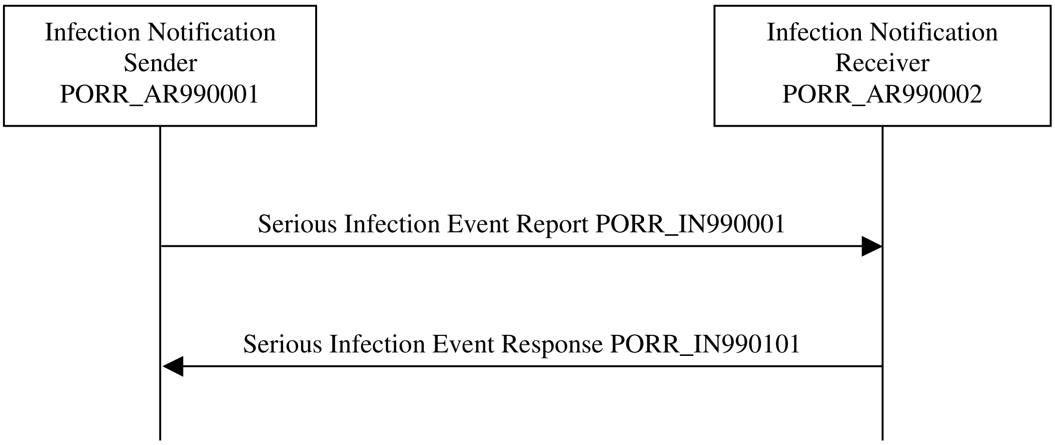
Infection Notification Sender PORR_AR990001
Infection Notification Receiver PORR_AR990002
Serious Infection Event Report PORR_IN990001
Serious Infection Event Response PORR_IN990101

Figure 10 Sending infectious disease observation report to Public Health Institution

3.3.10 Public Health Encounter Report Sender

HL7 v3 – HR ID	PORR_AR990003
Description	An application responsible for sending medical and non-medical information regarding patients encounter (information is collected and formatted for use in Public Health Institution) (see Figure 11).
Implemented in	**G2**

3.3.11 Public Health Encounter Report Receiver

HL7 v3 – HR ID	PORR_AR990004
Description	An application responsible for receiving and processing medical and non-medical information regarding patients encounter (information is collected and formatted for use in Public Health Institution) (see Figure 11).
Implemented in	**HZJZ**

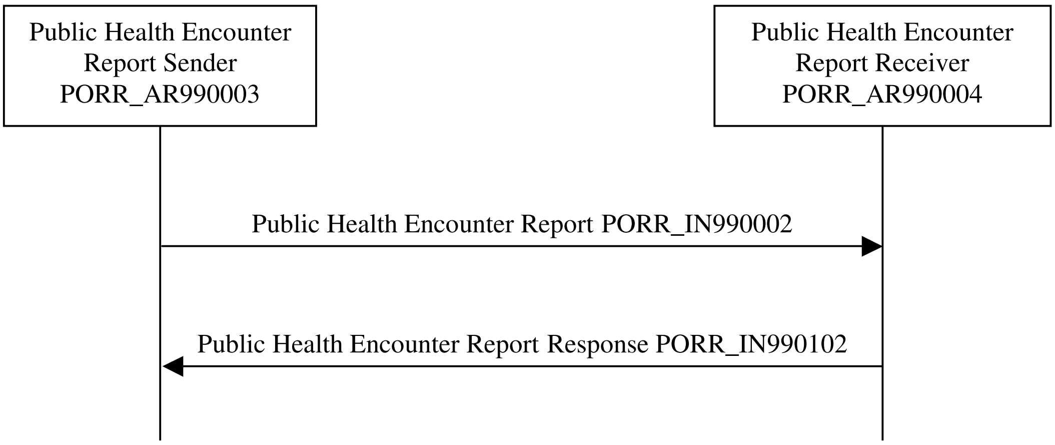
Public Health Encounter Report Sender PORR_AR990003
Public Health Encounter Report Receiver PORR_AR990004
Public Health Encounter Report PORR_IN990002
Public Health Encounter Report Response PORR_IN990102

Figure 11 Sending Public Health Encounter Report to Public Health Institution

3.3.12 Malignous Illness Report Sender

HL7 v3 – HR ID	FICR_AR990005
Description	An application responsible for sending Malignous Illness Report (information is collected and formatted for use in Public Health Institution) (see Figure 12).
Implemented in	**G2**

3.3.13 Malignous Illness Report Receiver

HL7 v3 – HR ID	FICR_AR990006
Description	An application responsible for receiving Malignous Illness Report (see Figure 12).
Implemented in	**HZJZ**

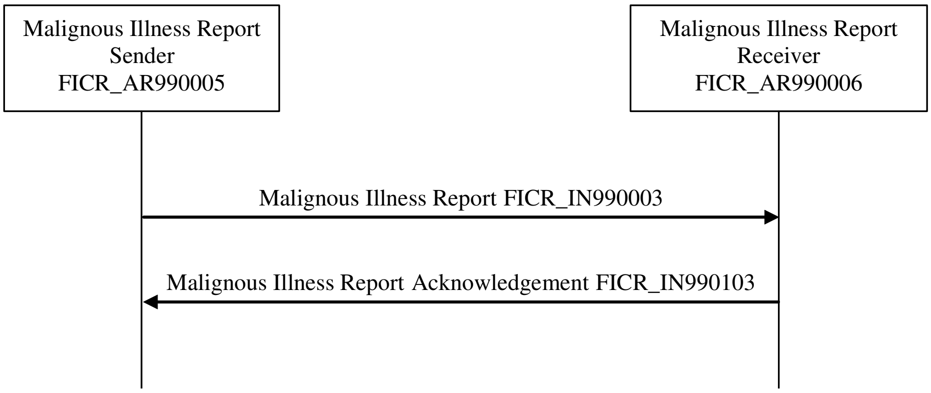
Malignous Illness Report Sender FICR_AR990005
Malignous Illness Report Receiver FICR_AR990006
Malignous Illness Report FICR_IN990003
Malignous Illness Report Acknowledgement FICR_IN990103

Figure 12 Sending Malignous Illness Report to Public Health Institution

3.3.14 Shortened Pompidou Report Sender

HL7 v3 – HR ID	PORR_AR990005
Description	An application responsible for sending Shortened Pompidou Report (information is collected and formatted for use in Public Health Institution) (see Figure 13).
Implemented in	**G2**

3.3.15 Shortened Pompidou Report Receiver

HL7 v3 – HR ID	PORR_AR990105
Description	An application responsible for sending Shortened Pompidou Report (see Figure 13).
Implemented in	**HZJZ**

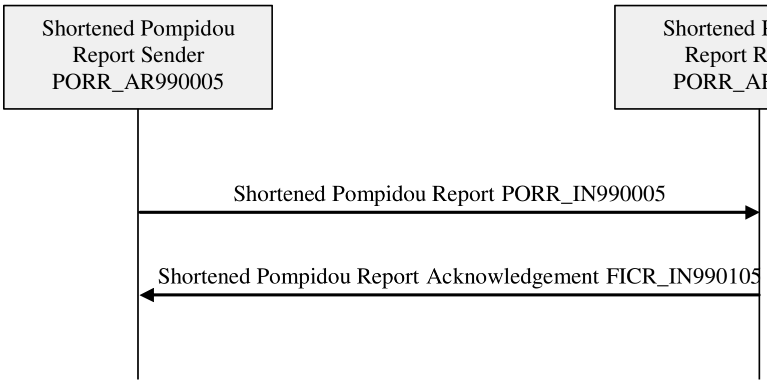
Shortened Pompidou Report Sender PORR_AR990005
Shortened Pompidou Report Receiver PORR_AR990105
Shortened Pompidou Report PORR_IN990005
Shortened Pompidou Report Acknowledgement FICR_IN990105

Figure 13 Sending Shortened Pompidou Report to Public Health Institution

3.3.16 Unwanted Immunization Effect Report Sender

HL7 v3 – HR ID	PORR_AR990006
Description	An application responsible for sending Unwanted Immunization Effect Report (information is collected and formatted for use in Public Health Institution) (see Figure 14).
Implemented in	**G2**

3.3.17 Unwanted Immunization Effect Report Receiver

HL7 v3 – HR ID	PORR_AR990106
Description	An application responsible for sending Unwanted Immunization Effect Report (information is collected and formatted for use in Public Health Institution) (see Figure 14).
Implemented in	**HZJZ**

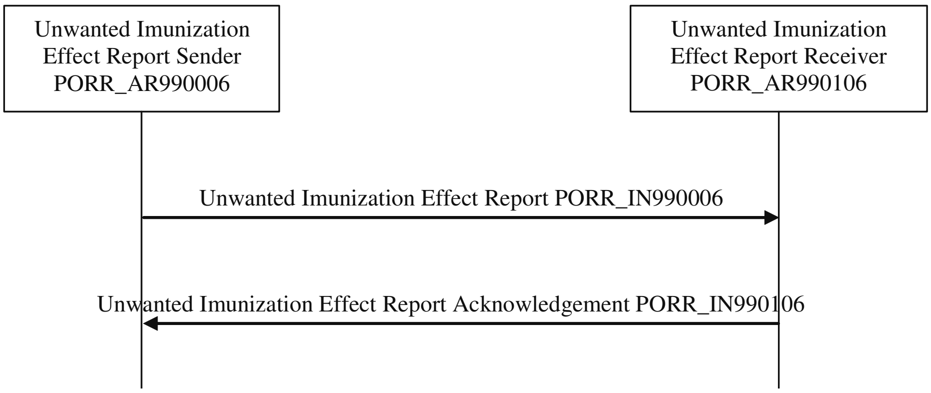
Unwanted Imunization Effect Report Sender PORR_AR990006
Unwanted Imunization Effect Report Receiver PORR_AR990106
Unwanted Imunization Effect Report PORR_IN990006
Unwanted Imunization Effect Report Acknowledgement PORR_IN990106

Figure 14 Sending Shortened Pompidou Report to Public Health Institution

3.3.18 Invoice Sender

HL7 v3 – HR ID	FICR_AR990007
Description	An application responsible for sending invoice regarding patients encounter (information is collected and formatted for use in Health Insurance Companies) (see Figure 15). An Invoice is an itemized list for services (e.g. diagnosis, treatment) or products (e.g. wheelchair, hearing aid) with expected remuneration (fees). Services and/or products may also include adjustments such as taxes, mark-ups, surcharges or discounts.
Implemented in	**G2**

3.3.19 Invoice Receiver

HL7 v3 – HR ID	FICR_AR990008
Description	An application responsible for receiving invoice regarding patients encounter (see Figure 15). An Invoice is an itemized list for services (e.g. diagnosis, treatment) or products (e.g. wheelchair, hearing aid) with expected remuneration (fees). Services and/or products may also include adjustments such as taxes, mark-ups, surcharges or discounts.
Implemented in	**HZZO**

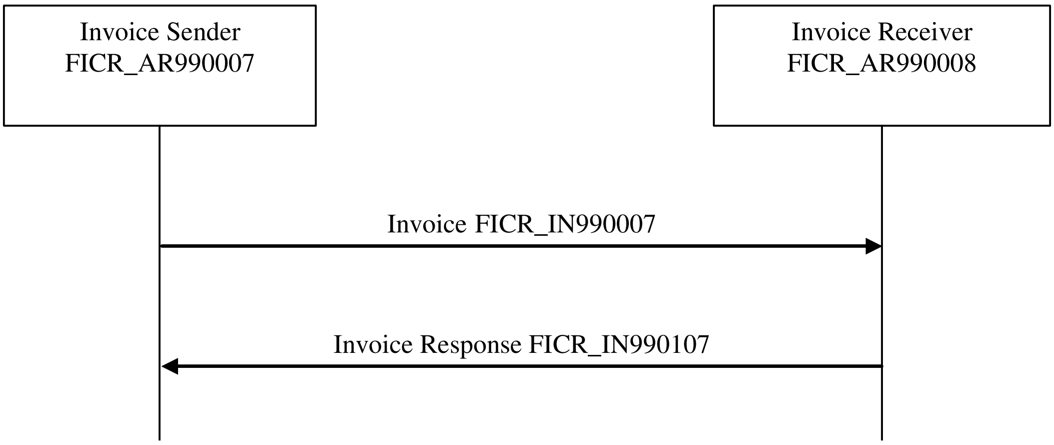

Figure 15 Invoice Adjudication, Final Results, Generic

3.3.20 Person Registry Query Placer

HL7 v3 – HR ID	QUPA_AR101101
Description	A Person Registry Query Placer initiates queries to Person Registries (see Figure 16).
Implemented in	**G2**

3.3.21 Person Registry Query Fulfiller

HL7 v3 – HR ID	QUPA_AR101102
Description	A Person Registry Query Fulfiller responds to queries sent to a Person Registry (see Figure 16).
Implemented in	**G1**

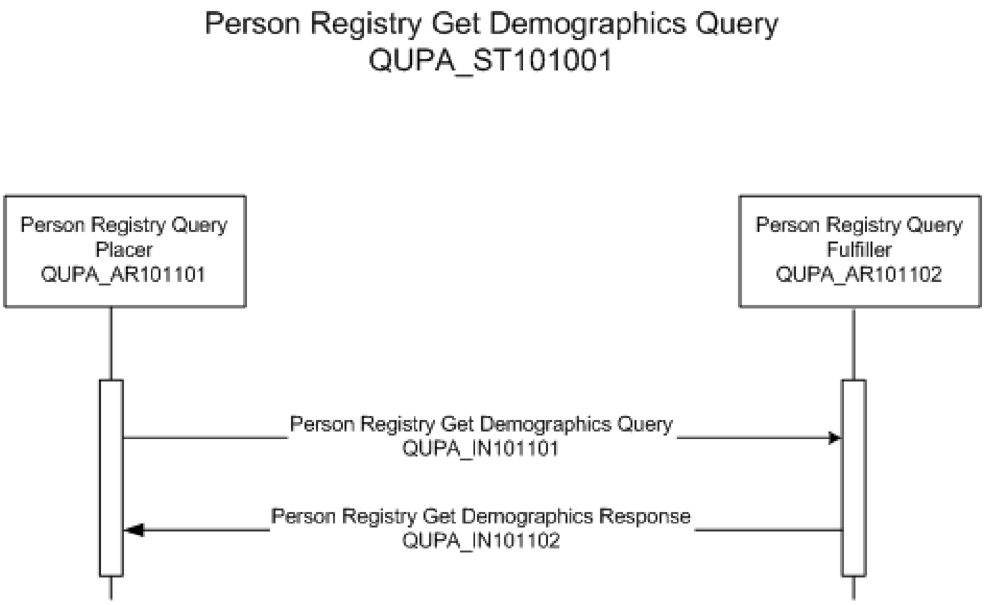
Person Registry Get Demographics Query
QUPA_ST101001
Person Registry Query Placer QUPA_AR101101
Person Registry Query Fulfiller QUPA_AR101102
Person Registry Get Demographics Query QUPA_IN101101
Person Registry Get Demographics Response QUPA_IN101102

Figure 16 Person Registry Get Demographics Query

3.3.22 Patient Care Provision Request Placer

HL7 v3 – HR ID	REPC_AR002030
Description	The application role includes the behaviours needed to create, communicate and appropriately manage a patient care provision request. This includes the ability to transmit patient care provision request, and to receive messages relating to the receiving application's acceptance of the request, management of intent to perform the requested patient care provision (see Figure 17).
Implemented in	**G2**

3.3.23 Patient Care Provision Promise Confirmation Receiver

HL7 v3 – HR ID	REPC_AR003060
Description	An application that is capable of accepting a confirmation from a system that has agreed to perform the actions necessary to deal with a commitment for a patient care provision (see Figure 17).
Implemented in	**G2**

3.3.24 Patient Care Provision Event Tracker

HL7 v3 – HR ID	REPC_AR004020
Description	An application that is capable of receiving a notification from another system about a patient care provision (see Figure 17).
Implemented in	**G2**

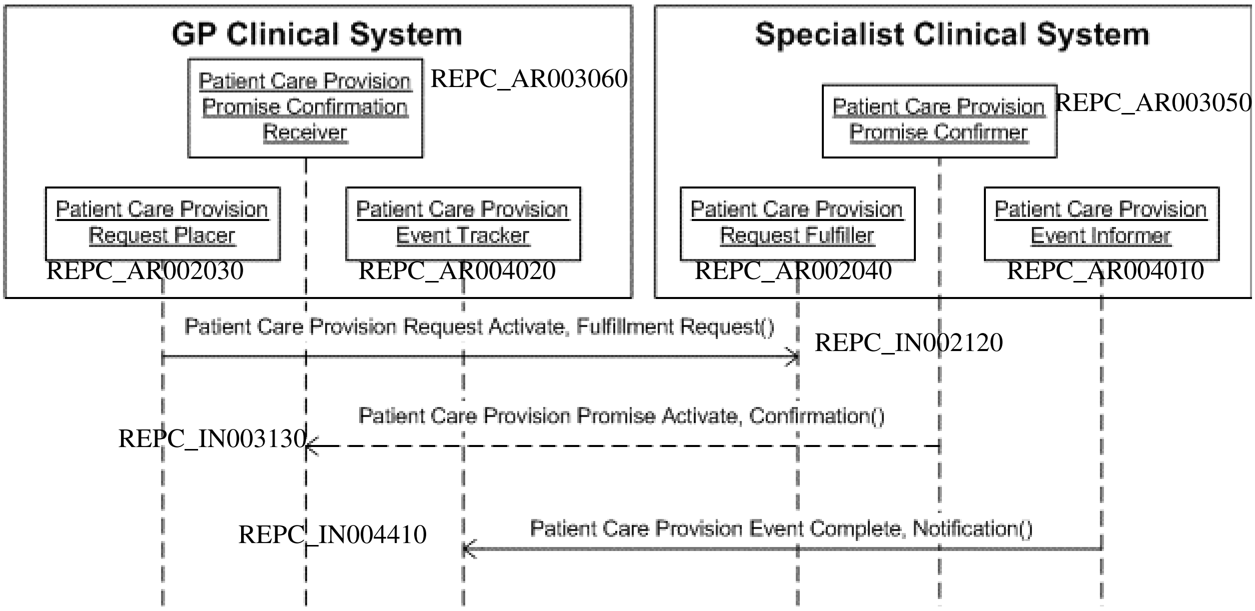
GP Clinical System
Specialist Clinical System
Patient Care Provision Promise Confirmation Receiver
REPC_AR003060
Patient Care Provision Promise Confirmer
REPC_AR003050
Patient Care Provision Request Placer
REPC_AR002030
Patient Care Provision Event Tracker
REPC_AR004020
Patient Care Provision Request Fulfiller
REPC_AR002040
Patient Care Provision Event Informer
REPC_AR004010
Patient Care Provision Request Activate, Fulfillment Request()
REPC_IN002120
Patient Care Provision Promise Activate, Confirmation()
REPC_IN003130
REPC_IN004410
Patient Care Provision Event Complete, Notification()

Figure 17 Deliver HI_Messages (Home Care Proposal)

3.3.25 Patient Care Supervision Request Placer

HL7 v3 – HR ID	REPC_AR002530
Description	The application role includes the behaviours needed to create, communicate and appropriately manage a patient care supervision request. This includes the ability to transmit patient care supervision request, and to receive messages relating to the receiving application's acceptance of the request, management of intent to perform the requested patient care supervision (see Figure 18).
Implemented in	**G2**

3.3.26 Patient Care Supervision Promise Confirmation Receiver

HL7 v3 – HR ID	REPC_AR003560
Description	An application that is capable of accepting a confirmation from a system that has agreed to perform the actions necessary to deal with a commitment for a patient care supervision (see Figure 18).
Implemented in	**G2**

3.3.27 Patient Care Supervision Event Tracker

HL7 v3 – HR ID	REPC_AR004520
Description	An application that is capable of receiving a notification from another system about a patient care supervision (see Figure 18).
Implemented in	**G2**

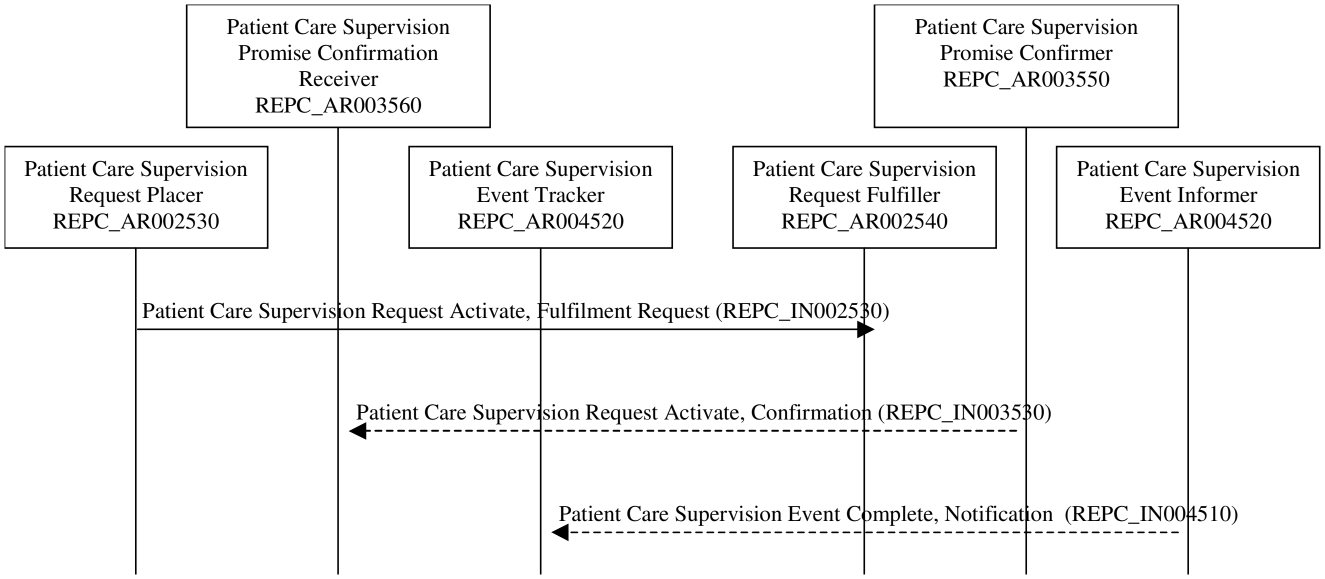
Patient Care Supervision Promise Confirmation Receiver REPC_AR003560
Patient Care Supervision Promise Confirmer REPC_AR003550
Patient Care Supervision Request Placer REPC_AR002530
Patient Care Supervision Event Tracker REPC_AR004520
Patient Care Supervision Request Fulfiller REPC_AR002540
Patient Care Supervision Event Informer REPC_AR004520
Patient Care Supervision Request Activate, Fulfilment Request (REPC_IN002530)
Patient Care Supervision Request Activate, Confirmation (REPC_IN003530)
Patient Care Supervision Event Complete, Notification (REPC_IN004510)

Figure 18 Deliver HI_Messages (Medical Committee Refferal)

3.3.28 Health Insurance Encounter Report Sender

HL7 v3 – HR ID	FICR_AR990001
Description	An application responsible for sending medical and non-medical information regarding patients encounter (information is collected and formatted for use in Health Insurance Companies) (see Figure 19).
Implemented in	**G2**

3.3.29 Health Insurance Encounter Report Receiver

HL7 v3 – HR ID	FICR_AR990002
Description	An application responsible for receiving and processing medical and non-medical information regarding patients encounter (information is collected and formatted for use in Health Insurance Companies) (see Figure 19).
Implemented in	**HZZO**

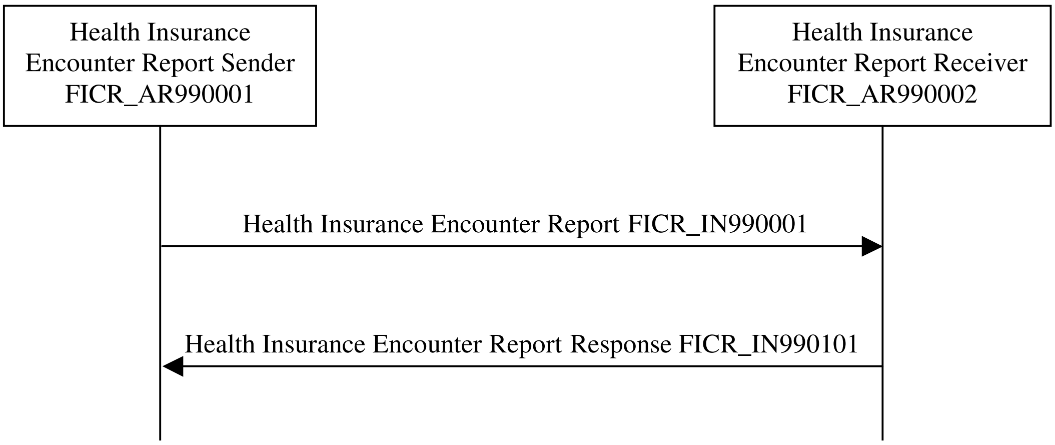
Health Insurance
Encounter Report Sender
FICR_AR990001
Health Insurance
Encounter Report Receiver
FICR_AR990002
Health Insurance Encounter Report FICR_IN990001
Health Insurance Encounter Report Response FICR_IN990101

Figure 19 Deliver HI_Messages (Insurance Company Encounter Report)

3.3.30 Injury and Illness Report Sender

HL7 v3 – HR ID	FICR_AR990003
Description	An application responsible for sending Injury and Illness Report (information is collected and formatted for use in Health Insurance Companies and Public Health Institute) (see Figure 20).
Implemented in	**G2**

3.3.31 Injury and Illness Report Sender

HL7 v3 – HR ID	FICR_AR990004
Description	An application responsible for receiving Injury and Illness Report (see Figure 20).
Implemented in	**G2**

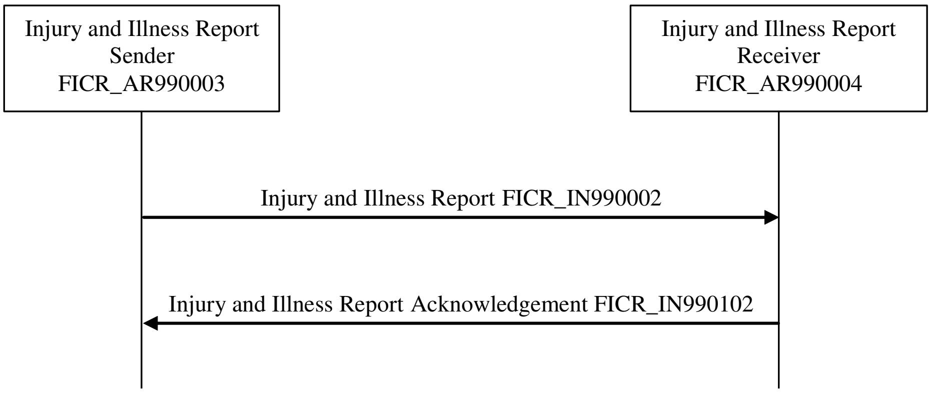
Injury and Illness Report Sender FICR_AR990003
Injury and Illness Report Receiver FICR_AR990004
Injury and Illness Report FICR_IN990002
Injury and Illness Report Acknowledgement FICR_IN990102

Figure 20 Sending Injury and Illness Report

3.3.32 PrescriptionHR Sender

HL7 v3 – HR ID	PORX_AR990001
Description	An application responsible for sending drug prescription (see Figure 21).
Implemented in	**G2**

3.3.33 PrescriptionHR Receiver

HL7 v3 – HR ID	PORX_AR990002
Description	An application responsible for receiving drug prescription (see Figure 21).
Implemented in	**HZZO**

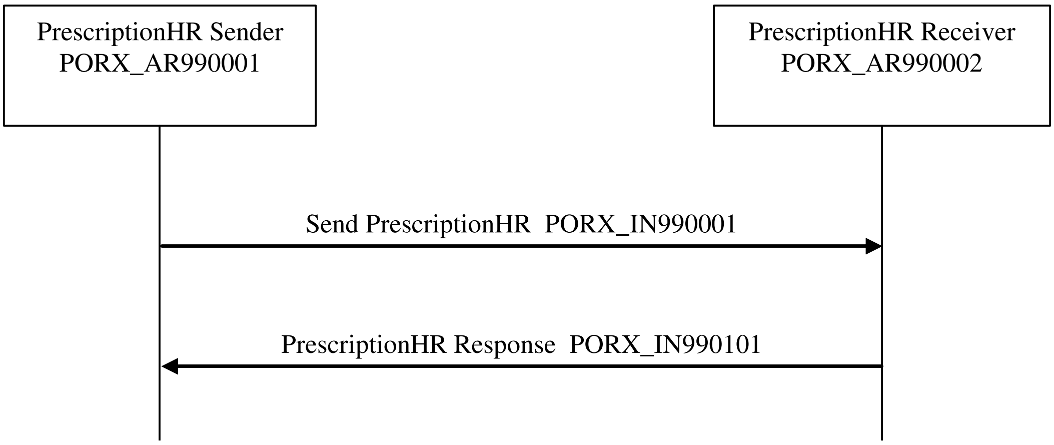
PrescriptionHR Sender
PORX_AR990001
PrescriptionHR Receiver
PORX_AR990002
Send PrescriptionHR PORX_IN990001
PrescriptionHR Response PORX_IN990101

Figure 21 Sending Prescription

3.3.34 PZZReferral Sender

HL7 v3 – HR ID	POLB_AR990001
Description	An application responsible for sending PZZ referral (see Figure 22).
Implemented in	**G2**

3.3.35 PZZReferral Receiver

HL7 v3 – HR ID	POLB_AR990002
Description	An application responsible for receiving PZZ referral (see Figure 22).
Implemented in	**HZZO**

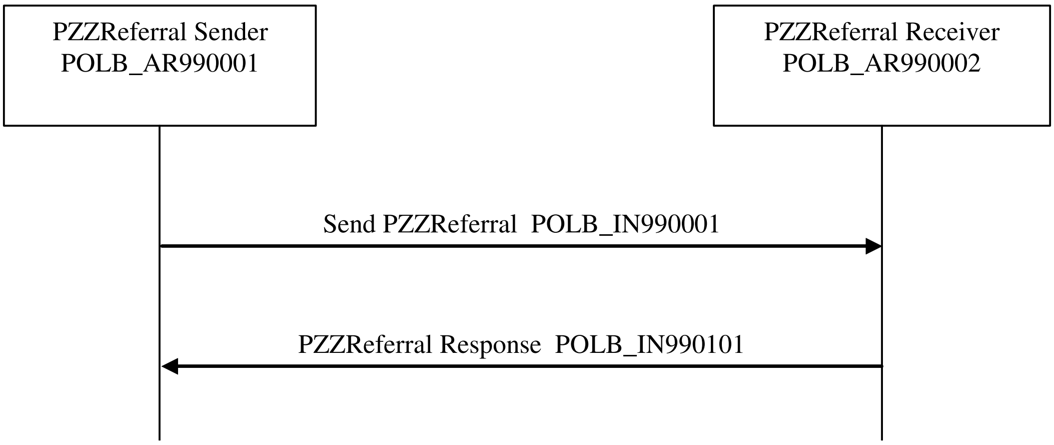
PZZReferral Sender
POLB_AR990001
PZZReferral Receiver
POLB_AR990002
Send PZZReferral POLB_IN990001
PZZReferral Response POLB_IN990101

Figure 22 Sending PZZ Referral

3.3.36 SKZZandHOSReferral Sender

HL7 v3 – HR ID	POLB_AR990003
Description	An application responsible for sending SKZZ and HOS referral (see Figure 23).
Implemented in	**G2**

3.3.37 SKZZandHOSReferral Receiver

HL7 v3 – HR ID	POLB_AR990004
Description	An application responsible for sending SKZZ and HOS referral (see Figure 23).
Implemented in	**HZZO**

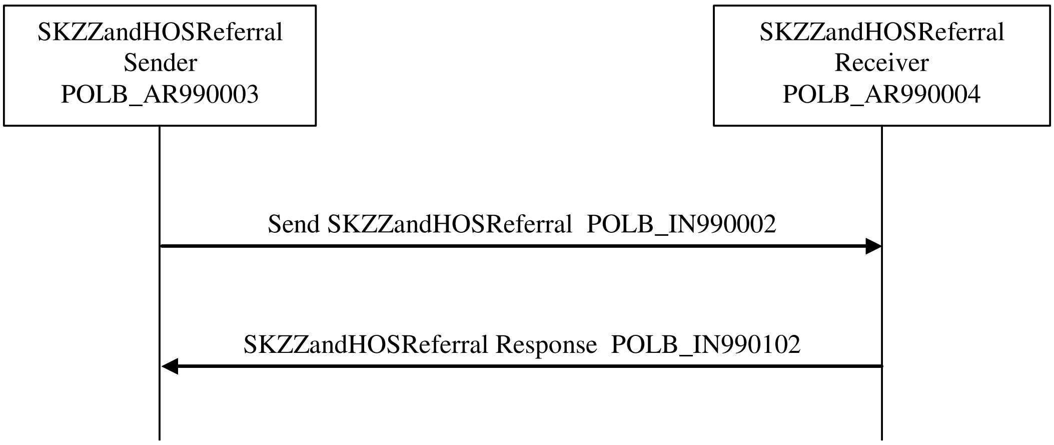
SKZZandHOSReferral
Sender
POLB_AR990003
SKZZandHOSReferral
Receiver
POLB_AR990004
Send SKZZandHOSReferral POLB_IN990002
SKZZandHOSReferral Response POLB_IN990102

Figure 23 Sending SKZZ andHOS referral

3.3.38 Domain specific application roles placement

Application role	Implemented on **G1** side	Implemented on **G2** side	Implemented on **HZZO** side	Implemented on **HZJZ** side
Eligibility Event Generic Query Placer (FICR_AR021001)	YES	YES	NO	NO
Eligibility Event No Policy Generic Query Placer (FICR_AR022001)	YES	YES	NO	NO
Eligibility Event Generic Query Fulfiller (FICR_AR023001)	YES	NO	YES	NO
Medical Record Update Request Placer (RCMR_AR990001)	NO	YES	NO	NO
Medical Record Update Request Fulfiller (RCMR_AR990002)	YES	NO	NO	NO
Medical Record Retrieve Request Placer (RCMR_AR990003)	NO	YES	NO	NO
Medical Record Retrieve Request Fulfiller (RCMR_AR990004)	YES	NO	NO	NO
Infection Notification Sender (PORR_AR990001)	NO	YES	NO	NO
Infection Notification Receiver (PORR_AR990002)	NO	YES	NO	YES
Public Health Encounter Report Sender (PORR_AR990003)	NO	YES	NO	NO
Public Health Encounter Report Receiver (PORR_AR990004)	NO	NO	NO	YES
Malignous Illness Report Sender (FICRR_AR990005)	NO	YES	NO	NO
Malignous Illness Report Receiver (FICR_AR990006)	NO	NO	NO	YES
Shortened Pompidou Report Sender (PORR_AR990005)	NO	YES	NO	NO
Shortened Pompidou Report Receiver (PORR_AR990105)	NO	NO	NO	YES
Unwanted Immunization Effect Report Sender (PORR_AR990006)	NO	YES	NO	NO

Unwanted Immunization Effect Report Receiver (PORR_AR990106)	NO	NO	NO	YES
Person Registry Query Placer (QUPA_AR101101)	NO	YES	NO	NO
Person Registry Query Fulfiller (QUPA_AR101102)	YES	NO	NO	NO
Patient Care Provision Request Placer(REPC_AR002030)	NO	YES	NO	NO
Patient Care Provision Promise Confirmation Receiver (REPC_AR003060)	NO	YES	YES	NO
Patient Care Provision Event Tracker (REPC_AR004020)	NO	YES	YES	NO
Patient Care Supervision Request Placer (REPC_AR002030)	NO	YES	NO	NO
Patient Care Supervision Promise Confirmation Receiver (REPC_AR003060)	NO	YES	YES	NO
Patient Care Supervision Event Tracker (REPC_AR004020)	NO	YES	YES	NO
Health Insurance Encounter Report Sender (FICR_AR990001)	NO	YES	NO	NO
Health Insurance Encounter Report Receiver (FICR_AR990002)	NO	NO	YES	NO
Injury and Illness Report Sender (FICR_AR990003)	NO	YES	NO	NO
Injury and Illness Report Receiver (FICR_AR990004)	NO	NO	YES	YES
Invoice Sender (FICR_AR990007)	NO	YES	NO	NO
Invoice Receiver (FICR_AR990008)	NO	NO	YES	NO
PrescriptionHR Sender (PORX_AR990001)	NO	YES	NO	NO
PrescriptionHR Receiver (PORX_AR990002)	NO	NO	YES	NO
PZZReferral Sender (POLB_AR990001)	NO	YES	NO	NO
PZZReferral Receiver (POLB_AR990002)	NO	NO	YES	NO

SKZZandHOSReferral Sender (POLB_AR990003)	NO	YES	NO	NO
SKZZandHOSReferral Receiver (POLB_AR990004)	NO	NO	YES	NO

4 Additional requirements on G2

4.1 Requirements regarding smart cards

4.1.1 Application start

Requirement ID	
Description	The first thing that G2 application must do upon starting, is acquire work permission (by performing Acquire Work Permission Use case). No communication of any other kind with G1 is allowed prior successful execution of this use case.

4.1.2 Smart card unplug

Requirement ID	
Description	G2 application is allowed to work only if users smart card is plugged into card reader. In case of unplugging smart card, G2 application has to be terminated.

4.2 Requirements regarding communication with *G1_IS*

The communication between *G2_Application* and *G1_IS* is performed via Web Services and HL7/CEN service request messages.

On the Web Services layer there are three types of Web Services methods responsible for communication with *G2_Application*s. First type of Web Service methods is synchronous methods that return response immediately. Second type is asynchronous that returns response deferred by invoking Web Service method exposed by *G2_Application*. Third type of Web Service methods is asynchronous methods that stores response messages to message queue and *G2_Application* invokes polling Web Service to poll response message from that message queue.

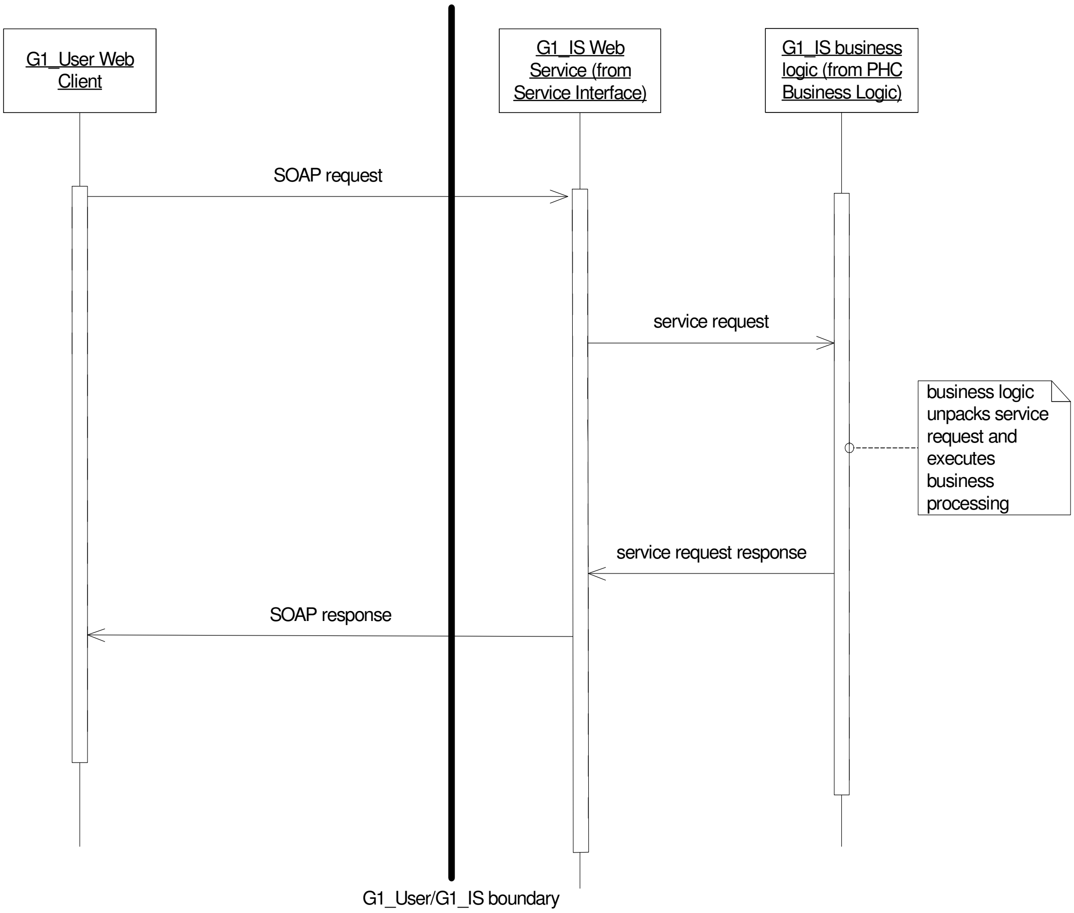
G1_User Web Client
G1_IS Web Service (from Service Interface)
G1_IS business logic (from PHC Business Logic)
SOAP request
service request
business logic unpacks service request and executes business processing
service request response
SOAP response
G1_User/G1_IS boundary

Figure 24 - Web Services Communication between G1_IS and G1_User Applications (synchronous)

Asynchronous service request-response is realized using following two mechanisms:

- If *G1_User* exposes Web Service then *G1_IS* accepts service request and immediately returns accept acknowledge while response to service request is returned to *G1_User* by sending message to its Web Service (Figure 25).

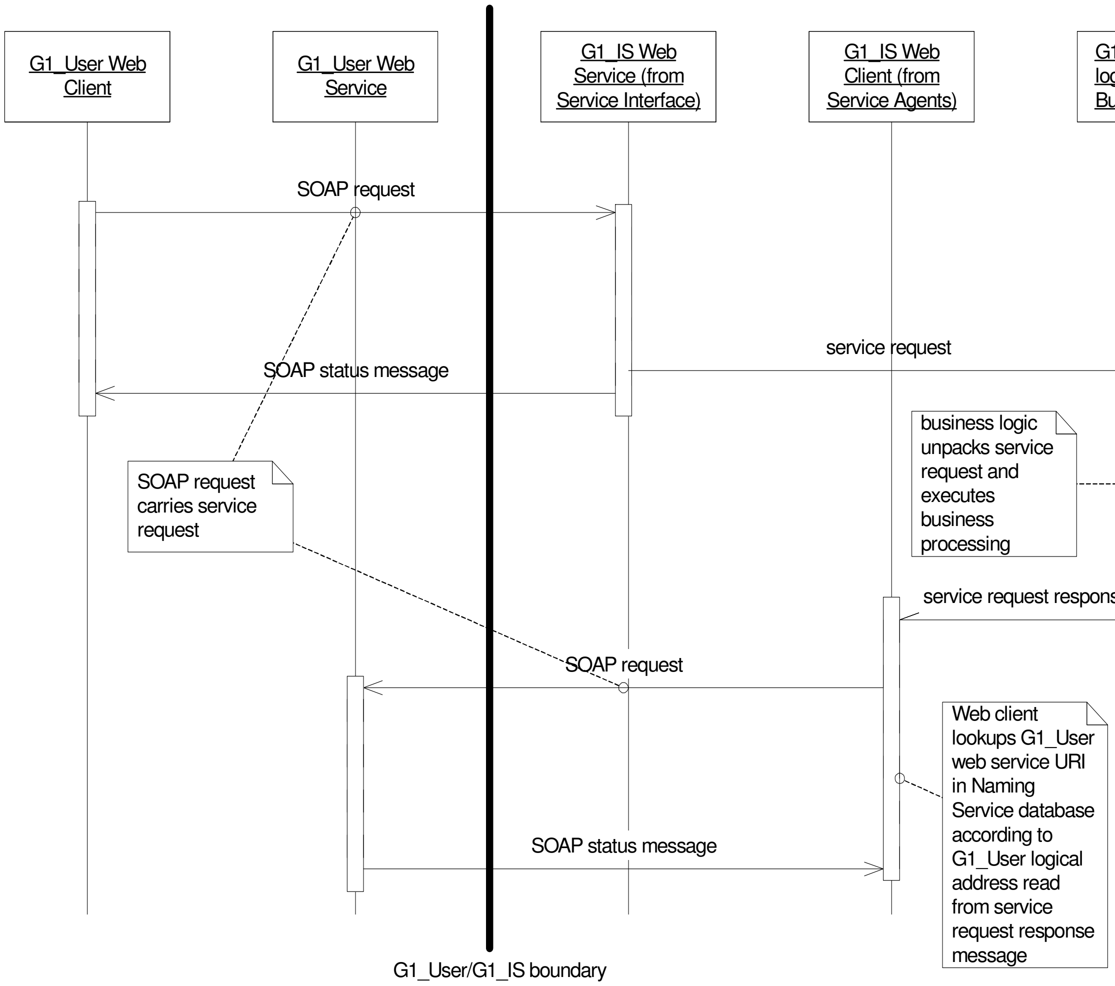
G1_User Web Client
G1_User Web Service
G1_IS Web Service (from Service Interface)
G1_IS Web Client (from Service Agents)
G1_IS business logic (from PHC Business Logic)
SOAP request
service request
SOAP status message
business logic unpacks service request and executes business processing
SOAP request carries service request
service request response
SOAP request
Web client lookups G1_User web service URI in Naming Service database according to G1_User logical address read from service request response message
SOAP status message
G1_User/G1_IS boundary

Figure 25- Web Services Communication between G1_IS and G1_User Applications (direct Web Service access))

- If *G1_User* does not expose Web Service then it should use polling mechanism for retrieving service request response messages. In this case *G1_IS* accepts service request and immediately responses to client with acknowledge message. After client successfully sends message request to *G1_IS* it sends message poll request that asks *G1_IS* if it has some message for it. If *G1_IS* has message or messages for client it sends one message to client and requires that client acknowledge message. Client acknowledges message reception and requests *G1_IS* to send next message if it has one. This process continues until *G1_IS* sends all messages it has in that moment for that particular client. After client receives all messages from *G1_IS* it sends message poll request to *G1_IS* in some predefined time intervals to check if *G1_IS* has some new messages for that client (Figure 26).

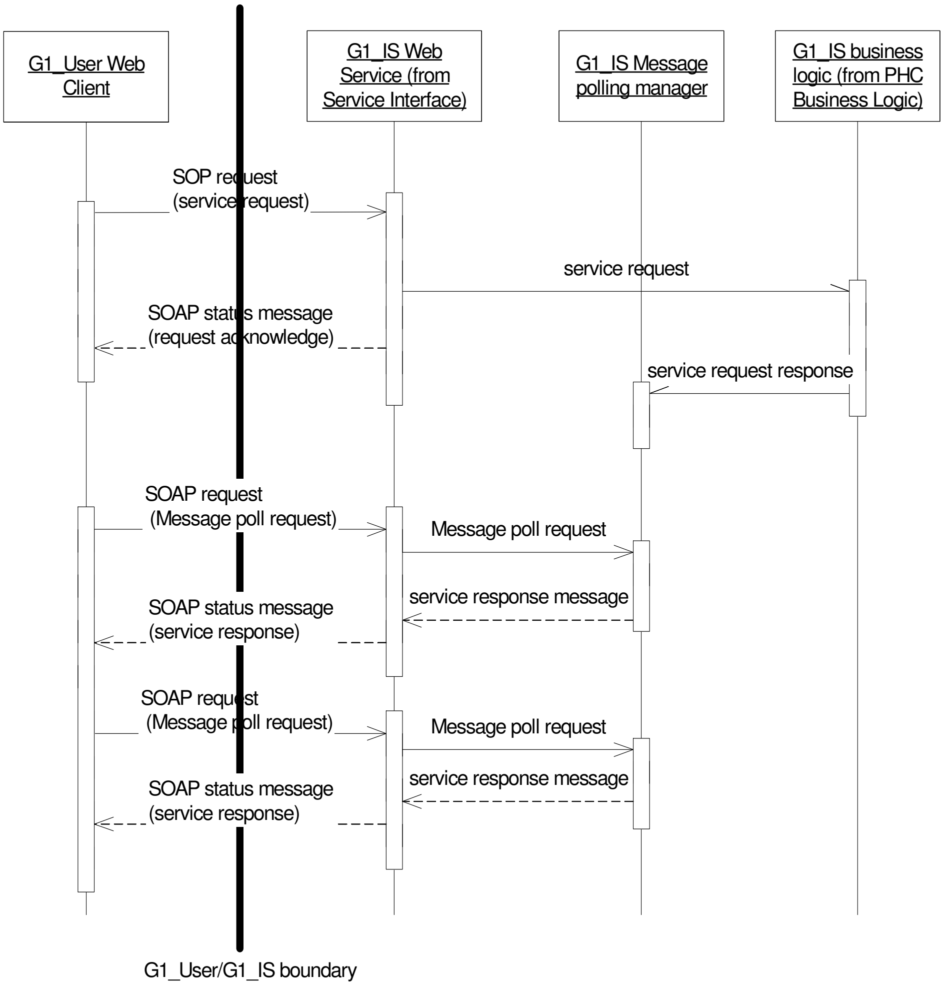
G1_User Web Client
G1_IS Web Service (from Service Interface)
G1_IS Message polling manager
G1_IS business logic (from PHC Business Logic)
SOP request (service request)
service request
SOAP status message (request acknowledge)
service request response
SOAP request (Message poll request)
Message poll request
service response message
SOAP status message (service response)
SOAP request (Message poll request)
Message poll request
service response message
SOAP status message (service response)
G1_User/G1_IS boundary

Figure 26 - Web Services Communication between G1_IS and G1_User Applications (polling)

Messaging methods of HL7 protocol described in Transmission Infrastructure domain in combination with Web Service method that receives HL7 XML message as argument (service request) and returns HL7 message (acknowledge or service request response) support above described communication methods.

In case of Acquire Work Permission Web Service receives HL7 XML service request message through method argument and after service request processing returns HL7 XML service request response message as method return value (see 3.2.5 Request Message Sender with App Acks (Immediate) and 3.2.6 Request Message Receiver with App Acks (Immediate)). *G1_IS* returns accept acknowledge, application acknowledge and service request response message as HL7 application acknowledge message.

For all other service requests *G2_Application* should use second Web Service. This Web Service has two methods that both receive HL7 XML service request messages through method argument and returns HL7 XML acknowledge message (accept or application acknowledge) as methods return value. First method of this Web Service receives service requests in form of HL7 XML messages through method argument and return HL7 Accept acknowledge as appropriate (see 3.2.1 Notification Message Sender – No Acknowledgements, 3.2.2 Notification Message Receiver – No Acknowledgements, 3.2.3 Notification Message Sender with Accept Acks and 3.2.4 Notification Message Receiver with Accept Acks).

Response to service request is returned to service requestor two ways: by direct access to service requestors Web Service (see 3.2.7 Request Message Sender with App Acks (with Accept Acks Deferred) and 3.2.8 Request Message Receiver with App Acks (with Accept Acks Deferred)) or by storing it to persistent storage so service requestor can poll it by using second method of second Web Service (see 3.2.9 Message Queue Manager and 3.2.10 Message Queue Poller).

HL7 and CEN protocols have mandatory fields for source and destination address that should be filled with source and destination logical address represented as OID so that *G1_IS* can route received message to appropriate service request handler.

4.3 Requirements regarding information set & information delivery

4.3.1 Message delivery

Requirement ID	
Description	If there are no technical problems regarding link to the central system, client application must send all messages or requests immediately upon their creation. In another words, although allowed, offline work mode is to be used only in case of technical difficulties.

4.3.2 Information set

Requirement ID	
Description	Client application must be capable to provide central system with the information described in [5]

4.4 Requirements regarding security issues

4.4.1 Security policy

Requirement ID	
Description	Any client application has to comply with rules described in Security Policy defined by Ministry of Healthacare.

4.5 Requirements Regarding Operating System

4.5.1 Operating System - Authentication

Requirement ID	
Description	Operating system MUST use user authentication mechanism for getting access to operating system and applications.

4.5.2 Operating System - Authorization

Requirement ID	
Description	Operating system MUST have possibility to give per user authorization for system resources and application access and usage.

4.5.3 Operating System - Audit

Requirement ID	
Description	Operating system MUST be able to make logs of each system and critical resource access with user, time and date information.

4.5.4 Operating System – System administration

Requirement ID	
Description	Operating system in use MUST support user groups. At least two user groups MUST be set: administrator and medical user. System administrator MUST obey security rules concerning data confidentiality as stated in Security Policy document.

4.5.5 Operating System – User permissions

Requirement ID	
Description	Operating system MUST be able to set permissions per each individual user. Permissions SHOULD be set using least privilege rule.

4.5.6 Operating System – Time synchronization

Requirement ID	
Description	Operating system SHOULD be able to synchronize internal clock with some referential time.

4.5.7 Operating System – System protection

Requirement ID	
Description	Appropriate protective software SHOULD be installed to protect the local machine against attacks. Updates of the definition files as well as the patches to the software should be performed in the specified time intervals. Protective software that should be installed is anti virus software, local firewalls etc.

4.5.8 Operating System – Removable media

Requirement ID	
Description	Use of the removable media (e.g. compact discs, floppy discs) MUST be specified regarding medical data sensitivity. This implies specific details about storing medical data on the removable media. Improper use of the removable media can compromise confidentiality of the medical data.

4.5.9 Stored Objects - Classification

Requirement ID	
Description	Objects stored on the local machine SHOULD be classified. This means that objects relevant to the use of the G2 application should have a level of confidentiality assigned to them. According to this appropriate permissions can be assigned to specified users or user groups.

4.5.10 Stored Objects – Access Rights

Requirement ID	
Description	Access rights to object that contains patient medical information, such as database with health care records, message queue store on PC, folders used for temporary or permanent medical information storage, MUST be set up to most restricted mode that will still allow client application to run. Only assigned medical person SHOULD be allowed to read and modify that objects. In case that system administrator MAY access those data because of operating system limitations, person that has system administration rights MUST act according to Security Policy document.

4.5.11 Stored Objects – Back up

Requirement ID	
Description	Back up of the stored objects mentioned in the previous chapter SHOULD be performed. This mechanism can protect against loss of data important for the proper behaviour of the G2 application. The critical data SHOULD be identified and proper back up procedures SHOULD be defined. Confidential data that is backed up MUST be protected granting access only to the users with adequate permissions. Back up of the private data SHOULD be performed according to the document “Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka”.

4.6 Medical Data Records

4.6.1 Medical Data Records – Access

Requirement ID	
Description	Only authenticated, authorized and logged access to medical data records SHOULD be allowed. Access to medical database has to be assigned only to assigned physician. Nurse MAY have read access to some patient medical data, according to business process. Each access to medical database SHOULD be to be logged. Records that contain private data SHOULD be comply with the specifications in the document “Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka”.

4.6.2 Medical Records - Database Architecture

Requirement ID	
Description	Architecture of the medical records database must separate medical and personal patient data and implements mechanisms that ensures binding of these two.

4.6.3 Medical Records - GIP handling

Requirement ID	
Description	GIP MUST NOT get stored into database or printed in decrypted form. Generally, in non-volatile memory only encrypted GIP MAY exist.

4.7 Requirements Regarding G2 Application Security issues

4.7.1 G2 application – Access

Requirement ID	
Description	Access to the G2 application MUST be enabled only to the authenticated and authorized user. Access controls SHOULD be implemented in away that they give permissions to the confidential data only to the specified user. G2 application SHOULD grant access to it's features according to the least privilege control. User can use only those features that are required for his work. For example nurse should not be able to see confidential private medical data of the patient. Some of the data accessible by application is medical private data that only patient and his assigned MD should be able to see according to the Croatian law. This means that mechanisms implementing role base access are not appropriate when accessing this type of data.

4.7.2 G2 application – Authentication

Requirement ID	
Description	Users accessing the NISHI system are authenticated using strong authentication. With that in mind authentication to the G2 application and medical data stored locally SHOULD be strong authentication as well. This implies the use of the smart cards. When starting the G2 application smart card holding the users certificate MUST be inserted in the smart card reader. G2 application MUST check if the card is inserted and use only the certificates on the card for authentication. Upon removal of the card the use of the application SHOULD be disabled.

4.7.3 G2 application – Accountability

Requirement ID	
Description	Logging of the access to the G2 application and possibly of some critical actions using G2 application SHOULD be logged. Logging enables the auditing of the local system. In the process of auditing malicious actions can be identified and appropriate users can be held responsible for the actions.

4.8 Requirements Regarding Connection to NISHI Security

4.8.1 NISHI requirements – Authentication

Requirement ID	
Description	NISHI system implements strong authentication using mechanism of client authentication over HTTPS. G2 application acts as a client application to the user (MD or Nurse) when trying to access resources on the NISHI system. Therefore G2 application MUST implement logic to successfully provide authentication information to the NISHI system. In order to connect to the NISHI system the principal MUST get permission to work, in another words get authenticated by the NISHI. This is performed invoking a successful Acquire Work Permission service. [slučaj uporabe “Prijava na sustav” u [6]. Authentication is performed based on the public/private key pair with appropriate certificate stored on the smart card. Key usage field in the certificate MUST specify that keys can be used in this purpose.

4.8.2 NISHI requirements – Authorization

Requirement ID	
Description	Upon successful authentication, authorization is performed. NISHI systems checks whether authenticated principal is registered as a user in the PHC IS system. This is performed in the process of acquiring work permission (Acquire Work Permission Web Service xxx). Once the G2 application has acquired work permission for user, it receives a token that SHOULD be preserved and used to access other NISHI resources (Web Services) as long as the user is using the G2 application or until session expires. This is implementation of a Single Sign On mechanism. The token is received as a cookie and MUST NOT be saved on persistent memory. Different web services have different access controls and permissions implemented. Based on the issued Single Sign On cookie, authenticated principal is given the right to perform certain actions.

4.8.3 NISHI requirements – Integrity

Requirement ID	
Description	XML messages sent from the G2 application to the NISHI system MUST be signed. The process of signing MUST be performed right after the message is created. Signature generation MUST be performed using the private key stored on the smart card. Unsigned messages will be refused by the NISHI system. Unsigned messages MUST NOT be saved locally or put to message queue. The XML messages MUST be signed following the XML Digital Signature Specification. Key usage element of the certificate used for signing MUST specify non-repudiation or digital signature usage. Specific details about the XML Digital Signature syntax used in the PHC IS are described in the [7]. Document describes used algorithms, versions and specific instructions. The implementation of the digital signature ensures end-to-end integrity.

4.8.4 NISHI requirements - Confidentiality

Requirement ID	
Description	Certificate of the CA (Certificate Authority) that issued the server certificate of the NISHI system MUST be added to the G2 application trust store. In order to protect data leaving the G2 local site and coming to the NISHI system secure channel is implemented. Since the communication is preformed over HTTP the SSL/TLS is used as a secure channel. Server certificates are assigned to NISHI servers. With the implementation of the secure channel, along with the confidentiality the server side authentication is enabled as well. This means that G2 applications are positive that they are contacting the right server.

4.8.5 NISHI requirements - GIP decryption

Requirement ID	

Description	In order to get the medical data of the patient from the NISHI system the appropriate encrypted GIP MUST be decrypted by the G2 application. Key usage element of the certificate used for decrypting MUST specify key encipherment. Decryption key used for MUST be stored on the smart card. Decrypted GIP MUST NOT be stored on persistent memory. The encrypted GIP is encrypted according to Cryptographic Message Specification (CMS/PKCS7) format specification. Additionally encrypted GIP in CMS format is transformed from binary form to the base64 form to be suitable for transmission.

5 References

[1] HL7 v3 – HR

[2] HRN ENV 13606

[3] RFC 2119

[4] Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka, NN 139/2004.

[5] Ispitivanje prihvaćanja korisnika ISPZZ sustava

[6] Informacijski sustav primarne zdravstvene zaštite – Poslovni proces

[7] Informacijski sustav primarne zdravstvene zaštite – Funkcijska specifikacija