



University of Cyprus

ΚΟΙΝΟΠΡΑΞΙΑ: ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ ΚΑΙ ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ



Project Title:

Deployment of Generic Cross Border eHealth Services in Cyprus

Agreement number: INEA/CEF/ICT/A2015/11S1451

Action No: 2015-CY-IA-0095

Τίτλος: Annex TE 1 NCPeH CY Technical deliverable – Part A

Release: v7.0

Αρ. Αναφ. Φακέλου: ΠΚ/2018/05/03

Λευκωσία 24 Ιουλίου, 2020

Βασικές Πληροφορίες Έργου

Πληροφορίες Έργου	
Τίτλος Έργου	NCPeH CY
Κωδικός Έργου	2015-CY-IA-0095
Ιδιοκτήτης Έργου	
Στοιχεία Επικοινωνίας Συντονιστή έργου	Καθ. Κωνσταντίνος Παττίχης Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, Λεωφόρος Πανεπιστημίου 1 Αγλαντζιά Λευκωσία 2109 ΚΥΠΡΟΣ (+357) 22892697 (+357) 22892701 pattichi@cs.ucy.ac.cy

Ιστορικό αναθεωρήσεων

Αριθμός Έκδοσης	Ημερομηνία	Συγγραφείς	Εκδότης	Σχόλια
1.0	30/04/2017	Καθ. Παττίχης Κωνσταντίνος Μόνικα Καλακουτή Φλουρής Ταντελής Ελευθερία Γεωργίτση Δρ Βάσος Σκουτέλλας Μιχάλης Αντωνίου Μάριος Νεοφύτου Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΥΥ & ΠΚ	Πρώτο Προσχέδιο
2.0	21/06/2018	Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΠΚ	Δεύτερο Προσχέδιο
3.0	18/09/2018	Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΠΚ	Τρίτο Προσχέδιο
4.0	19/03/2019	Δρ Βάσος Σκουτέλλας Μιχάλης Αντωνίου Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΥΥ & ΠΚ	Τέταρτο Προσχέδιο
5.0	03/04/2019	Δρ Βάσος Σκουτέλλας Μιχάλης Αντωνίου Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΥΥ & ΠΚ	Πέμπτο Προσχέδιο
6.0	05/07/2019	Δρ Βάσος Σκουτέλλας Μιχάλης Αντωνίου Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΥΥ & ΠΚ	Έκτο προσχέδιο
7.0	24/07/2020	Δρ Βάσος Σκουτέλλας Μιχάλης Αντωνίου Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου	ΥΥ & ΠΚ	Τελική

Θεώρηση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Θεώρησης
Δρ Βάσος Σκουτέλλας	Συντονιστής ελέγχου ποιότητας παραδοτέων	07/10/2020

Έγκριση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Έγκρισης
Καθ. Χρίστος Σχίζας	Πρόεδρος Εθνικής Αρχής Ηλεκτρονική Υγείας	08/10/2020

Executive Summary – Part A

The objective of this document is to describe the National Contact Point electronic Health (NCPeH) architecture and the basic technical needs for implementing the Patient Summary and ePrescription and eDispensing Cross-bordering Services in Cyprus.

Cyprus is committed to deploy and provide a cross border eHealth service under the CEF 2015 eHealth time frame (2017 to 2020).

Cyprus's goal is to deliver high quality cross-border healthcare for its citizens living abroad and visiting citizens from other EU Member States. Furthermore, due to the fact of being a tourist destination it's reasonable to expect that deployment of cross border services will influence on economic growth.

The document covers the following sections:

- Section A1 Introduction to the project Deployment of Generic Cross Border eHealth Services in Cyprus
- Section A2 National System Architecture for the Deployment of Generic Cross Border eHealth Services in Cyprus
- Section A3 Zone Description
- Section A4 System Components Description
- Section A5 Data Flows Description
- Section A6 Functional and Non-Functional Requirements
- Section A7 How we ensure confidentiality, integrity, availability, non-repudiation, authenticity and auditability

Table of Contents

Executive Summary – Part A.....	4
A1. Introduction to the project Deployment of Generic Cross Border eHealth Services in Cyprus	8
a. Cyprus National Service provision objectives.....	9
b. Cyprus eHealth Information Services	9
A2. National System Architecture for the Deployment of Generic Cross Border eHealth Services in Cyprus	11
a. Production Environment.....	12
i. Hardware Needs.....	14
b. Testing Environment.....	15
i. Hardware Needs.....	17
A3. Zone Description	18
a. Cyprus Governmental Network	18
i. Internal Portal Zone	20
ii. Internet Public Portal Zone.....	20
iii. Internet Supporting Zone	21
iv. Application Zone.....	22
v. Audit and Monitoring Zone	23
vi. Data Zone.....	23
vii. National Gateway Zone	24
viii. National Infrastructure	24
b. TESTA Zone.....	26
c. EU Zone	26
A4. System Components Description.....	28
a. Authorization and Authentication Service (Application Zone).....	28
i. Internal Portal Zone (NCP Active Directory)	28
ii. Internet Public Portal Zone (2-way SSL + Ariadni + NCP Active Directory)	28
b. National Infrastructure Service.....	29
i. Medico HIS	29
ii. Pharmaceutical Services	29
c. OpenNCP Portal Service (Application Zone).....	30
d. Audit Trail Service (Audit Monitoring Zone).....	30

e.	National Gateway	31
i.	APIs	34
f.	National Contact Point	36
i.	Development Lifecycle	36
ii.	Using the OpenNCP Admin Portal	38
iii.	Adding a new country on the OpenNCP	38
iv.	Communication Gateway	39
v.	OpenNCP REST APIs	42
vi.	Secure Communication with other NCPeHs	58
vii.	OpenNCP Audits	59
viii.	More information	68
ix.	OpenNCP A description	69
x.	OpenNCP B description	69
A5.	Data Flows Description	70
a.	Access through National Portal	70
i.	Public Sector Doctor	71
ii.	Private Sector	72
iii.	Supporting Services	75
1.	WIKI website and Service Desk Monitoring	75
b.	Cross-border through TESTA	76
i.	Cyprus acting as Country-A for Patient Summary Service	76
ii.	Cyprus acting as Country-A for ePrescription Service	77
c.	Patient Summary and ePrescription Services: Step-by-step	79
A6.	Functional and Non-Functional Requirements	85
A7.	How we ensure confidentiality, integrity, availability, non-repudiation, authenticity and auditability	89
a.	Confidentiality and Integrity	89
b.	Availability	89
c.	Non-repudiation	90
d.	Authenticity	90
e.	Auditability	90
AI.	Appendix VM Preparation	91
All.	Appendix Servers Preparation	94

AIII.	Appendix OpenNCP Properties	99
AIV.	Appendix Terminology Server	107
AV.	Appendix SMP and Certificates.....	108
a.	SMP	108
b.	Certificates	130
AVI.	Appendix Pharmaceutical Product Data Exchange web service API documentation..	136
a.	Introduction	3
b.	Communicating with API	3
c.	API Operations	4
d.	API Data Objects	5
e.	API Errors	10
f.	Annex 1	11

A1. Introduction to the project Deployment of Generic Cross Border eHealth Services in Cyprus

The main objective of the project *Deployment of Generic Cross Border eHealth Services in Cyprus* is to support Cyprus efforts to be part of a secure peer-to-peer network allowing the exchange of Patient Summaries and/or ePrescriptions, which will pave the way to reach the following general objectives:

1. Enable seamless cross-border care and secure access to patient health information between European healthcare systems, particularly with respect to the exchange of Patient Summary and ePrescription.
2. Contribute to patient safety by reducing the frequency of medical errors and by providing quick access to patient health information, as well as by increasing the accessibility of a patient's own prescriptions, also when abroad.
3. Provide medical personnel with life-saving information in emergency situations and reduce the repetition of diagnostic procedures.

The work activities underlying this application implement the main organisational, semantic and technical guidelines and specifications, namely:

- EU General Data Protection Regulation - for organisations and for individuals
- Directive 2011/24/EU on the application of patients' rights in cross-border healthcare
- Guidelines on an Organisational Framework for eHealth National Contact Point
- Governance model for the eHealth Digital Service Infrastructure during the CEF funding
- Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange
- Guidelines on ePrescription dataset for electronic exchange
- Multilateral legal agreement (as soon as there is a formal endorsement by the eHN)
- The EXPAND revision of organisational, semantic and technical requirements and specifications;

The solution proposed by the current project aims at reaching the **Technology Readiness Level 9 - Actual system proven in operational environment** - namely by start providing operational eHealth cross border services (PS or eP) by 2021, respectively.

The current application provides a quantifiable scenario of services usage to better allow the impact evaluation, namely by clearly identifying known or future population flows that may benefit from the provision of the proposed eHealth services.

a. Cyprus National Service provision objectives

Cyprus is committed to deploy and provide a cross border eHealth service under the CEF 2015 eHealth time frame (2017 to 2020). The exact timing and range of services that will be provided by Cyprus are reflected in deliverable D1.1 from Activity 1 / Task 1.

Cyprus's goal is to deliver high quality cross-border healthcare for its citizens living abroad and visiting citizens from other EU Member States. Furthermore, due to the fact of being a tourist destination it's reasonable to expect that deployment of cross border services will influence on economic growth. In summer season, Cyprus can predict that the usage of this service will be on a daily basis. Making country safer and environment patient friendly, Cyprus is improving daily life not only for its own citizens, but also for citizens from EU countries.

Concretely, when a citizen makes an unplanned cross-border healthcare visit to a health provider in the European Union, the health professional will have access to the person's Patient Summary and other relevant Electronic Health Record documents.

On the other hand, services ePrescription and eDispensation support the concept that a patient being abroad can receive the equivalent medication treatment that would receive in his/her home country. This means that this service aims the cross-border dispensing of ePrescriptions and support the documentation of dispensed drugs. Using Dispensation data from the dispensing pharmacy in the country of temporary stay, the health services, in the home country, can update the medication record of the patient, making health care and prescriptions safer.

Reimbursement services are out of scope of this call and will be solved via a different channel. Therefore, Cyprus will use CEF funds to support cross-border ePrescription / eDispensation service and to facilitate medical interventions with cross border Patient Summary usage, both developed under the epSOS and EXPAND project.

b. Cyprus eHealth Information Services

Cyprus aims to operate the following eHealth Information services:

Service	Role	RANGE	START PROVISION
Patient Summary A	Country A (country of citizen affiliation)	National	2021-Q1
Patient Summary B	Country B (country of treatment)	National	2020-Q1
ePrescription A	Country A (country that prescribed the medicine)	National	2020-Q1
ePrescription B (eDispensation)	Country B (country that dispensed the medicine)	National	2020-Q1

According to the Directive 2011/24/EU, Cyprus established the NCP role with all the authority suggested by the cross-border Directive 2011/24/EU. The Cyprus NCPeH will act as the national contact point, adhering to the Directive and ensuring a better and safer cross-border health care (according to Chapter 2, Article 4.2a.). Overall, Cyprus is in line with the objectives of Directive 2011/24/EU and hope that the deployment of eHealth solutions in future shall increase safety and quality of care throughout the EU, notably by: providing immediate clinical information needed in an emergency situation abroad and ensuring continuity of care across EU borders.

The eHealth Network adopted the ePrescription guidelines in November 2014, and guidelines for minimum / non-exhaustive patient summary dataset in November 2013. These guidelines and their successors will be a primary reference for deployment of both services under CEF call in Cyprus. As member of the eHN, Cyprus has agreed to apply Patient Summary, ePrescription guidelines on a national level and follow the “Guidelines on an Organisational Framework for eHealth National Contact Point”. Cyprus’s aim is to organize the NCPeH role as a communication gateway and a mediator for delivering the cross-border services for EU citizens. In compliance with Guidelines on an Organisational Framework for eHealth NCP, Cyprus will set up requirements, core characteristics, responsibilities and duties needed for NCPeH [1].

For a quick review of the needs of the connector, the reader can refer only to:

- Section A2 National System Architecture for the Deployment of Generic Cross Border eHealth Services in Cyprus
- Section A3 Zone Description
- Section A4 System Components Description

For a more complete view of the needs of the connector, the reader can refer to all the sections of this document that cover the following:

- Section A1 Introduction to the project Deployment of Generic Cross Border eHealth Services in Cyprus
- Section A2 National System Architecture for the Deployment of Generic Cross Border eHealth Services in Cyprus
- Section A3 Zone Description
- Section A4 System Components Description
- Section A5 Data Flows Description
- Section A6 Functional and Non-Functional Requirements
- Section A7 How we ensure confidentiality, integrity, availability, non-repudiation, authenticity and auditability

A2. National System Architecture for the Deployment of Generic Cross Border eHealth Services in Cyprus

This Section describes the NCPeH CY System Architecture for the deployment of generic cross border eHealth services in Cyprus. Regarding the development of the national architecture, we have two distinct environments, the Production Environment and the Testing Pre-Production Environment and respectively.

Production environment is a High-Available (HA) environment with cluster database server, load balancer for application server, and DNS failover setup for primary and secondary web servers. Testing environment is not HA environment and is deployed on three servers, one for TESTA network Server which is responsible for cross border PS, one for Application services and one for the Presentation Layer. All testing servers have limited resource. Currently, NCPeH CY Infrastructure is in Famagusta General Hospital (FGH).

Cross-border services are deployed and operated in two access zones, Internal Public Zone for public sector doctors and Internet Public Portal Zone for private sector doctors and pharmacists. The key difference between the two deployments is the way the users are authenticated and accessed to the NCPeH CY portal. For both access zones, the NCPeH CY Architecture supports four services, namely Patient Summary Country A (PS-A), Patient Summary Country B (PS-B), electronic Prescription Country A (eP-A) and electronic Dispensation (eP-B or eD). Country A refers to the country of origin while Country B to the country of treatment.

To support PS-A service, Cyprus is responsible to collect some general information about demographics of a Cypriot citizen and clinical data based on the PS Functional Requirements. PS-A service fulfils the PS Functional requirements v.2.2.2¹.

To support PS-B service, Cyprus is responsible to retrieve a European Citizen PS through the National Contact Point.

To support eP-A service, Cyprus is responsible to create an eP document for a Cypriot citizen, based on the eP Functional Requirements. eP-A service fulfils the eP Functional requirements v.2.2.3².

1

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/PS+Functional+requirements?preview=/37752803/65979535/PS%20functional%20requirements_v2.2.2.pdf

2

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eP+Functional+requirements?preview=/37752807/65979538/eP%20functional%20requirements_v2.2.3.pdf

To support the eD service, Cyprus is responsible to be able to dispense an eP coming from a European Citizen. eD service fulfils the eP Functional requirements v.2.2.3².

a. Production Environment

Production or Operation environment runs on TESTA connection and it will be used when the Testing environment is validated.

The configurations for the Production environment will be provided a restricted way when NCPeH CY will successfully fulfilled the readiness criteria that enable it to GoLive.

Production environment is a High-Availability³ environment with cluster database server, load balancer for application server, and DNS balancer for web server.

As can be seen in Figure 1, Testing environment is composed of seven Zones. A high-level description of the Zones is given in Section A3.

³ High availability is a characteristic of a system, which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.

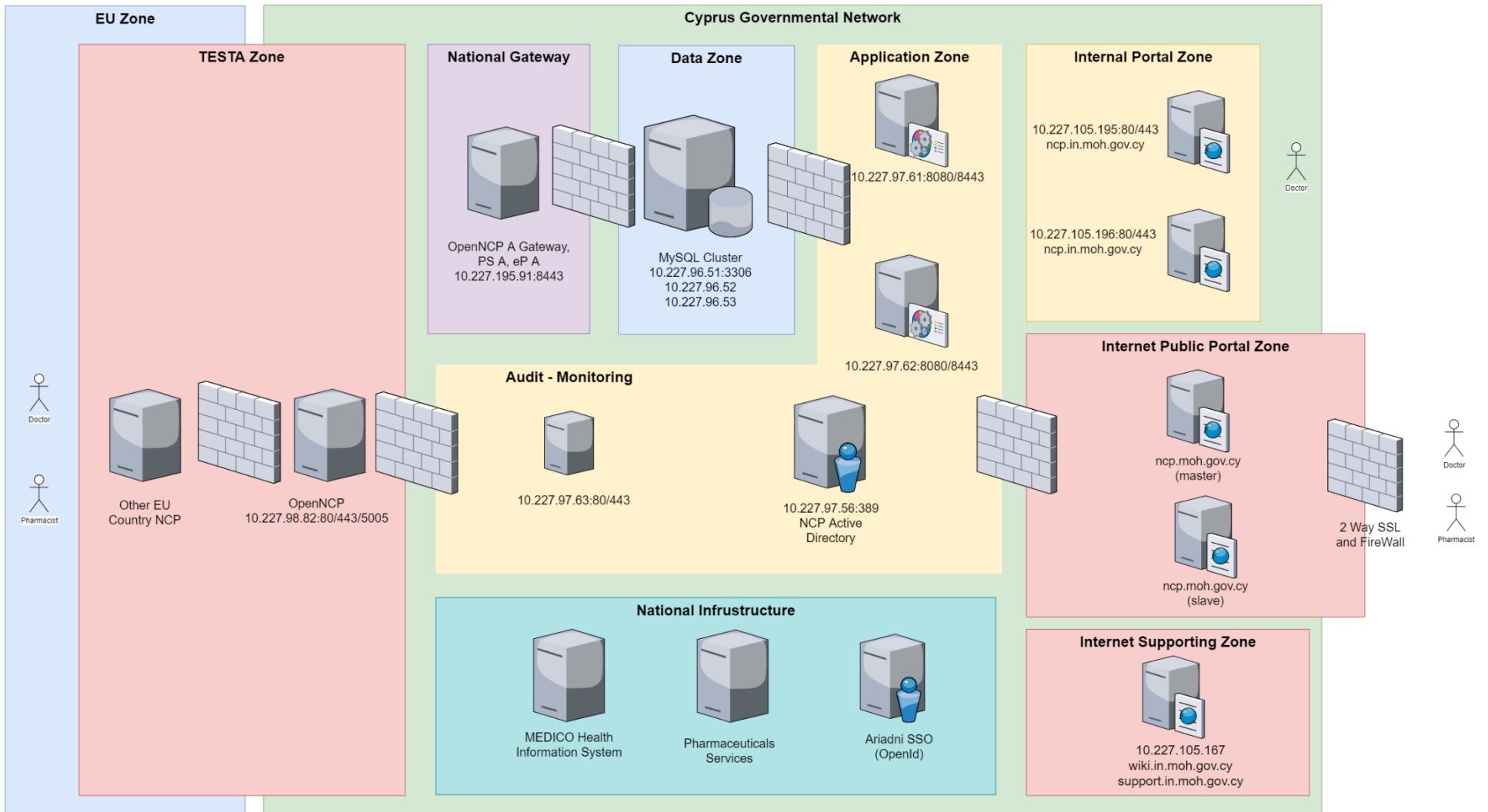


Figure 1: Production Environment NCPeH CY System Architecture

i. Hardware Needs

To support the NCPeH production environment, we use the following hardware specifications (minimum 2 physical machines).

A/A	VM	VM Name	Services	IPs	Physical Machine	Cores	RAM	Disk
1	Public Zone Master Server	master_web	Apache	ncp.moh.gov.cy	1	4	8	20
2	Public Zone Slave Server	slave_web	Apache	ncp.moh.gov.cy	2	2	4	20
3	Internal Zone Master Server	master_web	Apache	10.227.105.195	1	4	8	20
4	Internal Zone Slave Server	slave_web	Apache	10.227.105.196	2	2	4	20
5	Supporting Server	slave_web	Apache	10.227.105.167	2	1	2	30
6	APP Server A	app_A	Tomcat	10.227.97.61	1	4	16	20
7	APP Server B	app_B	Tomcat	10.227.97.62	2	4	16	20
8	Active Directory			10.227.97.56	2	2	4	40
9	Patient Summary CDA Server	ps_CDA	Tomcat	10.227.105.191	1	2	4	20
10	Audit and Monitoring Server	audit	Tomcat	10.227.97.63	2	4	8	240
11	MySQL Master Node	master_node	MySQL	10.227.96.51	1	8	32	512
12	MySQL Cluster Node A	node_A	MySQL	10.227.96.52	1	8	32	512
13	MySQL Cluster Node B	node_B	MySQL	10.227.96.53	2	8	32	512
14	OPENNCP A, OPENNCP B	openncp	ubuntu	10.227.98.82	1	4	8	40
Total						57	178	2026

Physical 1: 10.227.98.81, Physical 2: 10.227.97.65, RAM in GB, Disk in GB.

b. Testing Environment

Testing environment is used to verify whether it meets expectations and configuration before going in Production. As can be seen in Figure 2, Testing environment is composed of four Zones. In each Zone, a single server with limited resources has been installed.

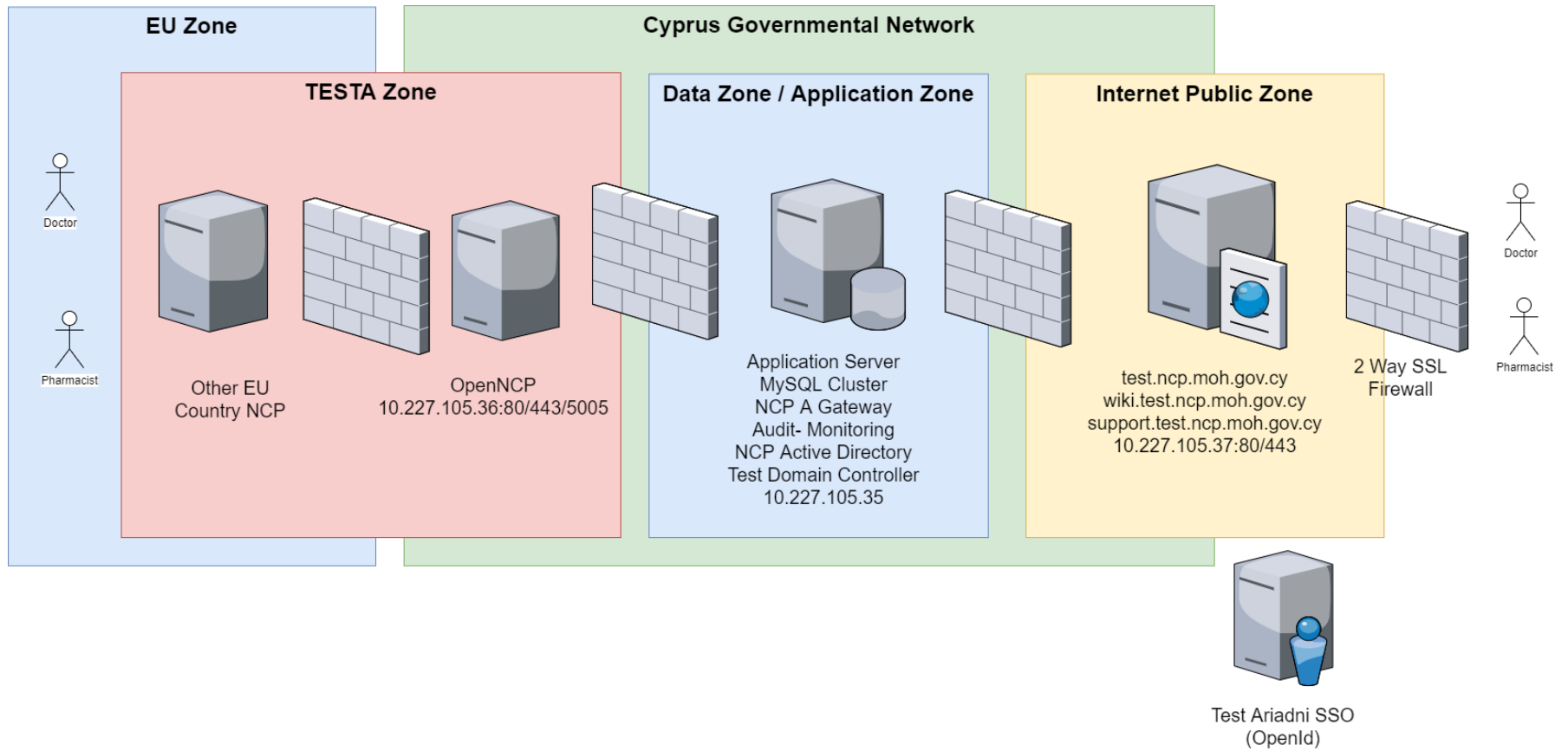


Figure 2: Testing Environment NCPeH CY System Architecture

i. Hardware Needs

To support the NCPeH testing environment, we use the following hardware specifications (minimum 2 physical machines).

A/A	VM	VM Name	OS	Services	IPs	Physical Machine	Cores	RAM (GB)	Disk (GB)	
1	Web Server	test_web	Ubuntu	Apache	10.227.105.37	1	1	2	20	
2	APP/Data Server	test_app	Windows	Tomcat	10.227.105.35	1	2	4	20	
3	OPENNCP A/B	test_openncp	Ubuntu	ubuntu	10.227.105.36	1	4	8	40	
							Total	7	14	80

A3. Zone Description

In this section we give a high-level Zone description of the NCPeH CY system architecture based on the Testing and the Production environments referenced in Section A2. The system architecture is divided in zones. Each zone communicates through other zone via firewall. Government firewalls preventing denial-of-service (DoS) attacks.

a. Cyprus Governmental Network

The NCPeH CY system architecture is installed in a restricted and secured governmental network. Famagusta General Hospital (FGH) and Nicosia General Hospital (NGH) are within this restricted environment.

The National Portal supports cross-border services and can be accessed only by authorized and authenticated Health Providers, doctors and pharmacists. National Portal is available through Internal Portal Zone for public sector doctors or Internet Public Zone for private sector doctors and pharmacists. It's important to note here that the portal supports roles in order to maintain data integrity. We are implementing user access controls and version control to prevent erroneous changes or accidental deletion by authorized users.

Doctor role is able to access PS-A, PS-B and eP-A services while Pharmacist role is able to access only eD service. The National Portal can be access by Public Sector doctors and Private Sectors doctors and pharmacists. Both Public Sector and Private Sector HCPs must register to the NCP Active Directory following the guidelines referenced in Section 4.2 of Annex OP 2 Operation and Organizational Structure. in order to gain access to the National Portal.

To provide information about how patients' health data are used and processed by the electronic cross-border health services in Cyprus as country of residence, the Patient Information Notice (PIN) is provided in our NCPeH CY website⁴. Also, the PIN document can be found in Sections 5 in Greek language and 6 in English language in Annex OP 8 NCPeH CY Patient Consent and PIN. PIN document is provided to fulfil the requirement of the EU General Data Protection Regulation to inform citizens about the processing of their personal data.

As patient, each Cypriot citizen must give his/her consent for the storage, use and exchange of individual medical and personal data in the National Contact Point of Cyprus. Patient consent mandatory for both services, PS and eP, and must be given before any medical data is stored on the National Portal. Also, patient consent must be given when an eP of an EU patient will be retrieved in Cyprus. The patient consent can be found in NCPeH CY website⁵, either in Sections 1

⁴ <http://ncp.cs.ucy.ac.cy/pin/>

⁵ <http://ncp.cs.ucy.ac.cy/patient-consent/>

and 2 in Greek language and 3 and 4 in English language in Annex OP 8 NCPeH CY Patient Consent and PIN.

In terms of patient identity traits, patient id and date of birth are mandatory fields.

NCPeH CY system is designed and implemented in order to fulfill the following technical specifications and standards, using a 3-Tier architecture for maximizing data protection and minimizing security risk

3-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. 3 Tier Architecture of the infrastructure is separated in different zones using different Vlans and Firewalls for maximum Zone discrimination.

The 3-tiers, or layers as involve:

- **Presentation Layer:** This is the front-end layer and it consists of the user interface (UI). UI is typically a graphical interface, accessible through a web browser or web-based application and which displays content and information useful to the end user. This tier's development builds upon web technologies and communicates with other layers through Application Programming Interface (API) calls. API is a set of clearly defined methods of communication among various components. A good API makes it easier to develop a computer program by providing all the building blocks, which are then assembled together by the programmer.
- **Application Layer:** It uses an application server and contains the functional business logic of the system which drives an application's core capabilities.
- **Data Layer:** This layer handles a database management system that provides access to application data. Data is accessed by the application layer via API calls.

This architecture provides us with the ability to extend, modularize, and scale up your system. It adds reliability and accommodates independence of the underlying servers or services. Moreover, it provides an ease of maintenance of the code base, managing presentation code and business logic (application layer) separately, so that a change to business logic, for example, does not impact the presentation layer.

Scalability is another great advantage of a 3-layer architecture. By separating the different layers, we can scale each one independently, depending on the need at any given time. For example, if we are receiving many web requests but not many application layer requests, we can scale your web servers without touching our application servers.

All transactions inside Government Network are performed using 1-Way Secure Socket Layer (SSL). SSL is the standard technology used for enabling secure communication between different zones.

i. Internal Portal Zone

Internal Portal Zone is available only through the Governmental network and supports Public Sector Doctors. Their authentication and authorization procedures are performed through NCP Active Directory. More information can be found in Section iv.1 and Annex OP 2 Operation and Organizational Structure, Section A5.a.i

The Portal Zone consists of two servers that host the National Portal. The portal contains online forms having all the appropriate fields based on epSOS specifications in order to create the PS, eP and eD documents that are then transferred via the NCP to other member states (MS) to support the cross-border services.

In Production Environment, the Internal Portal Zone consists of two servers that host the National Portal and served it on HTTPS. The portal implements the User Interface (UI) of NCPeH CY and supports the functionality for creating/editing and preview the PS and to prescribe and dispense prescriptions: eP and eD documents. These functionalities support doctors to create, edit PS and prescript for local patient and to preview PS of foreign patients. Additionally, the portal support pharmacist to dispense for foreign patients.

The portal is deployed on two web servers, master and slave, in failover setup on DNS. Additionally, web servers are setup for load balancing and are proxies for application servers of Application Zone. National portal endpoint for internal zone is <https://ncp.in.moh.gov.cy>.

The portal communicates through Rest full Application Programming Interface (REST API) with application zone (10.227.97.61 and 10.227.97.62) over HTTPS on port 8443.

Web Servers do not have write access to the filesystem for preventing file injections.

In Testing Environment, the Portal endpoint is <https://test.ncp.moh.gov.cy>.

ii. Internet Public Portal Zone

Internet Public Portal Zone hosts the national portal UI and supports private sector doctors and pharmacist. Private Sector doctors and pharmacists are able also to use and support PS-A, PS-B, eP-A and eD services. Internet Public Portal Zone consists of two servers.

The main difference from internal portal zone are 1) the authorization is done via Government Gateway Portal (SSO) ARIANDI and 2) the server authenticates clients via 2-way SSL. More information about the Two-Way SSL mechanism can be found in Section A4.a.ii. Client Certificates are issued by UCY for private sector health care providers. Private sector doctors and pharmacists are able also to use and support PS-A, PS-B, eP-A and eD services through Internet Public Zone. National portal endpoint for public zone is <https://ncp.moh.gov.cy>.

The portal communicates through Rest full Application Programming Interface (REST API) with application zone (10.227.97.61 and 10.227.97.62) over HTTPS on port 8443. Supporting material dose not communicate with application zone.

Web Servers do not have write access to the filesystem for preventing file injections. In order to access the National Portal the Private Sector Healthcare Providers (HCPs), doctors and pharmacists, firstly he/she must register to the Government Gateway Portal (ARIANDI) following the guidelines referenced in Annex I of Annex OP 2 Operation and Organizational Structure for pharmacists and Annex II of Annex OP 2 Operation and Organizational Structure for doctors. Such users are authenticated as citizens of Cyprus using ARIADNI Single-Sign-On (SSO). ARIADNI provides security through secure connections, encryption use of digital certificates, and user IDs. Then HCPs are redirected to the National Portal and must provide their Certificate in order to be authenticated and authorized to use the cross-border services. It's important to note here, that once a Private Sector HCP is registered to the NCP Active Directory and got a time-limited certificate, this must be installed in the browser of the HCP on his personal computer. This certificate includes the HCP role and it's used by the NCP Active Directory to authorize him/her to access the NCPeH National Portal. Once the certificate will expire, the HCP is responsible to request and install a new one.

iii. Internet Supporting Zone

Internet Supporting Zone host two services, WIKI and Service Desk Monitoring.

1. NCPeH CY WIKI Website

NCPeH CY WIKI is a technical communication document intended to give assistance to people using the particular system. This wiki contains both a written guide and associated images (screenshots) of the human-machine interface. The language used is matched to the intended audience, health professionals, medical doctors and pharmacists.

The WIKI website is available on <https://wiki.ncp.moh.gov.cy>.

2. NCPeH CY Service Desk Monitoring Support

The Service Desk is based on the OpenSupports ticketing system⁶. OpenSupports is an open source ticket system for giving support to clients of a company or to users of a platform. It provides better management of users' inquiries. Users can send tickets through OpenSupports and the staff can handle them appropriately.

Based on the eHDSI Country Service Desk Guideline V1.1.1 2018/08/01 document⁷ the Service Desks on national level need to provide support for different groups of actors. Our system provides support for all recommended actors:

- **Patient:** Patient, residing in Cyprus, who aims to use cross-border eHealth services. These patients may have questions related to the cross-border services provision and its possibilities.

⁶ <https://www.opensupports.com/>

⁷ [Country Service Desk Guideline, eHealth DSI –ePrescription and Patient Summary](#)

- *Note:* Patient does not have access to the NCPeH CY Service Desk to ask questions. Patient's questions are supported by phone calling to 22604100. The officer that will answer the phone is responsible to register the issue to OpenSupports. More information can be found in Annex OP 1 Service Operation Plan in Section 3.
- **Health professional:** Health professional, acting within Cyprus, as end-user of the system.
- **Third party vendors / Software integrators:** Companies integrating communication with national eHDSI services (e.g. NCPeH) into their primary software.
- **Foreign country Service Desk:** Contacting or being contacted by Service Desk from another country operating within eHDSI, for resolving issues arising from cross-border exchange.
 - *Note:* Other countries contact by email to ncphelpdesk@cs.ucy.ac.cy and the related officer is responsible to register the issue to OpenSupports. As the issue will be fixed, the officer will reply by email to the foreign country contact point to reference the progress. More information can be found in Annex OP 1 Service Operation Plan in Section 3.

The OpenSupports ticketing system is available on <https://support.ncp.moh.gov.cy>.

More information about OpenSupports can be found in Annex OP 9 Service Desk Monitoring Tool.

iv. Application Zone

Two servers on the Application Zone host the application responsible to manage patients' data. More specifically, for patient's medical data storage and retrieval. The portal communicates through Application Programming Interface with application servers. Application Server expose many interfaces for authorized HTTP JSON POST requests regarding insertion and selection of patient's medical data.

Validation and Sanitation of all input data is performed for preventing SQL Injections and XSS Scripting to ensure that the application is robust against all forms of input data, whether obtained from the user, infrastructure, external entities or database systems.

Application Zone is responsible to implement the business logic of the application. Application zone host the services of 1) authentication and authorization service (AAS) that relates to NCP Active Directory Server 2) OpenNCP connector service NCP B services (NCPBS) and 3) the national PS and eP service (PSePS) for supporting doctors to create/edit patient PS and eP, 4) audit trail services (ATS) for collecting and trail user interactions and Zabbix for monitoring and analysis, applications and infrastructure and 5) the NCP active directory, for manage users (add, edit, delete doctors, pharmacists, operators and administrators).

Application zone is in network separate zone and hosted from the servers 10.227.97.61, 10.227.97.62, 10.227.97.63 and 10.227.97.56.

Application zone is communicated with 1) Data Zone to 10.227.96.51 on port 3306 over SSL, 2) National Infrastructure Zone – MEDICO HIS (10.227.24.22 on port 1521) and Pharmaceuticals services (<https://www.phs.moh.gov.cy/hio-services/ProductSyncService?wsdl>), 3) and TESTA Zone to 10.227.98.82 on port 5005.

1. NCP Active Directory

The Application Zone also hosts the NCP Active Directory which is located in Famagusta General Hospital inside the governmental network. All HCPs, both Public Sector and Private Sector, which have access to the system are registered on NCP AD. The registration of every end user is performed by authorized IT persons from the Ministry of Health.

v. Audit and Monitoring Zone

The Audit and Monitoring Zone hosts the Audit and Monitoring Server where an auditing service has been installed and all transactions are recorded and stored for auditing and monitoring.

As NCPeH CY, we have a specific procedure to monitor (and notify when not available or reduced availability) system's technical gateway services availability. Our system also ensures that event logs recording user activities, exceptions and faults are logged, collected, retained and protected appropriately and retrieved in case analysis for information security events or breaches is required. We collect and record all activities of every single user in a different database dedicated for user management and we have a user management system to retrieve in case analysis. Also, Apache tomcat catalogue saves all logs procedures performed on our server.

vi. Data Zone

Our MySQL cluster is composed of three MySQL database servers that all store all the patients' summary and ePrescription medical data complied to epSOS Master Value Catalogue v.3.1.0⁸ codings. We also have a different database dedicated for user management and user's monitoring and different database to keep logs about the usage of NCPeH services either from Cyprus or from a European country.

Data zone is hosted Database Cluster (MySQL cluster server). Database Cluster is run on servers 10.227.96.51, 10.227.96.52 and 10.227.96.53.

Data validation is also performed in Data Zone. Also, database user access level is allowed only via Store Procedures.

In the MySQL cluster, we store only the encrypted combination of patient's ID and date of birth using AES encryption, based AES symmetric key 256 bit and an encrypted string is generated. Patient demographics retrieved from National Infrastructure are identified by this encrypted string. Database encryption technology delivers powerful protection for the sensitive patient

⁸ <https://ec.europa.eu/cefdigital/wiki/display/EHSEMANTIC/MVC+3.1.0+-+Release+Details>

information stored in database. We use an encryption functionality that allows us to specify which data elements (or all data elements) are encrypted. This method encrypts the data before it is written to the database tables; access to decrypt the data can be tightly restricted so that any person or application without appropriate rights will only see meaningless cipher text, even while the server or application is running.

vii. National Gateway Zone

National Gateway Zone hosts the OpenNCP-A Gateway which supports the PS-A and eP-A services. National Gateway is responsible to construct the structured CDA Patient Summary (PS), and structured CDA electronic Prescription (eP) documents. It supports CDA XML Layer 3 and PDF Layer 1 formats.

When Cyprus is acting as country A, NCPeH CY is responsible to provide to country B the requested documents, PS and/or eP.

The clinical information is gathered on demand per service, and the cross-border documents are constructed on the fly. The services require a patient ID and the corresponding date of birth in JSON form. This info is provided from the OpenNCP portal, using the National Connector. Then, a mechanism is triggered on OpenNCP-A Gateway, which is responsible to search the exact combination of the given patient's ID and date of birth in the SQL database cluster. If the combination of patient's ID and date of birth is found in the database, then the employed mechanism retrieves all the appropriate patient's demographics and clinical data and constructs the requested CDA document in XML and PDF form.

National Gateway is running on server 10.227.195.91 and serves over HTTPS to TESTA Zone 10.227.98.82.

viii. National Infrastructure

National infrastructure zone hosts the services that are connected to the NCPeH infrastructure via Application Zone services. NCPeH application zone is connected to 1) MEDICO Health information System for access patient demographics data, 2) to pharmaceutical services for importing licensed pharmacist in NCPeH for supporting the prescription functionality of NCPeH and 3) to ARIADNI Single Sign On Government Portal for authenticate private sector doctors and pharmacists.

1. MEDICO Health Information System

For security and ethical purposes, a Cypriot citizen's demographics data are retrieved per request on the fly from the MEDICO Health Information System (HIS) and are not stored in MySQL Cluster in the Data Zone. It's one-way application programming interface which only retrieves data for a specific patient. MEDICO HIS is only accessible via the governmental restricted and secured network; thus, no patient's data is share outside this network.

MEDICO HIS contains the Cypriot citizens demographics data based on Civil Registry Identification.

In the MySQL cluster, we store only the encrypted combination of patient's ID and date of birth. This encrypted field is used only to identify a specific patient. Specifically, a medical doctor provides to the NCPeH CY Portal these two fields for a given patient. Then, the application server generates an encrypted string. If this string exists in the database, then the patient is identified and the doctor can view his/her PS, update it and create an eP. In case where a PS or an eP will be filled for the very first time for a given patient, then this time only the encrypted string will be stored in the database. This string will then be used to identify the patient in a future appointment.

The data that are retrieved are:

- First name
- Last name
- Maiden name
- Sex
- Street name
- Address number
- Postal code
- Flat number (if any)
- District
- Town
- Country
- Landline phone number
- Mobile phone number
- Citizen alive flag (yes/no)

2. Pharmaceutical Services

The Pharmaceutical Services of the Ministry of Health in Cyprus are responsible to provide to the NCPeH CY System all the need information regarding the available medications in Cyprus. More specifically, the Pharmaceutical Services provide periodically to the NCPeH System through an Application System Interface (API), a list that contains the current available medications. The list of the medications is coded based on the MVC coding the then is stored in the Data Zone and it's being used while the Medication Section of PS for a patient is completed or an eP is completed.

For each medication, the Pharmaceutical Services provide the following fields:

1. Brand name
2. Availability for substitution
3. Active ingredient
4. Strength and Strength unit
5. Pharmaceutical Dose form
6. Route of Administration
7. Type of package

8. Size of Package and Size unit.

3. Ariadni SSO

The Government Gateway Portal is given the name Ariadni. It enables users to access the electronic services (eServices) that are made available by the Government of Cyprus over the Internet. The system is retrieving required information from the interconnected back-end systems, thus minimising or completely avoiding any bureaucratic procedures. Individuals, organisations, and agents need to register to login to the system. Ariadni provide the platform with the necessary common core services enabling the delivery of eServices and the execution of online transactions in a secure manner.

b. TESTA Zone

For data exchange with other EU countries, the NCPeH CY system establishes a secure connection with other NCPeH, following TESTA network connection. TESTA is the backbone of European intra-administration communications. It's a private, highly secured network, a special Internet, for public administrations in Europe. With TESTA, officials in disparate ministries can communicate with colleagues in other countries and work on common projects being confident that, as they exchange confidential information, their files are safe from possible interception and will be delivered.

Cyprus is acting as NCP-B (own country) for PS and eP. So, Cyprus has in place a standardised software solution – OpenNCP – supporting cross-border exchange of personal healthcare data as NCP-B, with specifications of protocols, procedures and exchanged documents. Mainly OpenNCP implements XCA and XCDP IHE profiles for supporting cross border data exchange. We connect NCP Technical Gateway to the National Infrastructure through National Gateway for PS-A and eP-A services support and Application Zone for PS-B and eD services support.

National Connector is deployed on separate VM in separate Zone. We created a Virtual Local Area Network (Vlan) in our network and connect all the EU NCP Servers in this Vlan. Through a firewall we open only specific ports for communication from EU NCP Servers to Cyprus National Health Information System.

For data exchange with other EU countries, the NCPeH establishes a point to point secure connection with other NCPeH.

c. EU Zone

Cyprus is acting as NCP-A for other countries for PS and eP. So, Cyprus has in place a standardised software solution – OpenNCP – supporting cross-border exchange of personal healthcare data as NCP-A, with specifications of protocols, procedures and exchanged documents. We connect NCP Technical Gateway to the National Infrastructure.

Cross-border services PS-A, eP-A, PS-B and eD are supported through EU Zone and TESTA ZONE. In each EU Country, only authenticated and authorized HCPs gain access to the NCPs to support the cross-border services.

A4. System Components Description

a. Authorization and Authentication Service (Application Zone)

Authentication and authorization service have different levels of security, depending on the zone of the user. There are two zones and two end points for the service, one for each zone:

i. Internal Portal Zone (NCP Active Directory)

Level 1. NCP Active Directory Authentication and Authorization

Authentication and authorization are performed via NCP Active Directory. NCP Active Directory is hosted in separated VM inside NCPeH infrastructure and it is visible only inside application zone logical machines. Active Directory is mainly acting as LDAP server on port 389. User are authenticated and authorized according to NCP Active Directory group assignments which are setup in end user registration procedure.

ii. Internet Public Portal Zone (2-way SSL + Ariadni + NCP Active Directory)

If the user is trying to access National Portal via internet more security levels are added.

Level 1. Two Way SSL (Client Authentication)

In Two-Way SSL authentication, the client and server need to authenticate and validate each other's identities. The authentication message exchange between client and server is called an SSL handshake, and it includes the following steps:

1. Client prepares an Authentication Request containing the desired request parameters.
2. Client sends the request to the Authorization Server.
3. Authorization Server Authenticates the End-User.
4. Authorization Server obtains End-User Consent/Authorization.
5. Authorization Server sends the End-User back to the Client with an Authorization Code.
6. Client requests a response using the Authorization Code at the Token Endpoint.
7. Client receives a response that contains an ID Token and Access Token in the response body.
8. Client validates the ID token and retrieves the End-User's Subject Identifier.

Clients certificates are issued by UCY according to management procedures described in Part B B.12.

Level 2. Ariadni: National Authentication Gateway

Ariadni is the national authentication gateway based on the well know OpenID open standard and decentralized authentication protocol. NCPeH CY authentication service is based on Authorization Code Flow. The Authorization Code Flow goes through the following steps.

1. Client prepares an Authentication Request containing the desired request parameters.
2. Client sends the request to the Authorization Server.
3. Authorization Server Authenticates the End-User.
4. Authorization Server obtains End-User Consent/Authorization.
5. Authorization Server sends the End-User back to the Client with an Authorization Code.
6. Client requests a response using the Authorization Code at the Token Endpoint.
7. Client receives a response that contains an ID Token and Access Token in the response body.
8. Client validates the ID token and retrieves the End-User's Subject Identifier.

Level 3. NCP Active Directory Authentication and Authorization

After the user is authenticate from Ariadni SSO, a final level of security is performed which is the same internal zone authentication and authorization. Ariadni returns the legal identification number of the user, to NCPeH system. Then NCPeH system is asking NCP active directory for the authorization access of the user. According to NCP Active directory the user is revoked or continue to NCPeH portal.

b. National Infrastructure Service

i. Medico HIS

NCPeH CY is connected directly to Medico HIS Demographics table with only read access level. The connection is performed directly to oracle cluster. NCPeH Services is call oracle cluster based on end user keywords name and date of birth.

ii. Pharmaceutical Services

The Pharmaceutical Product Data Exchange Web Service API enables users to programmatically retrieve data from the Pharmaceutical Services database. The core messaging technology for the API is Simple Object Access Protocol (SOAP), which is an XML and HTTP based protocol with wide support in the industry. The API uses document/literal style SOAP 1.1. The operations provided by a web service are defined in a WSDL (Web Services Definition Language) file which is posted on the web service's website.

For more information please refer to AVI Appendix Pharmaceutical Product Data Exchange web service API documentation.

c. OpenNCP Portal Service (Application Zone)

OpenNCP B portal is based on gnomon OpenNCP Rest API, which is in detail described in section A2.f.v.

d. Audit Trail Service (Audit Monitoring Zone)

1. Zabbix Monitoring Tool

We have installed Zabbix Server Software in Audit and Monitoring server in 10.227.97.63 to monitor the server activity as well as the activity of all active nodes of the infrastructure. More information can be found in in Annex OP 3 Zabbix Open-source monitoring tool.

2. Audit Log Monitoring Tool

As we mention in Section A3.a.vi, we have a dedicated database to store the logs about the usage of NCPeH CY. All the NCPeH CY transactions are stored in that specific database.

The idea of the Audit logging is that ultimately the use of an audit log is a specialized functionality that needs to have all events that happened on all the various systems in the NCPeH CY architecture. The goal of the Audit Log Monitoring Tool is to support security surveillance to look for abuse of policy, abuse of systems, and to inform an accounting of disclosures. It is intended to be used by the security officer to detect anomalies that need further investigation.

Audit Log Monitoring Tool is installed in Audit and Monitoring server in <http://10.227.97.63/datatables/>. Security officer can use search form using keywords like date of incident or log type id or data. A screenshot of the Audit Log Monitoring Tool can be seen in Figure 3: Audit Log Monitoring Tool.

Show entries Search:

Log id	User id	P id	Log Type id	DT	Data
21	-1	1	117	2018-02-10 09:30:54	{patient_id=123456, dob=1990-01-01}
22	-1	1	117	2018-02-10 09:37:29	{patient_id=123456, dob=1990-01-01}
23	-1	1	117	2018-02-10 09:38:22	{patient_id=123456, dob=1990-01-01}
24	-1	1	117	2018-02-10 09:55:07	{patient_id=123456, dob=1990-01-01}
25	-1	1	117	2018-02-10 09:55:25	{patient_id=123456, dob=1990-01-01}
26	-1	1	117	2018-02-10 09:55:28	{patient_id=123456, dob=1990-01-01}
27	-1	1	117	2018-02-10 09:56:42	{patient_id=123456, dob=1990-01-01}
28	-1	1	117	2018-02-10 09:56:48	{patient_id=123456, dob=1990-01-01}
29	-1	1	117	2018-02-10 09:57:41	{patient_id=123456, dob=1990-01-01}
30	-1	1	117	2018-02-10 09:59:04	{patient_id=123456, dob=1990-01-01}

Showing 1 to 10 of 11,737 entries Previous **1** 2 3 4 5 ... 1174 Next

Figure 3: Audit Log Monitoring Tool

Performance of periodic reviews of audit logs is useful for:

- a. Detecting unauthorized access to patient information.
- b. Establishing a culture of responsibility and accountability.
- c. Reducing the risk associated with inappropriate accesses.
- d. Providing forensic evidence during investigations of suspected and known security incidents and breaches to patient privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied.
- e. Detecting new threats and intrusion attempts.
- f. Identifying potential problems.

e. National Gateway

National Gateway is responsible for PS and eP document construction. It supports API services that are triggered by the OpenNCP National Connector within the TESTA Zone. TESTA ZONE and National Gateway communicate through firewall and both zones are within the restricted and secured private network. Thus, no cross-border data goes outside this network.

All the fields of the PS are coded based on the Wave 2 version of the epSOS Master Value Catalogue⁹.

⁹ MVC 3.1.0 (14.01.2020)

The CDA Patient Summary includes all the fields referenced by the Patient Summary Functional Requirements. Thus, Cyprus supports all mandatory and optional sections of the Patient Summary:

- Allergies and Other Adverse Reactions (mandatory)
- Surgical Procedures (mandatory)
- Medical Devices (mandatory)
- Medication Summary (mandatory)
- Active Problems (mandatory)
- History of Past Illness (optional)
- Immunizations (optional)
- Pregnancy History (optional)
- Social History (optional)
- Coded Vital Signs (optional)

The generated PS CDA XML and PDF documents are created using the aforementioned sections. PS XML L3 and PDF L1 document examples can be found in Sections 1.1 and 1.2 of Annex TE 2 Reference Test Documents respectively.

The generated eP CDA XML and PDF documents are created using Medication Summary extended fields to support all the required fields of an eP CDA document, based on the eP functional requirements_v2.2.3. eP XML L3 and PDF L1 document examples can be found in Sections 1.3 and 1.4 of Annex TE 2 Reference Test Documents respectively.

Based on pharmacists' comments, each eP in Cyprus is available for dispensation in an EU country six months from the onset date.

To validate our NCPeH CY operation, we participated on the Formal Pre-Production -Testing Events – Wave 2. The Report Summaries that includes the results can be found in Annex TE 4 NCPeH CY Pre-Production Testing Results.

To validate our CDA documents, we participated in the Functional end-2-end testings of the Wave 2 Conformance Tests - where our PS, eP and eD documents were evaluated. As Cyprus, we fulfilled the PS and eP criteria. The full results of the Functional End-to end testings can be found in Annex TE 4 NCPeH CY Pre-Production Testing Results.

Also, it's important to mention that while we are creating the CDA documents we take into consideration some assumptions regarding missing values – not completed by the health care provider in our portal.

The following procedures are performed in OpenNCP A Gateway by the CDA constructor mechanism.

For example, in patient demographics, if a patient's email is not given, we set: NullFlavor.UNK. The same stands also for:

- Author telecom: NullFlavor.NI
- Authoring device: NullFlavor.NI
- Legal Authenticator Assigned Entity: NullFlavor.NI

Allergies Section:

If no allergy is given, since this section is mandatory, we set:

- Observation Onset Date: NullFlavor.UNK
- Observation End Date: NullFlavor.UNK

If an allergy is still active, we set:

- Symptom End data: NullFlavor.NA

Medical Devices Section:

If no medical device is given, since this section is mandatory, we set:

- Medical Device Supplier: NullFlavor.NA
- Medical Device Onset Date: NullFlavor.UNK
- Medical Device Code: NullFlavor.NA

For an installed medical device, if no onset date is given, we set: NullFlavor.UNK

Medication Summary Section (for PS/eP):

If no medication summary is given, since this section is mandatory, we set:

- Medication Summary Onset Date: NullFlavor.UNK
- Medication Summary End Date: NullFlavor.UNK
- Medication Intakes Frequency: NullFlavor.NA
- Medication Dose Quantity: NullFlavor.NA
- Medication High Dose Quantity: NullFlavor.NA
- Medication Low Dose Quantity: NullFlavor.NA
- Medication Subject: NullFlavor.NA

Active Problems Section:

If no active problem is given, since this section is mandatory, we set:

- Active Problem Code: NullFlavor.NA
- Active Problem Onset Date: NullFlavor.UNK
- Active Problem End Date: NullFlavor.UNK

Surgical Procedures Section:

If no surgical procedure is given, since this section is mandatory, we set:

- Surgical Procedure Onset Date: NullFlavor.UNK
- Surgical Procedure End Date: NullFlavor.UNK

Social History Section:

If no end date is given, thus a social history subject is still active we set: NullFlavor.NA

Vital Signs Section:

If no onset date is given, we set: NullFlavor.UNK

For Repeat Number, we set: NullFlavor.NI

The following APIs are installed on the OpenNCP A Gateway (IP 10.227.195.91:8443) that are responsible PS-A and eP-A services.

i. APIs

1. *getPatient()*

For a given patient ID and date of birth of a Cypriot citizen, OpenNCP returns his/her demographics data using *getPatient()* API. The endpoint is <http://10.227.195.91:8443/cefcy/getPatient> using POST method.

JSON input example:

```
{"patient_id":"1", "dob":"1990-01-01"}
```

Sample response:

```
{"success":1,"patient_demographics":{"country":"CY","administrativeGender":"M","streetAddress":"21, Dimokritou, 1000, Strovolos, Nicosia","patientId":"1","familyName":"Petrou","givenName":"Leonidas","telephone":"99000000","birthDate":"1990-01-01","email":"l.petr@testmail.com"}}
```

2. *listDocuments()*

For a given patient, *listDocuments()* API returns a patient's metadata either for PS or eP available documents. The endpoint is <http://10.227.195.91:8443/cefcy/listDocuments/> using POST method.

JSON input example:

```
For PS: {"patient_id":"1", "dob":"1990-01-01", "document_type":"ps"}
```

```
For eP: {"patient_id":"1", "dob":"1990-01-01", "document_type":"ep"}
```

Sample responses:

For PS:

```
{ "metadata": { "type": "PS", "format": "pdf", "patientId": "1", "effectiveTime": "2019-05-08", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "PSid.1.pdf", "title": "Patient Summary (eHDSI/Cyprus) for Patient ID 1" }, "metadata": { "type": "PS", "format": "cda", "patientId": "1", "effectiveTime": "2019-05-08", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "PSid.1.cda", "title": "Patient Summary (eHDSI/Cyprus) for Patient ID 1" }, "success": 1 }
```

For eP:

```
{ "metadata": { "type": "eP", "format": "pdf", "patientId": "1", "effectiveTime": "2019-05-29", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "ePid.1005.1.pdf", "title": "levothyroxine sodium" }, "success": 1, "metadata": { "type": "eP", "format": "cda", "patientId": "1", "effectiveTime": "2019-05-29", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "ePid.1005.1.cda", "title": "levothyroxine sodium" }, "metadata": { "type": "eP", "format": "pdf", "patientId": "1", "effectiveTime": "2019-06-16", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "ePid.1006.1.pdf", "title": "teriparatide" }, "metadata": { "type": "eP", "format": "cda", "patientId": "1", "effectiveTime": "2019-06-16", "author": "Vasilios Scoutellas", "repositoryId": "2.16.620.1.101.10.3.29.54290", "id": "ePid.1006.1.cda", "title": "teriparatide" } }
```

3. getDocument()

For a given patient, *getDocument()* API is responsible to provide a specific document, either PS or eP based on a specific document ID. The endpoint is <http://10.227.195.91:8443/cefcy/getDocument> using POST method.

JSON input examples:

```
{ "patient_id": "1", "dob": "1990-01-01", "document_id": "PSid.1.cda" }
{ "patient_id": "1", "dob": "1990-01-01", "document_id": "PSid.1.pdf" }
{ "patient_id": "1", "dob": "1990-01-01", "document_id": "ePid.1005.1.cda" }
{ "patient_id": "1", "dob": "1990-01-01", "document_id": "ePid.1005.1.pdf" }
```

Sample responses:

Document samples can be found in Sections 1.1, 1.2, 1.3 and 1.4 of Annex TE 2 Reference Test Documents respectively.

4. get_eD_XML()

If an ePrescription is dispensed in an EU country, NCP-B of EU member state sends the eD document to NCP-A in Cyprus. NCP-A in Cyprus then triggers the *get_eD_XML()* API which is responsible for the identification of original prescription and medicinal product dispensed by country B. This API updates the database and marks a specific eP as dispensed. Thus, *listDocuments()* will no longer show this specific eP as available.

The endpoint is http://10.227.195.91:8443/cefcy/get_eD_XML using POST method.

f. National Contact Point

The solution use OpenNCP v4.0.3 and is deployed in <http://10.227.98.82>. OpenNCP is implementing the NCP gateway and comes from the solution provider and by definition, it conforms to the technical specifications of eHealth DSI architecture and common components. By September 2020, we will update our instance to OpenNCP v4.1.0.

No modifications or additions occurred in the software, in which case it could have potentially caused a breach of the specifications.

i. Development Lifecycle

The National Connector code lives in Gnomon Code Repository which is based in the Bitbucket Solution. The access to this repository is restricted to specific users and groups.

The development lifecycle of the National Connector is the following:

- Development of the code (<https://code.gnomon.com.gr>)
- Local Builds and junit test execution
- Automated Builds via Jenkins (<https://jenkins.gnomon.com.gr>)
- Automated release of artifacts (<https://artifactory.gnomon.com.gr>)
- Deployment in the Acceptance Environment
- Manual testing

The development lifecycle can be seen in the following figure.

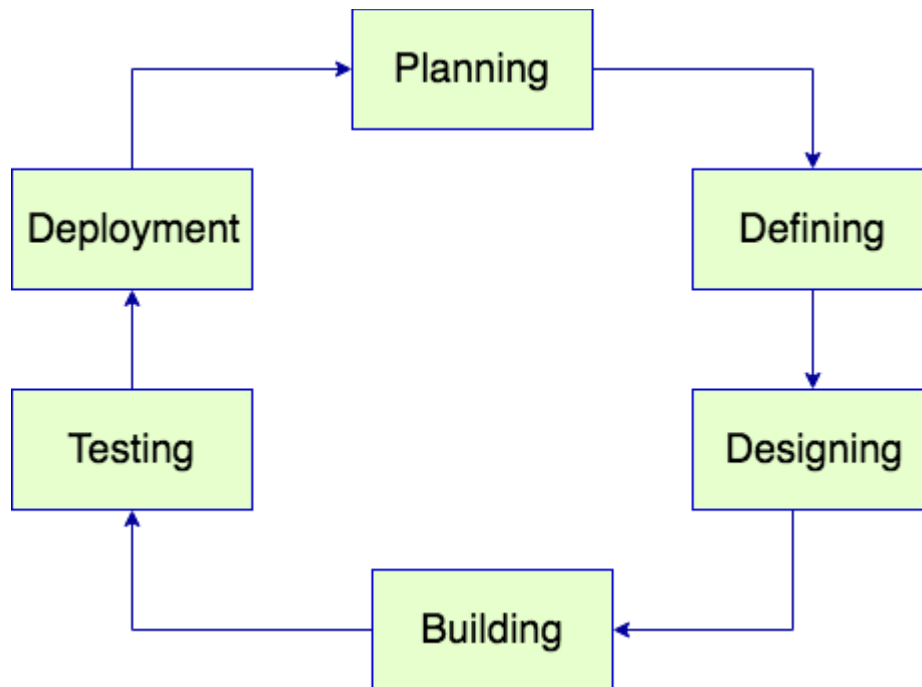


Figure 4 National Connector Development Lifecycle

1. Step 1

First is installed under `/home/openncp/apps/openncp-ws-server/webapps/` the `epsos_rep` war `http://artifactory.gnomon.com.gr/artifactory/ext-snapshot-local/com/gnomon/epsosrep/2.0-SNAPSHOT/epsosrep-2.0-20180531.173142-1.war`. This is the back-end API for getting the CDA Documents

2. Step 2

We have to get the latest version of the national connector library from `http://artifactory.gnomon.com.gr/artifactory/ext-snapshot-local/gi9/ccd/gnomon/openncp/openncp-nc-cy/6.1-SNAPSHOT/openncp-nc-cy-6.1-20180529.141210-18.jar` and copy it to the `/home/openncp/apps/openncp-ws-server/WEB-INF/lib` folder and also deploy the `EPSOS_REP` war file to your Tomcat Instance #1.

3. Step 3

Restart `openncp-server`

More information regarding the architecture and implementation can be found in the following Annexes:

- System Architecture Specification online document¹⁰

¹⁰

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/System+Architecture+Specification?preview=/37752811/65975839/System%20Architecture%20Specification_v2.1.0.pdf

- X.509 Certification Profiles online document¹¹
- Cryptographic Algorithms online document¹²
- Security Services Specifications online document¹³

HP Authentication

We follow the guidelines referenced in NCPeH Architecture Specification v2.1.0¹⁴ document, Section 3.6.3.

ii. Using the OpenNCP Admin Portal

The url of the portal is <http://10.227.98.82> from inside TESTA NG.

Admin account is available to do the basic configuration like configuring the LDAP connectivity as can be seen in the figure below.

iii. Adding a new country on the OpenNCP

1. We have to add the oid of the country in the pn-oid.xml file exists under /home/openncp/apps/epsos-configuration
2. We have to add the InternationalSearch mask of the country in the folder /home/openncp/apps/epsos-configuration/forms/
3. We have to add the new country code in the InternationalSearchMask.xml file that exist inside /home/openncp/apps/epsos-configuration/forms/
4. The endpoints of the countries will be populated in the epsosproperties database when the first query will be done for this new country

¹¹

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/X.509+Certificate+Profiles?preview=/37752981/65975951/X.509%20Certificate%20Profiles_v2.1.0.pdf

¹²

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Cryptographic+Algorithms?preview=/37752866/65975592/Cryptographic%20Algorithms_v2.1.0.pdf

¹³

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Security+Services+Specification?preview=/37752830/65975814/Security%20Services%20Specification_v2.1.0.pdf

¹⁴

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Specifications?preview=/35210463/47187038/NCPeH%20Architecture%20Specification_v2.1.0.pdf

← Add LDAP Server

Server Name

Default Values

- Apache Directory Server
- Fedora Directory Server
- Microsoft Active Directory Server
- Novell eDirectory
- OpenLDAP
- Other Directory Server

Reset Values

Connection

Base Provider URL

Base DN

Principal

Credentials

Users

Authentication Search Filter

Import Search Filter

User Mapping

UUID

Screen Name

Email Address

Password

First Name

Middle Name

Last Name

Full Name

Groups

Import Search Filter

Group Mapping

Group Name

Description

User

Test LDAP Groups

Export

Users DN

User Default Object Classes

Groups DN

Group Default Object Classes

Figure 5 OpenNCP Portal Admin Account

iv. Communication Gateway

The overall communication gateway architecture of Cyprus is illustrated in Figure 6.

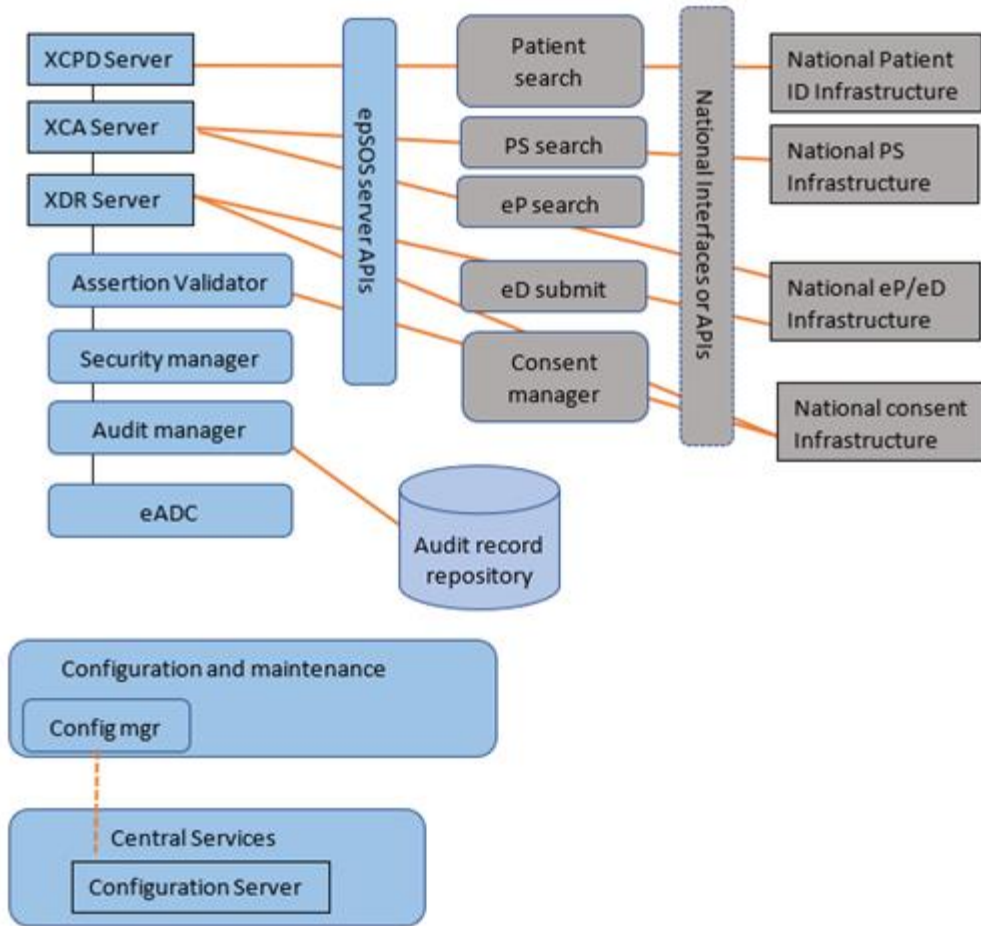


Figure 6: Communication Gateway Architecture of Cyprus

Protocols Terminators (PT)

PT support data exchange between affiliate countries. It is consisted from the following subcomponents:

a) XCPD Server: Responsible to support the patient identification and authentication service and implemented as an IHE XCPD transaction. The input data are the demographic data (identity traits) and output data are the list of matching patients and their demographic data.

b) XCA Server: Supports the fetch document service and implemented as an IHE XCA. IHE XCA basically supports two functionalities 1) XCA List which has input data: Patient ID and document class code and output data the list of documents along with their metadata and 2) XCA Retrieve having as input data Document ID, home community ID, and repository ID and gives as output data the documents.

c) XDR Server operates as a Data service provider and it is implemented based on IHE XDR (Cross-Enterprise Document Reliable Interchange). It has input data the Document and its metadata and gives output data success or error message.

Assertion validator

Assertion validator is responsible for validating the assertion while the data transfer is happening. It includes procedures for validating XCPD, XCA, XDR header contents and for identity and treat relationship assertions. Further assertion validator implements the policy manager interface which is responsible for answering questions related to processing of different document types, in different use cases, by healthcare professionals of with different roles and permissions and working in different healthcare facilities. In addition, assertion validator contains an interface for consent checks (in the supplied example, the answer is always yes) and helper methods for processing SAML messages.

Security manager.

The security manager contains procedures for the certificate validation, for creating and validating XML signature, for reading key store, for constructing TRC Assertions and for constructing and signing non-repudiation evidences.

Audit manager

The audit manager includes the procedures for creating ATNA log messages, the message sending procedure (asynchronous call) and the data model classes for RFC 3881 schema.

eADC

eADC referees for EPSOS automatic data collector. The development of eADC in epSOS was for statistical reasons. eADC service generates an entry in the database for each service call, stuff like XCPD, XCA, XDR etc. There are no tools available for checking eADC databases, except for direct access.

Configuration and maintenance

Configuration and maintenance module for reading OpenNCP configuration settings/properties from configuration database. Configuration settings are used by almost all components, including portals.

More information can be found in eHDSI Central Terminology Services Specifications v2.2.0 document¹⁵.

Audit Record repository (ARR)

¹⁵

<https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Central+Terminology+Services+Specification?preview=/37752987/65975564/eHDSI+Central+Terminology+Services+Specifications+v2.2.0.pdf>

ARR implementation is a fork of original OpenATNA project, modified for OpenNCP needs (<https://www.projects.openhealthtools.org/sf/projects/openatna/>). The original project is no longer active, but there seem to be also other forks, like (<https://github.com/jembi/openxds>). ARR contains the server for receiving and storing IHE ATNA compliant RFC 3881 audit messages and the openATNA-web, a user interface application for browsing the logs. Both are packed to run as WAR artefacts in Tomcat.

v. OpenNCP REST APIs

This sub-section includes all the OpenNCP REST APIs version 2.

1. Authorization

Basic Authorization: **Authorization** : Basic + " " + {username : password}<- Base64 encoded

JWT Authorization: **X-Authorization** : Bearer + " " + {JWT}

Service URL	Service Description	Basic Authentication	JWT	Request	Response
GET /api/openncp/forms/languages/get	get the list of available languages for translating the document	Yes	No		200 OK 401 Unauthorized 500 Failure Example: <pre>{ "timestamp":1510131788548, "status":200, "data":{ "languages":{ "de_BE":"de-BE", "en_GB":"en-GB", "nl_BE":"nl-BE", "fr_BE":"fr-BE" } } }</pre>

<p>GET /api/openncp/forms/countries/{language}</p>	<p>get list of countries</p>	<p>Yes</p>	<p>No</p>	<p>PathParam: language</p>	<p>200 OK 401 Unauthorized 500 Failure</p> <p>Example:</p> <pre>{ "timestamp":1510131853621, "status":200, "data":[{ "name":"AT", "code":"AT" }, { "name":"CH", "code":"CH" }, { "name":"CZ", "code":"CZ" }, { "name":"DE", "code":"DE" }] }</pre>
--	------------------------------	------------	-----------	----------------------------	---

<p>GET <u>/api/openncp/forms/countries/attributes/{country}/{language}</u></p>	<p>get list of attributes related to a country</p>	<p>Yes</p>	<p>No</p>	<p>PathParam: language, country</p>	<p>200 OK 401 Unauthorized 500 Failure</p> <p>Example (Austria):</p> <pre>{ "timestamp":1510132078582, "status":200, "data":{ "identifiers":[{ "key":"patient.search.patient.id*", "domain":"2.16.17.710.780.1000.990.1" }, { "key":"patient.data.givenname*", "domain":"2.16.17.710.780.1000.990.1" }], "friendlyName":"healthInsuranceId" }, "demographics":[{ "label":"patient.data.surname*", "length":3, "mandatory":true, "userValue":null, "key":"patient.data.surname", "type":"text", "userDateValue":null }, { "label":"patient.data.givenname*", "length":3, "mandatory":true,</pre>
--	--	------------	-----------	-------------------------------------	---

					<pre>"userValue":null, "key":"patient.data.givenname", "type":"text", "userDateValue":null }, { "label":"patient.data.birth.date", "length":0, "mandatory":false, "userValue":null, "key":"patient.data.birth.date", "type":"calendar", "userDateValue":null }] }</pre>
--	--	--	--	--	--

					<pre>"createdAt": 1516620220000, "expiration": 1516622020000 } }</pre>
--	--	--	--	--	--

<p>GET /api/openncp/auth/login</p>	<p>Initiates Single-Sign-On Authentication Redirects to login page of country</p>	<p>Yes</p>	<p>No</p>		<p>302 Found 401 Unauthorized 500 Failure</p> <p>After successful login, a response that contains JWT is sent to a specific POST method.</p> <p>Then the client saves locally the JWT and redirects to home page.</p>
------------------------------------	---	------------	-----------	--	---

<p>POST /api/openncp/secure/xcpd</p>	<p>get patient details</p>	<p>Yes</p>	<p>Yes</p>	<p>Example</p> <pre>{ "demographics": { "address": "string", "birthDate": "2017-07-11T09:54:33.737Z", "city": "string", "country": "string", "email": "string", "firstname": "string", "gender": "string", "lastname": "string", "phone": "string", "postalCode": "string" }, "destination": "string", "identifiers": { "identifier": [{ "extension": "string", "root": "string" }] } }</pre> <p>Example (Portugal):</p> <pre>{ "identifiers":{ "identifier":[{</pre>	<p>200 OK 401 Unauthorized 500 Failure</p> <p>Example (Portugal):</p> <pre>{ "timestamp": 1510134403255, "status": 200, "token": { "jwt": "jwt value", "createdAt": 1510134379000, "expiration": 1510136179000 }, "data": { "name": "MARCIA FILIPA MARQUES SA", "familyName": "", {</pre>
--------------------------------------	----------------------------	------------	------------	--	---

				<pre> "root": "2.16.17.710.860.1000.990.1", "extension": "294584908" }], }, "demographics": null, "destination": "PT" } </pre>	<pre> "country": "PT", "birthDate": null, "administrativeGender": "F", "city": "Almada", "root": "2.16.17.710.860.1000.990.1", "extension": "294584908", "postalCode": "2800-0", "email": null, "address": "PRACETA PCT D LEONOR MASCARENHAS 39 1 ESQ", "telephone": null } } </pre>
--	--	--	--	---	--

<p>GET /api/openncp/secure/xca/list/{doctype}</p>	<p>get patient documents</p>	<p>Yes</p>	<p>Yes</p>	<p>PathParam: doctype Possible Values: {ps, ep}</p> <p>RequestParam: purpose Possible Values: {EMERGENCY, TREATMENT}</p> <p>Example http://192.168.1.212:10000/secure/xca/list/ps?purpose=EMERGENCY</p>	<p>200 OK 401 Unauthorized 500 Failure</p> <p>Example (Portugal):</p> <pre>{ "timestamp":1510134516413, "status":200, "token":{ "jwt":"jwt value", "createdAt":1510134379000, "expiration":1510136179000 }, "data":{ "documents":[{ "title":"Patient Summary", "description":"The Patient Summary document (CDA L3 /</pre>
---	------------------------------	------------	------------	---	---

					<p>Structured body) for patient 294584908",</p> <p> "author":null,</p> <p>"creationDate":"20130503",</p> <p> "healthcareFacility": "",</p> <p> "file":null,</p> <p>"uuid":"2.16.840.1.113883.19.5%5E2.25.9139295586369480952779965774588992728.1",</p> <p>"formatCode":"urn:epSOS:ps:ps:2010",</p> <p>"nodeRepresentation":"urn:epSOS:ps:ps:2010",</p> <p> "schema":"epSOS formatCodes",</p> <p>"repositoryId":"2.16.620.1.101.10.5.3",</p>
--	--	--	--	--	---

					<pre>"hcid":"urn:oid:2.16.17.710.820.1000.990.1", "docType":"ps" }, { "title":"Patient Summary", "description":"The Patient Summary document (CDA L1 / PDF body) for patient 294584908", "author":null, "creationDate":"20130503", "healthcareFacility":""," "file":null, "uuid":"2.16.840.1.113883.19.5% 5E2.25.913929558636948095277 9965774588992728.2",</pre>
--	--	--	--	--	---

					<pre>"formatCode": "urn:ihe:iti:xds- sd:pdf:2008", "nodeRepresentation": "urn:ihe:it i:xds-sd:pdf:2008", "schema": "IHE PCC", "repositoryId": "2.16.620.1.101.10 .5.3", "hcId": "urn:oid:2.16.17.710.820.1 000.990.1", "docType": "ps" }] } }</pre>
--	--	--	--	--	---

<p>POST /api/openncp/secure/xca/retrieve/{doctype}/{language}/{transform}</p>	<p>get patient summary</p>	<p>Yes</p>	<p>Yes</p>	<p>PathParam: doctype Possible Values: {ps, ep}</p> <p>PathParam: doctype Possible Values: {1, 0}</p> <p>PathParam: language</p> <p>Body { "hcid": "string", "repositoryId": "string", "uuid": "string" }</p> <p>Example http://192.168.1.212:10000/secure/xca/retrieve/ps/en/0</p> <p>{ "hcid": "urn:oid:2.16.17.710.860.1000.990.1", "repositoryId": "2.16.620.1.101.10.3.29.54290", "uuid": "2.16.620.1.101.10.3.29.54290%5E2.25.2.PS.1" }</p>	<p>200 OK 401 Unauthorized 500 Failure</p> <p>Returns the CDA in XML if transform is 0 or in HTML if transform is 1</p>
---	----------------------------	------------	------------	---	---

<p>POST /api/openncp/service/transform/document/{language}</p>	<p>transform XML patient summary to HTML</p>	<p>Yes</p>	<p>No</p>	<p>@RequestBody cda RequestParam commonstyle(true/false)</p> <p>Example http://192.168.1.212:10000/secure/transform/document/en?commonstyle=false</p> <p>Body <ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:epsos="urn:epsos-org:ep:medication" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd"> </ClinicalDocument></p>	<p>Returns the patient summary in HTML format</p>
<p>POST /api/openncp/secure/dispensation</p>	<p>send dispensation document</p>	<p>Yes</p>	<p>Yes</p>	<p>Post the Dispensation Document</p>	

2. Error Handling - Responses

No Patients found

```
{
  "timestamp": 1544526148973,
  "status": 200,
  "data": {
    "cause": null,
    "stackTrace": null,
    "code": 5004,
    "description": "No Patients found",
    "message": null,
    "localizedMessage": null,
    "suppressed": []
  }
}
```

No Document Exist

```
{
  "timestamp": 1544526886197,
  "status": 200,
  "data": {
    "cause": null,
    "stackTrace": null,
    "code": 6007,
    "description": null,
    "message": "XDSMissingDocument",
    "localizedMessage": "XDSMissingDocument",
    "suppressed": []
  }
}
```

vi. Secure Communication with other NCPeHs

Within eHealth DSI, the consumer (Query operations) and the provider (Retrieve operations) do not know each other. The Circle of Trust is among NCPs. They are solely able to establish mutual trust relationships. The final trust relationship is (n:n) and set up based on direct trust relationships among NCPs. The key issue is that an NCP can rely on the agreed behaviour of another NCP. More information can be found in eHDSI System Architecture Specification v.3.0.0¹⁶.

1. Secure Exchange of messages

CEF eHDSI OpenNCP is securing the exchanges between the nodes based on a trust model supporting X509 certificates. The security is relying on the Public Key Model (CEF PKI). Almost all the NCPeH configuration is automatically managed. The only manual action happens during the installation phase.

16

https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/System+Architecture+Specifications?preview=/37752811/110494953/eHDSI_System_Architecture_Specification_v3.0.0_OR.pdf

- Configure Service Consumer & Provider keystores
- Configure Signature keystore
- Update NCPeH truststore (import Root CA and Chain for CEF PKI, eHDSI Gazelle, SMP Servers).

There are 3 tomcat instances installed. The SSL Configuration in each of them is like below

- OpenNCP Portal (1 way SSL)
- NCP-B (1 way SSL)
- NCP-A (2 way SSL)

2. Two-Way SSL

Two-way TLS is used between NCPs and from the NCP (pharmacy system connector) to pharmacy systems. This ensures integrity of the data exchange.

Establishing the encrypted channel using certificate-based 2-Way SSL involves:

1. OpenNCP Client from Country B request access to a protected resource from NCP-A (XCPD, XCA)
2. The NCP-A Server presents its certificate to the NCP-B client
3. The NCP-B client verifies the NCP-A server certificate.
4. If successful, the NCP-B sends its certificate to the NCP-A Server
5. The NCP-A Server verifies the NCP-B client's credentials.
6. If successful, the NCP-A Server grants access to the protected resource requested by the NCP-B Client.

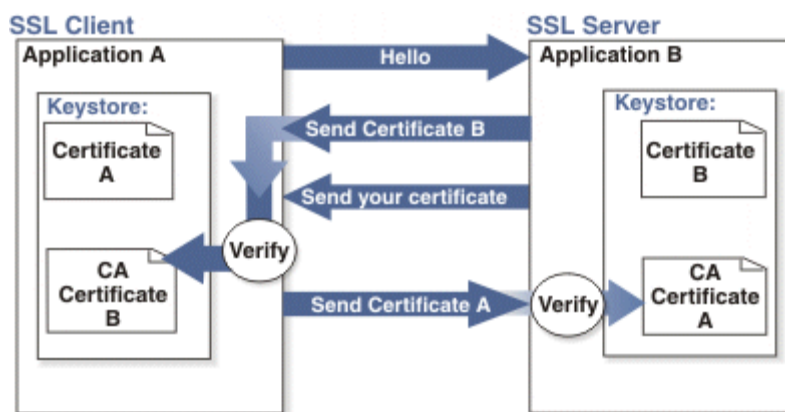


Figure 7 Two-Way SSL between NCPs

vii. OpenNCP Audits

There are three kind of audits.

- ATNA Audits

- Obligations
- Audits from eADC components

1. ATNA Audits

If you have enabled the property WRITE_TEST_AUDITS then you can find audits in your server in the path defined in property TEST_AUDITS_PATH. All audits are also persist in openatna database.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AuditMessage>
  <EventIdentification EventActionCode="E" EventDateTime="2018-02-06T14:53:48.384+01:00"
EventOutcomeIndicator="0">
    <EventID code="ITI-55" displayName="XCPD::CrossGatewayPatientDiscovery" codeSystemName="IHE
Transactions"/>
    <EventTypeCode code="epsos-11" displayName="epsosIdentityService::FindIdentityByTraits"
codeSystemName="epSOS Transaction"/>
  </EventIdentification>
  <ActiveParticipant UserID="Liferay" UsersRequestor="true">
    <RoleIDCode code="Resident Physician" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.2"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="SPPprovidedID&doctor@openncp.com@Liferay&gt;" AlternativeUserID="doctor"
UsersRequestor="true">
    <RoleIDCode code="medical doctor"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="CN=ncp-ppt.cy.ehealth.testa.eu, O=University of Cyprus, C=CY"
UsersRequestor="true" NetworkAccessPointID="62.62.115.79" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="ServiceConsumer" displayName="epSOS Service Consumer" codeSystem="epSOS"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="CN=ncp-ppt.mt.ehealth.testa.eu, O=Ministry for Health, C=MT"
UsersRequestor="false" NetworkAccessPointID="62.62.113.141" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="ServiceProvider" displayName="epSOS Service Provider" codeSystem="epSOS"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="MT-1"/>
  <ParticipantObjectIdentification
ParticipantObjectID="9999001M^^^&2.16.470.1.100.1.1.1000.990.1&ISO"
ParticipantObjectTypeCode="1" ParticipantObjectTypeCodeRole="1">
    <ParticipantObjectIDTypeCode code="2" displayName="Patient Number" codeSystemName="RFC-3881"/>
    <ParticipantObjectName>Patient</ParticipantObjectName>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="urn:uuid:55116477-717f-4812-887f-35249eddfd4f"
ParticipantObjectTypeCode="4">
    <ParticipantObjectIDTypeCode code="req" displayName="Request Message" codeSystemName="epSOS
Msg"/>
    <ParticipantObjectDetail type="securityheader"
value="PHNvYXBibnY6SGVhZGVyIHhtbG5zOnNvYXBibnY9Imh0dHA6Ly93d3cudzMub3JnLzlwMDMvMDUvc29hcC1l
bnZlbg9wZS1geG1sbnM6d3NhPSJodHRwOi8vd3d3LnczLm9yZy8yMDA1LzA4L2FkZlJlc3NpbmciPjx3c3NlOINiY3VyaX
R5IHhtbG5zOndzc2U9Imh0dHA6Ly9kb2NzLm9hc2lzlW9wZW4ub3JnL3dzcy8yMDA0LzAxL29hc2lzlTlwMDQwMS13
c3Mtd3NzZWN1cm10eS1zZWNIeHQtMS4wLnhzZCI+PHNhbWwyOkFzc2VydGlubiB4bWxuczpzYW1sMj0idXJuOm9hc
2lzOm5hbWVzOnRjOINBTUw6Mi4wOmFzc2VydGlubiG5zOnNvYXBibnY9Imh0dHA6Ly93d3cudzMub3JnLzlwMDMvMDUvc29hc
c5vcmcvc29hcC9lbnZlbg9wZS8iIHhtbG5zOnhzPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaGVtYSIgSUQ9II8
4NTNjZmNIYS1hM2E1LTQ5OWEtYjVjMS0yZjVmNm15MWI0NmEiElzc3VlSW5zdGFudD0iMjAxOC0wMi0wNlQxMzo1
```

MzozNi41NjRaliBWZXJzaW9uPSlyLjAiPjxzYW1sMjJc3N1ZXIgtMftZVF1YWxpZmlhcj0idXJuOmVvc29zOndwMzQ6YX
NzZXJ0aW9ucyI+dXJuOmllkDpDWTpb3VudHJ5Qjwvc2FtbDI6SXNzdWVpPjxkcZpTaWduYXR1cmUgeG1sbnM6ZHM9
Imh0dHA6Ly93d3cudzMub3JnLzlwMDAvMDkveG1sZHNpZyMiPjxkcZpTaWduZWRJbMzVpPjxkcZpDYW5vbmljYWxpe
mF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWwMxNG4jliAvPj
xkcZpTaWduYXR1cmVNZXR0b2QgQWxb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjcjN
hLXNoYTEiIC8+PGRzOlJlZmV5ZjZSBVUkk9liNfODUzY2ZjZWETYNhNS00OTIhLWl1YzEtMmY1ZjZiOTFiNDZlHj48ZH
M6VHJhbnNmb3Jtcz48ZHM6VHJhbnNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8wOS94bW
xkc2InI2VudmVsb3BlZC1zaWduYXR1cmUiIC8+PGRzOlRyYW5zZm9ybSBbbGdvcmI0aG09Imh0dHA6Ly93d3cudzMub
3JnLzlwMDEvMTAveG1sLWV4Yy1jMTRuYlYl+PGVjOkluY2x1c2I2ZU5hbWVzcGFjZXMgeG1sbnM6ZWM9Imh0dHA6Ly9
3d3cudzMub3JnLzlwMDEvMTAveG1sLWV4Yy1jMTRuYlYlUjZmI4TGZldD0ieHMilIC8+PC9kcZpUcmFuc2Zvcml0+PC9
kcZpUcmFuc2Zvcml1zPjxkcZpEaWdlc3RNZXR0b2QgQWxb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3
htbGRzaWcjc2hhMSIglZ48ZHM6RGlnZXNOVmFsdWU+MGZCc0MxRW1EdUIGN0I4cVZqK2EvVDErQTIFPTwvZHM6RG
lnZXNOVmFsdWU+PC9kcZpSZWZlcmVuY2U+PC9kcZpTaWduZWRJbMzVpPjxkcZpTaWduYXR1cmVWYXw1ZT5tMHZhd
HNNckNSOXDBOGdjSldvWlhzEXBWWUZwZ0FIQlVQKlZT0xTZHVpRDlIb1UzUUtYU9Oa3QxUUExdzJBWGY1cU5WW
ldEL08raXQ0Mw1XRdJ5aXQ5MVV5WlITQmFPYnpvNm11dGRxMnZHNzZOeXF3eEtuVUIWVEZY2RZdFBLd2JFalUxSj
g4N0IYY3hSQUlJQWtvTRoeVBUbU9KM2EzWUpeWNRKdG9PC9kcZpTaWduYXR1cmVWYXw1ZT48ZHM6S2V5S5W5
mbz48ZHM6WDUwOURhdGE+PGRzOlgl1MDIDZXJ0aWZpY2F0ZT5NSUIEUgPdq0FzZwDbD0lCQWdJQlp6QU5CZ2txa
GtpRzl3MEJBUTBGQURBMU1Rc3dDUVIEVIFRROV3SkNSVEVUTUJFR0ExVUVDZ3dLClNVaEZJRvYxy205d1pURVJNQTh
HQTFVRUF3d0ISVWhFVTBrZ1EwRXdiaGNOTVRjeE1qQTFNRMxTmPJMfdoY05NamN4TWpBMU1EYzEKTmpJMFdq
QINNUXN3Q1FZRFZRUUdFd0pEV1RFZE1Cc0dBMMVVFQ2d3VZXNXBkbVZ5YzJsMGVTQnZaaUJEZVhCeWRYTXhKREF
pQmdOVgpCQU1NRzI1amNDMxMjZmZm91WTRndVpXaGxZV3gwYUM1MfPjYtYjZUzVsZFRDQm56QU5CZ2txaGtpRzl3M
EJBUUUVGQUFPQmpRQXdnWWtDCmdZRUfud3ZENk8xeGRFMW5HMWt6RXXraTVXRWRXm3Z1dnp6TVIDRVBFNnp
5TVvtQVJGL29ZTnpITiFuNDI6ajRsbpHYm9JZ2I4VWYKTzLUk1qNGV2V1Z5dXZxOSt5SmFneWcrK2J5cTJ6SW9pUE11
YWIkMjZjV0NKODV0MlJpSWkyZ2dDVStxQXpWTEtPMXJUaDluNVM4ZwpDT1k1MytjVm5LWGVwR0QRRepDRGdIVU
NBd0VBQWFPQ0FUOHdnZ0U3TUVR0ExVVRld1JDTUUVBd1BxQThvRHFT0doMGRlQnpPaTh2CloyRjZaV3hzWIM1b
GFHUnphUzVwYUdVdFpYVnliM0JsTG01bGRDOW5jM012WTNkC0x6SXZmKzqY213dVkzSnNRRWNHQ1dDR1NBR0
cKk0VJQkIBUTZGamhVzEhSd2N6b3ZMMmRoZW1Wc2JHVXVaV2hrYzJrdWFXaGxMV1YxY205d1pTNXVaWFF2WjNO
ekwyTnliQzh5TDJOaApZM0pzTG1OeWJEQkhCZ2xnaGtnQmh2aENBUU1FT2hZNGFIUjBjSE02THk5bllYcGxiR3hsTG1
Wb1pITnBMbWxvWIMxbGRYSnZjR1V1CmJtVjBMMmR6Y3k5amNtd3ZNaTlqWVdOeWJDNWpbjXd3SHdZRFZSMGpC
Qmd3Rm9BVTfDRHI2MzZCE54cTI2eWd5TIhStkpCa0E3RXcSFFZRFZSME9CQlIFRkJKThPERkN3NmQ2VjdkTWkvSz
A1WmXebXh5dU1Bd0dBMMVVRXdfQj93UUNQUF3RGdZRFZSMFBBUUGvQkFRRApBZ2JBTUEwR0NtCudTSWlZrFFF
QkRRVUFBNEdCQUZ4dUVlci84dzlFUkpkS2ZtaW5vZXVdDlA1VXIVRFVNdFRaalZtSVFnaXdEdCV5CnNXOVdYU3VGTfd
FOWlwTWx2SkVCQXFCcENsdUx2VzhPMm92YVptSGxuQUJ5Ky9VTWpFU2U2dy9JMFawYINDNnVRakhwSx01WU9K
YVikdEhld3FERTVaSInvt05DL1FOUkpmafiWtZJeXbQWlNHThMvZEPBQjk4UFpiT1hIPC9kcZpYNTA5Q2VydGImaWN
hdGU+PC9kcZpYNTA5RGFOYt48L2RzOktleUluZm8+PC9kcZpTaWduYXR1cmU+PHNhbWwyoIN1YmplY3Q+PHNhbW
wyOk5hbWVJRCBgb3JtYXQ9InVybjpvYXNpczpuYW1lczp0YzpzTQU1MOjEuMTpuYW1laWQtZm9ybWF0OmVtYWlsQ
WRkcmVzcyl+ZG9jdG9yQG9wZW5uY3AuY29tPC9zYW1sMjJpOYW1SUUQ+PHNhbWwyoIN1YmplY3RDb25maXJtYXRp
b24gTWV0aG9kPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6Y206c2VuZGVyLXZvdWNoZXMilIC8+PC9zYW1s
MjJpTdWJqZWNOpJxzYW1sMjJpDb25kaXRpb25zIe5vdEJlZm9yZT0iMjAxOC0wMi0wNiQxMz01MjJpNi41NjRaliBOB3R
Pbk9yQWZ0ZXI9IjIwMTgtMDItMDZUMTU6NTM6MzYuNTY0WlglZ48c2FtbDI6QXV0aG5TdGFOZw1lbnQgQXV0aG5J
bnN0YW50PSlyMDE4LTAyLTA2VDEzOjUzOjM2LjU2NFoiPjxzYW1sMjJpBdXR0bkNvbNRIeHQ+PHNhbWwyoOkF1dGhuQ
29udGV4dEh5YXNzUmVmPnVybjpvYXNpczpuYW1lczp0YzpzTQU1MOjluMDphYzpjGfzc2VzOIBhc3N3b3JkPC9zYW1
sMjJpBdXR0bkNvbNRIeHRDbGFzc1JlZj48L3NhbWwyoOkF1dGhuQ29udGV4dD48L3NhbWwyoOkF1dGhuU3RhdGVtZW5
0PjxzYW1sMjJpBdHRyaWJ1dGVtdGF0ZW1lbnQ+PHNhbWwyoOkF0dHJpYnV0ZSBGcmllbmRseU5hbWU9IlhtUEEgc3Vi
amVjdCltMftZT0idXJuOm9hc2lzOm5hbWVzOnRjOnhhY21sOjEuMDpzdWJqZWNOOnN1YmplY3QtaWQilE5hbWVG
b3JtYXQ9InVybjpvYXNpczpuYW1lczp0YzpzTQU1MOjluMDphdHRybMftZS1mb3JtYXQ6dXJpIj48c2FtbDI6QXR0cmliD
RlVmfSdWUgeG1sbnM6eHNpPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaGVtYS1pbN0Yw5jZSigeHNpOnR
5cGU9InhzOnN0cmliZyl+ZG9jdG9yPC9zYW1sMjJpBdHRyaWJ1dGVWYXw1ZT48L3NhbWwyoOkF0dHJpYnV0ZT48c2Ft
bDI6QXR0cmliDRIIEZyaWVvZGx5TmftZT0iWFNQQSByb2xlllBOYW1PSJ1cm46b2FzaXM6bmFtZXM6dGM6eGFjBw
w6Mi4wOnN1YmplY3Q6cm9sZSIgTmftZUzvcmlhdD0idXJuOm9hc2lzOm5hbWVzOnRjOINBTUw6Mi4wOmF0dHJyY
W1lLWZvcmlhdDp1cmkiPjxzYW1sMjJpBdHRyaWJ1dGVWYXw1ZSb4bWxuczp4c2k9Imh0dHA6Ly93d3cudzMub3JnLz
lwMDEvWE1MU2NoZW1hLWluc3RhbMNIliB4c2k6dHlwZT0ieHM6c3RyaW5nIj5tZWRpY2FslGRvY3Rvcjwvc2FtbDI6Q
XR0cmliDRIIVmfSdWU+PC9zYW1sMjJpBdHRyaWJ1dGU+PHNhbWwyoOkF0dHJpYnV0ZSBGcmllbmRseU5hbWU9Ilht


```
nZUIEIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDA1LzA4L2FkZHJlc3NpbmciPnVyb1dWlkOjU1MTE2NDc3LTcx
N2YtNDgxMi04ODdmLTM1MjQ5ZWRkZmQ0ZjwvTWVzc2FnZUIEPjx3c2E6VG8+aHR0cHM6Ly82Mi42Mi4xMTMuMT
QxOjk0NDMvb3Blbm5jcC13cy1zZXJ2ZXlvc2VydmljZXMvWENQRf9TZXJ2aWNIPC93c2E6VG8+PC9zb2FwZW52OkhY
WRlcj4="/>
```

```
</ParticipantObjectIdentification>
<ParticipantObjectIdentification ParticipantObjectID="urn:uuid:dbf62bfb-f6a1-425c-b22f-36da8b3740fb"
ParticipantObjectTypeCode="4">
  <ParticipantObjectIDTypeCode code="rsp" displayName="Response Message" codeSystemName="epSOS
Msg"/>
  <ParticipantObjectDetail type="securityheader"
value="PHNvYXBlbnY6SGVhZGVyIHhtbG5zOnNvYXBlbnY9Imh0dHA6Ly93d3cudzMub3JnLzlwMDMvMDUvc29hcC1l
bnZlbG9wZSIgZ4="/>
</ParticipantObjectIdentification>
</AuditMessage>
```

The possible audits are:

Service	Operation	Event ID	Event Name	Who
epSOSIdentificationService	FindIdentityByTraits	epsos-11	epsosIdentityService::FindIdentityByTraits	NCP-A
epSOSIdentificationService	FindIdentityByTraits	epsos-11	epsosIdentityService::FindIdentityByTraits	NCP-B
epSOSIdentificationService	FindIdentityByTraits	epsos-11	epsosIdentityService::FindIdentityByTraits	NCP-A
epSOSPatientService	List	epsos-21	epsosPatientService::List	NCP-B
epSOSPatientService	List	epsos-21	epsosPatientService::List	NCP-A
epSOSOrderService	List	epsos-31	epsosOrderService::List	NCP-B
epSOSOrderService	List	epsos-31	epsosOrderService::List	NCP-A
epSOSDispensationService	Initialize	epsos-41	epsosDispensationService::Initialize	NCP-B

epSOSDispensationService	Initialize	epsos-41	epsosDispensationService::Initialize	NCP-A
epSOSDispensationService	Discard	epsos-42	epsosDispensationService::Discard	NCP-B
epSOSDispensationService	Discard	epsos-42	epsosDispensationService::Discard	NCP-A
epSOSConsentService	Put	epsos-51	epsosConsentService::Put	NCP-B
epSOSConsentService	Put	epsos-51	epsosConsentService::Put	NCP-A
epSOSConsentService	Discard	epsos-52	epsosConsentService::Discard	NCP-B
epSOSConsentService	Discard	epsos-52	epsosConsentService::Discard	NCP-A
epSOSConsentService		epsos-53	epsosConsentService::PIN	NCP-B
Country-B Identity Provider	Issuance of HCP Identity Assertion	epsos-91	identityProvider::HcpAuthentication	NCP-B
Country-B NCP	Issuance of a TRC Assertion	epsos-92	ncp::TrcAssertion	NCP-B
SMP	SMP::Push	ehealth-194	SMP::Push	NCP-A
SMP	SSM_import	ehealth-194	SMP::Query	NCP-B

2. Non-Repudiation audits

The obligation audits are being written in /home/openncp/apps/epsos-configuration/obligations. The non-repudiation procedures specified and developed by eHDSI are applied, even if it is acknowledged that the current procedures are not fully capable of dispute resolution.


```

DQ4WjBRMQswCQYDVQGEWJNVDEcMBoGA1UECgwTTWluaXN0cnkgZm9yIUhYVWx0aDEkMCIGA1UEAwbbmNw
LXBwdC5tdC5laGVhbHRoLnRlc3RhLmV1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCIhDbs6VUBKh5cPexB
oIX8G8T4EmXI/8t0QHwnqAJ+tyjiLvrWpYZCPT82/C6A+nVZAVo5AIBlpQ0KeOLQXyptOdWI7m4KzRNK3//gVTNmWAa
k+AWSzBSPq5mXLE7I+UrJK7B5m866m5YhFk15sKxYIETCyivOABqXYKuRmkvCAwIDAQABo4IBVDCCAIAwSQYDVR0f
BEIwQDA+oDygoOy4aHR0cHM6Ly9nYXplbGxLMVoZHNpLmloZS1ldXJvcGUubmV0L2dzcY9jcmwvMi9jYWNYbC5jcm
wwRwYjYIZIAYb4QgEEBDoWOGh0dHBzOi8vZ2F6ZWxsZS5laGRzaS5paGUtZXVyb3BlLm5ldC9nc3MvY3JslZlVY2Fjcm
wuY3JSMecGCWCGSAGG+EIBAwQ6FjhodHRwcovL2dhemVsbGUuZWwhkc2kuaWhlLWV1cm9wZS5uZXQvZ3NzL2Ny
bc8yL2NhY3JslmNybDAfBgNVHSMEGDAWgBTUIPK/foF03Gr2/KDI1dE0kGQDsTAdBgNVHQ4EFgQU3KaYdzManYnx
UHI510KZ6DIPxswDAYDVR0TAQH/BAIwADAObgNVHQ8BAf8EBAMCBSAwEwYDVR0IBAwwCgYIKwYBBQUHAWewD
QYJKoZIhvcNAQENBQADgYEABLDYbKldZg5Q66fJE6LZBnljyy25JQPZfN4jYAr3P6IhopwxUaAv8BKry8xcS0rBSWJu2
FmRyJJIvleCjBIO1maL80rKb5gV1G7rYRqYy6CwWkf92oh6xURrcqXEovmtVvW4DNhHRTX+sbJSdpWN/723lec0GN6H
w/jmWO+o=</ns4:X509Certificate>
  </ns4:CertificateDetails>
</ns4:SenderDetails>
<ns4:RecipientsDetails>
  <ns4:EntityDetails>
    <ns4:CertificateDetails>
<ns4:X509Certificate>MIIDPTCCAqagAwIBAgIBVzANBgkqhkiG9w0BAQOFADA1MQswCQYDVQGEWJCRTEtMBEGA
1UECgwKSUUhFIEV1cm9wZTERMA8GA1UEAwwIRUUhEU0kgQ0EwHhcNMTcxMTE3MDgzNTE5WhcNMjcxMTE3MDgz
NTE5WjBRMQswCQYDVQGEWJNVDEcMBoGA1UECgwTTWluaXN0cnkgZm9yIUhYVWx0aDEkMCIGA1UEAwbbmNw
LXBwdC5tdC5laGVhbHRoLnRlc3RhLmV1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCTZbGIPhVSBTvjPK
X4Xn3etwO0Lc8us5B0SNR+zwpezrJulj6qyNoUYZu679ObXxMrSJMltWBz/VFqDlsvMLwrW2M8el5kXGhlzI9ilaTK6ZXI
9qWos/alkJrXhIXy0I+y5ITN3kcC0KvqBJLJOR/BDXuXUXSasS0W8/DVG32BQIDAQABo4IBPzCCATswSQYDVR0fBEIwQD
A+oDygoOy4aHR0cHM6Ly9nYXplbGxLMVoZHNpLmloZS1ldXJvcGUubmV0L2dzcY9jcmwvMi9jYWNYbC5jcmwwRwYj
YIZIAYb4QgEEBDoWOGh0dHBzOi8vZ2F6ZWxsZS5laGRzaS5paGUtZXVyb3BlLm5ldC9nc3MvY3JslZlVY2FjcmwuY3JSM
EcGCWCGSAGG+EIBAwQ6FjhodHRwcovL2dhemVsbGUuZWwhkc2kuaWhlLWV1cm9wZS5uZXQvZ3NzL2Nybc8yL2Nh
Y3JslmNybDAfBgNVHSMEGDAWgBTUIPK/foF03Gr2/KDI1dE0kGQDsTAdBgNVHQ4EFgQUUGxNbowfnfKphaV8NvLSBk
VdM5NVYwDAYDVR0TAQH/BAIwADAObgNVHQ8BAf8EBAMCBSAwDQYJKoZIhvcNAQENBQADgYEA8POGiLJ74dV+
0ISwwwAcVWuzl7x5Q3bm6BPxTlror/llEybkgm7m4BS12g7brrEHA5hRtobUOqnHAYueYqhykbWeSW4QoIJFETlwkBv
OlmRlFvRNjsgyAdWYUJz4u0hW9uczuAleSRP6Dlcv6KeBwmJT8msP9vX4IgrWxkQ=</ns4:X509Certificate>
  </ns4:CertificateDetails>
</ns4:EntityDetails>
</ns4:RecipientsDetails>
<ns4:SenderMessageDetails isNotification="false">
  <ns4:MessageSubject>ITI-55</ns4:MessageSubject>
  <ns4:UAMessageIdentifier>_56698af9-90f3-4177-bffe-
0cff570a0086__20180205120803099</ns4:UAMessageIdentifier>
  <ns4:MessageIdentifierByREMMD>_56698af9-90f3-4177-bffe-
0cff570a0086__20180205120803099</ns4:MessageIdentifierByREMMD>
  <DigestMethod Algorithm="SHA256" />
  <DigestValue>GGixioNpn+BdA1WAwwTDNz9tiaPomvYyflwUNSH6hpY=</DigestValue>
</ns4:SenderMessageDetails>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
      </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

```

```

    <ds:DigestValue>LaXHnjLZOadhdt1KLo4WppGg4w8=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>idXhnFH078+5yPD7YILN97pHLJIttxvL7whr+hc62hb84yKjmj2mtPIXEWLUK6Z1sqybcuRpzVEQa3
O7WXv2aNoEjQmndhe2LYj0g1eSxvrPZtzDxzOBBmprnWifVXlpD3w/8D1LhKiNIX4gHTA3Doqe2XRX590s1H9kCYL7dU
Y=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>

<ds:X509Certificate>MIIDPTCCAqagAwIBAgIBVzANBgkqhkiG9w0BAQ0FADA1MQswCQYDVQQGEWJCRTEtMBEGA1
UECgwKSUhfIEV1cm9wZTERMA8GA1UEAwwiRUhEU0kgQQEwHhcNMTcxMTE3MDgzNTE5WjBMRQswCQYDVQQGEwJNVDEcMBoGA1UECgwTTWluaXN0cnkgZm9yIEhYwX0aDEkMCIGA1UEAwwbbmNwL
XBwdC5tdC5laGVhbHRoLnRlc3RhLmV1MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQCTZbGIPhVSBTvjPKX4X
n3etwO0Lc8us5B0SNR+zwpezrJulj6qyNoUYZu679ObXxMrSJMltWBz/vFqDlsvMLwrW2M8eI5kXGhZl9ilaTK6ZXI9qW
os/alkJrXhIXy0I+y5ITN3kcC0KvqBJLJOR/BDXuXUXSasS0W8/DVG32BQIDAQABo4IBPzCCATswSQYDVR0fBEIwQDA+o
DygOoY4aHR0cHM6Ly9nYXplbGxILmVoZHNpLmloZS1ldXJvcGUubmV0L2dzcY9jcmwvMi9jYWwNybC5jcmwwRwYJYIZI
AYb4QgEEBDoWOGh0dHBzOi8vZ2F6ZWxsZS5laGRzaS5paGUtZXVyb3Bllm5ldC9nc3MvY3JsLzlvY2FjcmwvY3JsMEcG
CWCGSAGG+EIBAwQ6FjhodHRwczovL2dhemVsbGUuZWwhkc2kuaWhlLWV1cm9wZS5uZXQvZ3NzL2NybC8yL2NhY3Js
LmNybDAfBgNVHSMEGDAWgBTUIPK/foF03Gr2/KDI1dE0kGQDsTAdBgNVHQ4EFgQUGxNbownfkphaV8NvLSBkVdM
5NVYwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBsAwDQYJKoZIhvcNAQENBQADgYEA8POGiLJ74dV+0ISw
wwAcVWuzl7x5Q3bm6BPxTIrorc/IIeybkgm7m4BS12g7brrEHA5hRtobUOqnHAYueYqhykbWeSW4QoIJFETlwkbvOlm
RIFvRNJsgyAdWYUJz4u0hW9uczuAleSRPf6Dlcv6KeBwmJT8msP9vX4IgrwxkwQ=</ds:X509Certificate>
    </ds:X509Data>
    <ds:KeyValue>
      <ds:RSAKeyValue>

<ds:Modulus>k2WxpT4YVUgU74zyl+F593rcDtC3PLrOQdEjUfs8KXs6ybil+qsjaFGGbuu/Tm18TK0iTJbVgc/1RagyLLzC8
K1tjPHpeZFxpYc5fYpWkyumVypalqLP2pZCa14SF8tCPSuSEzd5HAtCr6gSSyTkfwQ17l1F0mrEtFvPw1Rt9gU=</ds:Mod
ulus>
    <ds:Exponent>AQAB</ds:Exponent>
  </ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>
</ns4:SubmissionAcceptanceRejection>
<!-- Comment after -->

```

3. eADC audits

The ePOS Automatic Data Collection is designed in order to facilitate:

- The **automatic**, unsupervised *information gathering* and **data extraction** from every NCP transaction or consumer document that passes the NCP;
- **Persistent storage** of the resulting data sets in a RDBMS, available within each NCP;
- The flexible definition of extraction rules and their specific application onto transactions or consumer documents;

The Database schema for these audits is the one below.

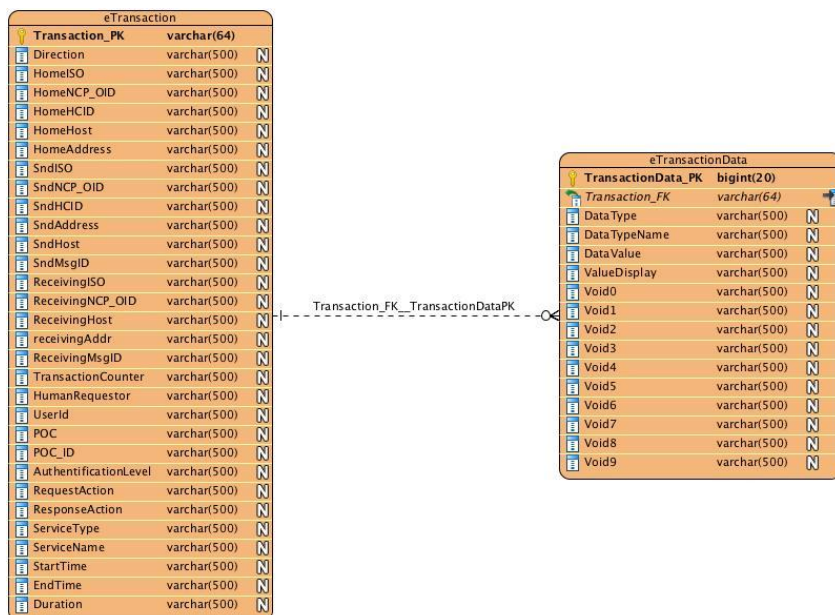


Figure 8 eADC Database Schema

More information can be found in eHDSI eADC Specifications v3.0.0¹⁷.

Using eADC database of OpenNCP we fulfill monitoring and reporting activities based of CEF Monitoring and Reporting framework, to ensure the systematic and continuous collection of data for transparency purposes and informed decision-making. For more information regarding these procedures, please refer to Annex TE 3 Monitoring and Reporting Tool.

viii. More information

More information regarding the installation and parameterization of the OpenNCP, can found as following:

- Virtual Machines Installation: AIII. Appendix VM Preparation
- Servers Preparation: AII. Appendix Servers Preparation
- OpenNCP Properties: A.III Appendix OpenNCP Properties
- Terminology Server: AIV. Appendix Terminology Server
- SMP and Certificates: AV. Appendix SMP and Certificates

ix. OpenNCP A description

The clinical information for PS and eP documents is collected on the fly from the Data Zone. Regarding PS, the clinical information is created from the DB PS latest version. More information can be found in Sections A3.a.vii, A4.e and A5.

x. OpenNCP B description

Application Servers in Application Zone are responsible to generate an eD document in case an eP of an EU citizen is dispensed in Cyprus.

1. create_eD()

For a given EU patient, *create_eD()* API is responsible to gather all the data needed for the construction of the eD document from a dispensed eP XML document and then construct the document based on the eP Functional Requirements guidelines. The endpoints are http://10.227.195.91/cefcy/create_eD and http://10.227.195.91:8443/cefcy/create_eD using POST method.

A5. Data Flows Description

a. Access through National Portal

When Cyprus is acting as a country B, NCPeH CY is responsible to request the documents from country A, PS and/or eP. Also, the system will support the eDispensation services. Thus, NCPeH CY is able to dispense an eP and generate an eD CDA XML document and then send it to the country A. The sequence diagrams showing the data flows of the afore-described procedure is depicted

i. Public Sector Doctor

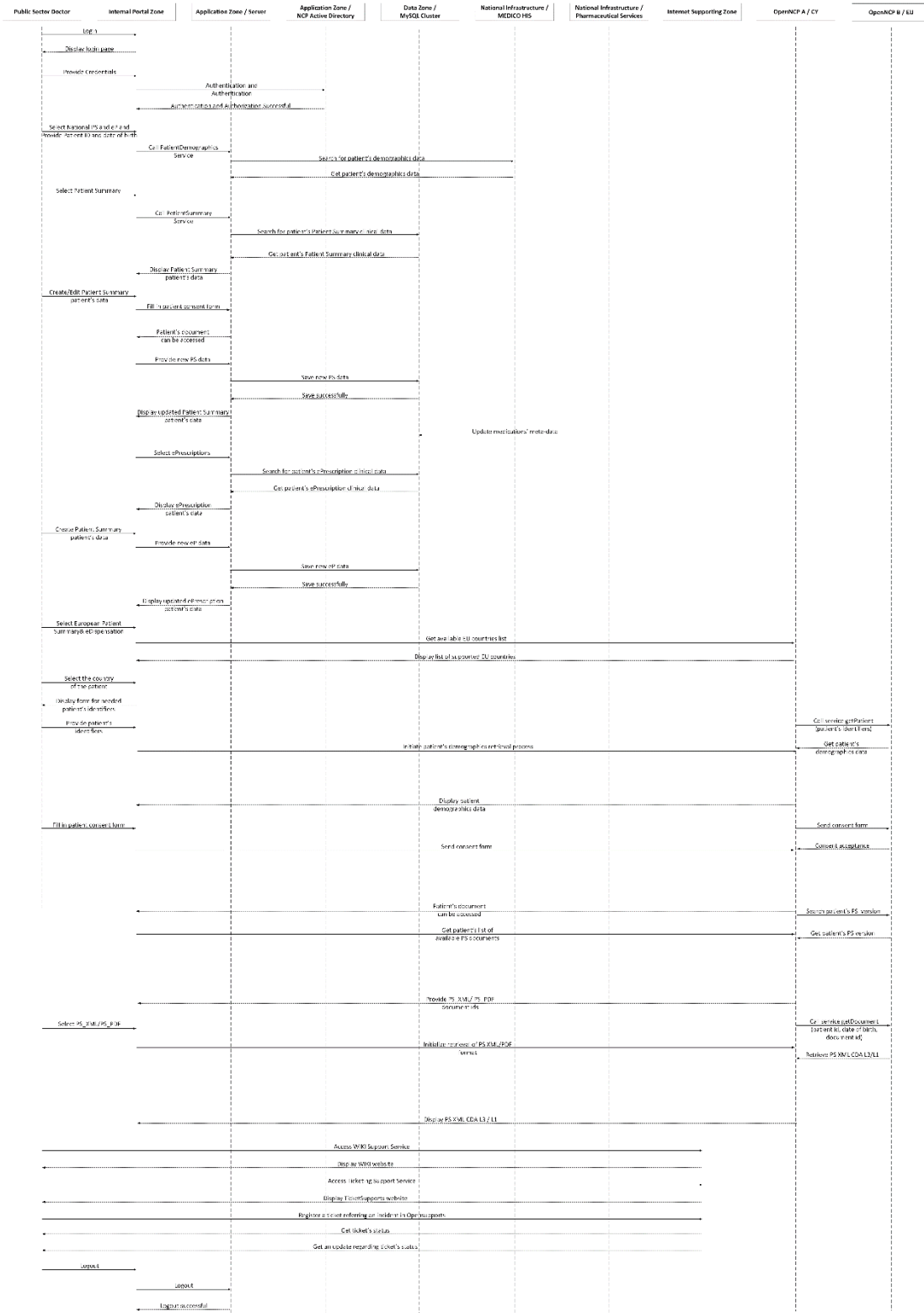


Figure 9: Public Sector Doctor access to services through National Portal

ii. Private Sector

1. User Authentication and Authorization through ARIADNI SSO and 2-way SSL

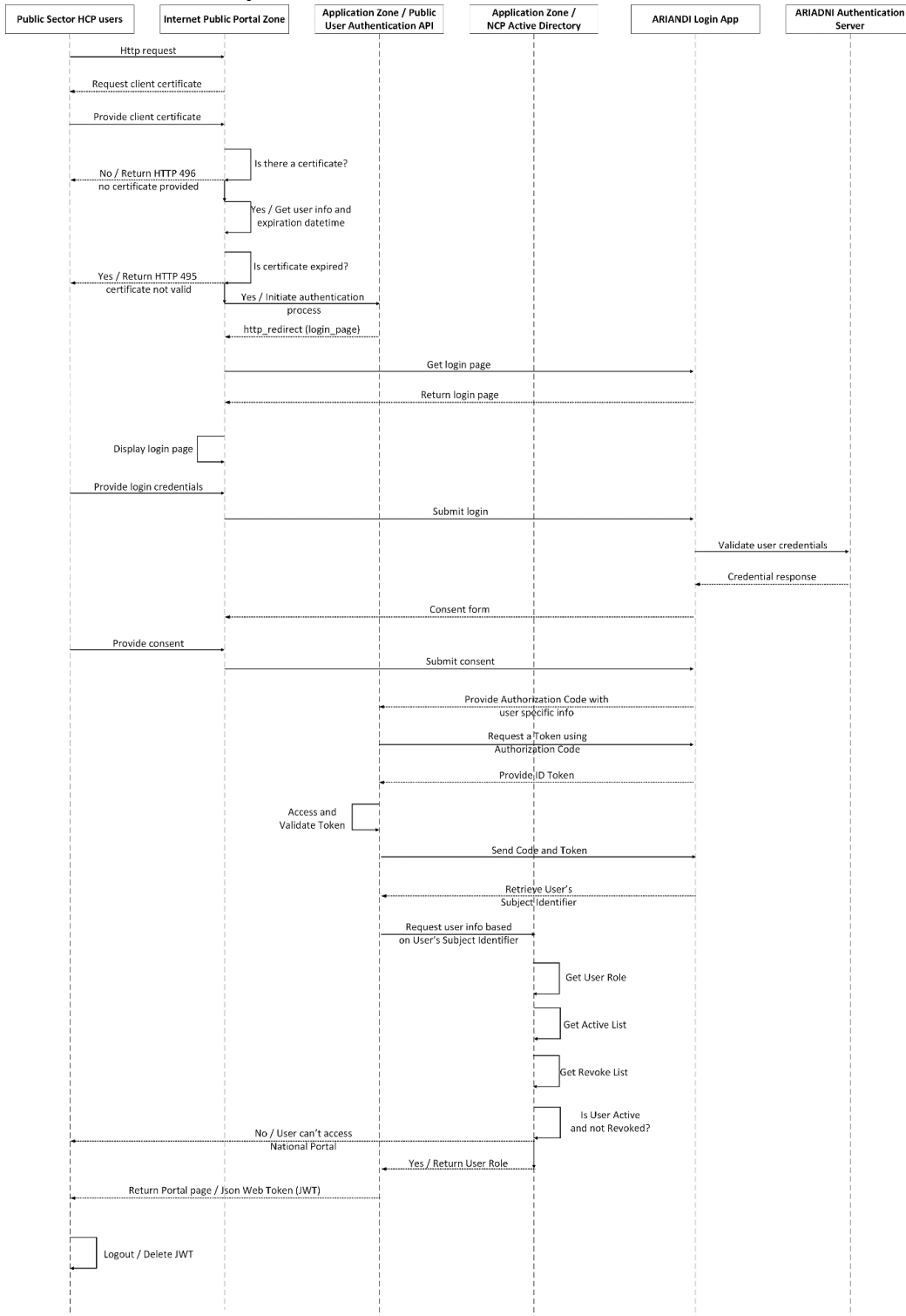


Figure 10: Private Sector User Authentication and Authorization dataflow

3. Pharmacist

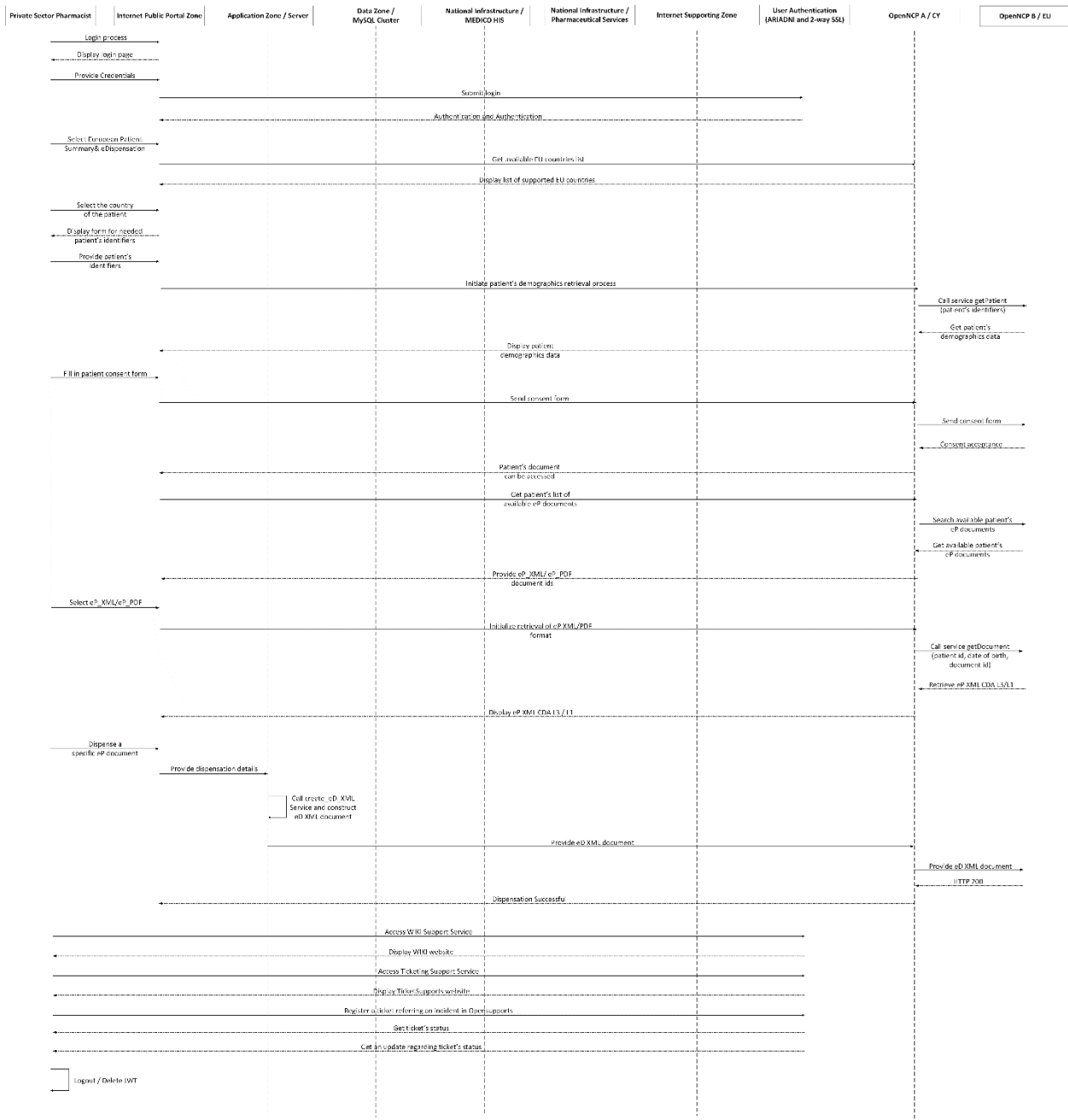


Figure 12: Private Sector Pharmacist access to services through National Portal

iii. Supporting Services

1. WIKI website and Service Desk Monitoring

a. Third Party Vendors / Software Integrators

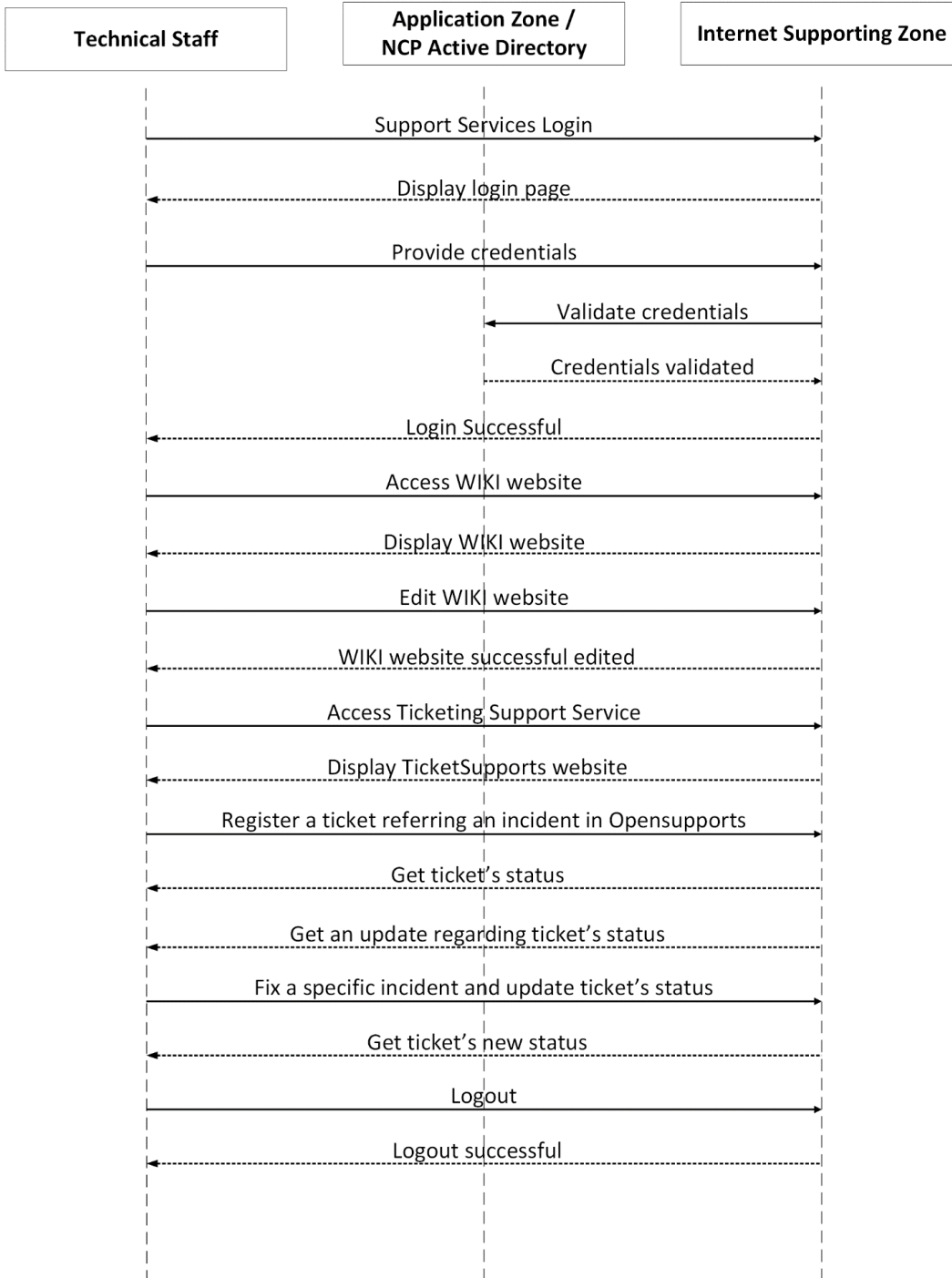


Figure 13: WIKI website and Service Desk Monitoring dataflow

b. Foreign country Service Desk

b. Cross-border through TESTA

When Cyprus is acting as a country A, NCPeH CY is responsible to provide to country B the requested documents, PS and/or eP.

i. Cyprus acting as Country-A for Patient Summary Service

The sequence diagram showing the data flow when Cyprus is acting as Country-A for PS service is depicted in Figure 14: Cyprus acting as Country A for PS service.

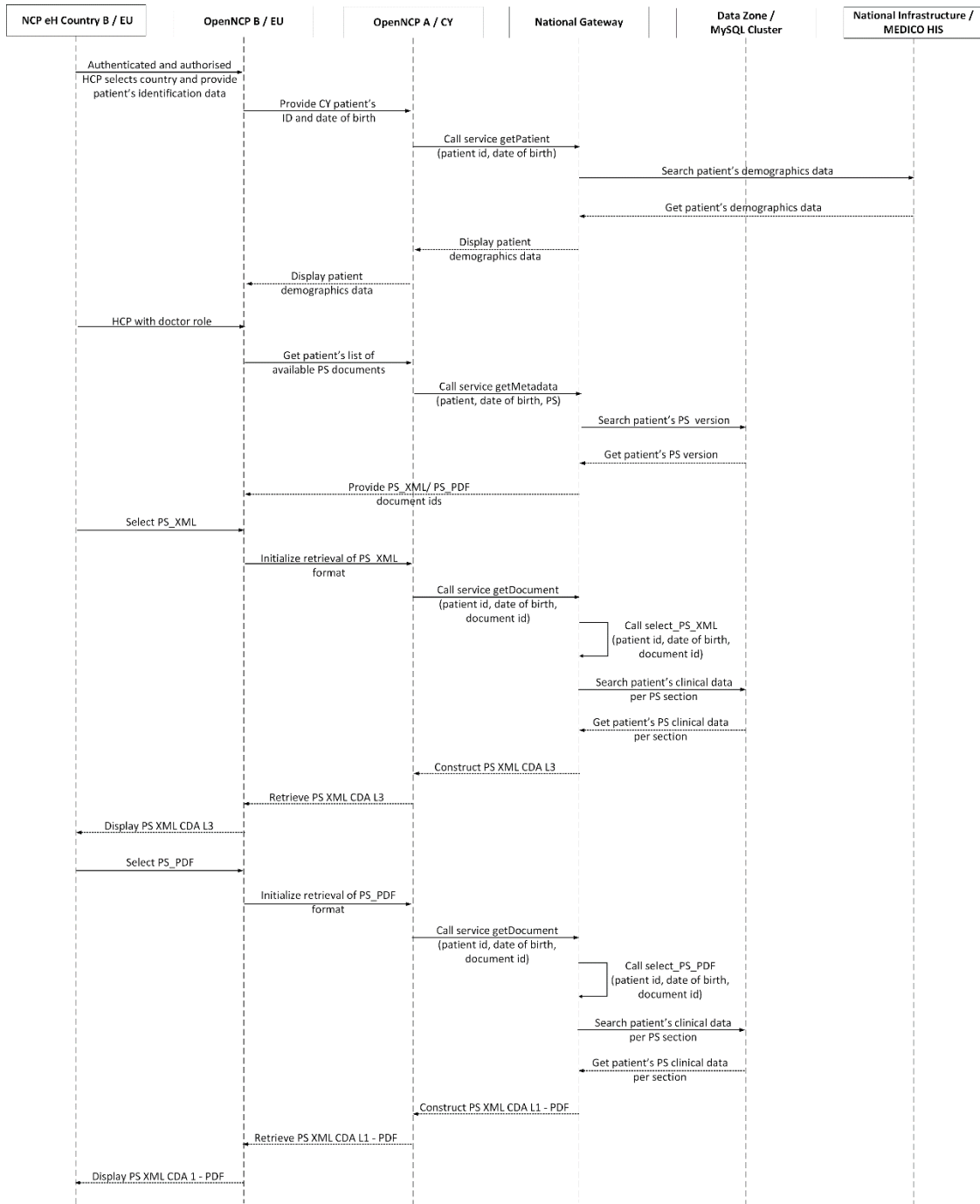


Figure 14: Cyprus acting as Country A for PS service

ii. Cyprus acting as Country-A for ePrescription Service

The sequence diagram showing the data flow when Cyprus is acting as Country-A for PS service is depicted in .

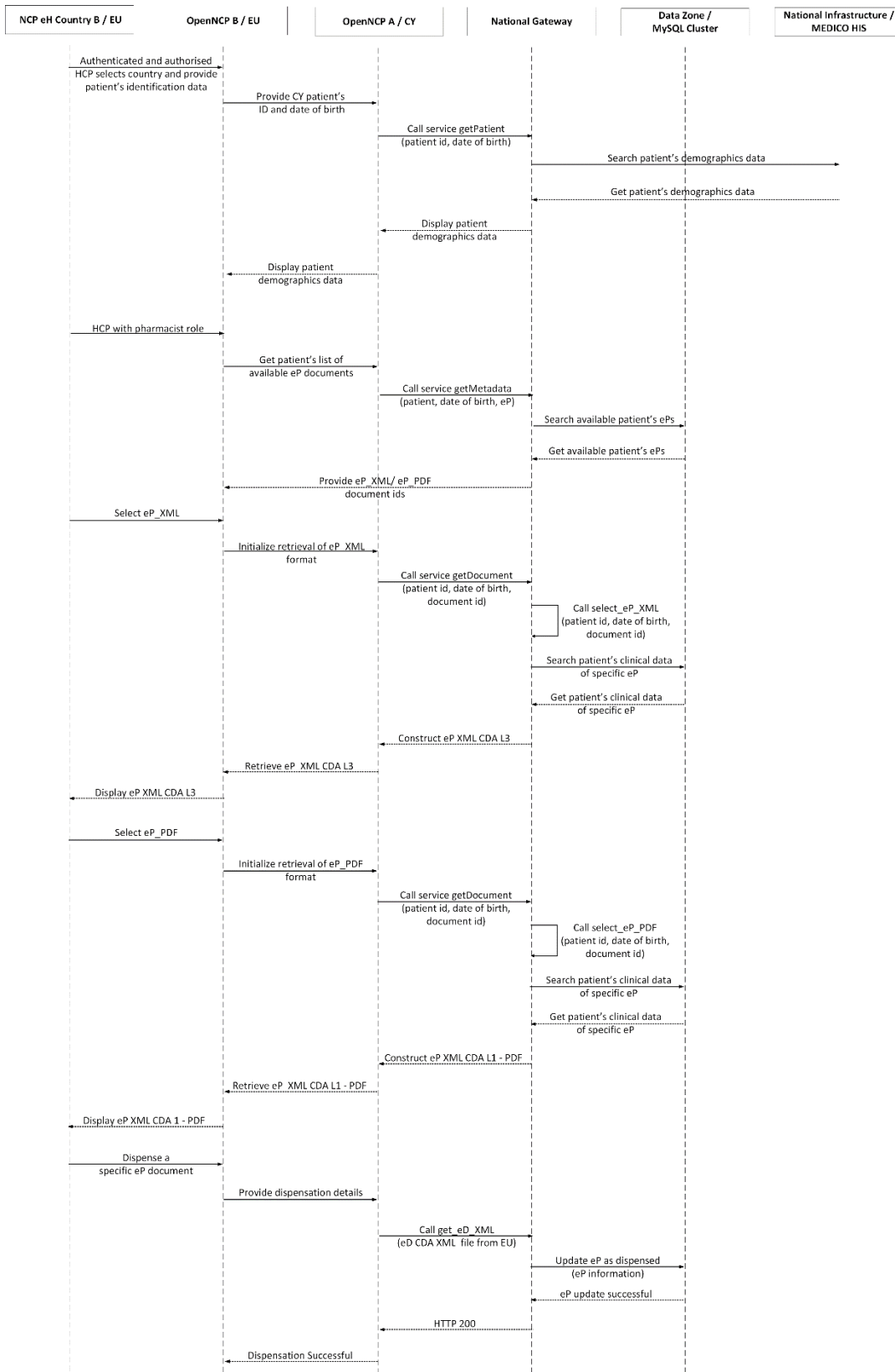


Figure 15: Cyprus acting as Country A for eP service

c. Patient Summary and ePrescription Services: Step-by-step

A patient must give his/her consent before his/her medical data are stored in the National Portal.

As can be seen in Figure 16, when an HCP reaches the National Portal can login using his/her credentials.

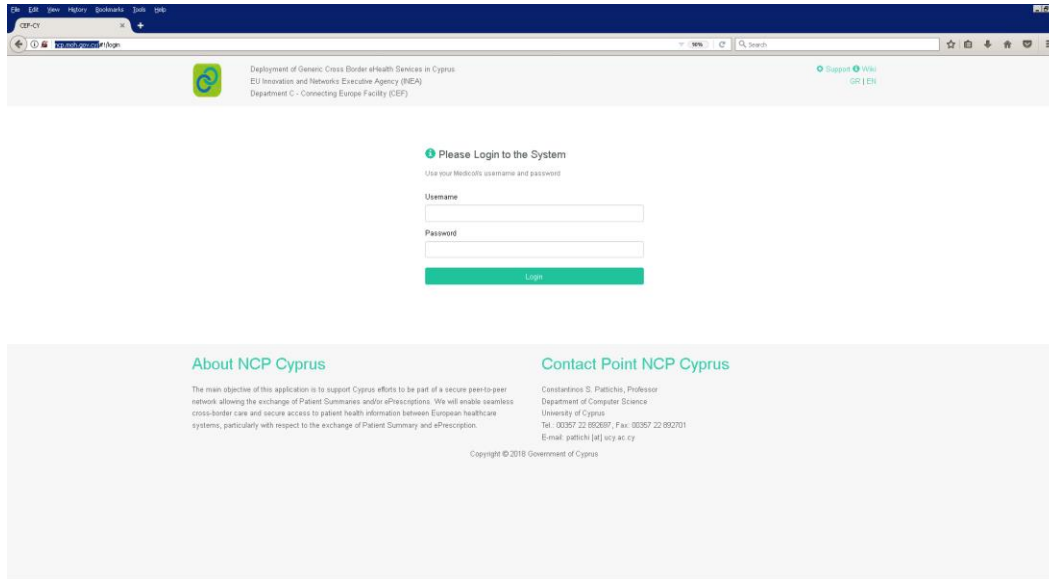


Figure 16: National Portal Login Page

On the next page as depicted in Figure 17, an HCP select to access either National Patient Summary and ePrescription page or European Patient Summary and eDispensation. National Patient Summary and ePrescription supports PS-A and eP-A services and European Patient Summary and eDispensation PS-B and eD services.

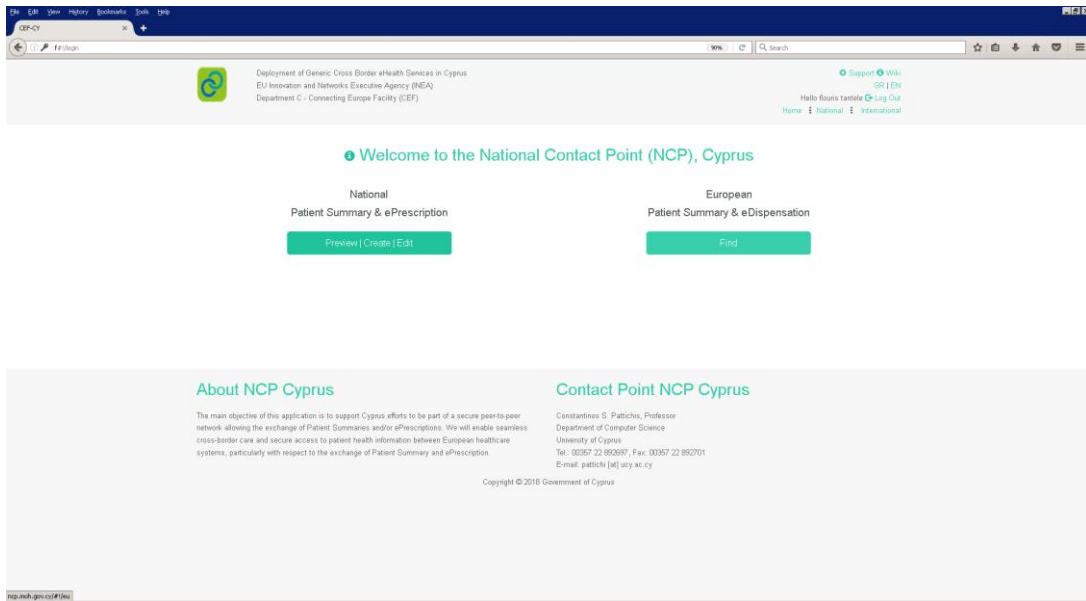


Figure 17: National Portal Welcome Page for an authenticated HCP

When an HCP push National Patient Summary and ePrescription button, he/she sees a page like Figure 18, where he/she must provide the patient identifies, namely patient ID and Date of birth in dd/mm/yyyy format. Both identifiers are mandatory fields.

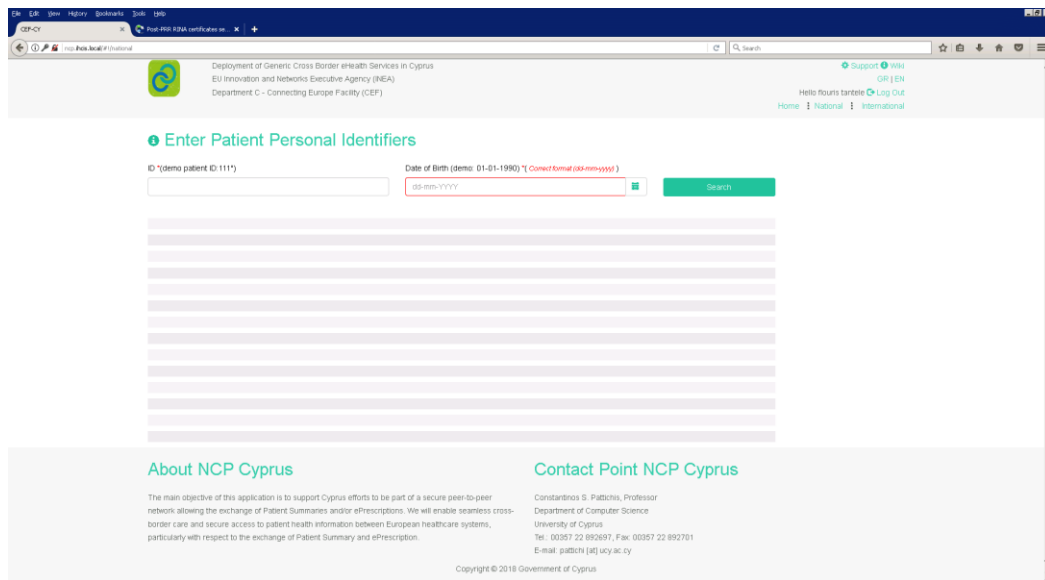


Figure 18: Patient Search Page for services PS-A and eP-A

Next, the HCP must select whether to Preview/Create/Edit a PS or Preview/Create an eP, based on his/her role, as can be seen in Figure 19.

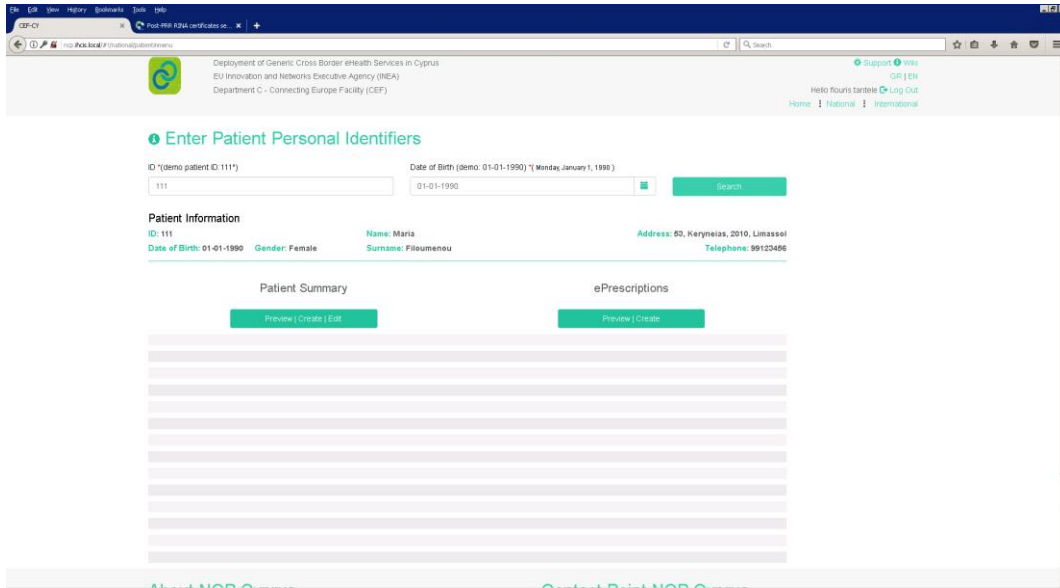


Figure 19: PS-A or eP-A service selection through National Portal

In Figure 20 we can see a preview of the PS sections. A doctor, both Public and Private Sector, have the access to add any information to any section of a PS for a specific Cypriot patient.

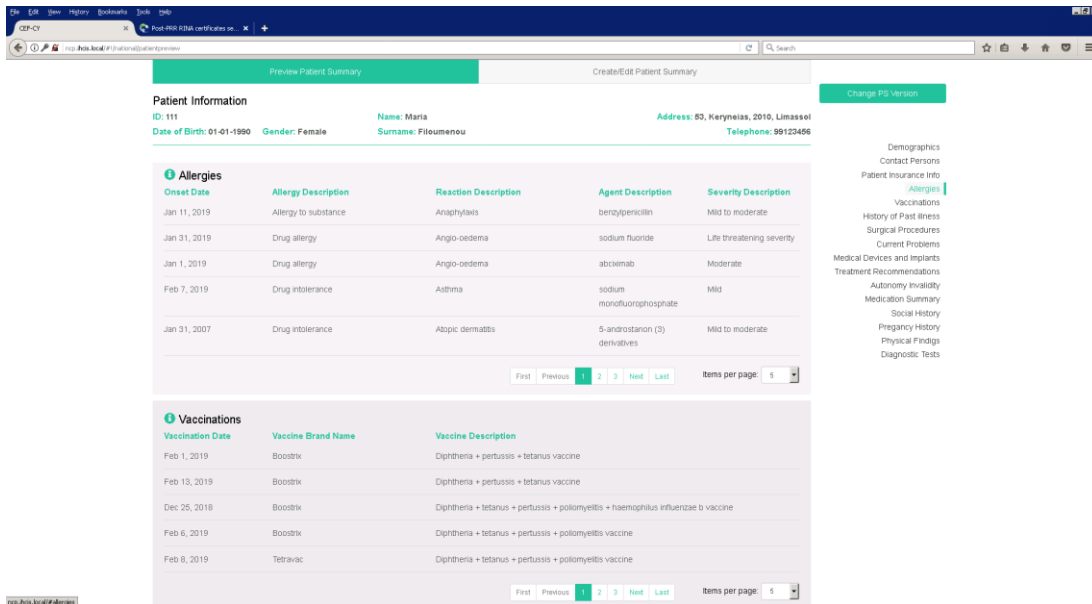


Figure 20: PS sections

A pharmacist has access to preview or create an eP. An example of the preview page can be seen in Figure 21. An example of eP creation is depicted in Figure 22.

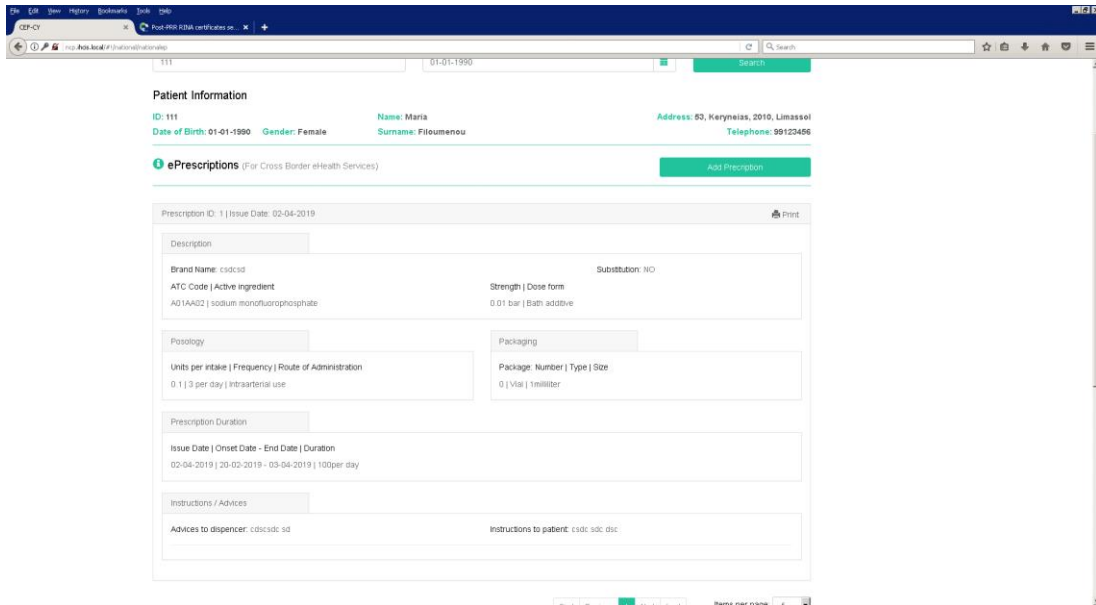


Figure 21: eP preview through National Portal

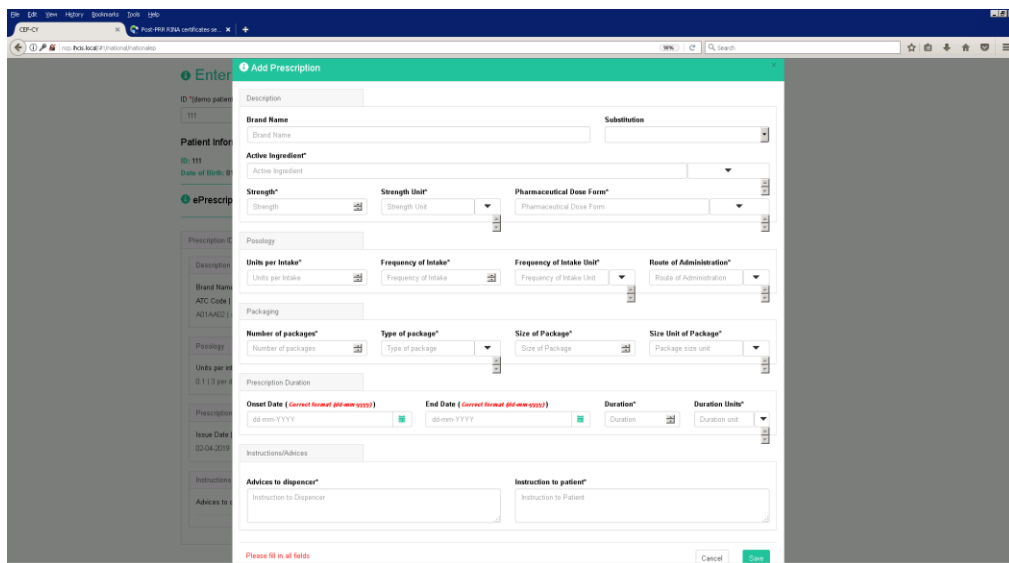


Figure 22: eP creation through National Portal

To support PS-B and eD cross-border services, HCPs can access the National Portal and push European Patient Summary and eDispensation button. On the next step, the HCP must select the country of origin of an EU patient from the country list, as depicted in Figure 23.

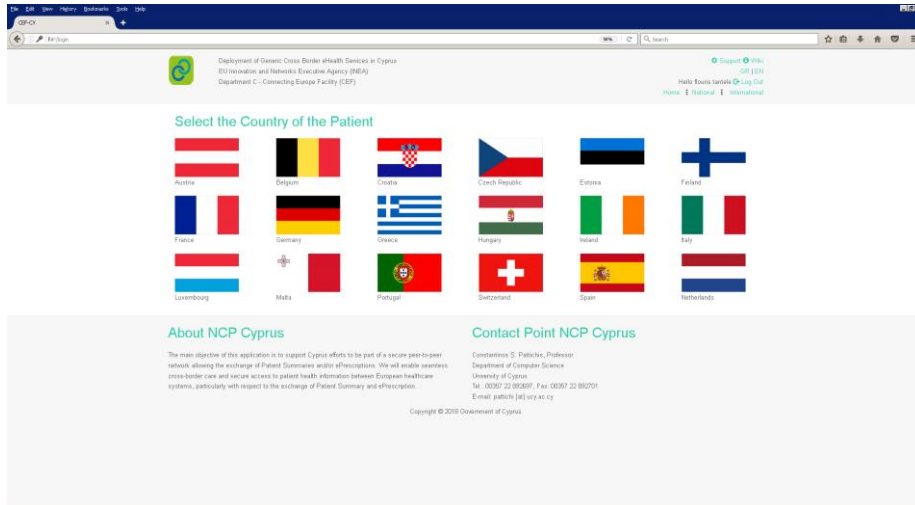


Figure 23: PS-B and eD services' support for European patients through National Portal

Next, based on the country, the HCP must provide the EU patient identifiers as can be seen in Figure 24.

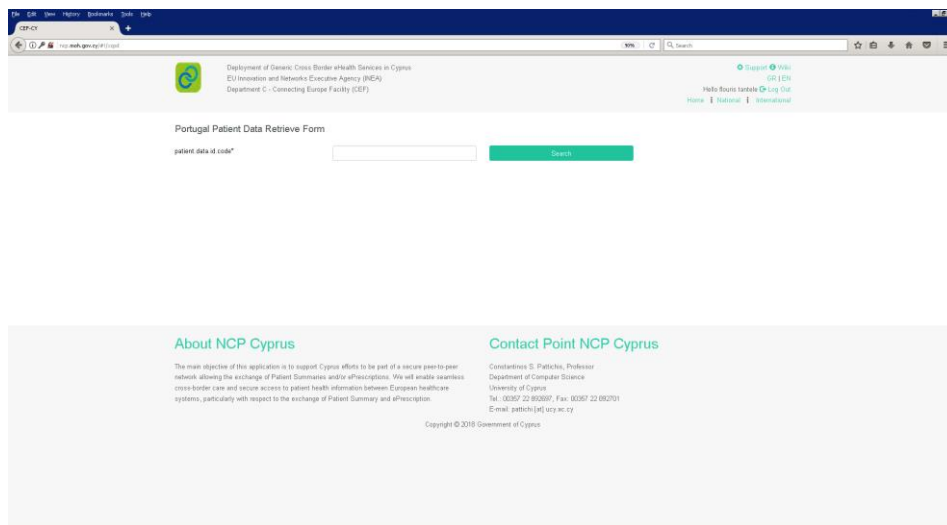


Figure 24: PS and eP document retrieval for a European patient

Then, as can be seen in Figure 25, the HCP gets the patient demographics and clicks the Retrieve Medical Document List button to retrieve the patient's available documents.

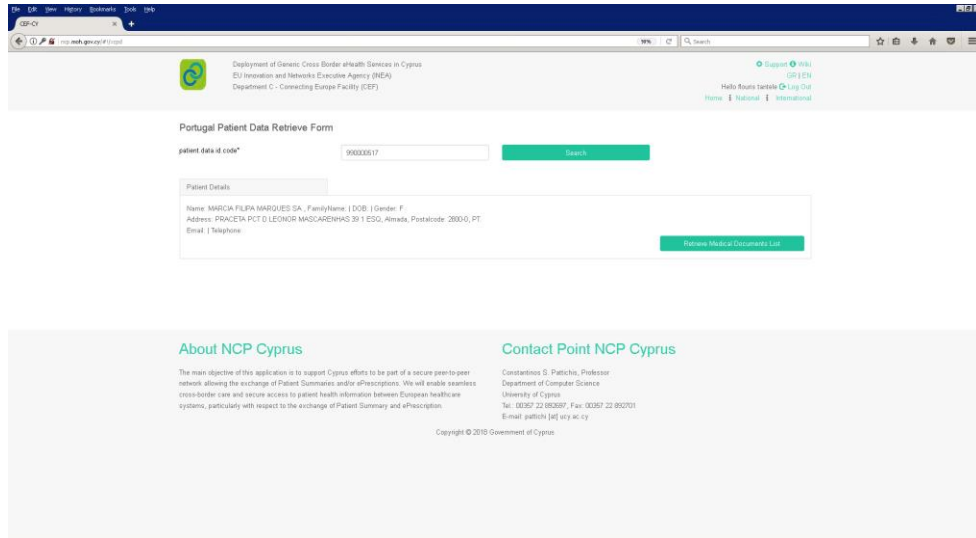


Figure 25: EU patient demographics through National Portal

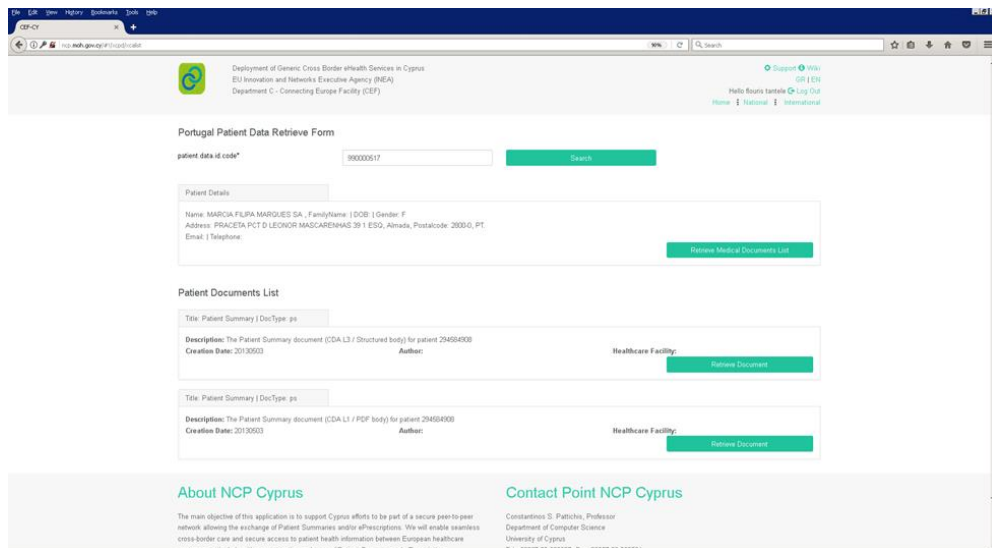


Figure 26: Medical Document List of an EU patient

The results of the previous act are shown in Figure 26. Finally, based on the HCP role, doctor or pharmacist, he/she can retrieve a specific document from the list.

A6. Functional and Non-Functional Requirements

In this section we give a brief description of the functional and nonfunctional requirements of the technical communication gateway. The implementation of the technical communication gateway is based on OpenNCP release 3.0.0, which is compliant with the technical communication gateway functional and nonfunctional requirements.

The following Functional and Non-Functional Requirements are aligned with Patient Summary, ePrescription and eDispensing guidelines.

Functional Requirement	Implementation
<p>FR01 - HP Identification and authentication</p>	<p>YES</p> <ul style="list-style-type: none"> • NCP Active Directory – Sections A3.a.iv.1, A4.a.i and A4.a.ii • Public Sector Doctors – Section 4.2 in Annex OP 2 Operation and Organizational Structure, Section A5.a.i in current document • Private Sector Doctors – Section 11 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.2 in current document • Private Sector Pharmacists – Section 12 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.3 in current document • 2-way SSL – Section A3.a.ii and A5.a.ii.1 for CY HPs in current document • NCP-A side – Section A4.f.iv in current document
<p>FR02 - Trust between countries</p>	<p>YES</p> <ul style="list-style-type: none"> • TESTA Network – Sections A3.b and A5.b in current document • 2 Way SSL Connection – Section 4.f.v.2 for EU HPs in current document
<p>FR03 - Patient identification</p>	<p>YES</p>

	<ul style="list-style-type: none"> Medico HIS identification (Based on Civil Registry Identification) – Section A3.a.viii.1 in current document
FR04 – Patient consent	YES – Section A3.a in current document
FR05 - Structured Information	<p>YES</p> <ul style="list-style-type: none"> CDA Documents based on MVC – Section A4.e
FR06- Equivalent information	<p>YES</p> <ul style="list-style-type: none"> Based on MVC – English Version – Section A4.e
FR07- Information Understandable	English Version
FR08 – Information selection	<p>YES</p> <ul style="list-style-type: none"> Based on MVC – English Version – Section A4.e
FR09 - Prescription presentation	<p>YES</p> <ul style="list-style-type: none"> ePrescription – Section A4.e in current document
FR10 - ‘Available’ (and thus, valid) prescription	<p>YES</p> <ul style="list-style-type: none"> In Cyprus, based on pharmacists’ comments, an eP is available for six months
FR11 - desirable but not minimum: Access to current prescriptions by dispenser	
FR12 - Original prescription	YES
FR13 - Identification of the medicinal product	<p>YES</p> <ul style="list-style-type: none"> Information provided by Pharmaceutical Services of Cyprus – Section A3.a.viii.2 in current document
FR14 - Substitution	YES
FR15 - Dispensed medicine information sent to country A	<p>YES</p> <ul style="list-style-type: none"> Section A4.e.i.4 in current document
FR16 - Identification of original prescription and medicinal product dispensed	<p>YES</p> <ul style="list-style-type: none"> Section A4.e.i.4 in current document
FR17 - Original dispensed medicine	<p>YES</p> <ul style="list-style-type: none"> Retrieved from eD XML document – Section A4.e.i.4 in current document

FR19 - Patient Summary of country A available	<p>YES</p> <ul style="list-style-type: none"> Gnomon API – Sections A4.f.iv and A4.f.vi in current documents National Portal – Section A5.c
FR20 – Information Traceability	<p>YES</p> <ul style="list-style-type: none"> Audit and Logs for all transactions – Section A4.d.2 in current document

Non-Functional Requirement	Implementation
NFR01 Service availability	<ul style="list-style-type: none"> High Available National Infrastructure – Section A3.a.i Backups Policies - Annex TE 1 NCPeH CY Technical deliverable – Part B, Section B13
NFR02 Communications	SSL Communication – Sections A3.a.i and A3.a.ii in current document
NFR03 Response time	Horizontally Scale Infrastructure and response time less than 10 seconds
NFR04 Confidentiality	<ul style="list-style-type: none"> All patient Data are Encrypted protected and safe-guarded – Section A3.a.viii.1 in current document HP involved are fully compliant with their professional code – Section A3.a.iv.1 in current document
NFR05 Access control	<ul style="list-style-type: none"> NCP Active Directory – Sections A3.a.iv.1, A4.a.i and A4.a.ii Public Sector Doctors – Section 4.2 in Annex OP 2 Operation and Organizational Structure, Section A5.a.i Private Sector Doctors – Section 11 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.2 in current document Private Sector Pharmacists – Section 12 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.3 in current document
NFR06 Audit Trail	<ul style="list-style-type: none"> ATNA – Section A4.f.vii.1 in current document

	<ul style="list-style-type: none"> • Audit Log Monitoring Tool – Section A4.d.2 in current document
NFR07 Integrity	OpenNCP Security Manager – Section A4.f.iv in current document
NFR08 Non-repudiation	<p>OpenNCP Evidence Emitter</p> <ul style="list-style-type: none"> • Non-repudiation Audits – Section A4.f.vii.2 in current document
NFR09 Trust between countries	<ul style="list-style-type: none"> • TESTA Network – Sections A3.b and A5.b in current document • 2-way SSL – Section A4.f.vi in current document
NFR10 Guaranteed delivery	OpenNCP Security Manager
NFR12 Supervision services	OpenNCP Configuration and Monitoring Service – Section A4.f.vii in current document

A7. How we ensure confidentiality, integrity, availability, non-repudiation, authenticity and auditability

a. Confidentiality and Integrity

We follow NCPeH CY Data confidentiality and integrity procedures.

As referenced in Section A3.a.viii.1, all patient data are encrypted protected and safe-guarded.

As referenced in Section A3.a.iv.1, health professionals involved are fully compliant with their professional code.

NCP active directory is responsible for the access control to the cross-border services and corresponding documents as referenced in Section A3.a:

- Public Sector Doctors – Section 4.2 in Annex OP 2 Operation and Organizational Structure, Section A5.a.i
- Private Sector Doctors – Section 11 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.2
- Private Sector Pharmacists – Section 12 in Annex OP 2 Operation and Organizational Structure, Section A5.a.ii.3

In terms of patient identity traits, patient id and date of birth are mandatory fields. For more information see Sections A3.a, A4.e.i.1 and A5.b.

eHDSI OpenNCP is securing the exchanges between the nodes based on a trust model supporting X509 certificates. More information can be found in Section A4.f.vi and in Appendix AV.b.

Also, about cross-border confidentiality more information about Secure Communication with Other NCPeH can be found in Section A4.f.vi.

b. Availability

Production environment is a High-Available (HA) environment with cluster database server, load balancer for application server, and DNS failover setup for primary and secondary web servers. More information can be found in Section A3.a.i.

In case of a failure, unplanned stop (bug, random error), partial planned stop (non-optimal running) or planned stop (maintenance, update) Zabbix Monitoring tool will trigger an alert. More information about Zabbix can be found in Section A4.d.1.

c. Non-repudiation

The Evidence Emitter Architectural Building Block enables National Contact points to generate and emit electronic evidence used for non-repudiation purposes, based on each domain respective regulations and technological need.

More information about cross-border non-repudiation can be found in Non-repudiation Audits in Section A4.f.vii.2.

No storage of EU citizens' private healthcare information is performed in the NCPeH CY system.

d. Authenticity

See Sections A3.a, A4.e.i.1 and A5.b.

Also, about cross-border authenticity more information about Secure Communication with Other NCPeH can be found in Section A4.f.vi.

e. Auditability

For auditing the NCPeH CY services, we use two tools:

1. ATNA – Section A4.f.vii.1 in current document
2. Audit Log Monitoring Tool – Section A4.d.2 in current document
3. Zabbix Server Software – Annex OP 3 Zabbix Open-source monitoring tool

AI. Appendix VM Preparation

VM Preparation

Setup Environment

An environment variable has been setup globally in the operating system in order to point to openncp configuration folder

```
export EPSOS_PROPS_PATH=/home/openncp/apps/epsos-configuration
```

Configure openNCP database connectivity

You must update the configmanager.hbm.xml that exists inside EPSOS_PROPS_PATH directory to fit with your JNDI settings (they exist in each tomcat server.xml file)

```
<?xml version='1.0' encoding='utf-8'?>
<!DOCTYPE hibernate-configuration PUBLIC "-//Hibernate/Hibernate
Configuration DTD 3.0//EN"
"http://www.hibernate.org/dtd/hibernate-configuration-3.0.dtd">
<hibernate-configuration>
<session-factory>
<property
name="hibernate.dialect">org.hibernate.dialect.MySQL5Dialect</property>
<property
name="connection.datasource">java:comp/env/jdbc/ConfMgr</property>
<property name="show_sql">>false</property>
<property name="current_session_context_class">thread</property>
<property
name="cache.provider_class">org.hibernate.cache.NoCacheProvider</property>
<property name="hibernate.hbm2ddl.auto">update</property>
<mapping
class="eu.europa.ec.sante.ehdsi.openncp.configmanager.domain.Property"/>
</session-factory>
</hibernate-configuration>
```

JDK Installation

OpenNCP runs using Oracle JDK 8, so you can install JDK 8 using the following commands:

```
sudo add-apt-repository ppa:webupd8team/java
```

```
sudo apt-get update
sudo apt-get install oracle-java8-installer
javac -version
sudo update-alternatives --config java
```

MySQL Server

Setup Database Server

MySQL Database Server is using for storing configuration parameters of OpenNCP, as well the audits and the portal database

MySQL Database Server is using for storing configuration parameters of OpenNCP, as well the audits and the portal database

```
sudo apt-get install mysql-server
sudo mysql_secure_installation
```

Create Schemas

The databases being used from OpenNCP are the following:

Database Name	Usage
epsosproperties	Storing configuration parameters of OpenNCP
eadc	Storing statistics about transactions
openncp_portal	Portal database
openatna	Storing the openatna audits of the transactions
openncp_ltrdb	Storing the terminologies (MVC)
ehealth_logs	Storing several application logs (from logback)

You can create the database schemas using the following commands:

```
CREATE DATABASE `epsosproperties` CHARACTER SET utf8 COLLATE
utf8_general_ci;
CREATE DATABASE `eadc` CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE DATABASE `openncp_portal` CHARACTER SET utf8 COLLATE
utf8_general_ci;
CREATE DATABASE `openatna` CHARACTER SET utf8 COLLATE utf8_general_ci;
CREATE DATABASE `openncp_ltrdb` CHARACTER SET utf8 COLLATE utf8_general_ci;
```

```
CREATE DATABASE `ehealth_logs` CHARACTER SET utf8 COLLATE utf8_general_ci;
```

You can find the sql scripts for creating these databases in the Appendix A – SQL Scripts

Restore Databases

If you already have the above scripts in sql format you can import them to the database using the following commands:

```
mysql -uroot -pchangeit eadc < eadc.sql  
mysql -uroot -pchangeit ehealth_logs < ehealth_logs.sql  
mysql -uroot -pchangeit epsosproperties < epsosproperties.sql  
mysql -uroot -pchangeit openatna < openatna.sql  
mysql -uroot -pchangeit openncp_ltrdb < openncp_ltrdb.sql  
mysql -uroot -pchangeit openncp_portal < openncp_portal.sql
```

All. Appendix Servers Preparation

Servers preparation

We have setup the following servers:

- Apache Web Server to proxy the openncp-portal
- Tomcat instance #1 (version 8) for openncp-ws-server, openatna, trc-sts
- Tomcat instance #2 (version 8) for openncp-client-connector, openncp-gateway
- Liferay 6.2 for openncp-portal

We download the latest artifacts from

<https://ec.europa.eu/cefdigital/artifact/content/repositories/eHealth/eu/europa/ec/sante/ehd/si/> and deploy to the application servers

Deployment

In the Tomcat Instance #1 we have to deploy by copying the war files to webapps directory of tomcat the following war files

- openatna-web.war
- openncp-ws-server.war

In the Tomcat Instance #2 we have to deploy by copying the war files to webapps directory of tomcat the following war files

- openncp-client-connector.war
- trc-sts.war
- openncp-gateway.war

In the liferay instance we have to deploy the war file by copying it to the deploy folder of Liferay. This will be moved to webapps automatically upon deployed successfully

- openncp-portal.war

OpenNCP Portal has its own configuration and this can be found in portal-ext.properties. The file is under /home/openncp/apps/liferay-portal-6.2-ce-ga6

```
jdbc.default.driverClassName=com.mysql.jdbc.Driver
jdbc.default.url=jdbc:mysql://localhost/openncp_portal?useUnicode=true&characterEncoding=UTF-8&useFastDateParsing=false
jdbc.default.username=root
```

```
jdbc.default.password=changeit
# EPSOS ROLES (These roles will be created by default on OpenNCP Portal
startup)
system.roles=Doctor,Pharmacist,Patient,Nurse
system.role.Doctor.description=Doctor Role
system.role.Pharmacist.description=Pharmacist Role
system.role.Patient.description=Patient Role
system.role.Nurse.description=Nurse role
```

Running Services

We can start the services by running the startup script exists in bin directory of each tomcat. For the Tomcat Instance #1 we have to add to setenv.sh the following property in order to initialize correctly the connection to ATNA repository

```
-DopenATNA.properties.path=file:$EPSOS_PROPS_PATH/ATNA_resources/openatna.
properties
```

Databases Configuration

The Database connections are being configured with JNDI inside server.xml

```
<GlobalNamingResources>
<!-- Editable user database that can also be used by
UserDatabaseRealm to authenticate users
-->
<Resource name="UserDatabase" auth="Container"
type="org.apache.catalina.UserDatabase"
description="User database that can be updated and saved"
factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
pathname="conf/tomcat-users.xml" />
<Resource name="jdbc/ConfMgr" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="epsosproperties"
dataSource.user="root"
dataSource.password="changeit"/>
<Resource name="jdbc/TSAM" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
```

```
singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="openncp_ltrdb"
dataSource.user="root"
dataSource.password="changeit"/>
<Resource name="jdbc/EADC_XCPD" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="eadc"
dataSource.user="root"
dataSource.password="changeit"/>
<Resource name="jdbc/EADC_XDR" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="eadc"
dataSource.user="root"
dataSource.password="changeit"/>
<Resource name="jdbc/EADC_XCA" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="eadc"
dataSource.user="root"
dataSource.password="changeit"/>
<Resource name="jdbc/LOGS" auth="Container"
factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource"
```



```

singleton="true"
minimumIdle="2" maximumPoolSize="5"
connectionTimeout="300000"
dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource"
dataSource.serverName="localhost"
dataSource.port="3306"
dataSource.databaseName="ehealth_logs"
dataSource.user="root"
dataSource.password="changeit"/>
</GlobalNamingResources>

```

Logger Configuration

Clinical Data logging

-Dserver.ehealth.mode=PAT/PROD

See more <https://ec.europa.eu/cefdigital/tracker/browse/EHNCP-1359>

The important log files can be found in the following paths

Server	Path
openncp-client-connector	/home/openncp/apps/opennc-client/log/openncp-client-connector.log
openncp-server	/home/openncp/apps/opennc-client/log/openncp-gateway.log
openncp-portal	/home/openncp/apps/opennc-client/log/openncp-trc-sts.log

Logback Configuration

As probably expected, the log levels used are the classic five (5) levels, meaning TRACE, DEBUG, INFO, WARN, ERROR.

The levels are ordered as follows,

TRACE < DEBUG < INFO < WARN < ERROR

The basic selection rule is the following, a log request of level p issued to a logger having an effective level q, is enabled if $p \geq q$.

Regarding our installation, we can set the root log at the logback.xml file. The latter is located under the paths referred in the table below.

Machine	Filepath
Liferay	/home/openncp/apps/liferay-portal-6.2-ce-ga6/tomcat-7.0.62/webapps/epsosportal/WEB-INF/classes
openncp-client	/home/openncp/apps/openncp-client/webapps/openncp-client-connector/WEB-INF/classes

openncp-server

openncp-server /home/openncp/apps/openncp-server/webapps/openncp-ws-server/WEB-INF/classes

The part of the file that has to be modified for the case is the following,

logback.xml

```
<root level="INFO">  
<appender-ref ref="STDOUT"/>  
<appender-ref ref="FILE"/>  
</root>
```

EXAMPLE

Let's assume that the root level is set to INFO and that we have the following lines in our code. Those will give an output (or not) depending on the level they use.

Let's assume that the root level is set to INFO and that we have the following lines in our code. Those will give an output (or not) depending on the level they use.

```
// This request is enabled, because WARN >= INFO  
logger.warn("Low fuel level.");  
  
// This request is disabled, because DEBUG < INFO.  
logger.debug("Starting search for nearest gas station.");
```

All. Appendix OpenNCP Properties

Following is a list of the OpenNCP properties that are used during its operation. These properties being set in epsosproperties database schema.

Key	Value	Purpose
COUNTRY_CODE	CY	Country code according to ISO 3166-1 alpha-2 (see e.g. Wikipedia for a list of possible values)
COUNTRY_NAME	CYPRUS	Name of country according to ISO 3166-1 alpha-2 (see e.g. Wikipedia for a list of possible values)
LANGUAGE_CODE	en-GB	Language code according to ISO 639x
HOME_COMM_ID	2.16.17.710.860.1000.990.1	Participating Nation OID (used in Portal for patient consent submission, Protocol Terminators and eADC)
COUNTRY_PRINCIPAL_SUBDIVISION	CY-1	ISO 3166-2 code for country subdivision (used in Portal, Protocol Terminators, TRC-STS and epSOS Web Portal for audit purposes)
TRUSTSTORE_PATH	/home/openncp/apps/epsos-configuration/certs_CY/truststore.jks	Path to truststore
TRUSTSTORE_PASSWORD	bootCamp	Truststore password
SP_KEYSTORE_PATH	/home/openncp/apps/epsos-configuration/certs_CY/sp/sp.jks	Path to Service Provider keystore

Key	Value	Purpose
SP_KEYSTORE_PASSWORD	changeit	Service Provider keystore password
SP_PRIVATEKEY_ALIAS	<u>ncp-ppt.cy.ehealth.testa.eu</u>	Service Provider private key alias
SP_PRIVATEKEY_PASSWORD	changeit	Service Provider private key password
SC_KEYSTORE_PATH	/home/openncp/apps/e-psos-configuration/certs_CY/sc/sc.jks	Path to Service Consumer keystore
SC_KEYSTORE_PASSWORD	changeit	Service Consumer keystore password
SC_PRIVATEKEY_ALIAS	<u>ncp-ppt.cy.ehealth.testa.eu</u>	Service Consumer private key alias
SC_PRIVATEKEY_PASSWORD	changeit	Service Consumer private key password
NCP_SIG_KEYSTORE_PATH	/home/openncp/apps/e-psos-configuration/certs_CY/sign/sign.jks	Path to NCP Signature keystore
NCP_SIG_KEYSTORE_PASSWORD	changeit	NCP Signature keystore password
NCP_SIG_PRIVATEKEY_ALIAS	<u>ncp-ppt.cy.ehealth.testa.eu</u>	NCP Signature private key alias
NCP_SIG_PRIVATEKEY_PASSWORD	changeit	NCP Signature private key password
secman.sts.url	<u>http://localhost:9090/trc-sts/STSServiceService</u>	TRC-STs URL
automated.validation	TRUE	Enable the OpenNCP Messages validation (true). This will call the XDStarClient online validator to validate messages.

Key	Value	Purpose
automated.validation.new	FALSE	Using the Gazelle Remote validation through the new OpenNCP Gazelle Validator component (true) - EXPERIMENTAL and not recommended (recommend to set to false).
automated.validation.remote	TRUE	When OpenNCP Messages validation is enabled, it allows to enable the Gazelle Validation (true) or only generate the Objects for manual validation (false).
SERVER_IP	127.0.0.1	IP address of the machine running OpenNCP
audit.repository.port	2862	OpenATNA's TLS Server port
audit.repository.url	localhost	OpenATNA's Server location
<u>audit.time.to.try</u>	200	Timeout value (milliseconds) for sending audit message
auditrep.forcewrite	TRUE	Force AuditManager to write audit message
WRITE_TEST_AUDITS	TRUE	Determines if test audits should be written
TEST_AUDITS_PATH	/home/openncp/apps/epsos-configuration/audits/1	Path where test audits will be written. It must contain the ending slash.
ncp.country	CY	Local NCP infos (used for audit purposes) – country code
ncp.email	<u>admin@ncp.cy</u>	Local NCP infos (used for audit purposes) – NCP administrator email

Key	Value	Purpose
scheduled.time.between.failed.logs.handling.minutes	60	Interval (minutes) in which OpenATNA checks if some audit log was not persisted. In case these logs are found, they will be attempted to re-persist.
certificates.storepath	/home/openncp/apps/epsos-configuration/certs_CY/	Path to folder where the other countries certificates will be stored
ncp.countries	lu,at,ch,gr	The SMP gateway will download the InternationalSearchMask of each one of these countries when you click on "Sync Search Mask" (deprecated)
APP_BEHIND_PROXY	FALSE	Proxy configurations (to use in case your OpenNCP is running behind a proxy)
APP_PROXY_HOST	localhost	Proxy configurations (to use in case your OpenNCP is running behind a proxy)
APP_PROXY_PORT	8080	Proxy configurations (to use in case your OpenNCP is running behind a proxy)
APP_PROXY_USERNAME	proxyuser	Proxy configurations (to use in case your OpenNCP is running behind a proxy)
APP_PROXY_PASSWORD	proxypass	Proxy configurations (to use in case your OpenNCP is running behind a proxy)
pn.uniqueid	1	Used during submission of eDispensation and eConsent (i.e., not needed for countries that don't provide these services). It's an incremental

Key	Value	Purpose
		value that is calculated and appended to the country OID (HOME_COMM_ID) in order to generate an unique ID.
PORTAL_ADMIN_PERMISSIONS	PRD-006,PRD-003,PRD-004,PRD-005,PRD-010,PRD-016,PPD-032,PPD-033	Portal Administrator permissions (epSOS EED SAML Binding)
PORTAL_CHECK_PERMISSIONS	FALSE	(? Check user permissions ?)
PORTAL_CLIENT_CONNECTOR_URL	http://localhost:9090/openncp-client-connector/services/ClientConnectorService	URL of the web service exposed by epsos-client-connector to allow communication with the Portal
PORTAL_CONSENT_ENABLED	TRUE	(? Activate Portal option to provide consent document ?)
PORTAL_CONSENT_OID	2.16.17.710.860.1000.990.1	(? OID sent in Consent Submission ?)
PORTAL_CUSTODIAN_NAME	<CountryCustodianName >	(? Name of organization ?)
PORTAL_CUSTODIAN_OID	2.16.17.710.860.1000.990.1	(? Organization OID ?)
PORTAL_DISPENSATION_COUNTRY	CY	Country code according to ISO 3166-1 alpha-2 (see e.g. Wikipedia for a list of possible values)
PORTAL_DISPENSATION_OID	2.16.17.710.860.1000.990.1	(? OID of dispensation country ?)
PORTAL_DOCTOR_OID	2.16.17.710.860.1000.990.1	(? Doctor OID ?)
PORTAL_DOCTOR_PERMISSIONS	PRD-006,PRD-003,PRD-004,PRD-005,PRD-	Portal Doctor permissions (epSOS EED SAML Binding)

Key	Value	Purpose
	010,PRD-016,PPD-032,PPD-033	
PORTAL_ENTRY_OID	2.16.17.710.860.1000.990.1	(? Organization OID ?)
PORTAL_HOSPITAL_OID	2.16.17.710.860.1000.990.1	(? Hospital OID ?)
PORTAL_LEGAL_AUTHENTICATOR_CITY	Nicosia	(? Legal Authenticator City ?)
PORTAL_LEGAL_AUTHENTICATOR_FIRSTNAME	<LegalAuthenticatorFirstname>	(? Legal Authenticator Firstname ?)
PORTAL_LEGAL_AUTHENTICATOR_LASTNAME	<LegalAuthenticatorLastname>	(? Legal Authenticator Lastname ?)
PORTAL_LEGAL_AUTHENTICATOR_ORG_OID	2.16.17.710.860.1000.990.1	(? Legal Authenticator Organization OID ?)
PORTAL_LEGAL_AUTHENTICATOR_PERSON_OID	2.16.17.710.860.1000.990.1	(? Legal Authenticator Personal OID ?)
PORTAL_LEGAL_AUTHENTICATOR_POSTALCODE	N/A	(? Legal Authenticator Postal Code ?)
PORTAL_NURSE_PERMISSIONS	PRD-006,PRD-004,PRD-010	Portal Nurse permissions (epSOS EED SAML Binding)
PORTAL_ORDER_OID	2.16.17.710.860.1000.990.1	(? OID of ordering country ?)
PORTAL_PATIENTS_OID	2.16.17.710.860.1000.990.1	(? Patients OID ?)
PORTAL_PATIENT_PERMISSIONS	PRD-006,PRD-003,PRD-004,PRD-005,PRD-010,PRD-016,PPD-032,PPD-033	Portal Patient permissions (epSOS EED SAML Binding)
PORTAL_PHARMACIES_OID	2.16.17.710.860.1000.990.1	(? Pharmacies OID ?)

Key	Value	Purpose
PORTAL_PHARMACIST_OID	2.16.17.710.860.1000.990.1	(? Pharmacist OID ?)
PORTAL_PHARMACIST_PERMISSIONS	PRD-006,PRD-004,PRD-010,PPD-046	Portal Pharmacist permissions (epSOS EED SAML Binding)
PORTAL_PROPERTIES_UPDATED	TRUE	(? True if Portal properties were updated by Portal Configuration Portlet ?)
PORTAL_TEST_ASSERTIONS	FALSE	(?)
secman.cert.validator.checkforkeyusage	FALSE	(? Determines if Security Manager validates certificate key usage extension ?)
secman.digest.algorithm.default	http://www.w3.org/2000/09/xmlsig#sha1	Security Manager digest algorithm
secman.signature.algorithm.default	http://www.w3.org/2001/04/xmlsig-more#rsa-sha256	Security Manager signature algorithm
secman.sts.checkHostname	FALSE	(? Verify hostname when requesting assertion from TRC-STs ?)
SC_SMP_CLIENT_PRIVATEKEY_ALIAS	ncp-ppt.cy.ehealth.testa.eu	SMP Client private key alias of the Service Consumer keystore
SC_SMP_CLIENT_PRIVATEKEY_PASSWORD	changeit	SMP Client private key password of the Service Consumer keystore
SMP_ADMIN_URL	https://smp-cert-auth-test.publisher.ehealth.testa.eu	PUT/DELETE URL Internet: https://smp-cert-auth.publisher.ehealth.edelivery.tech.ec.europa.eu
SMP_SUPPORT	CEF EDELIVERY SUPPORT	SMP Support Name

Key	Value	Purpose
SMP_SUPPORT_EMAIL	<u>CEF-EDELIVERY-SUPPORT@ec.europa.eu</u>	SMP Support Email
SML_DOMAIN	ehealth.testa.eu	Domain for the Dynamic Discovery Client (OR <u>ehealth.edelivery.tech.ec.europa.eu</u> (Internet))

AIV. Appendix Terminology Server

User Interface for terminology server

There are 3 environments for these services:

- Training Environment for test purposes
- Acceptance Environment for pre-production environments
- Production Environment

The following URL's can be used for accessing the terminology services (portal and rest api).

Development

- <https://webgate.training.ec.europa.eu/ehealth-term-portal/>
- <https://webgate.training.ec.europa.eu/ehealth-term-server>

Acceptance

- <https://webgate.acceptance.ec.testa.eu/ehealth-term-serve>
- <https://webgate.acceptance.ec.europa.eu/ehealth-term-portal/> (through internet)

User Roles and Passwords

The following users have been created to acceptance environment by Solution provider.

The user credentials come from DG and are being used for accessing the terminology portal.

Username	password	Comments
ncpeh@cy	123456	user for tsam syncing
curator@cy	123456	accepts the current MTC for the TSAM sync to work
translator@cy	123456	user for updating the translations
mapper@cy	123456	user for doing the terminologies mapping

AV. Appendix SMP and Certificates

a. SMP

The SMP-Editor must be deployed in the same environment as the NCP because it depends on the properties database for performing most features.

The SMP-Editor has been tested and validated on Tomcats 8.5.X

Installation Manual

In order to run the SMP-Editor it must be deployed in the same environment as the NCP.

Some extra steps are also needed:

1. The certificates of the SMP server endpoints for both GET and PUT must be included in the truststore:
 - a. GET: <https://smp-ehealth-trn.acc.edelivery.tech.ec.europa.eu/>
This URL is directly accessible in your browser since this is a regular SSL connection (the client application is not verified by the server. Only the server is verified).
 - b. PUT: <https://smp-ehealth-trn-cert-auth.acc.edelivery.tech.ec.europa.eu/>
This case is a little different since the URL requires 2-way authentication: not only the server is verified by the client, but also the client has to be verified by the server. Therefore a private key (in .p12 format) that is linked to a certificate known at the server side has to be added to the client.

You can find the certificates issuing the following commands:

```
openssl s_client -host smp-ehealth-trn.acc.edelivery.tech.ec.europa.eu -port 443 -prexit -showcerts
openssl s_client -host smp-ehealth-trn-cert-auth.acc.edelivery.tech.ec.europa.eu -port 443 -prexit -showcerts
```

- c. or you can get the certificates from your browser. Once you have the certificates (in PKCS12 format) you add them to the truststore used by OpenNCP.
2. The certificate for the client authentication in the SMP server must be included in the Service Consumer keystore;
3. The property APP_BEHIND_PROXY must be in the database, if it is set to "true" the other proxy properties must also be defined;
4. The following properties must be added to the database:

Key	Value	Purpose
-----	-------	---------

SC_SMP_CLIENT_PRIVATEKEY_ALIAS	smp-client-key	SMP Client private key alias of the Service Consumer keystore
SC_SMP_CLIENT_PRIVATEKEY_PASSWORD	changeit	SMP Client private key password of the Service Consumer keystore
SMP_ADMIN_URL	Internet: https://smp-cert-auth.publisher.ehealth.edelivery.tech.ec.europa.eu Testa: https://smp-cert-auth-test.publisher.ehealth.testa.eu/	PUT/DELETE URL
SMP_SUPPORT	eHDSI DG Sante Support	European Commission - DG Santé support name
SMP_SUPPORT_EMAIL	sante-ehealth-dsi-support@ec.europa.eu	European Commission - DG Santé support email
SML_DOMAIN	Internet: trn.acc.edelivery.tech.ec.europa.eu (Training)	Domain for the Dynamic

	Testa: ehealth.testa.eu (Acceptance)	Discovery Client
--	--------------------------------------	------------------

The alias in the keystores must be according to the ones defined in the database.

The key pair password must be equals to the one from the keystore.

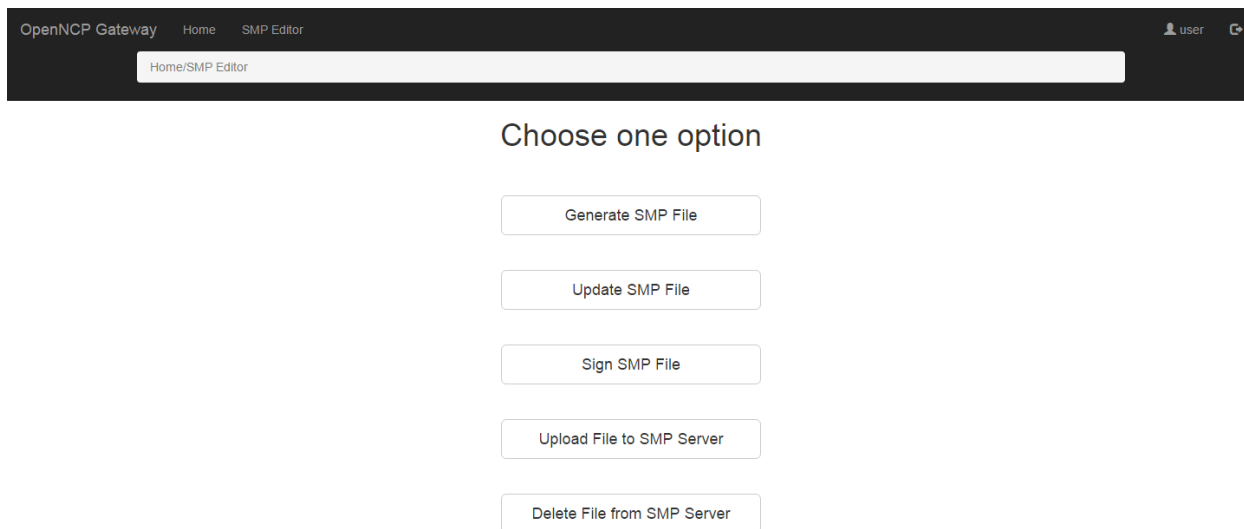
1. Home Page

The home page gives access to the 5 features: Generate SMP File; Update SMP File; Sign SMP File; Upload File to SMP Server and Delete File from SMP Server.

The current implementation of the openncp-gateway does not support any external authentication mechanism. User access is managed by an embedded in memory configuration.

In order to login the portal, testing credentials are login: user and password: password.

An authentication and authorization mechanism will be implemented soon.



2. Generation of SMP files

2.1. Create New File

Services to be upload and mapping with smp file types

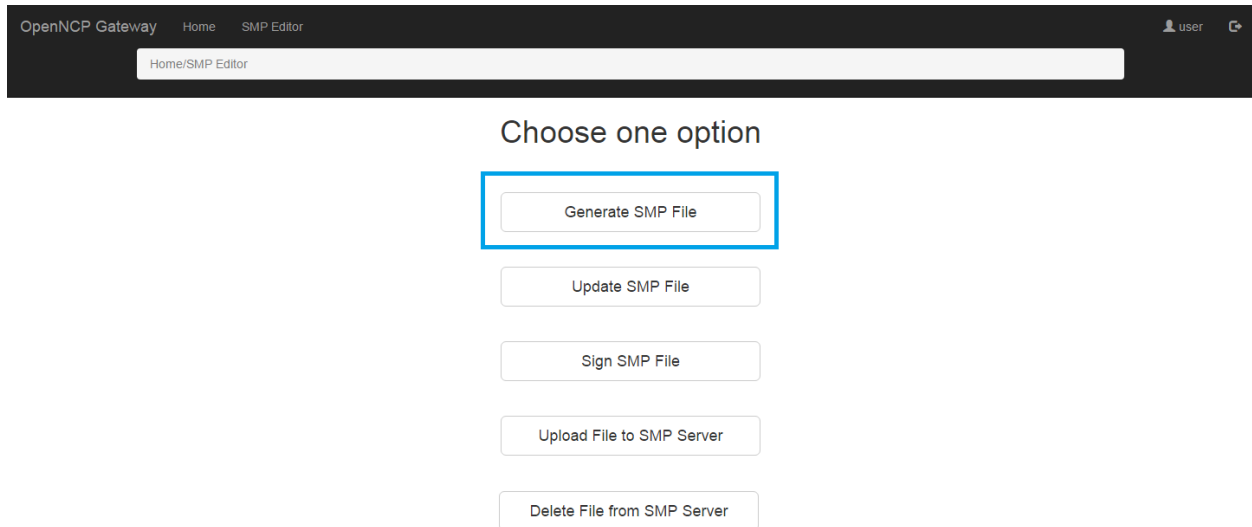
XCPD -> Patient Identification and Authorization

XCA QUERY ->
Request_of_Data_Query.DocumentIdentifier=urn:health:RequestOfData::XCA::CrossGatewayQuery##ITI-38
XCA RETRIEVE ->
Request_of_Data_Retrieve.DocumentIdentifier=urn:health:RequestOfData::XCA::CrossGatewayRetrieve##ITI-39
XDR (DISPENSATION) ->
Provisioning_of_Data_Provide.DocumentIdentifier=urn:health:ProvisioningOfData:Provide::XDR::ProvideandRegisterDocumentSet-b##ITI-41
XDR (BPPC) -> Provisioning_of_Data_BPPC.DocumentIdentifier=urn:health:ProvisioningOfData:BPPC-RegisterUpdate::XDR::ProvideandRegisterDocumentSet-b##ITI-41

NOT USED:
XCF ->
Request_of_Data_Fetch.DocumentIdentifier=urn:health:RequestOfData::XCF::CrossGatewayFetchRequest##ITI-63

IDENTITY PROVIDER XUA
REDIRECT
VPN GATEWAY CLIENT
VPN GATEWAY SERVER

The option Generate SMP File will lead to a serie of forms in order to create a new SMP file.



First the user must choose the type of SMP File that he wants to create.

Generate SMP File

Choose one type to create

-- Choose an option --

- Choose an option --
- VPN Gateway Server
- VPN Gateway Client
- Country B Identity Provider
- Patient Identification and Authentication
- Provisioning of Data - Provide
- Provisioning of Data - BPPC
- Request of Data - Fetch
- Request of Data - Query
- Request of Data - Retrieve
- International Search Mask
- Redirect

Cancel Next

Then, the user must fill in the fields of the form. The fields have tooltips at the end that explain their purpose according to the specification.

For the Endpoint URI, the value can be found in the OpenNCP properties database (epsosproperties db schema)

Service	OpenNCP property key
Patient Identification and Authorization	cy.PatientIdentificationService.WSE
Request of Data - Query	cy.PatientService.WSE/eu.OrderService.WSE
Request of Data - Retrieve	cy.PatientService.WSE/eu.OrderService.WSE
Provision of Data - Provide	cy.DispensationService.WSE
Provision of Data - BPPC	cy.ConsentService.WSE

Generate SMP File

VPN Gateway Server

Country

-- Choose an option --

Endpoint

Endpoint URI ?

Service Activation Date ? Date when the service has started.

Service Expiration Date ?

Service Description ?

Technical Contact URL ?

Technical Information URL ?

Cancel Ok

The form varies according to the type of SMP file chosen in Figure below.

Generate SMP File

Redirect

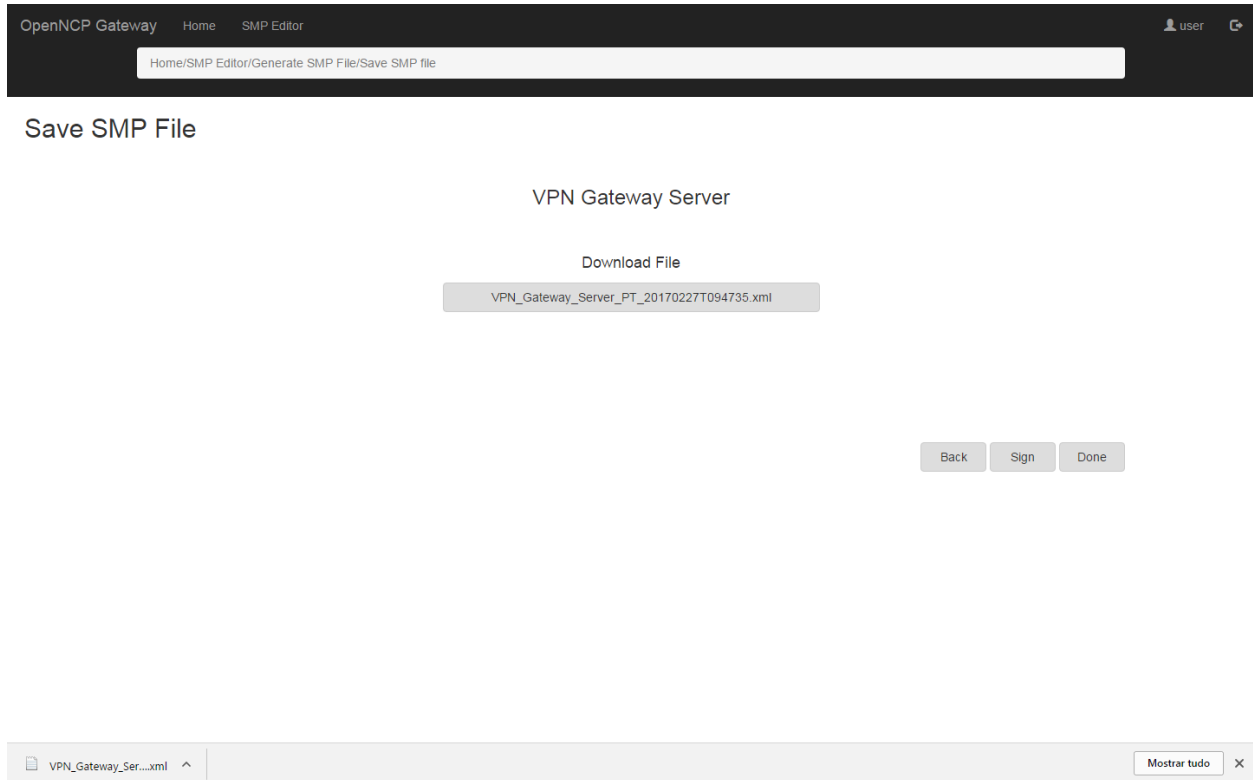
Redirect URL ?

Certificate UID ? Holds the Subject Unique Identifier of the certificate of the destination SMP.

Cancel Ok

After submitting the form, the user can download the generated file by pressing the button with its name, under the tag "Download File".

Then, the user can press "Done" and go to the home page, or he can press "Sign" and go to the form that signs the new file.



The application makes some verifications when submitting the form:

- Checks the certificate file by trying to obtain its Certificate Subject Name – if it cannot obtain it alerts "Invalid certificate file!" (The certificate file is retrieved from the `openncp_properties` table under the key defined in the `smpeeditor.properties` file for each file type)
- Checks the extension file by:
- Check the XML structure– "Invalid extension file!"
- Check against the OASIS BDX-SMP XSD (`bdx-smp-201605`) – "Extension is not compliant with the xsd schema!" (The extension file must have extension `.xml`)

Generate SMP File

International Search Mask

Extension is not compliant with the xsd schema!

Country

Endpoint

Service Activation Date	<input type="text" value="2017-02-01 06:30"/>	?
Service Expiration Date	<input type="text" value="2017-02-28 23:55"/>	?
Service Description	<input type="text"/>	?
Technical Contact URL	<input type="text"/>	?
Technical Information URL	<input type="text"/>	?
Extension	<input type="button" value="Escolher ficheiro"/> Nenhum ficheiro selecionado	?

For the Redirect option, the application verifies the Redirect URL. It must contain the Participant Identifier and the Document Identifier according to the specification:

- Participant Identifier: **“urn:ehealth:” + country code + “ncpb-idp”** e.g. urn:ehealth:pt:ncpb-idp
- Document Identifier: **“urn:ehealth:” + interaction pattern + “::” + event name + “##” + EventID** e.g. urn:ehealth:RequestOfData::XCA::CrossGatewayQuery##ITI-38

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Generate SMP File

Generate SMP File

Redirect

Could not find participantID and documentTypeID in the Redirect URL attribute!

Redirect URL ?

Certificate UID ?

Cancel Ok

2.2. Update an Existing File

The option Update SMP File will lead to a series of forms in order to update an existing SMP file.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor

Choose one option

Generate SMP File

Update SMP File

Sign SMP File

Upload File to SMP Server

Delete File from SMP Server

First the user must choose the file that he wants to update.

Update SMP File

Choose the file to update

SMP File Escolher ficheiro Nenhum ficheiro selecionado

Cancel Ok

Then, the form relative to the uploaded file is shown filled with the data read. For the extension is shown its content.

The user then changes the fields wanted and submits.

Update SMP File

Country B Identity Provider

Country Portugal

Identity Provider Issuance Type Proprietary

Endpoint

Endpoint URI	https://openncp.pt:8443/services/xcpd	?
Service Activation Date	2017-02-01 02:10	?
Service Expiration Date	2017-02-28 10:45	?
Service Description	Servide Description	?
Technical Contact URL	xyz@email.com	?
Technical Information URL	http://openncp.pt/info	?

Cancel Ok

If the chosen file has already a National Authority signature, the application warns the user of that fact.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Update File

Update SMP File

Patient Identification and Authentication

This file has a signature! If you proceed you will have two options:

- Generate an unsigned ServiceMetadata file
- Sign the updated ServiceMetadata file

Country

Portugal

Endpoint

Endpoint URI ?

Service Activation Date ?

Service Expiration Date ?

Service Description ?

Technical Contact URL ?

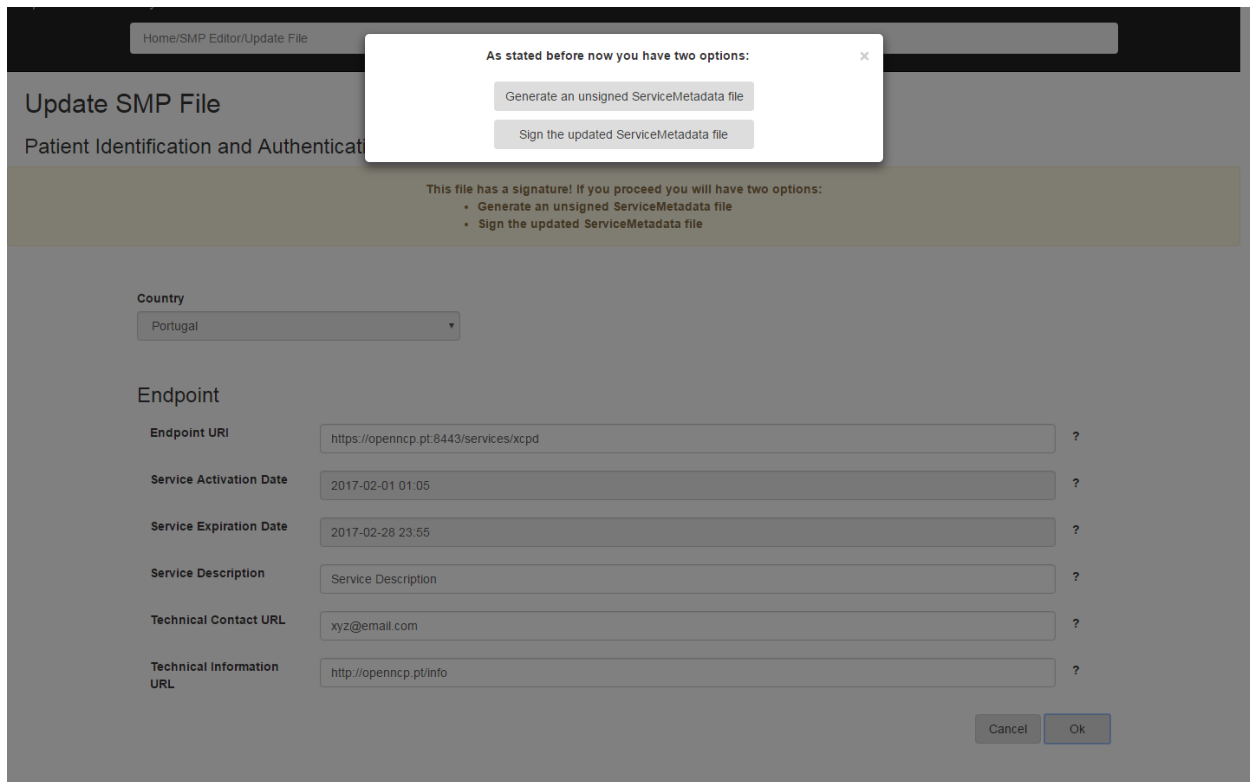
Technical Information URL ?

Cancel Ok

Then, when submitting the changes, the user must choose between:

- Generate an unsigned ServiceMetadata file – generate an unsigned file and go to the download page.
- Sign the updated ServiceMetada file – go to the sign form.

In both cases the old signature is discarded.



Also, for the update feature the application verifies the certificate and extension files (if changed) and the Redirect URL.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Update File

Update SMP File

International Search Mask

Invalid extension file!

This file has a signature! If you proceed you will have two options:

- Generate an unsigned ServiceMetadata file
- Sign the updated ServiceMetadata file

Country

Portugal

Endpoint

Service Activation Date	2017-02-01 00:05	?
Service Expiration Date	2017-03-31 23:55	?
Service Description	Service Description	?
Technical Contact URL	xyz@email.com	?
Technical Information URL	http://openncp.pt/info	?
Extension	<patientSearch xmlns="http://eu.europa.ec.sante.ehdsi/ehncp/ism"> /1 min and max 1 max no length check </	?

3. Signing of SMP files

The option Sign SMP File will lead to a form in order to sign the chosen SMP file(s).

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor

Choose one option

Generate SMP File

Update SMP File

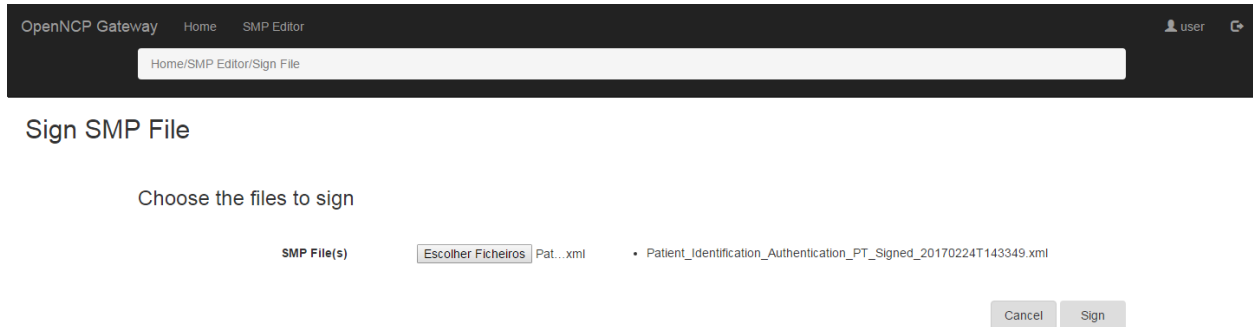
Sign SMP File

Upload File to SMP Server

Delete File from SMP Server

The user can choose one or more files to sign.

The keystore and passwords are retrieved from the database.



After choosing the files, the content of the selected file(s) is shown to the user, in order to confirm the data that he is about to sign.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Sign File

Sign SMP File

You are about to perform a qualified signature over the following information:

VPN Gateway Server

Country	pt	?
Participant Identifier	urn:ehealth:pt:ncpb-idp	?
Document Identifier	urn:ehealth:VPN:\VPNGatewayServer##ehealth-105	?
Process Identifier	urn:ehealth:ncp:vpngateway	?

Endpoint

Endpoint URI	ipsec://teste.com	?
Service Activation Date	2017-02-01 01:05	?
Service Expiration Date	2017-02-28 23:55	?
Certificate	Issuer: 1.2.840.113549.1.9.1=#1617699e65732e67617267616e746140676d61699c2e636f6d,CN=ines,OU=SPMS,O=SPMS,L=Porto,ST=Porto,C=pt Serial Number #15630198956697564838	?
Service Description	Service Description	?
Technical Contact URL	xyz@email.com	?
Technical Information URL	http://openncp.pt/info	?

Are you sure you want to sign the file(s)?

Cancel Ok

If the selected file has already a National Authority signature the application warns the user that if he proceeds it will replace the signature of the file.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Sign File

Sign SMP File

You are about to perform a qualified signature over the following information:

Redirect VPN Gateway A

The chosen file has a signature. If you proceed you will override it.

Country pt ? Two-letter country code according to ISO 3166-1 alpha-2

Redirect URL http://localhost:8083/ehealth-actorid-qns%3A%3Aurn%3Apt%3Ancpb/services/ehealth-resid-qns%3A%3Aurn%3A%3A%3Aepsos%23? ?

Certificate UID PID:9208-2001-3-279815395 ?

Are you sure you want to sign the file(s)?

Cancel Ok

After confirming, the user is redirected to the download page, where he can download each file individually.

OpenNCP Gateway Home SMP Editor user

Home/SMP Editor/Sign SMP File/Save SMP File

Save SMP File

Download File

VPN_Gateway_Server_PT_Signed_20170227T101346.xml

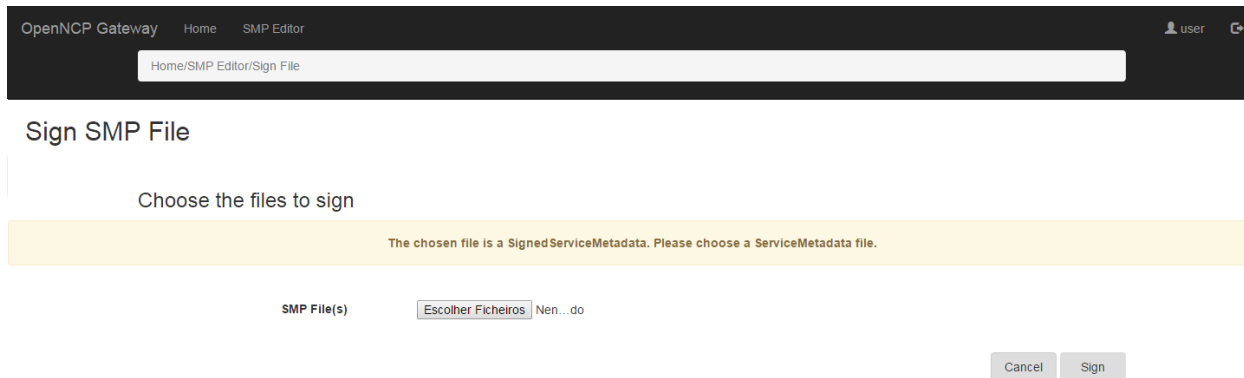
Redirect_Request_of_Data_Query_PT_Signed_20170227T101346.xml

Back Done

Redirect_Request_...xml VPN_Gateway_Ser...xml

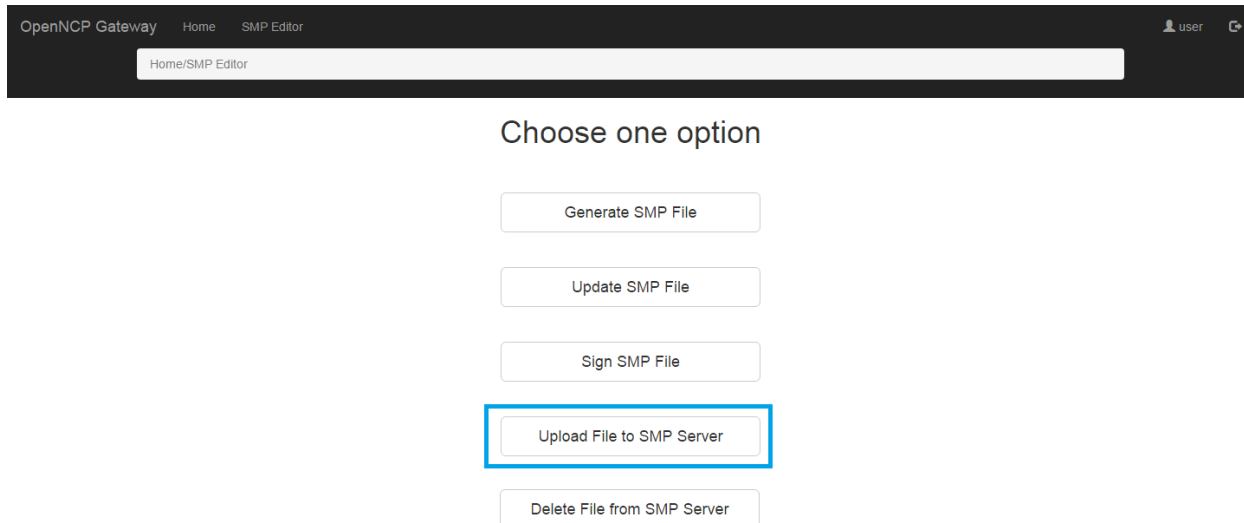
Mostrar tudo X

The user cannot sign a file that is already a SignedServiceMetadata. It only allows the signature of ServiceMetadata files.



4. Upload of SMP files to the SMP Server

The option Upload File to SMP Server will lead to a form in order to upload the chosen SMP file(s).



The user can choose one or more files to upload.

Upload File to SMP Server

Choose the files to upload

SMP File(s) Escolher Ficheiros 4 fiche...

- Country_B_Identity_Provider_PT_Signed_20170224T163834.xml
- Patient_Identification_Authentication_PT_Signed_20170224T143349.xml
- Request_of_Data_Query_PT_Signed_20170224T151347.xml
- International_Search_Mask_PT_Signed_20170224T143440.xml

Cancel Upload

After uploading, a results page is shown to the user, where he can see if the upload of each file succeeded or failed.

If succeeded, the user can check the SMP information uploaded using the given URLs.

Upload File to SMP Server

Info

Request_of_Data_Retrieve_PT_Signed_20170227T164241.xml	Failure!	+
VPN_Gateway_Server_PT_Signed_20170227T161552.xml	Created!	+
<p>Check your SMP information at</p> <p>ServiceGroup https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp</p> <p>Signed ServiceMetadata https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AVPN%3A%3AVPNGatewayServer%23%23ehealth-105</p>		
Provisioning_of_Data_Provide_PT_Signed_20170227T122050.xml	Created!	+
International_Search_Mask_PT_Signed_20170227T115021.xml	Created!	+

Back Done

If failed, the user can check why. The details contain: the error code; the description of the specification for each error type and also the error description returned by the server.



Upload File to SMP Server

Info

Request_of_Data_Retrieve_PT_Signed_20170227T164241.xml	Failure! +
400 (OUT_OF_RANGE): Bad Request - Some numeric (or date field) is out of the valid range. Expiration date has passed	
VPN_Gateway_Server_PT_Signed_20170227T161552.xml	Created! +
Provisioning_of_Data_Provide_PT_Signed_20170227T122050.xml	Created! +
International_Search_Mask_PT_Signed_20170227T115021.xml	Created! +

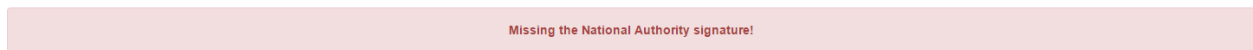
Back Done

The user cannot upload a file that does not contain the National Authority signature.



Upload File to SMP Server

Choose the files to upload



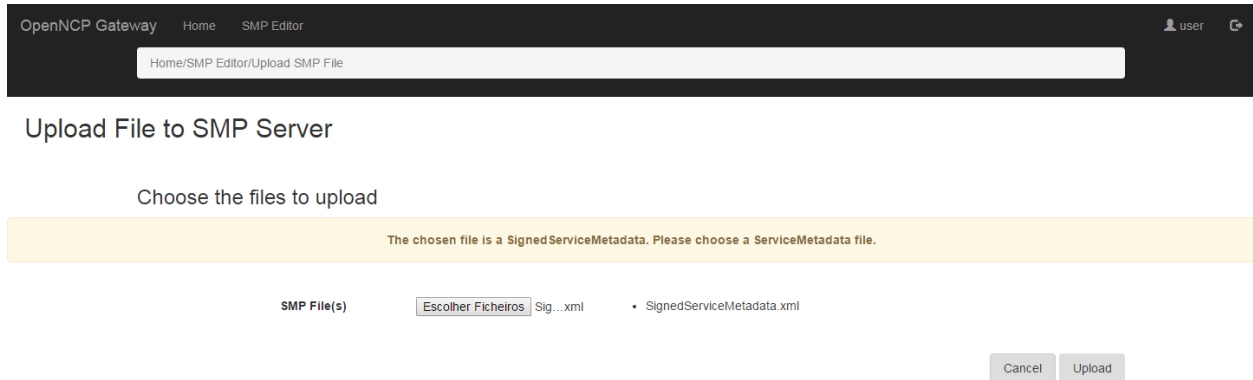
SMP File(s)

Escolher Ficheiros Cou...ml

• Country_B_Identity_Provider_PT_20170222T104823.xml

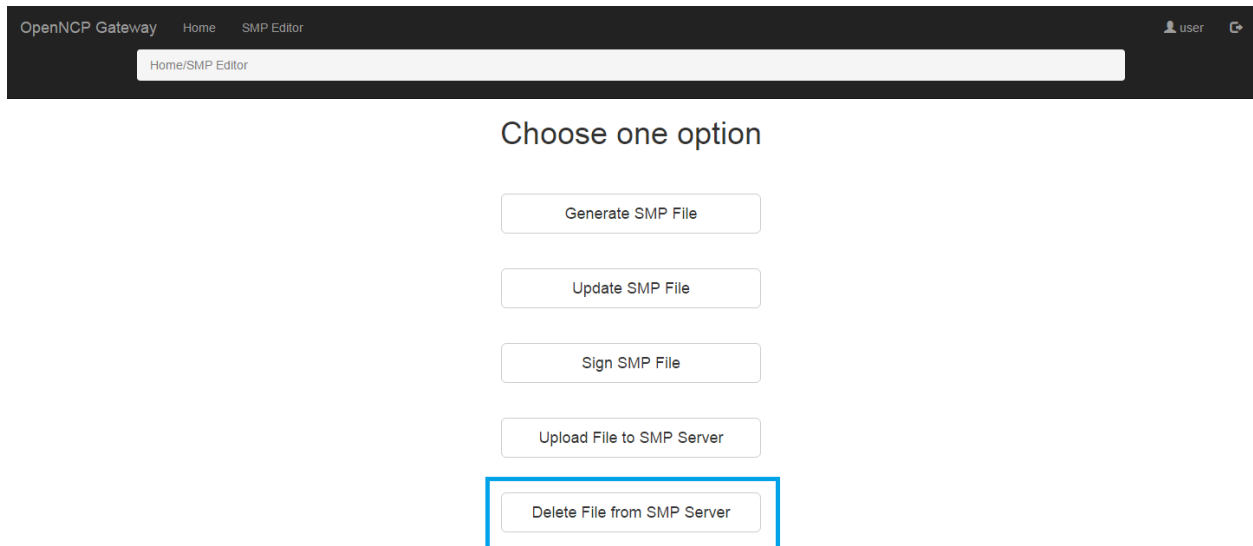
Cancel Upload

The user cannot upload a file that is already a SignedServiceMetadata. It only allows to upload ServiceMetadata files.



5. Delete SMP files from SMP Server

The option DeleteFile from SMP Server will lead to a form in order to delete the chosen SMP file(s).



First, the user must choose his country in order to GET from the server the files in the ServiceGroup.

Delete File from SMP Server

Choose your country

Country Portugal

Cancel Ok

Then, the user must choose the files to delete.

Delete File from SMP Server

Files on the server

Country
Portugal

Documents

- Country B Identity Provider**
 <https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3ACountryBidentityProvider%3A%3AidentityProvider%3A%3AHPAuthentication%23%23epos-91>
- International Search Mask**
 <https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AISM%3A%3AInternationalSearchMask%23%23ehealth-107>
- Provisioning of Data - Provide**
 <https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AProvisioningOfData%3AProvide%3A%3AXDR%3A%3AProvideandRegisterDocumentSet-b%23%23ITI-41>
- Request of Data - Fetch**
 <https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3ARequestOfData%3A%3AXCF%3A%3ACrossGatewayFetchRequest%23%23ITI-63>
- VPN Gateway Client**
 <https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AVPN%3A%3AVPNGatewayClient%23%23ehealth-106>

Back Delete

After deleting, a results page is shown to the user, where he can see if the delete of each file succeeded or failed.

Delete File from SMP Server

Files deleted

Country B Identity Provider
https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3ACountryBIdentityProvider%3A%3AIdentityProvider%3A%3AHPAuthentication%23%23sepos-91 Deleted!

International Search Mask
https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AISM%3A%3AInternationalSearchMask%23%23ehealth-107 Deleted!

Back Done

If failed, the user can check why. The details contain: the error code; the description of the specification for each error type and also the error description returned by the server.

Delete File from SMP Server

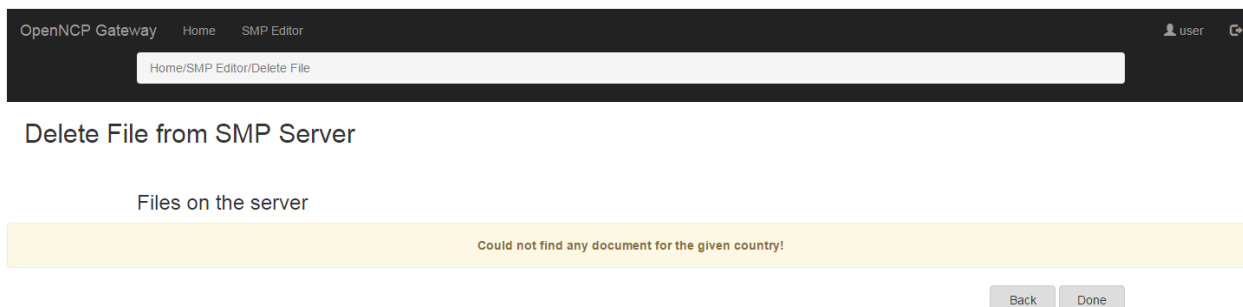
Files deleted

VPN Gateway Server
https://smp.acc.edelivery.tech.ec.europa.eu/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Apt%3Ancpb-ldp/services/ehealth-resid-qns%3A%3Aurn%3Aehealth%3AVPN%3A%3AVPNGatewayServer%23%23ehealth-105 Failure!

404: The requested information was not found!
ehealth-participantid-qns::urn:ehealth:pt:ncpb-ldp / ehealth-resid-qns::urn:ehealth:VPN::VPNGatewayServer##ehealth-105

Back Done

If the chosen country has no uploaded files an alert is shown.



b. Certificates

Acceptance and Production Certificates

The certificate for Acceptance Environment and Production Environment can be created using the instruction in the [\(eDelivery\)\(PKI for eHealth\)\(SOD\)\(0.07\).pdf](#)

- epSOS SP + SC = CEF PKI TLS
- epSOS SIG = SIG

Signature Certificate Attributes

Country: CY

O: Ministry for Health, Cyprus

OU1: CEF_eDelivery.testa.eu

OU2: eHealth

OU3: NCP_PPT-GTC_OID-1.3.130.0.2018.996911

First name (CN): <blank>

Last name (CN): GRP:EHEALTH_NCP_PPT_CY_001

E-mail: CEF-EDELIVERY-SUPPORT@ec.europa.eu

Street: to be filled

Street no.: to be filled

Zip Code: <blank>

City: Nicosia

Identification data: email to be filled

TLS Certificate Attributes

Country (C)	Organisation's Country Code (2 characters, in accordance to ISO 3166-1, alpha-2, case sensitive)	CY
Organisation/company (O)	Organisation Name of the Certificate Owner (case sensitive)	Ministry for Health, Cyprus
Locality (L)	City from the address of the Organisation	Nicosia
Server name (CN)	Fully Qualified Domain Name of the endpoint. It should be exactly the same that is used by the endpoint in the context of the TLS/HTTPS communication.	ncp-ppt.cy.ehealth.testa.eu
E-mail (E)	Primary contact of the Organisation	<u>ftanteles@dits.mof.gov.cy</u>

Test Certificates

We have created certificates free of charge using Gazelle PKI infrastructure <https://gazelle.ehdsi.eu/gss/home.seam>

Request a new Certificate

You have to fill the following form for all kind of test certificates you want to create. For now it is requested to create "Service Consumer", "Service Provider" and "Signature Certificate".

The required parameters that have to be filled are Country (e.g. Cyprus), Organization (e.g. University of Cyprus) and Common Name (ncp-ppt.cyehealth.testa.eu for all certificates)

Request a new certificate

This page is dedicated to request a certificate for your system. The issued certificate can only be used for testing purpose.

⚠ If you already have a public/private key pair and a certificate signing request (CSR), you can submit your request [here](#) . Otherwise, please fill the following form.

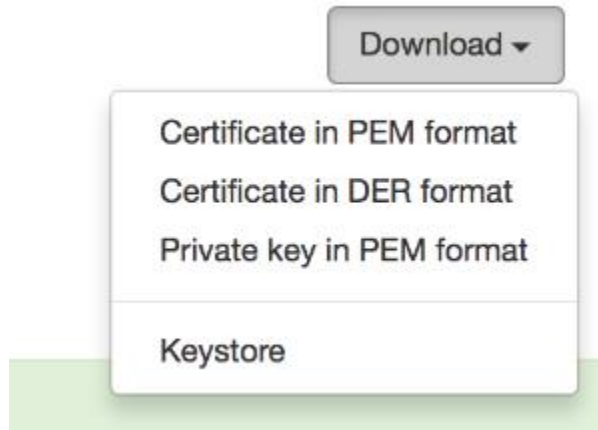
Request a certificate without CSR

PKI Certificate Authority	<input type="text" value="C=BE,O=IHE Europe,CN=EHDSI CA"/>
Certificate type *	<input type="text" value="Client and Server"/>
key size	<input type="text" value="1024"/>
Country (C) *	<input type="text" value="Afghanistan (AF)"/>
Organization (O) *	<input type="text"/>
Common name (CN) *	<input type="text"/>
Title (T)	<input type="text"/>
Given name (GIVENNAME)	<input type="text"/>
Surname (SURNAME)	<input type="text"/>
Organizational unit (OU)	<input type="text"/>
E-Mail (E)	<input type="text"/>

After that you have to go from the menu to the "List of certificate requests"

Request Id	Subject	Type	CA subject	Requester	Date	Signed ?	Action
176	C=GR,O=IDIKA,CN=ncp-ppt.gr.ehealth.testa.eu	epSOS NCP signature	C=BE,O=IHE Europe,CN=EHDSI CA	karkk001 (ehdsi)	5/24/18 3:37:04 PM (CEST GMT+0200)	✓	Q ⚙
175	C=GR,O=IDIKA,CN=ncp-ppt.gr.ehealth.testa.eu	epSOS service provider	C=BE,O=IHE Europe,CN=EHDSI CA	karkk001 (ehdsi)	5/24/18 3:36:41 PM (CEST GMT+0200)	✓	Q ⚙
174	C=GR,O=IDIKA,CN=ncp-ppt.gr.ehealth.testa.eu	epSOS service consumer	C=BE,O=IHE Europe,CN=EHDSI CA	karkk001 (ehdsi)	5/24/18 3:36:14 PM (CEST GMT+0200)	✓	Q ⚙
173	C=IE,O=HSE,CN=ncp-ppt.ie.ehealth.testa.eu	epSOS NCP signature	C=BE,O=IHE Europe,CN=EHDSI CA	karkk001 (ehdsi)	5/8/18 11:10:17 AM (CEST GMT+0200)	✓	Q ⚙
172	C=IE,O=HSE,CN=ncp-ppt.ie.ehealth.testa.eu	epSOS service provider	C=BE,O=IHE Europe,CN=EHDSI CA	karkk001 (ehdsi)	5/8/18 11:09:57 AM (CEST GMT+0200)	✓	Q ⚙

and click the right link for going to the page with the certificate details from where you can download the certificates. You will be asked for giving the alias for the key and the password of the keystore



Install the new certificates

After that you have to put the exported certificates under \$EPSOS_PROPS_PATH directory (proposed to be inside a folder with name certs_{countrycode}, e.g certs_IT for Italy, or certs_CY for Cyprus. You have also to update the epsosproperties database with the **path, alias and passwords** for the new certificates. The appropriate properties are the following:

- NCP_SIG_KEystore_PATH
- NCP_SIG_PRIVATEKEY_ALIAS
- SC_KEystore_PATH
- SC_PRIVATEKEY_ALIAS
- SP_KEystore_PATH
- SP_PRIVATEKEY_ALIAS
- SC_SMP_CLIENT_PRIVATEKEY_ALIAS
- SMP_KEystore
- SC_SMP_CLIENT_PRIVATEKEY_PASSWORD

You have also to update the ArrConnections.xml file exist under EPSOS_PROPS_PATH/ATNA_Resources directory to fit in your keystore settings

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Copyright (c) 2009-2011 Misys Open Source Solutions (MOSS) and others
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at
    http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
  implied. See the License for the specific language governing
  permissions and limitations under the License.
  Contributors:
```

```

    Misys Open Source Solutions - initial API and implementation
-->
<!-- The Audit Record Repository Actor Server Connections -->
<!-- For IHE Actor -->
<Configuration>
  <SecureConnection name="arr-tls">
    <HostName>127.0.0.1</HostName>
    <Port>2862</Port>
    <!-- Trust and Keystore -->
    <KeyStore>/opt/epsos-configuration/certs_CY/sp/sp.jks</KeyStore>
    <KeyPass>changeit</KeyPass>
    <TrustStore>/opt/epsos-configuration/certs_CY/sc/sc.jks</TrustStore>
    <TrustPass>changeit</TrustPass>
  </SecureConnection>
  <!-- use IP address instead of localhost for UDP -->
  <StandardConnection name="arr-udp">
    <HostName>127.0.0.1</HostName>
    <Port>2861</Port>
  </StandardConnection>
</Configuration>

```

Monitor electronic certificates expiration

A script is running using crontab and inform the system administrator for certificates expiration. Then, the administrator is responsible to update it. The script is located under `/home/openncp/apps/epsos-configuration/certs_CY`

```

#!/bin/bash
CERTIFICATES_PATH=/opt/epsos-configuration/certs_CY
NOTIFIER_EMAIL=eyiapatou@dits.mof.gov.cy
NUM_DAYS=2000
CHECK_DAYS=$((NUM_DAYS*24*60*60))
echo "Checking for expiration in the next $NUM_DAYS days"
if openssl x509 -checkend $CHECK_DAYS -noout -in $CERTIFICATES_PATH/sign/sign.pem
then
  echo "SIGN Certificate is good for another day!"
else
  echo "Certificate has expired or will do so within 24 hours!"
  mail -s "Certificate Expiration for Signature Certificate" $NOTIFIER_EMAIL < /dev/null
  echo "(or is invalid/not found)"
fi
if openssl x509 -checkend $CHECK_DAYS -noout -in $CERTIFICATES_PATH/sc/sc.pem
then
  echo "SC Certificate is good for another day!"
else
  echo "Certificate has expired or will do so within 24 hours!"
  mail -s "Certificate Expiration for SC Certificate" $NOTIFIER_EMAIL < /dev/null
  echo "(or is invalid/not found)"
fi
if openssl x509 -checkend $CHECK_DAYS -noout -in $CERTIFICATES_PATH/sp/sp.pem
then

```

```
echo "SP Certificate is good for another day!"  
else  
echo "Certificate has expired or will do so within 24 hours!"  
mail -s "Certificate Expiration for SP Certificate" $NOTIFIER_EMAIL < /dev/null  
echo "(or is invalid/not found)"  
fi
```

AVI. Appendix Pharmaceutical Product Data Exchange web service API documentation



Pharmaceutical Product Data Exchange

Web Service API Documentation

Date : 15-07-2019
Version: 1.2.1

Table of Contents

1	INTRODUCTION.....	3
2	COMMUNICATING WITH API	3
3	API OPERATIONS.....	4
3.1	getSyncList.....	4
3.2	getProductByBarcode.....	4
3.3	getProductByDrugidPacknr.....	4
3.4	getProductsByDate	5
4	API DATA OBJECTS	5
4.1	TermScheme.....	5
4.2	TermID	5
4.3	TermDescription	5
4.4	Term	6
4.5	OrgID.....	6
4.6	Address	6
4.7	Company.....	7
4.8	Form	7
4.9	ActiveSubstance	7
4.10	Container	7
4.11	Product	8
4.12	SyncList.....	9
4.13	SyncListItem.....	9
5	API ERRORS.....	10

a. Introduction

The Pharmaceutical Product Data Exchange Web Service API (hereafter “API”) enables users to programmatically retrieve data from the CypDIS DRA database. This document assumes familiarity with web services in general, and with the programming language you will be using.

b. Communicating with API

The core messaging technology for the API is Simple Object Access Protocol (SOAP), which is an XML and HTTP based protocol with wide support in the industry. The API uses document/literal style SOAP 1.1.

To use the API, write a client program in the programming language that you are familiar with. We have tested Java. Write your client program to send a request to one of the operations, such as the *getSyncList* or *getProductByBarcode*. The relevant operation will process the request and send back a response, which your client program needs to parse.

The only software you need to install to use the API is the software for the programming language and toolkit that you will be using to write your client programs. For example, if you intend to write your client programs in Java, you will need to install the Java Development Kit and also a SOAP toolkit such as Metro, Apache CXF etc.

The operations provided by a web service are defined in a WSDL (Web Services Definition Language) file which is posted on the web service’s website. To connect to a web service, you need to know the URL for the WSDL. For the API, the URL for the WSDL is:

Development:

<https://demo.mimerhellas.com/cypdis-services/ProductSyncService?wsdl>

Production:

<https://www.phs.moh.gov.cy/hio-services/ProductSyncService?wsdl>

Security is required.

The API uses basic authentication over SSL.

c. API Operations

Service	Operation
ProductSyncService	getSyncList
	getProductByBarcode
	getProductByDrugidPacknr

1. getSyncList

Parameters

Name	Type	
date	Date	

Response

Type	Error	Comments
SyncList	ApplicationException	An object of type SyncList which contains SyncListItems.

2. getProductByBarcode

Parameters

Name	Type	Comments
barcode	String	

Response

Type	Error	Comments
Product	ApplicationException	

3. getProductByDrugidPacknr

Parameters

Name	Type	Comments
drugid	String	
packnr	String	

Response

Type	Error	Comments
------	-------	----------

Product	ApplicationException	
---------	----------------------	--

4. getProductsByDate

Parameters

Name	Type	
date	Date	

Response

Type		
List	ApplicationException	A list containing objects of type Product. see 4.11

d. API Data Objects

1. TermScheme

Fields

	Type	Comments
termScheme	String	The coding scheme.

2. TermID

Extends TermScheme.

Fields

	Type	Comments
termID	String	The identifier of the term according to the specified coding scheme.
Mappings	List	Mappings of the identifier with other coding schemes.

3. TermDescription

Fields

	Type	Comments
lang	String	The language of the description.
Description	String	The description in the specified language.

4. Term

Extends TermID.

Fields

	Type	Comments
description	TermDescription	see 4.3
translations	List	Translations of the description in other languages.

5. OrgID

Extends TermScheme.

Fields

	Type	Comments
orgID	String	The organization identifier according to the specified coding scheme.
locID	String	The location identifier according to the specified coding scheme.
Mappings	List	Mappings of the organization with other coding schemes.

6. Address

Fields

	Type	Comments
street	TermDescription	see 4.3
city	TermDescription	see 4.3
zip	String	
country	Term	see 4.4
phone	String	
fax	String	
email	String	

7. Company

Extends OrgID.

Fields

Name	Type	Comments
address	Address	see 4.6
description	TermDescription	see 4.3

8. Form

The Pharmaceutical form type which extends Term.

Fields

	Type	Comments
strength	String	

9. ActiveSubstance

Extends Term.

Fields

	Type	Comments
quantity	Integer	
quantityUnit	Term	see 4.4

10.Container

Fields

	Type	Comments
containerType	Term	Blister, bottle etc see 4.4
numberOfContainers	Integer	2 blisters
containerMaterial	String	PVC/ALU etc
containerSize	Integer	7 tabs (per blister)
containerSizeUnit	Term	see 4.4

11.Product

Fields

Name	Type	Comments
drugid	String	
packnr	String	
barcode	String	
productName	String	
packageDescription	String	
packageSize	Integer	
packageSizeUnit	Term	see 4.4
legalStatus	Term	see 4.4
narcoticCategory	Term	see 4.4
maStatus	Term	see 4.4
formList	List of type Form	see 4.8
atcList	List of type Term	see 4.4
routeList	List of type Term	see 4.4
activeSubstanceList	List of type ActiveSubstance	see 4.9
containerList	List of type Container	see 4.10
marketingAuthorizationHolder	Company	see 4.7
localRepresentative	Company	see 4.7
parallelImporter	Company	see 4.7
manufacturerBatchRelease	Company	see 4.7
spcLink	String	HREF of the document
pillink	String	HREF of the document
wprice	BigDecimal	Current net (no VAT) wholesale price

12.SyncList

Fields

	Type	Comments
syncListItem	List	

13.SyncListItem

Fields

Name	Type	Comments
drugid	String	
packnr	String	
barcode	String	
lastUpdate	Date	

e. API Errors

All API operations throw error of type ApplicationException.

Fields

	Type	Comments
message	String	

Codes

	Comments
EMPTY_PARAMETER	The parameter is required.
INVALID_DRUGID	The length of the drugid parameter is not 7.
INVALID_PACKNR	The length of the drugid parameter is not 2.
PRODUCT_NOT_FOUND	The product with barcode or drugid/packnr was not found.
SQL_EXCEPTION	Database layer error.

<https://www.phs.moh.gov.cy/hio-services/ProductSyncService?wsdl>

f. Annex 1

1	Code (Αρ. τιμολόγησης)
2	MAH License number
3	Product name
4	Active ingredient
5	Active ingredient & Strength
6	Prescription or Over The Counter (Rx or OTC)
7	Prescription Status (Δικαίωμα Επανάληψης 3 ή 6 μήνες)
8	Bar code (GTIN 13 ψηφεία)
9	ATC Code
10	DDD/unit
11	MAH
12	Στοιχεία επικοινωνίας MAH
13	MAH ID (internal or SPOR)
14	Manufacturer (Batch Release)
15	Manufacturer code (internal or SPOR)
16	Local representative (Τοπικός αντιπρόσωπος)
17	Local representative code (internal or SPOR)
18	Στοιχεία επικοινωνίας local representative
19	Parallel importer (Παράλληλος Εισαγωγέας)
20	Parallel importer Id (internal or SPOR)
21	Στοιχεία επικοινωνίας Parallel Importer
22	Package size
23	Strength
24	Packaging -Term name (SPOR)
25	Packaging - Source Id (SPOR)
26	Packaging description
27	Unit of measurement - Term name (SPOR)
28	Unit of measurement - Source Id (SPOR)
29	Pharmaceutical Dose Form - Term Name (SPOR)
30	Pharmaceutical Dose Form - Source Id (SPOR)
31	Route of admin - Term name (SPOR)
32	Route of admin - Source Id (SPOR)
33	Branded-EPR (BREPR) /Branded Originator EPR (BROEPR) /Generic with ref. product (GRef)/ Generic -EPR (GEEPR)/Generic -Cost (GEC) /Biological (BL) /Biosimilar (BS)
34	Innovative (INV) / METOO /MTG* /ORPHAN Σημ.: 1) Κατηγοριοποίηση αφορά μόνο πρωτότυπα 2) *MTG= Όσα Meetoo έχει λήξει η πατέντα έστω και ενός της κατηγορίας και υπάρχει γενόσημο
35	Inpatient /Daycase /Outpatient
36	Outpatient injectables
37	Max Wholesale price (no VAT)

38	Status (Withdrawn or not)
39	Withdrawn date
40	Rapid alert withdrawal
41	SPC/PIL
42	Άλλο;