European Security in Health Data Exchange

Deliverable D6.1

Use case specification and validation methodology

Editors:
Andrea Micheletti
Mariet Nouri Janian
Eleonora Lavalle
Paola Aurucci

Responsible Partner: FCSR
Status-Version: Final
Date: 22/12/2017
Distribution level: PU
Abstract: This deliverable includes a detailed description of the SHiELD project use cases, with the related storyboard and actors involved. Moreover it is reported the validation methodology for the different technological tools and for the validation with end-users and experts. The last part of the deliverable includes the description of the preparatory steps for use cases.
implementation and the synthetic data sets considered.

**Keyword List:**
Patient, Travelling, Sensitive data, Data exchange between EU countries, Electronic Health Record, Emergency Medical Service, Use cases, Stakeholders, Actors, End-users, Privacy, Security, Requirements, Validation, Verification, Methodology, Metrics, OpenNCP.

**Disclaimer**
This document reflects only the author’s views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein.

---

**Document Description**

**Document Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modifications Introduced</th>
<th>Modification Reason</th>
<th>Modified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>09/02/2017</td>
<td>First draft version</td>
<td>Modification Reason</td>
<td>Riccardo Dodi</td>
</tr>
<tr>
<td>V0.2</td>
<td>11/04/2017</td>
<td>Draft version</td>
<td>Modification Reason</td>
<td>Andrea Micheletti</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Riccardo Dodi</td>
</tr>
<tr>
<td>V0.3</td>
<td>30/06/2017</td>
<td>Second draft version</td>
<td>Modification Reason</td>
<td>Eleonora Lavalle</td>
</tr>
<tr>
<td>V0.4</td>
<td>17/10/2017</td>
<td>Version before General Assembly Milano</td>
<td>Modification Reason</td>
<td>Andrea Micheletti</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Eleonora Lavalle</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mariet NouriJanian</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contribution from:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Osakidetza and IBM</td>
</tr>
<tr>
<td>V0.5</td>
<td>02/11/2017</td>
<td>Updated Version</td>
<td>Modification Reason</td>
<td>Andrea Micheletti</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mariet NouriJanian</td>
</tr>
<tr>
<td>V0.6</td>
<td>16/11/2017</td>
<td>Updated Version</td>
<td>Modification Reason</td>
<td>Mariet NouriJanian</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contribution from:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tecnalia, Metrarc,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lancashire</td>
</tr>
<tr>
<td>V0.7</td>
<td>30/11/2017</td>
<td>Updated Version</td>
<td>Modification Reason</td>
<td>Mariet NouriJanian</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contribution from:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ibermatica, Symphonic</td>
</tr>
</tbody>
</table>

---

Project Title: SHIELD
Contract No. GA 727301

http://www.project-shield.eu/

Page 3 of 95
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.8</td>
<td>13/12/2017</td>
<td>Final version for internal review</td>
<td>Andrea Micheletti Mariet NouriJanian</td>
</tr>
<tr>
<td>V0.9</td>
<td>21/12/2017</td>
<td>Final version after internal review</td>
<td>Andrea Micheletti Mariet NouriJanian</td>
</tr>
<tr>
<td>V1.0</td>
<td>22/12/2017</td>
<td>Final version after review process</td>
<td>Andrea Micheletti Mariet NouriJanian</td>
</tr>
</tbody>
</table>
Table of Contents

Table of Contents ................................................................. 5
List of Figures ........................................................................ 6
List of Tables .......................................................................... 6
Terms and abbreviations ..................................................... 8
Executive Summary ............................................................ 9
1 Introduction ........................................................................ 11
2 Use Cases specification ..................................................... 12
   2.1 Use Case 1: “Break glass” circumstance ......................... 12
   2.2 Use Case 2: Surgical intervention .................................. 16
   2.3 Use case 3: Chronic conditions + remote monitoring ...... 18
   2.4 Key Features transversal to the different use cases .......... 21
      2.4.1 Data access ......................................................... 21
      2.4.2 Privacy ............................................................. 22
      2.4.3 Data hiding ....................................................... 22
      2.4.4 Data sensitivity and offline analysis ....................... 23
3 Validation methodology ...................................................... 24
   3.1 Technical validation ...................................................... 25
      3.1.1 “Privacy – by – design” (WP4) tools technical validation ... 25
      3.1.2 “Data protection and privacy” (WP5) tools technical validation ... 27
   3.2 End-users and Experts validation ................................... 30
      3.2.1 Stakeholders maps ................................................. 30
      3.2.2 “Who” – list of end-users and possible experts to involve ... 35
      3.2.3 “What” – what we want to validate ............................ 36
      3.2.4 “How” – how we want to validate .............................. 37
      3.2.5 Recruitment, Document preparations and evaluation methodologies .. 38
4 Preparatory steps for use cases implementation .................. 40
   4.1 SHIELD working scenario proposal: openNCP installations ... 40
      4.1.1 SHIELD OpenNCP installations for the scenarios .......... 41
      4.1.2 OpenNCP base scenario and SHIELD scenarios base requirement .. 41
   4.2 Synthetic data sets ........................................................ 46
      4.2.1 Use case 1: Break glass circumstance ....................... 48
      4.2.2 Use case 2: Surgical intervention ............................. 54
      4.2.3 Use case 3: Chronic conditions + Remote monitoring .... 64
5 Conclusions ......................................................................... 71
6 Annex 1 – Requirements definition and classification ......... 72

Project Title: SHIELD
Contract No. GA 727301
http://www.project-shield.eu/
7 Annex 2 – OpenNCP Installation details ............................................................ 74
  7.1 OpenNCP Common installation .................................................................... 74
  7.2 OpenNCP additional references ................................................................... 75
    7.2.1 SHiELD OpenNCP ................................................................................ 76
      7.2.1.1 OpenNCP Installation overview .................................................. 76
      7.2.1.2 OpenNCP Installation manual .................................................... 79
  8 References ........................................................................................................ 95

List of Figures

FIGURE 1: USE CASE 1, "BREAK GLASS" CIRCUMSTANCE – GRAPHICAL REPRESENTATION ....... 14
FIGURE 2: DATA EXCHANGE GATEWAY BETWEEN TWO DIFFERENT JURISDICTIONS ................. 16
FIGURE 3: USE CASE 2 "SURGICAL INTERVENTION" – GRAPHICAL REPRESENTATION ............ 17
FIGURE 4: USE CASE 1 STAKEHOLDER MAP – "BREAK GLASSES" CIRCUMSTANCE .................. 32
FIGURE 5: USE CASE 2 STAKEHOLDERS MAP – SURGICAL INTERVENTION ......................... 33
FIGURE 6: USE CASE 3 STAKEHOLDERS MAP – CHRONIC CONDITIONS + REMOTE MONITORING ................................................................................. 34
FIGURE 7. OPENNCP WEB PORTAL LOGIN ........................................................................... 41
FIGURE 8. OPENNCP WEB PORTAL PATIENT SEARCH ............................................................. 42
FIGURE 9. PATIENT CONSENT .......................................................................................... 44
FIGURE 10. REQUEST TO PATIENT DEMOGRAPHICS ............................................................ 45
FIGURE 11. RESPONSE TO PATIENT DEMOGRAPHICS ......................................................... 45

List of Tables

TABLE 1: USE CASES IDENTIFICATION - OVERVIEW ....................................................... 12
TABLE 2: PRIVACY – BY – DESIGN TOOLS VS. USE CASES .............................................. 25
TABLE 3: SYSTEM MODELLER _ METHODOLOGY + METRICS .......................................... 26
TABLE 4: SECURITY KNOWLEDGE BASE _ METHODOLOGY + METRICS .......................... 26
TABLE 5: SECURE DESIGN PATTERN TOOL _ METHODOLOGY + METRICS ...................... 27
TABLE 6: DATA PROTECTION AND PRIVACY TOOLS VS. USE CASES .............................. 27
TABLE 7: MOBILE DEVICES SECURITY _ VALIDATION METHODOLOGY + METRICS ........ 28
TABLE 8: DATA SENSITIVITY ANALYSIS _ VALIDATION METHODOLOGY + METRICS ...... 28

Project Title: SHIELD
Contract No. GA 727301
http://www.project-shield.eu/
TABLE 9: CONSENT MANAGEMENT _ VALIDATION METHODOLOGY + METRICS ........................................ 29

TABLE 10: DATA HIDING TOOL _ VALIDATION METHODOLOGY + METRICS ...................................... 29

TABLE 11: SECURITY MONITORING TOOL _ VALIDATION METHODOLOGY + METRICS ......................... 30

TABLE 12: DIVISION OF END-USERS FOR EACH USE CASE ..................................................................... 36

TABLE 13: FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS ......................................................... 37
### Terms and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td>Advisory Board</td>
</tr>
<tr>
<td>CA</td>
<td>Consortium Agreement</td>
</tr>
<tr>
<td>CT</td>
<td>Computed Tomography</td>
</tr>
<tr>
<td>ED</td>
<td>Emergency Department</td>
</tr>
<tr>
<td>EHIC</td>
<td>Electronic Health Insurance Card</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>EMS</td>
<td>Emergency Medical Service</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GP</td>
<td>General Physician</td>
</tr>
<tr>
<td>HR</td>
<td>Health Record</td>
</tr>
<tr>
<td>HC</td>
<td>Healthcare</td>
</tr>
<tr>
<td>HCP</td>
<td>Healthcare professional</td>
</tr>
<tr>
<td>HCR</td>
<td>Healthcare Records</td>
</tr>
<tr>
<td>INR</td>
<td>International Normalized Ratio</td>
</tr>
<tr>
<td>json</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>MRI</td>
<td>Magnetic Resonance Imaging</td>
</tr>
<tr>
<td>PT</td>
<td>Prothrombin Ratio</td>
</tr>
<tr>
<td>SUS</td>
<td>System Usability Scale</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UX</td>
<td>User Experience</td>
</tr>
</tbody>
</table>
Executive Summary

This deliverable (D6.1) is the outcome of task 6.1 from work package six (WP6), and it reports “Use case specification and validation methodology”. This work has been carried out in the first year of the SHiELD project, from January until December of 2017.

This period of the project has been devoted to:

✓ **Chapter (2): Description and specification of three use cases**

In all the three use cases, we assume a citizen travels abroad and she/he needs health assistance; the foreign healthcare professional – being a general physician, a specialist doctor or an emergency practitioner – needs to access and/or manage the patient’s health data.

The use cases are described with the following schema:
- Storyboard (textual and visual description)
- Patient’s profile and doctor’s profile
- SHiELD key features to be investigated

The three use cases are:

- **Use Case 1: “Break glass” circumstance**
  An Italian citizen travelling in Spain incurs a stroke and is taken to the nearest Spanish hospital. In emergency department the physicians can get the patients’ *medical history* in summary form thanks to SHiELD platform.

- **Use Case 2: Surgical intervention**
  A Spanish patient has had a surgical intervention (e.g. urological surgery) and he is planning to travel across the EU within two months of the surgery. Patient with the scope of having the details of the surgical intervention at his disposal for any urgent medical assistance during travel, decides to use SHIELD platform’s mobile interface and share some medical histories with foreign doctors. In this case the patient for privacy issues can decide “when” and “where” to share his medical information.

- **Use case 3: Chronic conditions + remote monitoring**
  An Italian woman with type 1 diabetes mellitus under treatment with insulin, stays in the UK for work reasons for three months. She’s been living in the Basque country for ten years.
  The patient, before travelling to UK, gives consent to access her medical history. The patient uses Osakidetza’s "Carpeta Salud" mobile application to monitor her pre-prandial glycaemia, as prescribed by her GP. During her stay in the UK, she has agreed with her Spanish doctor that, since this is another country, she will
record her eating habits as well as her physical activity. Because of the stress caused by her new job in a certain point she had necessity of emergency assistance, so medical staff thanks to SHiELD platform had access to her medical and daily recorded information.

✓ **Chapter (3): Validation Methodology**

The use cases defined in the previous chapter will be validated in two different phases:

- **Technical validation**
  In technical validation phase every technological tool developed will be validated following a defined methodology and specific metrics prepared by the responsible partner of every tool. This part of validation will take place during the implementation phase by the developers.

- **End-users and Experts Validation**
  The main SHiELD platform functionalities will be validated with experts and end-users by going through the platform and checking the design, accessibility, and usability of the product.

In this chapter we have defined and described different validation methodologies (Expert review, Usability testing and questionnaire).

✓ **Chapter (4): Preparatory steps for use cases implementation**

This part of the deliverable includes details about the preparatory steps for use cases implementation, meaning the openNCP installations, and details about synthetic data sets to be used.

The last part of the deliverable includes two annexes: “Annex 1 – Requirements definition and classification” and “Annex 2 – OpenNCP Installation details”.

Project Title: SHIELD
Contract No. GA 727301

http://www.project-shield.eu/
1 Introduction

First objective of this document is to “specify three different use cases“ that represent real-life-strength scenarios; these use cases will help the development of the project in different tasks of work packages. This part is included in chapter 2.

Second objective is to find out “validation methodologies and metrics” to assess the effectiveness and efficiency of the SHiELD platform developed regarding Security and Privacy and the technologies used. This part is included in chapter 3.

Third objective is to describe the “Preparatory steps for use cases implementation” and the “synthetic data sets” regarding each use case. This part is included in chapter 4.

The definition of the use cases and validation methodologies benefit of inputs coming from different tasks of other work packages, including WP2 – Task 2.1, 2.2, WP3 – Task 3.1, WP4 – Task 4.1.
2 Use Cases specification

Main principles of use cases

Following the scope of the SHiELD project and what is described in the SHiELD DoA, three use cases have been prepared with different characteristics. The main principles considered for defining the use cases are the followings:

- Citizen / Patient, with related personal data, centered point of view
- Citizen / Patient needs and the related level of healthcare services
- Health data needed

The outcome of applying these main principles is a table that specifies the use cases in function of the “citizen / patient typology”, the related healthcare needs and the level of healthcare services for each of them.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Citizen / Patient “typology”</th>
<th>Citizen / Patient needs</th>
<th>Level of HC services</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Citizen with clinical history of heart disease</td>
<td>• Healthcare intervention due to unexpected situation (e.g. stroke, heart attack, physical trauma) • Life threatening situation</td>
<td>1. Emergency HC services if needed (territorial EMS involvement)</td>
</tr>
<tr>
<td>2</td>
<td>Patient with Surgical intervention + follow up management</td>
<td>• Drug therapy compliance • Needs to follow medical advices • Healthcare intervention in case of complications (related to the surgical intervention)</td>
<td>1. Surgical intervention (hospital) 2. Supporting the patient with specific needs 3. HC services if needed (outpatient services and/or hospital in case of complications)</td>
</tr>
<tr>
<td>3</td>
<td>Patient with Chronic conditions + remote monitoring</td>
<td>• Drug therapy compliance • Monitoring specific parameters (weight, blood pressure, glucose levels, ECG, etc.) • Healthcare intervention in case of decompensation, exacerbation or complication of the chronic condition</td>
<td>1. Supporting the patient with specific needs 2. HC services if needed (outpatient services and/or hospital)</td>
</tr>
</tbody>
</table>

Table 1: Use cases identification - overview

2.1 Use Case 1: “Break glass” circumstance

Storyboard

Project Title: SHIELD
Contract No. GA 727301  http://www.project-shield.eu/
An Italian citizen travelling in Spain incurs a stroke and is taken to the nearest Spanish hospital. While receiving first aid from the Emergency medical services (EMS), the coordination center informs the EMS in which hospital the patient should be taken to. At the same time a message is sent to a workstation located in the emergency department of the hospital responsible for alerting the first-aid unit.

As soon as the message is received a medical team is created for the stroke assistance. For this purpose, different physicians are summoned:

- emergency physicians;
- neurologist;
- neuroradiologist;
- anaesthesiologist;

In order to ensure the best assistance, the medical staff wishes to check the patient’s Electronic Health Record (EHR) to know their medical history (e.g. their epSOS patient summary). Since the patient is foreign, this is possible thanks to the SHiELD platform, which ensures the communication between NCPs of different countries within Europe in a secured manner.

This is fundamental, not only to discover possible illnesses or chronic conditions, but also to ensure that the patient does not suffer from allergies to drugs; also if the patient receives treatment for a chronic condition, that should be relevant in order to be able to perform a therapeutic management as efficiently as possible.

Indeed, the first aid protocol for a stroke may vary in case of other pathologies or allergies. For example, in case of renal failure the cranium CT scan (the traditional examination in case of stroke) can be replaced with an MRI in order to avoid contrast agent, which can aggravate kidney conditions. The fibrinolytic treatment has shown an important reduction in mortality and morbidity in patients with stroke, but all treatments may have contraindications when applied, and it is so important to know about them in order to not generate iatrogenic damage in the patient. Examples for such contraindications are oral anticoagulant treatment, recent history of severe bleeding, severe liver disease, hemorrhagic retinopathy, etc.

It could be possible that the patients receive endovascular treatment. This case needs general anesthesia in an operating room, and having access to patient’s HCR for the anesthesiologist could be vital.

This is just to demonstrate the importance of the patient clinical history; the epSOS clinical record summary with the mandatory basic dataset will be enough to perform an appropriate management at the time of the incident. It could be possible to extend this information to other examinations (e.g. blood tests, bio images etc.) made in the 60 days
preceding the “break glass” circumstance, that are usually sufficient to give a general overview of the clinical condition. This means that the chance of patient survival increases if the physician has access to the patient’s clinical record as quickly as possible. Consequently, a better patient response is expected, the faster the therapy is provided. In the management of stroke in the emergency services there is a saying that “time is brain”.

![Diagram]

Figure 1: Use Case 1, “Break glass” circumstance – graphical representation

**Patient’s profile:**

The patient under consideration is an Italian patient, with a clinical history of heart disease, male, 65 years old. In this use case the patient is supposed to have at least one previous hospitalisation in order to have electronic health records to share across countries (surgical intervention for a heart valve replacement).

Going into details regarding his health condition, the anamnesis contains some risk indicators, such as:

- smoker
- poor exercise
- stroke in family
- overweight

These conditions are indicators of high risk stroke and are relevant information for the Spanish doctor during the treatment, but not mandatory in the “Break glass” circumstance.

Indeed, in case of stroke the doctor benefits from all the information retrieved from the patient’s medical history. Since the patient has a previous intervention, his medical record could contain chest X-rays, electrocardiograms and analytical reports.
analytical reports will also be of interest because the patient is in treatment with anticoagulants, so in order to see the status of his coagulation before the event.

**Doctors’ profiles:**

When a patient with a stroke is taken to hospital, the team is made up of different specialists to suit the patient’s needs and is set up before the patient’s arrival. The group consists of:

- The **ED doctor** who is a general physician, able to give a general overview of the health condition;
- The **Neurologist** who is the specialist responsible for diseases linked to the brain, they’re responsible for identifying the entity and the type of stroke (haemorrhagic or blood clot caused) and for establishing the first line of treatment;
- The **Neuroradiologist** is the specialist responsible for evaluating and informing the neuroimaging test (CT scan or MRI) necessary to obtain a correct diagnosis (haemorrhagic or ischemic infarction), location of the lesion, extent of the lesion... in order to choose the appropriate treatment for the patient. Neuroradiologists also perform endovascular treatment.
- The **Anaesthesiologist** is responsible for checking the patient’s aerial functionality. They’re involved only if the patient is not able to self-breathe or is unconscious. A general anesthesia could be also necessary in order to provide endovascular treatment.

**Administrative profiles:**

- The **Hospital admission technician** is in charge of collecting administrative data for the patient in case they don’t carry ID, as well as of communicating with relatives or friends of the patients, to try and collect all necessary information required during their stay at the hospital.

**Connections with other WPs**

- **WP3:** possibility to analyze legal and regulatory requirements concerning data protection in e-Health interoperability. In particular, the output from T3.1 can be useful to understand the compatibility of the SHiELD solution with the current security challenges.
- **WP4:** possibility to capture potential threats to health data and to demonstrate data protection and regulatory compliance requirements in two different European jurisdictions.
- **WP5:** in particular, T5.2 “Data sensitivity analysis tools” will be tested during the pilot phase moreover; T5.3 “Consent management” after the patient is
conscious or with the consent of a relative; T5.5 “Security monitoring and compliance assurance” can be applied to this particular use case.

Figure 2: Data exchange gateway between two different jurisdictions

### 2.2 Use Case 2: Surgical intervention

**Storyboard**

A Spanish patient has had a surgical intervention (e.g. urological surgery) and he is planning to travel across the EU within two months of the surgery.

The patient wants to have details of the surgical intervention at his disposal in case it is needed for medical assistance during the travel abroad. At this scope the patient, together with the Italian urological surgeon, decides - using the mobile interface of the “SHiELD” platform - which information would be useful to share with a foreign doctor during the trip. They decide to share part of the hospital discharge letter, including detailed information about the patient’s clinical history and the recent surgery. The SHiELD solution will also give the possibility to hide sensitive information capturing patient consent.

Moreover, the patient, using the “SHiELD platform”, can make the decision, relevant for privacy issues, of when and where to share this information. This is meant to limit the availability of the shared information in time and location (e.g. “in Milan for the next 2 weeks”). Access preferences will be integrated into the access model to ensure the balanced concerns of patient privacy and treatment need.

In case of post-surgical complications during the trip, after providing first aid, the emergency physicians must have access to the EHR, including the most recent clinical and surgical steps.
Initially, the doctor has access to the epSOS Patient Summary with basic information, in order to discover the type of surgical procedure performed; then, they want to access detailed information about the surgical procedure itself, all the complementary tests carried out in the process, and therefore decide to visualise the extract of the discharge letter shared by the patient.

The patient and his doctor agree on the contents to be shared on the platform, in order to be available to a third party, (e.g. a foreign medical professional). As previously mentioned, data availability can be limited in time and location, for privacy issues and health records must only be accessed by authorised users. This allows the testing of the consent management tool.

![Figure 3: Use case 2 “Surgical intervention” – graphical representation](image)

**Patient’s profile:**

Spanish, male, age<60, prostate operation a month before travelling. While traveling in Italy, he presents an episode of fever, with low back pain and dysuria and decides to go to the emergency department in the hospital of the town where he is on vacation.

**Doctors’ profiles:**

When a patient with a post-surgery complication is taken to hospital, the Italian doctors involved are:

- The **ED doctor** who is a general physician able to give a general overview of the health condition
- The **Urological surgeon** who is the specialist called in case the disease needs to be treated with a surgical intervention
- **Other specialists** related to the post-surgery complication (nephrologist, internist, infectious unit doctors ...), may be required for intervention in specific cases: complicated infection, associated renal failure ...

**Administrative profiles:**
- The **Hospital admission technician** is in charge of collecting administrative data for the patient in case they don’t carry ID, as well as of communicating with relatives or friends of the patients, to try and collect all necessary information required during their stay at the hospital.

**Connections with other WPs**

- **WP3**: legal and regulatory requirements concerning data protection in e-Health interoperability will be tested among two different jurisdictions. In particular, T3.3 “Enhancing Authorization Mechanism” will be applied to patient consent for data sharing across borders.

- **WP4**: in addition to the possibility to capture potential threats to health data, privacy by design can be tested among two different jurisdictions.

- **WP5**: in this use cases all the tasks of this WP will be tested: T5.2 “Data sensitivity analysis tools”; T5.3 “Consent management” before and during patient travel once data is requested; T5.4 “Data hiding tool” according to patient preferences and regulation; T5.5 “Security monitoring and compliance assurance”.

![Data exchange gateway with the same jurisdictions and between two hospitals](image)

Figure 4: Data exchange gateway with the same jurisdictions and between two hospitals

### 2.3 Use case 3: Chronic conditions + remote monitoring

**Storyboard**

A 40 year old Italian woman with type 1 diabetes mellitus under treatment with insulin, stays in the UK for work reasons for 3 month. She’s been living in the Basque country for 10 years.

The woman, prior to her stay in the UK, gives consent to access her medical history. The patient uses Osakidetza’s "Carpeta Salud" mobile application to monitor her pre-
prandial glycaemia, as prescribed by her GP. During her stay in the UK, she has agreed with her doctor that, since this is another country, she will record her eating habits as well as her physical activity.

After a week in the UK, she begins to notice dizziness accompanied by general discomfort and sometimes nausea. As it does not happen every day and the glycaemia is within normal range, she decides to take care of her diet and continue with her usual treatment schedule. She blames these episodes on the stress caused by her new job. After several days without any improvement of her symptoms, being at work she presents a transient loss of consciousness (syncope) with a fall to the ground and a slight traumatic brain injury, with total recovery of consciousness. Her colleagues decide to take her to the nearest hospital emergency department.

During the patient’s anamnesis, she refers to a brain surgery she had as a child in Italy, but she does not know any details. This old episode could be of great importance for the management of the incident.

As in the other cases, in order to ensure the best assistance, the medical staff wish to check the patient’s EHR to access her medical history (e.g. her epSOS patient summary), but in this scenario, the accessibility to more than the patient summary could be helpful for the medical staff. Since the patient is foreign, this is possible thanks to the SHIELD platform, which ensures the communications between NCPs of different countries within Europe.

**Patient’s profile:**

The patient under consideration is an Italian patient, with a long history of DM-1 in treatment with insulin, which has had a syncope and has been with a general discomfort, dizziness and nausea for several days.

In this use case, the patient is supposed to have a basic dataset with mandatory data that will be useful in the management of the acute episode, such as: allergies and intolerances, vaccinations, lists of resolved, closed or inactive problems, surgical procedures, current problems/diagnosis and a list of current prescriptions.

It could also be useful to access to the “Carpeta Salud” app, where the patient has recorded her preprandial glycaemia in the last week, her diet intake and physical activity. This data is useful in order to have a register of activities and biological markers that can provide us with data related to the control of the DM, since a decrease of its diabetes could justify the problem presented by the patient at the EMS.

Checking resolved, closed or inactive problems, the emergency doctor is aware that the patient was treated for a brain tumor aged 25, so it would be useful to get access to extended data of this episode such as: hospital discharge reports, brain CT/MRI, reports.
of pathological anatomy etc. This could be solved by “SHiELD platform” with the exchange of clinical data by different countries’ NCPs.

**Doctor’s profiles:**

When a patient is taken to hospital, different doctors should have access to the patient’s electronic clinical data summary.

- **The ED doctor**, who is a general physician able to give a general overview of the health condition;
- **The Endocrinologist**, in the case that the patient requires new treatment and care regimen in case of a diabetic decompensation;
- **The Neurologist/Neuroradiologist**, in case that the patient has an alteration in the brain CT/MRI and they would have to determine that the patient experiences an acute neurological process.

**Administrative profiles:**

- **The Hospital admission technician** is in charge of collecting administrative data for the patient in case they don’t carry ID, as well as of communicating with relatives or friends of the patients, to try and collect all necessary information required during their stay at the hospital.

![Figure 5: Use case 3 “Chronic conditions + remote monitoring” – graphical representation](image_url)

**Connections with other WPs**

- **WP3**: legal and regulatory requirements concerning data protection in e-Health interoperability will be tested among three different jurisdictions. In particular,
T3.3 “Enhancing Authorization Mechanism” will be applied to patient consent for data sharing across borders.

- WP4: in addition to the possibility to capture potential threats to health data, privacy by design can be tested among three different jurisdictions.

- WP5: in this use cases all the tasks of this WP will be tested: T5.1 “Mobile device security” because part of information is going to be shared to the national contact point by the mobile device; T5.2 “Data sensitivity analysis tools”; T5.3 “Consent management” before patient travel once data is requested; T5.4 “Data hiding tool” according to patient preferences and regulation; T5.5 “Security monitoring and compliance assurance”.

Figure 6: Data exchange gateway between three different jurisdictions

2.4 Key Features transversal to the different use cases

2.4.1 Data access

Health records must be available in a secure way to authorised profiles, independently from the specific circumstance; in this context, we should focus primarily on the reliability aspects, since one or more issues can hinder an immediate and trusted access to the patients’ information (e.g. loss of consciousness, network issues, device malfunction...). The options are:

- Electronic card(s): a certified personal document, such as the EHIC (European Health Insurance Card), can be used to identify the patient and access their HR.
The doctor’s European Health Insurance Card could be also used to identify the doctor and to grant access to the SHiELD platform.

- “Trusted” App: the doctor can access the HR using the patient’s smartphone through a secured login.
- “Open” App: The patient’s smartphone is set to have an open access to some essential healthcare data to be used by healthcare professionals in emergency situations. The access to this data is not protected and can be performed directly from the home screen.

2.4.2 Privacy

The patient and their doctor agree on the contents to be shared on the platform, in order to be available to a third party, i.e. a foreign medical doctor. The availability can be limited in time and location to counteract privacy concerns (e.g. “in the city of Liverpool for the next 3 days”).

Health records must be accessed only by authorised users.

2.4.3 Data hiding

Regarding data hiding all the three scenarios need some hiding capabilities. The idea is to introduce fine-grained, policy driven, data hiding mechanisms which support different types of masking such as redaction, encryption as well as format preserving encryption. For example, if the involved patient states that they do not want to share some information, it can be useful to redact part of the documentation as required.

For the proposed use-cases personal data needs to be masked with the possibility of dynamically un-masking in case of “break glass” circumstances as outlined in Scenario I.

An example of data hiding on the following json input:

```json
{
  "patient": "john",
  "phone": "39 07 17903134",
}
```

Could result in:

```json
{
  "patient": "*******",
  "phone": "Ad034 gh503 dxc7x4",
}
```
Encryption and data hiding will be adjusted according to the use case requirements.

2.4.4 Data sensitivity and offline analysis

Regarding data sensitivity, the idea is to analyse clinical data (structured, semi-structured or non-structured) and identify the elements that contain sensitive information. Our plan is to start with structured data (data bases) and make use of existing data classifiers to identify known formats (e.g. credit cards) and predefined dictionaries for domain knowledge (e.g. disease). We plan to make use of metadata, i.e. the data base schema, column names to better understand the semantics of the field (e.g. 'name'). On top of this, we will try to develop additional heuristics.

This analysis will be performed offline and its results can be used to inform the hospital of where in its data stores (e.g. data bases) sensitive data exists. Based on the results, the hospital can apply the relevant privacy and security measures as required by regulation. Additionally, this information will be provided to WP4 to aid with identifying and capturing threats.
3 Validation methodology

For validating the SHiELD platform and the related prototypes, we consider the followings two main steps:

a) Verification of the SHiELD platform and the prototypes developed

This part, also called Technical Validation, regards the evaluation of the technical development phase of the platform and the related prototypes in order to determine whether they satisfy the conditions and requirements specified at the beginning of the technical implementation. This process is an internal process.

The technical validation verifies the quality and productivity of the platform but it does not ensure the level of usefulness by end-users point of view.

The technical validation will be done by technical partners and it includes the verification of the results of WP4 and WP5 following the methodologies and metrics determined in the chapter 3.1 “Technical Validation”.

b) Validation of the SHiELD platform by end-users and experts

The SHiELD platform according to the defined use cases will be validated by end-users and experts, in order to assess and ensure their relevance in real environments.

The end-users and experts’ evaluation of the platform (with the related prototypes) takes place during and at the end of the development phase to determine whether the end-users conditions and requirements are satisfied.

This validation will be done by the three partners responsible of the use cases (FCSR, OSA and LANCS) according to methodologies and metrics emphasized in the following chapter 3.2 “End-users and Experts validation”.

In next sections 3.2.2 – 3.2.4 we explain Who are the end-users and experts, What they validate and the methodologies (How) that will be used to validate the SHiELD platform.

Differences between verification and validation

Verification is the process of checking that the software meets the specification. “Did I build what I need?”

Validation is the process of checking whether the specification captures the customer’s needs. “Did I build what I said I would?”

The validation of the use cases will be conducted following the work plan described in SHiELD DoA, considering three overlapping phases starting with 6-monthly intervals (M13-M24, M19-M30, M25-M36).
3.1 Technical validation

As we mentioned before, Technical Validation will be done by technical partners and it regards the results of WP4 “Privacy – by – design” and WP5 “Data protection and privacy” with their determined methodologies and metrics.

3.1.1 “Privacy – by – design” (WP4) tools technical validation

This paragraph is dedicated to define the validation methodology and metrics for the “Privacy – by – design” tools.

The “Privacy – by – design” tools will be tested in all three use cases, as described in the following table 2.

<table>
<thead>
<tr>
<th>Use case 1: «Break glass circumstance»</th>
<th>Security modelling</th>
<th>Security knowledge base</th>
<th>Secure design patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use case 2: “Surgical operation + follow up”</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Use case 3: “Chronic condition”</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: Privacy – by – design tools vs. use cases

- Task 4.1: Security modelling

**Tool: System Modeller**

**Responsible partner: IT Innovation**

<table>
<thead>
<tr>
<th>Validation methodology</th>
<th>According to the KR03, System Modeller should</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• support the key steps in the risk analysis process (threat identification, risk assessment, risk treatment specification, residual risk acceptance, and documentation)</td>
</tr>
<tr>
<td></td>
<td>• reduce the amount of time and work needed for the threat identification and documentation steps compared to a manual analysis</td>
</tr>
</tbody>
</table>

Project Title: SHIELD
Contract No. GA 727301  
http://www.project-shield.eu/
• Task 4.2: Security knowledge base

**Tool: Security knowledge base**  
**Responsible partner: IT Innovation**

| Validation methodology | As defined in KR01, the knowledge base should “cover[s] general cyber security threats based on a suitable standard threat taxonomy such as RFC4949, plus specific threats arising in health data exchange such as de-anonymisation attacks using weaknesses in data exchange schema, and regulatory compliance requirements for the three member states involved in validation pilots.”

We can map our threat coverage onto the relevant standards or other threat classification schema. |

| Metrics | the knowledge base’s threat coverage in relation to the standards |

Table 4: Security knowledge base _ Methodology + Metrics

• Task 4.3: Secure design patterns

This tool is used during software development phases. It highlights bugs and vulnerabilities based on Common Weaknesses Enumeration (CWE). In addition, it helps adding specific chunks of Java code to the existing files in order to enhance security.

**Tool: Secure Design Pattern tool**  
**Responsible partner: Tecnalia**
### 3.1.2 “Data protection and privacy” (WP5) tools technical validation

This paragraph is dedicated to define the validation methodology and metrics for the “Data protection and privacy” tools.

The “Data protection and privacy” tools will be tested in the different use cases according to the following table 6.

<table>
<thead>
<tr>
<th>Data protection and privacy tools</th>
<th>Mobile devices security</th>
<th>Data sensitivity analysis</th>
<th>Consent management</th>
<th>Data hiding</th>
<th>Security monitoring and compliance assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case 1: «break glass circumstance»</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Use case 2: “surgical operation + follow up”</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Use case 3: “chronic condition”</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 6: Data protection and privacy tools vs. use cases

- **Task 5.1: Mobile devices security**

<table>
<thead>
<tr>
<th>Tool: Mobile Devices Security – Secure Data Exchange Tool</th>
<th>Responsible partner: Metrarc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation methodology</td>
<td>This tool’s security will be validated manually by evaluating the feature values read during the calibration phase.</td>
</tr>
</tbody>
</table>
The tool’s stability will be validated manually by using the data exchange application to attempt to transfer data between a mobile device and an epSOS-compliant data exchange service, and to attempt to view the transferred health data stored on the device at rest.

Considerations to be made whilst testing the tool:
- Use a device not enrolled in the system to break the hardware features, or deliberately break the system configuration (device tampering)
- Test with different users to break user features (device stolen)
- Test in different locations to break environment features (ensure data only accessible whilst working)
- Challenges of system correlations over a number of runs
- Look at devices with the same model & internal chipsets which are intrinsically the most difficult to differentiate based on OEM hardware and software alone
- Flexibility & scalability to manage different amount of devices and Doctors

Our test cases will be driven by use case requirements and examples.

The three main metrics will be:
- The strength of the ICMetric system, measured by the entropy of the features used in the key generation process
- The reproducibility rate of the correct key
- The number of false positives

<table>
<thead>
<tr>
<th>Metrics</th>
<th>The three main metrics will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The strength of the ICMetric system, measured by the entropy of the features used in the key generation process</td>
</tr>
<tr>
<td></td>
<td>The reproducibility rate of the correct key</td>
</tr>
<tr>
<td></td>
<td>The number of false positives</td>
</tr>
</tbody>
</table>

Table 7: Mobile devices security _ validation methodology + Metrics

- **Task 5.2: Data sensitivity analysis**

<table>
<thead>
<tr>
<th>Tool: Data sensitivity analysis</th>
<th>Responsible partner: IBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation methodology</td>
<td>This tool will be validated manually by running the tool and comparing its results against the results of a human privacy experts.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Precision and recall of the sensitive items</td>
</tr>
</tbody>
</table>

Table 8: Data sensitivity analysis _ Validation methodology + Metrics

- **Task 5.3: Consent management**

<table>
<thead>
<tr>
<th>Tool: Consent Management</th>
<th>Responsible partner: Symphonic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation methodology</td>
<td>This tool will be validated when requests are made for patient information. A combination of scenarios will be pushed through the</td>
</tr>
</tbody>
</table>
• Task 5.4: Data hiding tools

Table 9: Consent Management _ Validation methodology + Metrics

<table>
<thead>
<tr>
<th>Tool: Data Hiding Tool</th>
<th>Responsible partner: IBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation methodology</td>
<td>This tool will be validated manually by testing the tool while considering the following abilities:</td>
</tr>
<tr>
<td></td>
<td>• Handle, unpack and parse the required input formats and support different input structures</td>
</tr>
<tr>
<td></td>
<td>• Selection of relevant items for masking (fine grained)</td>
</tr>
<tr>
<td></td>
<td>• Masking &amp; Unmasking operations of the selected elements (e.g. redact, encrypt)</td>
</tr>
<tr>
<td></td>
<td>The test cases will be driven by use case requirement and examples.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metrics</th>
<th>The main metric will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>% successful masking (and unmasking) of required sensitive and personal items in the use case provided documents.</td>
</tr>
<tr>
<td></td>
<td>The type and complexity of required formats will be accounted for. This can complicate or simplify the process of parsing (e.g. json vs. pdf) as well as limit the ability to select specific items to mask (e.g. selection of items in structured formats vs unstructured formats)</td>
</tr>
</tbody>
</table>

• Task 5.5: Security monitoring and compliance assurance

Table 10: Data hiding tool _ Validation methodology + Metrics

<table>
<thead>
<tr>
<th>Tool: Security Monitoring Tool</th>
<th>Responsible partner: Symphonic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation methodology</td>
<td>This will be manually validated at both design-time and run-time. During design-time it will be validated that the policies match the use-case and present the correct decision in each case. Further validation will carry out cross-policy analysis to ensure there are no possible conflicts in the policies.</td>
</tr>
</tbody>
</table>
3.2 End-users and Experts validation

This part of the validation of the use cases will be done by two groups:

1- a validation with experts
2- a validation with end-users directly involved in the use cases

To define the experts and end-users to involve in the validation, the different stakeholders have been matched for each use case. In the chapter 3.2.1 the stakeholder maps have been defined with the following elements:

- the actors who are playing main roles in the use cases
- the connection between actors:
  - Direct influence on patients’ / citizens’ healthcare (solid lines)
  - Indirect influence on patients’ / citizens’ healthcare (dashed lines)
  - Lateral or bilateral communication

Actors are people who have different roles in SHiELD use cases.

A specific actor can also be an end-user of the SHiELD platform.

With end-user we define an actor that directly uses the functionalities of the SHiELD platform.

The end-users will be involved in the validation activities to test the functionalities of the SHiELD platform.

By experts are meant to be people who have knowledge of the technological sector in which SHiELD is positioned and that can be involved in the SHiELD platform validation.

3.2.1 Stakeholders maps

There is a stakeholder map for every use case, according to the main actors involved in the different healthcare phases.

The maps are designed by four circles, which represent different levels of proximity of stakeholders with the core actor. These four circles are:

- **Core Stakeholder**: the core actor of every use case, i.e. the “Patient” / “Citizen” who is travelling from country A to B or from country B to C.
➢ **Direct Stakeholders:** Stakeholders who directly are affecting the core actor. They can be Healthcare Professionals, General Physicians, Surgical Department of Hospital, Emergency Department of Hospital, etc. during patients care necessity in both countries.

➢ **Indirect Stakeholders:** Stakeholders who indirectly affect the core actor, e.g. “IT Department of Hospital”.

➢ **External Stakeholders:** Stakeholders who do not have any contact with core actor but their existence is important for the use case itself, e.g. “pharmaceutical companies”.


Use Case 1 _ “Break glasses” circumstance:

The following map illustrates all actors who directly or indirectly influence the patient / citizen; the highlighted area shows the actors who are mentioned in the use case storyboard.

![Figure 4: Use Case 1 stakeholder map _ “Break glasses” circumstance](image-url)
Use Case 2 _ Surgical intervention:

The following map illustrates all actors who directly or indirectly influence the patient / citizen; the highlighted area shows the actors who are mentioned in the use case storyboard.

![Use Case 2 stakeholders map - Surgical intervention](image)

Figure 5: Use Case 2 stakeholders map _ Surgical intervention
**Use Case 3 _ Chronic conditions + remote monitoring:**

The following map illustrates all actors who directly or indirectly influence the patient / citizen; the **highlighted** area shows the actors who are mentioned in the use case storyboard.

![Use Case 3 stakeholders map _ Chronic conditions + remote monitoring](image)

**Figure 6: Use Case 3 stakeholders map _ Chronic conditions + remote monitoring**
3.2.2 “Who” – list of end-users and possible experts to involve

With **end-user** we define an actor that directly uses the functionalities of the SHiELD platform. Following a list of the different end-users involved in the use cases:

- Citizen with clinical history
- Patient
- HC professional:
  - Emergency Doctor
  - General Physician
  - Surgeon
  - Neurologist/Neuroradiologist
  - Anaesthesiologist
- Hospital admission technician
- Medical documentation and archives technician

With **experts** we mean people who will not use directly the SHiELD platform but they have knowledge in technological, digital, e-health and etc. sector in which SHiELD is positioned and that can be involved in the SHiELD platform validation. Following a list of possible experts to involve:

- Hospital IT department, e.g. Hospital IT department CIO or Hospital responsible for the IT system maintenance
- Hospital Medical Direction staff
- Hospital Legal services
- Hospital Chief Executive Officer (CEO)
- Institutional epSOS referent
- Digital security expert
- E-health sector expert

Table 12 maps the different end-users and experts involved in each use case:

<table>
<thead>
<tr>
<th>Use case</th>
<th>End-users</th>
<th>Experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - “Break glass” circumstance</td>
<td>• Citizen with clinical history</td>
<td>• Hospital CIO</td>
</tr>
<tr>
<td></td>
<td>• General Physician</td>
<td>• Hospital IT department staff</td>
</tr>
<tr>
<td></td>
<td>• Emergency Doctor</td>
<td>• Hospital Medical Direction staff</td>
</tr>
<tr>
<td></td>
<td>• Neurologist/Neuroradiologist</td>
<td>• Institutional epSOS referent</td>
</tr>
<tr>
<td></td>
<td>• Anaesthesiologist</td>
<td>• Digital security</td>
</tr>
<tr>
<td></td>
<td>• Hospital admission technicians</td>
<td>• E-health sector</td>
</tr>
<tr>
<td></td>
<td>• Medical documentation and archives technicians</td>
<td></td>
</tr>
<tr>
<td>2 - Surgical intervention</td>
<td>• Patient</td>
<td>• Hospital CIO</td>
</tr>
<tr>
<td></td>
<td>• Emergency Doctor</td>
<td>• Hospital IT department staff</td>
</tr>
<tr>
<td></td>
<td>• Urological surgeon</td>
<td>• Hospital Medical Direction staff</td>
</tr>
<tr>
<td></td>
<td>• Other specialists</td>
<td>• Institutional epSOS referent</td>
</tr>
<tr>
<td></td>
<td>• Hospital admission technicians</td>
<td>• Digital security</td>
</tr>
<tr>
<td></td>
<td>• Medical documentation and archives technicians</td>
<td>• E-health sector</td>
</tr>
<tr>
<td>3 - Chronic conditions + remote monitoring</td>
<td>• Patient</td>
<td>• Hospital CIO</td>
</tr>
<tr>
<td></td>
<td>• ED doctor</td>
<td>• Hospital IT department staff</td>
</tr>
<tr>
<td></td>
<td>• Endocrinologist</td>
<td></td>
</tr>
</tbody>
</table>

Table 12 maps the different end-users and experts involved in each use case:
3.2.3 “What” – what we want to validate

According to the three SHiELD use cases descriptions and focusing mainly on characterizing the functionalities of the SHiELD platform, a list of requirements has been collected.

This list of requirements, further to guide the implementation phase, will be useful in order to decide the main SHiELD functionalities to validate.

In table 13 the requirements are specified in terms of classification, typology, ID, description and the involved use cases.

The definition of requirement classification and typology are included in Annex 1 “Requirements definition and classification”.

<table>
<thead>
<tr>
<th>#</th>
<th>Class</th>
<th>Type</th>
<th>ID</th>
<th>Description</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 2 3</td>
</tr>
<tr>
<td>1</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_1_F</td>
<td>The physician needs to access to SHiELD platform</td>
<td>x x x</td>
</tr>
<tr>
<td>2</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_2_F</td>
<td>The physician has to login to SHiELD platform with personal ID and password</td>
<td>x x x</td>
</tr>
<tr>
<td>3</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_3_F</td>
<td>The physician needs to access to patient profile</td>
<td>x x x</td>
</tr>
<tr>
<td>4</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_4_F</td>
<td>The physician has to compile the corresponding fields in SHiELD platform to search patient</td>
<td>x x x</td>
</tr>
<tr>
<td>5</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_5_F</td>
<td>The SHiELD platform has to give the possibility to the physician and patient together to choose the data needed to share (patient summary (EHR),...)</td>
<td>x x x</td>
</tr>
<tr>
<td>6</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_6_F</td>
<td>The SHiELD platform has to give the possibility to the physician and patient together to choose the data which they don't want to share</td>
<td>x x x</td>
</tr>
<tr>
<td>7</td>
<td>USER</td>
<td>N-FUNCTIONAL</td>
<td>U_7_NF</td>
<td>The SHiELD platform has to give the possibility to the patient to decide for how long s/he wants to share her/his data</td>
<td>x</td>
</tr>
<tr>
<td>No.</td>
<td>Role</td>
<td>Type</td>
<td>Requirement</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>USER</td>
<td>N-FUNCTIONAL</td>
<td>U_8_NF</td>
<td>The SHiELD platform has to give the possibility to the patient to decide <strong>where</strong> (in which country) s/he wants to share her/his data</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>USER</td>
<td>FUNCTIONAL</td>
<td>U_9_F</td>
<td>The medical staff of hosted country needs to access patient summary (EHR) through SHiELD platform</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>USER</td>
<td>FUNCTIONAL</td>
<td>U_10_F</td>
<td>The medical staff of hosted country has to login to SHIELD platform with personal ID and password</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>USER</td>
<td>N-FUNCTIONAL</td>
<td>U_11_NF</td>
<td>The medical staff of hosted country needs to to identify the nationality of the user / code system</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_12_F</td>
<td>The SHIELD platform has to get access to database of the patients' hospital</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>SYSTEM</td>
<td>FUNCTIONAL</td>
<td>S_13_F</td>
<td>the SHIELD platform has to retrieve the patient summary (EHR) from database of patients' hospital</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>SYSTEM</td>
<td>N-FUNCTIONAL</td>
<td>S_14_NF</td>
<td>The SHIELD platform has to synchronize the clinical data of EU countries hospitals inside of the agreement</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>SYSTEM</td>
<td>N-FUNCTIONAL</td>
<td>S_15_NF</td>
<td>The SHIELD platform has to ensure the data protection through legal and regulatory requirements (WP.3)</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>SYSTEM</td>
<td>N-FUNCTIONAL</td>
<td>S_16_NF</td>
<td>The SHIELD platform has to ensure the data protection regulatory compliance requirements in two different countries (WP.4)</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>SYSTEM</td>
<td>N-FUNCTIONAL</td>
<td>S_17_NF</td>
<td>The SHIELD platform has to ensure the &quot;Data sensitivity analysis tool&quot; (WP.5)</td>
<td></td>
</tr>
</tbody>
</table>

Table 13: Functional and Non-Functional requirements

The requirements mentioned in the table 13 will go on more details for the next deliverable (D6.2 due to month 18).

### 3.2.4 “How” – how we want to validate

The methodology proposed is common for all three use cases and as mentioned in chapter 3.b, users’ satisfaction will be evaluated according to the system developed and the initial requirements.

**Validation by Experts**

Project Title: SHIELD

Contract No. GA 727301

http://www.project-shield.eu/
These users will evaluate the SHiELD technical framework, components and architecture aspects. For this validation we introduce two methods: Expert reviews and Questionnaires.

The **Expert reviews** involve a single “expert” going through a product via User Interface (UI) and looking for issues with the design, accessibility, and usability of the product. The more expertise the reviewer has in usability and UX design – the more valuable their input (in most cases). The Expert has to inspect the platform and freely take notes of the issues detected. With this method we can review the entire platform and identify possible human errors or technical errors (e.g. bugs).

Another possible method to validate the platform with experts is to use **Questionnaires**; there are two possibilities:

- Structured Open-end questionnaire: specific questions regarding the SHiELD platform that experts can freely answer
- Structured Close-end questionnaires: specific questions to be answered choosing a score or a pre-formulated answer.

**Validation by End-users**

**Usability Testing**

Usability testing is a technique used in *user-centered interaction design* to evaluate a product or service “usability” (how easy it is to use) by testing it with representative users. This can be seen as *an irreplaceable usability practice*, since it gives direct input on how real users use the system.

Possible metrics to use in this test regards the Success Rate, Error Rate, Time to Completion and Subjective Measures (eg. SUS questionnaire (post-usability test)).

**Close-end Questionnaire by End-users**

A data gathering method that is utilized to collect, analyze and interpret the views of a group of people from a target population is questionnaire. The usual questions found in questionnaires are closed-ended questions, which are followed by response options. These close-end questionnaires can be 1) about subjective characteristics of target user (e.g. Technology adaption, Privacy and security perception, etc.) or 2) specifically about SHiELD platform (e.g. User Experience, User engagement, Privacy and Security, etc.).

**3.2.5 Recruitment, Document preparations and evaluation methodologies**

For every group of actors (“end-users” and “Experts”) users with the specific characteristic suitable to the scope of the SHiELD project and to every use case to test, will be selected. The recruitment and the definition of how many users to involve in each group of validation, have to be planned and done before starting the validation period specified.
All the documentations of the validation (e.g. questionnaires, data collection and analysis tools) have to be prepared before the testing phase.
4 Preparatory steps for use cases implementation

4.1 Shield working scenario proposal: openNCP installations

OpenNCP is a suite of epSOS [http://www.epSOS.eu/] NCP (National Contact Point) software publicly available under Open Source licensing (partly GPL v. 3 and partly ASL v. 2). The software acts as a bidirectional technical, organisational and legal interface between the existing national infrastructures and also acts as a mediator as far as the legal and regulatory aspects are concerned.

As described at the proposal the OpenNCP community [https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCPCommunityHome] has designed and developed a set of Open Source Components based on the services developed in epSOS that can be used by Participating Nations to build their local implementation of an NCP. Some of the countries involved in SHiELD use cases have previously piloted some of the services using OpenNCP implementations such as the patient summaries access (Spain and Italy) and electronic prescription (Spain). SHiELD plans to collaborate with the OpenNCP community, using its software and extending components such as the Security Manager, the Policy Manager and the Consent Manager Components in order to support new (and evolving) security requirements and legislations. FCSR will use OpenNCP software in SHiELD to provide an epSOS compliant data exchange gateway. Additionally, the OpenNCP community will be a target for dissemination and exploitation.

OpenNCP technology will be deployed and used within its standard design and operational parameters so that SHiELD will be free to move rapidly forward with its ground-breaking work and not become bogged-down with interoperability questions that have already been answered. At the same time, by re-using epSOS approach and methodology, SHiELD will prove the ability of eHealth to diffuse across the entire EEA, engaging previously reluctant states’ health systems by closing information security and privacy assurance and compliance gaps. SHiELD plans to improve the Security Manager, the Policy Manager and Consent Manager components defined by epSOS and already implemented by OpenNCP community including mechanism to improve the data security and privacy at design time and monitor to ensure is remains security and act in case of a break. SHiELD will also take into account the patient consent process and requirements are followed on different situations and the privacy of patient’s data and access to only the designated people.

SHiELD will improve the already mentioned OpenNCP components and will implement a few new ones as need. Different tools for different partners will be integrated and the complete installation manual will be developed at the end of the project. However, the SHiELD OpenNCP installation will be similar to the current OpenNCP installation (see chapter 7 “Annex 2” for installation description).
In chapter 7 “Annex 2” you will find the installations instructions for the current OpenNCP version and the particularities that SHIELD will introduce for the scenarios.

### 4.1.1 SHIELD OpenNCP installations for the scenarios

For the different scenarios SHIELD will manage three different interconnect virtual machines. Each virtual machine will simulate a national installation of SHIELD OpenNCP and will be connected to each local country system.

![SHIELD OpenNCP extension interconnected](image)

### 4.1.2 OpenNCP base scenario and SHIELD scenarios base requirement

After analyzing what OpenNCP is actually offering, we’ve made up an idea of what is missing for the use cases in the OpenNCP implementation. OpenNCP implementation provides a web portal interface to access to the patient data from one country (NCP-A) to another (NCP-B). The web portal will enable the doctor or physician to access the cross-borders patient information.

![OpenNCP web portal login](image)
After user authentication, the doctor would be able to search the patient using the corresponding fields. First, it is necessary to identify the nationality of the user/code system. In OpenNCP current implementation it includes: Austria, Switzerland, Czech Republic, Denmark, Spain, European Commission, Finland, France, Croatia, IHE, Italy, Malta, Portugal, Sweden and Slovenia. Notice that UK was not preconfigured in the first versions.

In SHIELD project, the use cases would be implemented among Spain, Italy and UK.

![OpenNCP web portal patient search](image)

Figure 8. OpenNCP web portal patient search.

From the country dropbox, it is possible to lookup for patients using some basic fields depending on the country selection.

Most of the fields currently implemented in OpenNCP are identification fields, and some of them also consider including name, surname or another codes.

<table>
<thead>
<tr>
<th>Country</th>
<th>[ SHIELD USE CASE ]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spain</strong></td>
<td></td>
</tr>
<tr>
<td>Patient Identifier Code (CIP)</td>
<td>1234</td>
</tr>
<tr>
<td>Regional Service Id (CITE)</td>
<td>5678</td>
</tr>
<tr>
<td><strong>ITALY</strong></td>
<td>[ SHIELD USE CASE ]</td>
</tr>
<tr>
<td>Fiscal Code</td>
<td>1234</td>
</tr>
<tr>
<td>patient.search.serial</td>
<td>5678</td>
</tr>
</tbody>
</table>

No UK configuration yet!

---

Project Title: SHIELD
Contract No. GA 727301

[http://www.project-shield.eu/](http://www.project-shield.eu/)
Each country has a different set of fields to lookup for patients in their respective health care systems. E.g. the fields preconfigured for Spain are the following:

<table>
<thead>
<tr>
<th>Spain</th>
<th>[ SHIELD USE CASE ]</th>
<th>HL7 v3 OID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Identifier Code (CIP)</td>
<td>351484</td>
<td>2.16.724.41</td>
<td>CIP CA (TIS) / CIC</td>
</tr>
<tr>
<td>Regional Service Id (CITE)</td>
<td>803402</td>
<td>2.16.724.42</td>
<td>Osakidetza</td>
</tr>
</tbody>
</table>

However, for SHIELD use cases this is scanty information to identify a patient properly. In a real situation it is probably that the patient could not have their wallet or their identification number and we have only to identify by name, age, phone, or even by the drive license number or so. Moreover, babies may not have CIP. And in a real situation there could exists more than one CIP or duplicated CIPs for the same person. Osakidetza provides an interface to lookup for other fields like:

<table>
<thead>
<tr>
<th>Spain</th>
<th>[ SHIELD USE CASE ]</th>
<th>HL7 v3 OID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Identifier Code (CIP)</td>
<td>351484</td>
<td>2.16.724.41</td>
<td>CIP CA (TIS) / CIC</td>
</tr>
<tr>
<td>Regional Service Id (CITE)</td>
<td>803402</td>
<td>2.16.724.42</td>
<td>Osakidetza (old OID)</td>
</tr>
<tr>
<td>Spanish ID (DNI)</td>
<td>351484</td>
<td>1.3.6.1.4.1.19126.3</td>
<td>Osakidetza (new OID)</td>
</tr>
<tr>
<td>Residence Card (T. Residencia)</td>
<td>A</td>
<td>2.16.840.1.113883.2.19.10.6</td>
<td></td>
</tr>
<tr>
<td>Passport (Pasaporte)</td>
<td>B</td>
<td>2.16.840.1.113883.2.19.10.5</td>
<td></td>
</tr>
<tr>
<td>Social Security Number (NASS)(SNS)</td>
<td>480053465954</td>
<td>1.3.6.1.4.1.19126.4</td>
<td></td>
</tr>
<tr>
<td>Nº Historia Clinica (CIC)</td>
<td>1769908</td>
<td>2.16.724.40</td>
<td>(epSOS document oid)</td>
</tr>
<tr>
<td>Nombre</td>
<td>A</td>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Primer Apellido</td>
<td>B</td>
<td>Surname (1)</td>
<td></td>
</tr>
<tr>
<td>Segundo Apellido</td>
<td>C</td>
<td>Surname (2)</td>
<td></td>
</tr>
<tr>
<td>Fecha Nacimiento</td>
<td>13/02/1943</td>
<td>Birthdate</td>
<td></td>
</tr>
<tr>
<td>Telefono</td>
<td>946018927</td>
<td>Telefone number</td>
<td></td>
</tr>
<tr>
<td>Sexo</td>
<td>M</td>
<td>Gender</td>
<td></td>
</tr>
</tbody>
</table>

Project Title: SHIELD 727301
The identification by traits will consist on filtering for one or many search fields to try to find the patient in the national health database. The identification of the patient is the first step to find their patient summary.

OpenNCP will gather through the different layers to reach the patient information. The following example is a representation of the connectivity in OpenNCP. On a first iteration, OpenNCP will validate the call to the client-connector WebService, which will connect to the proper NCP endpoint to the destination country (<COUNTRY>.PatientIdentificationService.WSE). Each country will have a customized implementation at the protocol terminator (openncp-ws-server and nc-implementation).

In this container (a jar that implements a ServiceLoader), the methods that will interact with HCP are implemented. The HCP will implement the incoming call (XML request message) and will produce also a XML output. These XML are encapsulated in typed java objects (e.g. PatientSummary, epSOSDocument, and so on).
Figure 10. Request to Patient Demographics.

Figure 11. Response to Patient Demographics.
4.2 Synthetic data sets

In all the three use cases there would be the possibility of accessing the Patient Summary Electronic Clinical Record. This record will contain based on epSOS project the basic and mandatory medical data, that includes the most important clinical facts required to ensure a secure healthcare management of the acute episode at a foreign European country. This summary will include the essential clinical information to give the health professionals the information they need to provide care in an unexpected or unscheduled medical situation (e.g. emergency, accident, a chronic condition exacerbation or decompensation, an acute clinical problem complication ...).

The mandatory dataset is a subgroup clinical data that should have a valid value. In the “openNCP platform” we will consider as mandatory dataset the next data:

- Patient identification: National Health Care patient ID
- Personal information: date of birth and gender
- Alerts: allergies and intolerances
- History of past illness: vaccinations, resolved, closed or inactive problems and surgical procedures
- Medical problems: list of current problems/diagnosis
- Medication summary: list of current medicines
- Nursing care programs

Beside these data in each use case it should be desirable to extend the health information from the clinical point of view.

Example of Patient Summary Electronic Clinical Record in Osakidetza (PDF document, unstructured data):
4.2.1 Use case 1: Break glass circumstance

A 65 years old male from Italy suffers from an ischemic stroke during city cruise in Bilbao. He is accompanied by his wife, who reports about hypertension and heart disease with valve replacement about 10 years ago. Treatment with anticoagulant agent is reported by her, though her husband apparently has omitted the last laboratory controls.

Other details regarding his health condition in the anamnesis contains some risk indicators such as:

- smoker
- poor exercise
- stroke in family
- overweight
- hypertension

When the Spanish medical doctor retrieves past medical information in patient’s EHR he is able to achieve:

- **blood tests** in order to check his PT whose INR should be in an interval between 1.5 and 4 to be “normal”, in this case the file contains structured data. In the presented use case, the patient’s INR is out of range and that’s the reason of the blood clotting. On the other side, the values related to renal function are in the physiological range and that means to the Spanish doctor that the patient does not suffer of renal failure and that he can be submitted to a further TC scan involving liquid dye without dangerous consequences.
- medical images to check mechanical valve position and status, the images are in a DICOM format. Hereafter there is an example of a single scan of a simulated patient with all the sensitive information highlighted.
- **dismissal letter** of past hospitalization.
- report of complementary tests as an echocardiogram
  The system (Osabide Global) create the echocardiogram as a PDF document (unstructured data) that is composed by the following parts:
electrocardiogram the patient on arrival at the emergency room has Atrial Fibrillation (AF), which is not included in the patient’s summary and which his wife does not know beforehand. A previous electrocardiogram is required to verify that the patient was previously in sinus rhythm and that AF is of a recent beginning.

The system (Osabide Global) create electrocardiogram as another PDF document (unstructured data) that is composed by the following parts:

**Report summary**

- Description of heart valves
- Description of mitral valve
- Description of tricuspid valve
- Description of aortic valve
- Description of pulmonary valve
- Measurements and calculations, Doppler
After achieving all the past information of the patient the medical staff in charge for stroke assistance decide to proceed with a TC scan to verify the entity of the stroke and to ensure the best therapy. This can be done with major accuracy using contrast liquid because the patient does not have kidney issues. Moreover, other blood tests are prescribed to verify the current status of blood coagulation and to check if there are other analytical alterations related to the process, such as: data suggestive of inflammation/infection, ionic decompensation, altered glycemia, anaemia...
4.2.2 Use case 2: Surgical intervention

As we have described before, the doctor access not only to Patient Summary but also to the complementary information carried out in the urologic intervention (detailed below). This complementary information has been agreed with his urologist and general practitioner, before traveling to Italy.

1. First of all, it will appear the “Discharge Report” in detail, as a PDF document (unstructured data):
2. Secondly, it will appear the “Preanesthesia” document, also in PDF format.

3. Thirdly, “Surgical Procedures” PDF document will be relevant in this case.
4. After the Surgical Procedures will follow the “Care Plan” document, also in PDF format.
5. After that, the main **clinical lab test** is also important. They are also unstructured data (PDF documents). Then, examples of different kinds of analytics.

All the analytics have the same structure, on the top the head report and then, the results.
5.1 Microbiology test (urine culture)

5.2 Blood test
5.2 Blood test

![Blood test results]

5.3 Urine test

![Urine test results]

6. Then, **Computerized Tomography (CT)** report appears in PDF format (unstructured data). Apart from that, we can also see a CT examples in detail through images in JPEG format (unstructured data).

All the radiological images reports have the same structure, on the top the head report and then, the information of the image results.
6.1 CT image 1

6.2 CT image 2
Finally, we have to keep in mind the **Intravenous urography** report in PDF. Also we can see an example of an Intravenous urography example in detail. The report of the performance of the intravenous urography is the same as the one in point 6. But the image in this case doesn’t have any data to be hid.

Intravenous urography image (JPEG format, unstructured data).

This image does not contain any information about the patient or the image performance.
After achieving all the agreed information of the patient the medical staff in charge of the acute clinical process of the patient, which could be a complication of his recent urological intervention, will have an improve possibility of managing the patient, thanks to the information shared through the SHiELD platform (openNCP). They will be able to have all the information related to the surgical intervention, with all the details: admission data, analytics, imaging tests, anaesthesia and surgical part and etc.
4.2.3 Use case 3: Chronic conditions + Remote monitoring

A) Spain

1. **Patient Summary Electronic Clinical Record** in Osakidetza (PDF document, unstructured data).

![Image of clinical record]

2. **Outpatient evolution reports** of the endocrine (PDF document, unstructured data).
3. Data collected in "My health folder" in "My diary" section.
4. The last **blood test** is also important in order to see parameters related with the DM control. They are also unstructured data (PDF documents).
5. The last **fundus** is also important in order to see if the patient has a DM with complications, such as retinopathy. They are also unstructured data (PDF documents).
B) **Italy**

1. “**Discharge Report**” in detail of the brain tumour intervention performed years ago, as a PDF document (unstructured data). The PDF document has the same sections as the discharge report described in chapter 3.4.2.2.

2. Other important documents:
   a. “**Tumour pathology report**” in order to see the possibility of malignancy or benignity. They are also unstructured data (PDF documents).
b. **“Surgical Procedures”** of the brain tumour intervention PDF document (unstructured data)

3. **Outpatient evolution reports** of the neurosurgeon (PDF document, unstructured data).

4. **Magnetic resonance imaging (MRI)** report appears in PDF format (unstructured data). Apart from that, we can also see a MRI examples in detail through images in JPEG format (unstructured data). The first image is before the surgery and the second one, the last MRI performed during the evolution of the illness. The PDF document has the same sections as the discharge report described in chapter 3.4.2.2.

After achieving all the health information of the patient the medical staff in charge of the acute clinical process of the patient, will have global information of the patient, related to its current acute clinical process, which will allow to perform a clinical management with greater efficiency and safety. They will be able to have all the information related not only to her current medical processes, as well as her chronic medication, but also, of an episode that could
be in resolution or be one of the causes of her current process. It is therefore important to be able to access past episodes that may be closed.
5 Conclusions

In this deliverable we have described three use cases to be exploited to assess the maturity and the effectiveness of the prototypes developed in the project.

The use cases represent real-life strength scenarios and they have been identified choosing different Citizen / Patient typologies, healthcare needs and the level of healthcare services to be provided.

The use cases differ in terms of Citizen / Patient health problems, data exchange permissions and dimensions, Privacy and Security issues and European jurisdictions; moreover, the three use cases have three different Stakeholder maps where the citizen / patient is always the core actor and the other actors are selected based on the use case storyboard.

Furthermore, in this deliverable we have described a Validation Methodology that includes specifications about verification of the technological solutions with the related metrics and specifications about validation with end-users and experts.

The last part of the deliverable includes details about the preparatory steps for use cases implementation, meaning the openNCP installations, and details about synthetic data sets to be used.

The next steps will regard, from one side the use cases implementation using synthetic data sets and on the other side to start the validation phase with the defined actors and the related SHiELD functionalities.
6 Annex 1 – Requirements definition and classification

Definition:

Requirements engineering
The process of establishing the services (performances) that the customer requires from a system and the constraints by defining, documenting and maintaining requirements document.

Requirement
It is the descriptions of the system services (performance) and constraints that are generated during the requirements engineering process.
In principle, the requirement describes what the system should do and how it does.
A requirement may range from a high-level abstract statement of performance / functionality or constraint to a detailed mathematical functional specification.

Requirements Classification I
Requirements are basically divided into two categories:

- Functional Requirements
- Non-Functional Requirements

Functional Requirement is a statement that describes the functionality performed, specifying how the system should react to particular inputs and how the system should behave in particular situations. It may be high-level but should describe the system details.

Non-Functional Requirements is a statement that describe a quality, property or constraint of the function described by the Functional Requirement. For instance: timing, speed, reliability, response time, storage capability, etc. A non-functional requirement can be also a specific programming language or development method.

Requirements Classification II
Another distinction that must be applied is related to the subject that requires the requirement, according this there are other four categories:
(each one of them can be functional or non-functional)

- Business Requirement
- User Requirement
- System Requirement
- Transitional Requirement

---

**Business requirement**, describes why the organization is undertaking the project and the high-level goals and objectives of the system (service/product).

According the hierarchy, business requirements come first, it serves as mandatory reference because all the further requirements must be compliance and consistency with the business ones.

**User Requirement**, refers to a statement in natural language (written for users), plus diagrams of the service (use cases, journey map, storyboard scenario), often referred to as user needs, describe what the user does with the system, such as what activities that users must be able to perform.

**System Requirement**, it states what the system shall do, like a functionality needed by the user to perform his task.

**Transitional Requirement**, describes the capabilities that a solution must have and the conditions needed to facilitate the transition from the current state to the future, but which are not needed once the system is fully functioning.
7  Annex 2 – OpenNCP Installation details

7.1 OpenNCP Common installation

The live page with the OpenNCP installation manual can be found here [https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Installation] and it is π detailed bellow.

Differente OpenNCP commponents
[https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Components] are deployed during the installation:

- Assertion Validator Home
- Audit Manager Home
- Authentication & Authorization Home
  - Policy Manager
- Automatic Data Collector
  - OpenNCP Integration
  - Setup eADC in OpenNCP
- CDA Display Tool Home
  - Using CDA Display Tool
  - Using TSAM Exporter
- Configuration Manager Home
- Consent Manager Home
- Data Model
- Datamodel Home
- eiD (for Patient identification, powered by e-SENS)
  - Smartcard-based eiD integration into OpenNCP
- Epsos-Web Home
  - Get Started
- Evidence Emitter (for ron-repudiation, powered by e-SENS)
- Gnomon Portal B Home
- GUI
  - 1.0
    - Configuring portal
    - Error Handling messages
    - Error messages handling
    - Installing epsos portlets
    - Installing OpenNCP Portal
    - PAC: Define custom fields for user
    - System configuration
    - TSAM Exporter
- NCP-PT Home
- OpenATNA Home
- OpenNCP Central Configuration
  - Configuration Manager
  - OpenNCP and central services PKI
- OpenSTORK Home
  - Component Specification
  - Development Issues
  - Meeting Notes
  - Releases
  - STORK in epSOS
These components not only include the OpenNCP core but some portals to test the different OpenNCP functionalities too. SHIELD will integrate the different tools and services using the defined portals. Additionally, to this installation each country / scenario will need to develop and install at national level those components and services to access the local national systems and data (not covered at the current installation instructions).

7.2 OpenNCP additional references

The OpenNCP community provides additional documentation and references that could be important to take into account before installing OpenNP. The most important references are the following ones.


In this document, the eHealth DSI architecture is partitioned into the three classical viewpoints: Business View, Information System View and Technology View. This approach, inter alia, supports a sufficient level of abstraction useful to architect a system of heterogeneous healthcare national infrastructure. Furthermore this level of heterogeneity makes eHealth DSI a typical field for a Service Oriented Architecture (SOA)
style. In this context the architecture must be abstracted from the complexity-characteristic-platform of underlying systems (loose coupling principle). The specific technical implementation of a service should be hidden for the consumer. The components of an eHealth DSI National Contact Point (NCP) can be viewed like a logical “wrapper” of the different National Infrastructures.

This document covers the most technical part (technology view), giving guidelines for an implementation of an eHealth DSI NCP. It is meant to embrace those works in the most comprehensive manner without repeating those results unnecessarily.

- OpenNCP NCPeH Architecture Specification [ NCPeH Architecture Specification ]

This document defines the architectural view on the “NCP-In-A-Transparent-Box”, describing the functionalities which are common and the “common components” implementing these functionalities. It documents which functionality can be developed in common and which “common components” will be specified.

- OpenNCP NCPeH Components Specification [ NCPeH Components Specification ]

This document covers the technical specifications of the eHealth DSI common components that have to be put in place by eHealth DSI countries in order to allow for a secure and privacy-aware exchange of identifiable medical data. The document is presented as a consolidated specification of the already implemented eHealth DSI solution. It furthermore serves as the foundation of the eHealth DSI services technical specification, which is aimed at reusing as much of the work already done and to preserve much of the backwards compatibility between both initiatives.

7.2.1 SHIELD OpenNCP

As commented SHIELD OpenNCP packages and final installation manual will detail further instructions needed to install and integrate SHIELD’s tools and services, but the current OpenNCP installation manual illustrates a common installation and the different steos.

7.2.1.1 OpenNCP Installation overview

OpenNCP Community maintains up-to-date instructions of the installation overview here [https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Installation]. At this section we replicate the current overview.

Some OpenNCP software components are licensed under the GPL v. 3 license, and some under the ASL v.2 license. Developers of software components are given the responsibility to check that no other licensing rights pertain to any elements embedded or related to a newly developed component, particularly but not limited to libraries.

For connecting the OpenNCP implementation to a participating nation’s national infrastructure, a separate national connector must be implemented by the NCP operator. The connector is not supplied as part of OpenNCP, because the implementations and functionalities of the national infrastructures differ among the participating nations.
epSOS participating nations and other enquirers are responsible in co-operation with the OpenNCP community, to ensure that the licenses of all open source components used in the project are compatible with the purpose and scope of the project.

- System Requirements
- Typical Hardware Requirements
  - 2 GHz Xeon Processor or equivalent
  - 20 GB Storage
  - 4 GB Memory
- Suggested Software Requirements
  - Linux or Microsoft Windows Operating System
  - Oracle Java SE Development Kit 7 jdk7u21 or earlier (refer to page comments)
  - Apache Tomcat 6.0.x or 7.0.x
  - Relational Database (tested with MySQL, Postgres, Oracle)
  - Openswan 2.6.x for IPsec (needed in epSOS, but not part of OpenNCP as such)
- Keystore storage recommendation
  It’s highly recommended to have each private key in a separate keystore file (one for signature key, one for service provided and one for vpn key)

Overview of components

OpenNCP consists of the following components all of which are available for download at JoinUp.

- Protocol Terminators
  The core of OpenNCP is the Protocol Terminators and consists of these two components:
  - epsos-ws-server - Server Side (Country A)
  - epsos-client-connector - Client Side (Country B)
  These components are packaged as web applications and are deployed to a servlet container such as Tomcat.

- TRC-STS
  This component is a "Security Token Service" (STS) for issuing “Treatment Relationship Confirmation” (TRC) Assertions. It is another web application that is deployed to Tomcat. TRC-STS is used by an epSOS portal (e.g. OpenNCP portal or epsos-web), which must include the TRC-STS client for retrieving the TRC assertions from the security token service.

- TSL-sync
TSL-sync connects to Central Services and downloads the Trusted Service Lists (TSL) with NCP endpoint addresses and certificates of the other Participating Nations. It is a web application deployed to Tomcat. TSL-sync may be configured to run for example every night.

- **TSAM-sync**

The Terminology Service Access Manager (TSAM) Synchronizer is another OpenNCP component. It is a standalone jar file with configuration files and a start script. This application may be scheduled to run for example on a daily basis and will download terminology data from the Central Services repository into the local database (LTR - Local Terminology Repository).

- **OpenATNA**

OpenATNA is an implementation of the Audit Trail and Node Authentication (ATNA) profile. It is a web application and is deployed to Tomcat. The application has two main functionalities: (1) receiving the audits from NCP components and storing them into the audit repository and (2) getting access to the stored audits using a web interface.

- **Database**

A local database is required for storing the following information:

- ATNA audit messages
- epSOS Automatic Data Collection (eADC) records
- TSAM data, i.e. code and value sets, code mappings etc.
- Configuration settings for the OpenNCP server, client and portal

The configuration settings also include the endpoint addresses of the other NCPs, received in the form of TSLs from the central services.

- **Portals**

There is a choice of two web portals:

- OpenNCP Portal (deployed on Liferay Community Server)
- epSOS-Web (deployed on Tomcat)

- **IPsec**

Communication between NCPs is secured using HTTPS over IPsec. IPsec is not part of the OpenNCP software, but it is needed for establishing VPN connections between epSOS NCPs. Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet. A common implementation of IPsec for Linux is Openswan. It must be installed on the NCP machine.

- **More information**

For further information refer to the [OpenNCP Installation Manual](http://www.project-shield.eu/). It describes the installation of the OpenNCP software in more detail and provides sample configuration files along with tips and tricks for successful deployment of the NCP.
• Support

The OpenNCP Community provides support and other benefits, including:
• Ongoing technical support.
• Release upgrades at no additional cost.
• Support requests may be sent in a number of ways:
  • Technical requests should be sent by electronic mail to jira@openncp.atlassian.net
  • General requests can be sent using the online support form http://www.epsos.eu/home/about-epsos/contact.htm

7.2.1.2 OpenNCP Installation manual

OpenNCP Community maintains up-to-date installation manual here [https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Installation+Manual]. At this section we replicate the current manual.

0. Recommendations

Before proceeding with the installation of OpenNCP please refer to OpenNCP Installation Overview page for the basic information about OpenNCP installation and architecture.

This installation manual was based on an installation with the following software:
• Java 1.8.0 (Current version is 1.8.0_131 or newer).
• GNU/Linux x86_64
• MySQL 5.6.25
• Apache Tomcat 8.5.15
• Liferay 6.2.5 CE GA6
• 1. Setup application server

We strongly recommend using the version 1.8.0_131 of the JDK 8 (or newer, also tested with 1.8.0_144).
The software components are able to run on all Java application servers, but we recommend you to install them at an Apache Tomcat instance.
You can download it at http://tomcat.apache.org/ and you should use Tomcat version 8.5.
To perform the installation and fine tuning of the server you may also follow this instructions: Apache Tomcat official documentation.
Don’t forget to give execution permission to the files in the bin folder. Also, add the JDBC connector (JAR file) of your database to your Tomcat’s lib folder as the drivers are marked as provided by the container into the Maven pom files of the components.
You must check if you have some other service running in Tomcat’s default ports (defined in its `conf/server.xml` file) and change them if you do.

- **1.1 JNDI Datasources**

You need to define JNDI DataSources to the Apache Tomcat configuration. The OpenNCP default installation is using MySQL as a database and HikariCP as a connection pool. The infrastructure manager is the responsible for the server configuration, and please take in consideration the maximum number of connections available on your database server if you are using connection pools.

There are different ways to define JNDI Datasources with Tomcat. OpenNCP team has decided to share the pools between the web application deployed.

- `/opt/apache-tomcat-server/conf/server.xml`:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
  <!-- Security listener. Documentation at /docs/config/listeners.html -->
  <Listener className="org.apache.catalina.security.SecurityListener" />
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <!-- Prevent memory leaks due to use of particular java/javax APIs--> 
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
  <!-- Global JNDI resources Documentation at /docs/jndi-resources-howto.html -->
  <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" />
    <!-- Define hereafter your OpenNCP Connection Pools: jdbc/ConfMgr, jdbc/TSAM, jdbc/EADC_XCPD -->
    <Resource name="jdbc/ConfMgr" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_properties" dataSource.password="openncp_pwd"/>
    <Resource name="jdbc/OPEN_ATNA" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_atna" dataSource.password="openncp_pwd"/>
    <Resource name="jdbc/TSAM" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource">
```

http://www.project-shield.eu/
<Resource name="jdbc/EADC_XCPD" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_ltrdb" dataSource.password="openncp_pwd"/>

<Resource name="jdbc/EADC_XDR" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_eadc" dataSource.password="openncp_pwd"/>

<Resource name="jdbc/EADC_XCA" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_eadc" dataSource.password="openncp_pwd"/>

<Resource name="jdbc/LOGS" auth="Container" factory="com.zaxxer.hikari.HikariJNDIFactory" type="javax.sql.DataSource" minimumIdle="2" maximumPoolSize="5" connectionTimeout="300000" dataSourceClassName="com.mysql.jdbc.jdbc2.optional.MysqlDataSource" dataSource.serverName="127.0.0.1" dataSource.port="3306" dataSource.databaseName="ehealth_logs" dataSource.password="openncp_pwd"/>

</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share a single "Container" Note: A "Service" is not itself a "Container", so you may not define subcomponents such as "Valves" at this level. Documentation at /docs/config/service.html -->

<Context>
  <!-- Default set of monitored resources. If one of these changes, the web application will be reloaded. -->
  <WatchedResource>WEB-INF/web.xml</WatchedResource>
  <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
</Context>
<ResourceLink global="jdbc/ConfMgr" name="jdbc/ConfMgr" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/TSAM" name="jdbc/TSAM" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/OPEN_ATNA" name="jdbc/OPEN_ATNA" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/EADC_XCPD" name="jdbc/EADC_XCPD" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/EADC_XCA" name="jdbc/EADC_XCA" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/EADC_XDR" name="jdbc/EADC_XDR" type="javax.sql.DataSource"/>
<ResourceLink global="jdbc/LOGS" name="jdbc/LOGS" type="javax.sql.DataSource"/>
</Context>

This is done in the conf/context.xml file. Here is an example file for Tomcat 6.0: context.xml. Just add the definition of the JNDI data sources and change the connection string depending on the DBMS you're using (for MySQL there's no need to change). We'll configure each one of them as we progress through the installation (keep them commented and uncomment when you configure).

For more background information and configuration tips on the JNDI please refer to this JIRA: EHNCP-27 - Database connection leaks throughout the code CLOSED

1.2 External dependencies

For scalability purpose between Apache Tomcat and MySQL, some Java dependencies have to be added to the external lib directory instead of embedded to the WAR archive. At least the two following dependencies must be added to your Apache Tomcat instance: /opt/apache-tomcat-server/lib/

- MySQL JDBC drivers: Depending of your database, you might choose your JDBC drivers version, default installation is using version 5.1.43 available from Maven repository or https://dev.mysql.com/downloads/connector/j/

    <dependency>
        <groupId>mysql</groupId>
        <artifactId>mysql-connector-java</artifactId>
        <version>5.1.43</version>
    </dependency>

- HikariCP: Default installation has been tested with HikariCP and the JAR might be download from Maven repository or https://brettwooldridge.github.io/HikariCP/

    <dependency>
        <groupId>com.zaxxer</groupId>
        <artifactId>HikariCP</artifactId>
        <version>2.6.3</version>
    </dependency>

Slf4j-api is required by HikariCP to work properly.

    <dependency>
        <groupId>org.slf4j</groupId>
        <artifactId>slf4j-api</artifactId>
        <version>1.7.25</version>
    </dependency>
2. Adjust configuration parameters

First, you'll need to have a folder named "openncp-configuration" that will hold your configuration files (you can take a quick look at the last step of the guide to see a recommended folder structure for the NCP). The folder is provided hereafter as a zipped file:

**File**

ZIP Archive openncp-configuration.zip

Folder content:
- /openncp-configuration
  - /ATNA_resources
  - /audit-backup
  - /EADC_resources
  - /forms
  - /TM_resources
  - configmanager.cfg.xml (this configuration file has been renamed)
  - hcer.properties
  - pn-oid.xml
  - tm.properties
  - tsam.properties

All the provided files will be used and configured in this manual.

At this step you need to add entries to your country at **pn-oid.xml**.

OIDs were defined within epSOS-I. It seems that the root used (2.16.17) is not officially assigned. Was it defined by IHE Services? Then we simply incremented the 8xx number for each country (2.16.17.710.8xx.1000.990.1). At the end, at least for **PRODUCTION** files folder. You can do this by executing the following command in the terminal window:

```
export EPSOS_PROPS_PATH=/opt/openncp-configuration/
```

For more information about environment variables, you can check: [https://help.ubuntu.com/community/EnvironmentVariables](https://help.ubuntu.com/community/EnvironmentVariables) for Ubuntu, but that can be applicable to other distros.

### 2.1 Configuration Manager Database

The bulk of NCP configuration properties (i.e. countries endpoints, truststore locations, and others) is stored in the Configuration Manager database. The "Setup" section of Configuration Manager explains how to create a database and a hibernate configuration file.

(If you already have an existent setup with the old configuration files - epsos.properties and others - you can also follow the "How To Migrate" section. If you are doing a fresh install please ignore this line.)

**Table openncp-property**

The openncp-property table structure has been updated as followed:

- name', 'varchar(255)', 'NO', 'PRI', NULL, ''
- value', 'varchar(255)', 'YES', '', NULL, ''
2.2 Creation of certificates and configuring Tomcat

You can find more details on how to create epSOS certificates [here](http://www.project-shield.eu/).

After that, you need to add a new Connector to your Tomcat's conf/server.xml file, in order to configure SSL connections to use the generated keystores and certificates:

```xml
<Connector port="PORT" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="true" sslProtocol="TLS"
    keyAlias="service.provider.certificate.alias"
    keystoreFile="/path/to/your/service-provider-keystore.jks"
    keystorePass="testKS"
    truststoreFile="/path/to/your/truststore.jks"
    truststorePass="changeit"/>
```

- **port**: should be the port that you want to use for SSL connections. It will be the port where your web services (PatientIdentification, Consent, etc.) will be exposed;
- **keyAlias**: your service provider certificate alias;
- **keystoreFile**: the path to your service provider key store. This means that your Tomcat will act as a service provider;
- **keystorePass**: your service provider keystore password;
- **truststoreFile**: the path to your truststore. This means that your Tomcat will only accept connections from your trusted third-parties;
- **truststorePass**: your truststore password.

If you are using self-signed certificates, you have to set the property `clientAuth` to false into the Tomcat Connector node defined just above in order to bypass the security restriction related to the certificate issuer.

Then, you should restart your Tomcat instance for the changes to take effect.

If incoming SSL (TLS) connections are terminated in your environment at a load balancer (LB), you need to set up your LB to forward client certificate information to OpenNCP. The subject DN of the certificate needs to be placed in an HTTP header by the LB before the request is forwarded to OpenNCP. Set up properties `TLS_TERMINATION_AT_LOAD_BALANCER` and `TLS_CLIENT_CERT_HEADER_NAME` (more information on page OpenNCP properties). In addition, depending on the environment, you might need changes to the Tomcat connector, for example an additional connector without enabled SSL.

2.3 NCP First-Time Configuration Utility

To facilitate the process of setting up your NCP instance, you can use a special utility to populate your database with the basic required parameters, related to your scenario.
To do that you just need to fill a provided unfilled properties file according to your scenario, configure the database connection file and execute the utility JAR. You must have the properties database (with no tables) already created, before using this utility. Find the JAR file in section 3.1 of this manual. You can download the properties and database files here:

<table>
<thead>
<tr>
<th>File ZIP Archive</th>
<th>OpenNCP-configuration-utility.zip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removed deprecated javax.net.ssl.* property (OpenNCP 2.4.0)</td>
<td></td>
</tr>
</tbody>
</table>

Once you have run the utility with success, you may delete both files and the JAR and check if the database was correctly filled, using the appropriate database administration tool. Be aware that this configuration utility will ignore properties with no value set, so these ones should be added manually to your database. Note: properties should not use environment variables like '$EPSOS_PROPS_PATH/...'. Instead, the full path should be used. A full list of the OpenNCP properties can be found here: OpenNCP properties

The following table also provides some important information about the central services (for configurations and terminologies):

<table>
<thead>
<tr>
<th>Service</th>
<th>Mode</th>
<th>URL</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP</td>
<td>PPT</td>
<td>sftp://fts.ec.europa.eu</td>
<td>22</td>
</tr>
<tr>
<td>SFTP</td>
<td>PROD</td>
<td>sftp://fts.ec.europa.eu</td>
<td>22</td>
</tr>
<tr>
<td>TSAM</td>
<td>PPT</td>
<td><a href="https://webgate.training.ec.europa.eu/ehealth-term-server">https://webgate.training.ec.europa.eu/ehealth-term-server</a></td>
<td></td>
</tr>
<tr>
<td>TSAM</td>
<td>PROD</td>
<td><a href="https://webgate.ec.europa.eu/ehealth-term-server">https://webgate.ec.europa.eu/ehealth-term-server</a></td>
<td></td>
</tr>
<tr>
<td>TSL</td>
<td>PPT</td>
<td><a href="https://webgate.acceptance.ec.europa.eu/ehealth/tsl/">https://webgate.acceptance.ec.europa.eu/ehealth/tsl/</a></td>
<td>None</td>
</tr>
<tr>
<td>TSL</td>
<td>PROD</td>
<td><a href="https://webgate.ec.europa.eu/ehealth/tsl/">https://webgate.ec.europa.eu/ehealth/tsl/</a></td>
<td>None</td>
</tr>
</tbody>
</table>

- 3. Install and setup components

- 3.1 OpenNCP artifacts

**OpenNCP version**
The OpenNCP current version is the **2.5.2.RC1**

In order to install OpenNCP, you must obtain the following artifacts (please use the latest versions for each component):
• **OpenNCP main components:**

  • Server Side - NCP-A

  • Client Side - NCP-B

  • OpenATNA

  • TRC-STS

  • OpenNCP Gateway

• **OpenNCP command line tools:**

  • TSL-Sync

  • TSL-Editor

  • TSAM-Sync

  • TSAM-Exporter


• **OpenNCP external tools:**
• Portal (WAR): https://ec.europa.eu/cefdigital/artifact/content/repositories/eHealth/eu.europa/ec/sante/ehdsi/openncp-portal/

• RichClient - eID Level 1 (JAR): https://joinup.ec.europa.eu/nexus/content/repositories/releases/eu/europe/ec/joinup/ecc/org/openecard/richclient/

3.2 TRC-STS

The main purpose of this component is to generate and return security assertions on demand. It is a WAR application that will run also on your Application Server instance. In order to install it, you will need to obtain the artifact, named openncp-trc-sts-X.X.X.war, then it is advised to rename it to just TRC-STS.war (so the database property of the exposed service remains the same between different versions of TRC-STS). Before the deploy, configure the jdbc/ConfMgr data source in your Tomcat conf/context.xml to connect to your OpenNCP properties database. Next you can just deploy it in your Application Server instance. You can follow these instructions for Tomcat 8.5.

This will deploy the Secure Token Service at http://<hostname>:<port>/TRC-STS/STSServiceService, where <hostname> and <port> are the hostname or IP address of the machine Tomcat is running and the port Tomcat is using (you can check it in Tomcat's conf/server.xml file).

After that, you can add/update the property "secman.sts.url" at your NCP properties database with the aforementioned URL.

3.3 Service Metadata Provider and Locator (SMP/SML)

OpenNCP

3.3.1 SMP Files

The configuration of your NCP-A should contain at least the following files:

- International Search Mask
  (urn:ehealth:ISM::InternationalSearchMask##ehealth-107)

Your International Search Mask should respect the following format with the mandatory namespace xmlns="http://ec.europa.eu/sante/ehncp/ism".

```xml
<?xml version="1.0" encoding="UTF-8"?>
<patientSearch xmlns="http://ec.europa.eu/sante/ehncp/ism">
  <country code="EU">
    <searchFields>
      <id domain="2.16.17.710.850.1000.990.1" label="ID Card Number" max="-1" min="-1"></id>
      <textField dtoIndex="1" friendlyName="surname" label="patient.data.surname" max="-1" min="3"></textField>
    </searchFields>
  </country>
</patientSearch>
```

- XCPD

3.3.2 SMP Editor
3.4 TSAM-Sync

The TSAM-Sync component is a standalone component able to retrieve the Terminologies from the eHealth Central Terminology Server according the credentials provided. The process will connect to the repository and load your terminologies into your Local Terminology Repository database.

This application is a standalone JAR that can be placed in custom location which only requires a configuration file detailed hereafter.

```
/opt
|-- ...
| -- openncp-tsam-sync
 | |-- application.yml
 | +-- openncp-tsam-sync-x.x.x.jar
 +-- ...
```

Before running the TSAM-Sync process, you should validate with your National Terminology responsible that all actions required into the central eHealth Terminology Portal have been achieved and validated (MVC published, Translations and/or Mappings uploaded and MTC nationally validated otherwise no data will be available for the synchronization).

If you need more details related to the eHealth Terminology Services, you could access the Terminology Server user guide.

eHealth Terminology Services

Please, take in consideration the following information related to the eHealth Central Terminology Services:

- **Production:**
  - Server: https://webgate.ec.europa.eu/ehealth-term-server

- **Pre-Production:**
  - Server: https://webgate.training.ec.europa.eu/ehealth-term-server

eHealth DSI Terminology Server documentation: https://ec.europa.eu/cefdigital/wiki/x/yQLQAg

You should configure the application.yml file as follows, providing your country specific configurations:

```
application.yml
  debug: false
ehealth:
  termserver:
    username: tsam_user
    password: password
logging:
```

Project Title: SHIELD

Contract No. GA 727301

http://www.project-shield.eu/
level:
  org.hibernate: ERROR
  org.springframework.web.client: DEBUG

openncp:
  ltrdb:
    host: 127.0.0.1
    port: 3306
    username: openncp_ltrdb_user
    password: LTRDB_PASSWORD
    database-name: openncp_ltrdb

tsam-sync:
  proxy:
    use: true
    host: my.proxy.host
    port: 9999
    use-authentication: true
    username: proxy_user
    password: proxy_password

spring:
  datasource:
    url: jdbc:mysql://127.0.0.1/openncp_ltrdb
    username: openncp_user
    password: password
    driver-class-name: com.mysql.jdbc.Driver
  profiles:
    active: mysql

For Oracle installations, use the same configuration for both openncp.ltrdb and spring.datasource and specify the connection using an URL. The following code block highlights the differences:

openncp:
  ltrdb:
    url: jdbc:oracle:thin:@//127.0.0.1:1234/databasename
    username: openncp_user
    password: password
    driver-class-name: oracle.jdbc.OracleDriver

spring:
  datasource:
    url: jdbc:oracle:thin:@//127.0.0.1:1234/databasename
    username: openncp_user
    password: password
    driver-class-name: oracle.jdbc.OracleDriver
  profiles:
    active: oracle

Before the deployment, please do not forget to configure the jdbc/TSAM data source in your Tomcat conf/context.xml and conf/server.xml related to the LTR database (ltrdb) connection.
If you do not have the LTR database already, you can just create the schema manually by using the following SQL script for MySQL: ltrdb-mysql.sql
Then run the JAR. It will create your tables and fill the database with the terminologies.

- **3.5 Transformation Synchronization Access Manager (TSAM)**

In order for the TSAM to work properly, you should setup the tsam.properties file, already provided and located under your EPSOS_PROPS_PATH. You can find an example bellow:

**tsam.properties Configuration File** Expand source
Give special importance to:
Languages
- **translationLanguage**: here you will place your country language;
- **transcodingLanguage**: this property will hold the country A language, defined as "en-GB" in epSOS;

Database Setup (you will need to fill these parameters according to the database you created in step 3.4)
- **ltr.hibernate.dialect**: the dialect used for DB connections

After setting up your config file for TSAM, please add the required library for DB connection, at server lib folder.
You can find more on TSAM implementation here: epSOS_TM_TSAM_implementation_v7.

- **3.6 Transformation Manager (TM)**

This component is used for data transformation from a national language to the epSOS Reference Terminology or for data transformation from the epSOS Reference Terminology to a national language.
In order for the TM to work properly, you should setup the tm.properties file, also provided and located under your EPSOS_PROPS_PATH.
It'll probably suit your needs with the default values, but you can always take a look at it.
You can find an example bellow:

**tm.properties** Expand source
You can find information on TM specifications in TM_specs_v0.7 and on the implementation (helpful to understand the previous properties) in epSOS_TM_TSAM_implementation_v7.

- **3.7 Automatic Data Collector (eADC)**

Automatic data collection is a feature requested to the NCP to provide information to evaluate the epSOS interoperability system performance and to collect statistics on the population using epSOS services.
To setup and install the Automatic Data Collector you can follow the instructions present on the following page: Setup eADC in OpenNCP

- **3.8 Audit Repository (OpenATNA)**
You'll need to deploy the openatna-web WAR to your Tomcat, but before that you need to do the following configurations:

- **TLS configuration**: parameters in section arr-tls of file `$EPSOS_PROPS_PATH/ATNA_resources/ArrConnections.xml` have to reflect the values of epsos properties database:
  - HostName -> audit.repository.url
  - Port (default: 2862) -> audit.repository.port (default: 6514)

- **Certificates**:
  1. copy your ServiceProvider.jks and ServiceConsumer.jks keystores into `$EPSOS_PROPS_PATH/ATNA_resources/certs` and refer to them in `$EPSOS_PROPS_PATH/ATNA_resources/ArrConnections.xml` (KeyStore -> ServiceProvider.jks and TrustStore --> ServiceConsumer.jks) **OR**
  2. In `ArrConnections.xml`, point to the keystore and truststore (ServiceProvider.jks and ServiceConsumer.jks, respectively) in `$EPSOS_PROPS_PATH/cert/PPT` instead of copying those to `$EPSOS_PROPS_PATH/ATNA_resources/certs` folder and change the passwords (don't use environment variables, use full paths instead).
  3. Example configuration can be seen in step 4: [OpenATNA Home](#)

- **Follow step 1 to set up the database**: [OpenATNA Home](#).

- In `$EPSOS_PROPS_PATH/ATNA_resources/openatna.properties`, you will need to change password of the DB and edit the actors.dir to point to the ATNA_resources folder.

- If you want to use the logviewer war, you have to add the openatna.properties files to atna.war/WEB-INF/classes

- If you want to use the logviewer war with MySQL, you have to add the jdbc-connector.jar to atna.war/WEB-INF/lib

- You should add this line to the TOMCAT setenv.sh script:

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

- **OpenATNA** uses property with name `scheduled.time.between.failed.logs.handling.minutes` in ConfigurationManager database to define the interval in which OpenATNA checks if some audit log was not persisted. In case these logs are found, they will be attempted to re-persist. The default value is 60 (minutes).

- Configure epsos properties to write test audits (see step 5: [OpenATNA Home](#))
Now you can deploy the WAR file in your Tomcat. If everything is OK your OpenATNA database structure should’ve been created and you should see the following lines at the end of the OpenATNA log file:

- Starting OpenATNA service..
- TLS Server running on port:2862
- UDP server started on port 2861

### 3.9 Server Side (NCP-A)

At this moment you probably have all the configurations finished and correctly adjusted. So in order to install the Server Side (NCP-A) you will need to obtain the artifact named **openncp-ws-server-X.X.X.war**, as explained in step 3.1. It is advised to rename the file to simply **openncp-ws-server.war**, then you should deploy it on your Tomcat instance (to deploy the application you may follow this instructions: [http://tomcat.apache.org/tomcat-7.0-doc/deployer-howto.html](http://tomcat.apache.org/tomcat-7.0-doc/deployer-howto.html) for Tomcat 7).

In case you change the default port, you have to modify the WEB-INF/conf/axis2.xml file to reflect the change (default: port 8080 / 8443). If not, and according to the configuration made in section 2.2, your web services will be exposed in the following URLs:

- https://<hostname>:<SSLport>/openncp-ws-server/services/XCPD_Service
- https://<hostname>:<SSLport>/openncp-ws-server/services/XCA_Service
- https://<hostname>:<SSLport>/openncp-ws-server/services/XDR_Service
- And so on.

In order to implement a National Connector to connect OpenNCP to your National Infrastructure, you have to develop some services. OpenNCP Bitbucket provides a skeleton where you can start to work: **epsos-nc-mock-it**. The following page provides some guidance on this task: [National Connector Implementation](http://www.project-shield.eu/).

### 3.10 Client Side (NCP-B)

For client side it is used the same approach used in Server side. You should download the artifact named **openncp-client-connector-X.X.X.war**, as explained in Step 3.1. It is also advised to rename the file to just **openncp-client-connector.war**, then you should deploy it on your Tomcat instance (to deploy the application you may follow this instructions: [http://tomcat.apache.org/tomcat-7.0-doc/deployer-howto.html](http://tomcat.apache.org/tomcat-7.0-doc/deployer-howto.html) for Tomcat 7).

In case you change the default port, you have to modify the WEB-INF/conf/axis2.xml file to reflect the change (default: port 8080 / 8443). If not, the following web service that allows the Portal to communicate with the OpenNCP will be exposed:


### 3.11 OpenNCP Portal or epSOS-Web

Project Title: SHIELD

Contract No. GA 727301

[http://www.project-shield.eu/](http://www.project-shield.eu/)
At this point, you'll either install OpenNCP Portal or epSOS-Web. OpenNCP Portal is the reference implementation and should be your choice in case you're following this manual and want to use the eID capabilities. epSOS-Web requires a set of different properties in the database. CDA Display Tool shall be used in both cases.

- **3.11.1 OpenNCP Portal**

To install the OpenNCP Portal, you may follow the provided instructions, available at:

1. [Installing OpenNCP Portal](#)
2. [Configuring portal](#)

- **3.11.2 epSOS-Web**

To install epSOS-Web follow the instructions available at: [epSOS-Web Get Started](#).

- **3.11.3 CDA Display Tool (TSAM-Exporter)**

In order to correctly translate the CDA, you must run the TSAM-Exporter (make sure you have fetched your country terminologies into your LTR database): [TSAM Exporter](#).

- **4. Database Logging**

The current implementation of OpenNCP is using Logback framework for the logging management. Logging level and configuration are managed through the logback.xml configuration files embedded into the artefacts.

In addition to the Console and File logging appender, a database appender has been defined. The DBAppender inserts logging events into three database tables in a format independent of the Java programming language. These three tables are logging_event, logging_event_property and logging_event_exception. They must exist before DBAppender can be used.

Logback ships with SQL scripts that will create the tables. They can be found under the logback-classic/src/main/java/ch/qos/logback/classic/db/script folder. There is a specific script for each of the most popular database systems if required.

In order to complete the installation a dedicated database should be created according the MySQL SQL script provided hereafter.

```sql
logback-mysql.sql
```

If the logged information are not enough efficient, you will find some guidelines about the Logging configuration in the following link: [Logging customization](#).
5. Final Considerations

After performing the installation of all components you may end with this sample folder setup (considering that we placed all the files under the /opt folder):

```
/opt
|-- /apache-tomcat-8.5.XX
  |-- /bin
  +-- /conf
      |-- context.xml
      |-- server.xml
  |-- /logs
  |-- /temp
  |-- /work
  +-- /webapps
      |-- /openncp-client-connector
      |-- /openncp-ws-server
      |-- /openatna-web.war
      |-- /openncp-gateway
      +-- /TRC-STS
-- /openncp-tsam-sync
  |-- application.yml
  +-- openncp-tsam-sync.jar
-- /openncp-tsam-exporter
  |-- openncp-tsamexporter.jar
  |-- logging.properties
  |-- run.sh
  +-- settings.properties
++ /openncp-configuration
    |-- /ATNA_resources
    |-- /cert
    |-- /EADC_resources
    |-- /EpsosRepository
    |-- /forms
    |-- /TM_resources
    |-- configmanager.cfg.xml
    |-- hcer.properties
    |-- pn-oid.xml
    |-- tm.properties
    +-- tsam.properties
```
8 References

Books:

Links:
- http://www.servicedesigntools.org/
- https://www.usability.gov/
- https://www.interaction-design.org/