
Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of

Patient Summary and electronic Prescription

# D3.B.1: epSOS 2 Implementation Strategy

| | |
|---|---|
| WORK PACKAGE | **WP3.B** |
| DOCUMENT NAME | D3.B.1: epSOS 2 Implementation Strategy |
| SHORT NAME | **D3.B.1** |
| DOCUMENT VERSION | **0.14** |
| DATE | **20/05/2011** |

| COVER AND CONTROL PAGE OF DOCUMENT | |
|---|---|
| Document name: | **D3.B.1** - epSOS 2 Implementation Strategy |
| Document Short name: | **D3.B.1** |
| Distribution level | **PU-when** released |
| Status | **Final** |
| Author(s):<br>Organization: | M.Melgara, J.Caumanns, M.Festen, F.Linden, C.Parisot, A.Wolfe, M.Yuksel, R. Zuffada<br>**KT3.B.1 Core Team** |

Dissemination level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.


ABSTRACT

"**D3.B.1 - epSOS 2 Implementation Strategy**" provides the analysis of pros and cons of epSOS 1 implementation strategies, adopted by the project and by PNs, and proposes new approaches for epSOS 2, in line with the WP2.2 Policies, aiming to assure the medium/long term sustainability, safeguarding the investments in specification, development and testing performed by epSOS and by the single PNs.


Change History

| Version | Date | Status Changes | From | Details | Review |
|---|---|---|---|---|---|
| V0.1 | 11/03/2011 | Draft | Lombardy | Initial Structure based on minutes by KT3.B.1 Tconf minutes on March 7th | KT3.B.1-CT |
| V0.2 | 14/03/2011 | Draft | Lombardy | Included contributions from Fraunhofer and Lombardy | |
| V0.3 | 16/03/2011 | Draft | Industry Team-Charles | Mark-up on 2.1-2.4 and Section 3 | |
| V0.4 | 21/03/2011 | Draft | Joerg's & marcello's comments | | |

| | | | | | |
|---|---|---|---|---|---|
| V0.5 | 28/03/2011 | Draft | Charles, Roberto, Marcello | Chapter on WP2.2, Implementation Strategy and revisions | |
| V0.6 | 28/03/2011 | Draft | Anna, Joerg, Fredrik, Charles, Roberto, Marcello | Review performed during tconf 28/3/11 | |
| V0.7 | 3/04/2011 | Draft | Anna, , Fredrik, Marcello Charles | Added contributions and comments | |
| V0.8 | 4/04/2011 | Draft | Anna, , Marcello Charles Mustafa Roberto | Added contributions and comments from the Tconf on 4/4/11.<br>Removed Appendix B<br>To revise Appendix A | |
| V0.9 | 6/04/2011 | Draft | Marcello Charles Joerg Roberto | Added contributions and comments after the Tconf on 4/4/11.<br>To revise Appendix A | |
| V0.10 | 12/04/2011 | Draft | Marcello Anna Charles Joerg | Included approved comments | |
| V0.11 | 18/04/2011 | Draft | Marcello Anna Charles Joerg | Consolidated version for TPM and NEPCs | |
| V0.12 | 20/04/2011 | Draft | Marcello | Consolidated version for TPM and NEPCs, after TPM of 19/4/2011 | |
| V0.13 | 10/05/2011 | Draft | Marcello | Included comments from external QA | |
| V0.14 | 20/05/2011 | Final | Marcello | Included comments from France external QA | |

TABLE OF CONTENTS

**1 Introduction ..... 5**
1.1 Background ..... 5
1.2 Scope of the task ..... 7
1.3 Relations with WP2.2 ..... 7
**2 epSOS Lesson learned Implementation strategy review ..... 10**
2.1 Followed approach ..... 10
2.2 Original Approach: IHE-Based Software ..... 11
2.3 Achieved Result: NCP-in-a-Box ..... 12
2.3.1 Central Services ..... 12
2.4 Assessment: ”IHE-Based Software Backbone” vs ”NCP in a Box” ..... 13
2.5 Detected issues ..... 15
**3 epSOS Future Implementation & Testing Strategy ..... 17**
3.1 General policies ..... 17
3.2 Options assessment ..... 17
3.3 Major goal: allow development of EU market solutions ..... 19
3.4 Proposed Implementation strategy ..... 19
3.4.1 Software Development Consortium ..... 20
3.4.2 Fostering of a Software Solutions Ecosystem ..... 21
3.5 Impact analysis on epSOS / PNs / Industries ..... 23
**4 Guidelines to specification and testing ..... 25**
4.1 Guidelines to Technical specifications ..... 25
4.2 Impact for a sustainable deployment and testing strategy ..... 26
**5 Conclusion ..... 27**
**Appendix A Abbreviations ..... 29**
**Definitions ..... 31**

# 1 Introduction

## 1.1 Background

The overarching goal of epSOS (Smart Open Services for European Patients) remains "to develop a practical eHealth framework and ICT infrastructure that will enable secure access to patient health information, particularly with respect to a basic Patient Summary and ePrescription, between European healthcare systems." [1]

epSOS 2 related activities enlarge the scope of epSOS 1, extending the defined services, the coverage of the European Large Scale Pilot (LSP) with many more participating countries and raising epSOS 2 to a more maturity of the operated pilot services .

The basic Pillars established for epSOS 1 implementation remain valid:

- epSOS has identified means of interoperability which will allow to connect services and architectures, potentially different in every Participating Nation (PN), to provide Patient Summary (PS) and ePrescription (eP) cross-border services.
- epSOS has defined, and it is currently developing and testing services to allow a patient from country A while being in country B, to exploit eP and PS services available in country A.
- epSOS LSP is based on legal, functional and technical pre-requisites that represent the pillar for the definition of the services and the architecture of epSOS.
- epSOS will enable the participating nations to integrate their national solutions and validate them for Cross-border interoperability of eP and PS
- epSOS will not develop European eP / PS services
- epSOS eP and PS Cross-border interoperability are based on already existing National eP and PS services,
- epSOS LSP should not interfere with National eP and PS services or request their modification,
- epSOS LSP services must be based on a Legal and Regulatory framework which includes the signature of contractual agreements among the Participating Nations to commit to their legal responsibilities and to assure the adequate level of trust.
- The National Contact Point (**NCP**) is the fulcrum of cross border interoperability, exploiting the role of connecting the National technical, organisational and legal environment to the European Level environment.

[1] Annex I, Ch. B1.1.2.1

Those basic pillars are representing the compulsory, binding boundary conditions for all the activities of epSOS 1 and most likely of epSOS 2.

WP3.9 “Proof of Concept implementation” defined in D3.9.1, Chapter 8, the epSOS 1 Implementation Strategy[2] .

The implementation strategy definition in epSOS I was performed by identified core-teams, composed by specific experts, other WP Leaders, the Technical Project Manager, the Project Co-ordinator, with the goal to build strategic approach, to identify pros/cons, to present it to the TPM, PEB, PSB. The approved strategy is actuated to allow the execution of the subsequent phases. The phase, in some cases, has included the definition of specific contracts with Suppliers or activity/funding assignment to beneficiaries.

The main steps were:

- Define the Pilot scope, identifying the service characteristics, among possible alternatives proposed in the functional and technical specifications of WP3.1 – WP3.7, making choices to allow the practical implementation of the Proof of Concept
- Define of the Implementation strategy: this topic is manyfold:
    - Build and support the decision process to allow PEB / PSB to decide if the NCP has to be developed as a customized solution by every MS, or as a common development.
    - PSB decision was to try to maximize the components in common, building the NCP-in-a-Transparent box, that could be used by MSs, both as a single box, or adopting specific components only
- Define the implementation scenarios, to allow the MS to choose the most suitable one, according to its own pre-existing infrastructure, its eHealth strategy, its implementation policy and attitude and its procurement strategy
- Define and perform the call for invitation for implementers of the NCP solutions and implementation scenarios
- Define the criteria for selecting offers and perform the evaluation process to allow PEB / PSB to select the solutions to be adopted and funded.

epSOS 1 implementation (see D3.9.1 Chapter 8.4 for details): It saw the development by a JARF funded team to (1) reuse/adapt from vendor provided catalogue of SW Components, (2) develop SW Components if needed, and integrate them as an NCP-in-a-box. This team is led by two epSOS beneficiaries and includes vendor contributors from the Industry team. PN develop their interfacing to this NCP. These components were adopted by all the PNs piloting in epSOS 1.

[2] As for all epSOS Deliverables, D3.9.1 can be downloaded from **www.epSOS.eu** > download area.

## 1.2 Scope of the task

KT3.B.1 starts from the epSOS 1 implementation strategy and achieved results. with the goal to define the overall epSOS2 Implementation and Testing Strategy[3], built on role of Industry Team in epSOS2 implementation process, building up-on the IT strategic go-to-marked vision and approach, combined with the epSOS Policies and Strategies, defined in WP2.2.

The methodological steps that will be followed will be:

- Develop, with WP2.2 global implementation policies
- Analyse adopted implementation strategy results, advantages and drawbacks
- Understand Industry Team Go-to-Market strategy in short (within the project time frame), medium (5 years) and longer term (10 years)
- Propose jointly agreed implementation approaches, covering co-related testing strategy, listing alternatives, pros/cons
- Refine the implementation strategy approved by WP2.2, PSB and provide implementation guidelines.

## 1.3 Relations with WP2.2

An effective development the KT3.B.1 must consider the close relationship with Work Package 2.2 in terms of synergies and coherence of outputs.

Under Work Package 2.2 three main aims are envisaged:

1. To update and then maintain the set of policies for epSOS2, building on the work of epSOS1 (T2.2.1 epSOS Policy development and maintenance);
2. To provide a comprehensive epSOS service description addressing legal, semantic, and organizational issues. This will aid local implementation activities (T2.2.2 epSOS Service Description);
3. To support stakeholder liaison and engagement both globally and in Europe through a programme of openness, transparency and validation (T2.2.3 Openness, Transparency and Validation).

More specifically:

- Under T2.2.1, the policy areas that need to be addressed are reviewed and defined and the specification of the Evolving Document "epSOS Policy" is determined as the basis for the first version of epSOS Policy in all key areas

[3] the strategy will impact each stage of the lifecycle: specification, development, testing, implementation, migration, service deployment

of epSOS policy. The result is epSOS Policy.1.0. The policy document may be updated at regular intervals, with proposals that will be brought to the PSB for approval.

- The goal of T2.2.2 is to provide support to fill the gap between the several specifications activities and the capability of the PNs to implement the epSOS services. T2.2.2 will provide integrated end-to-end description of the services, including the legal, organizational (clinical & functional), technical (these aspects will be kept at a high level), organisational and communication/marketing features that have to be addressed to implement the services, including those that have to be handled centrally.

Implementation and testing strategy, as under definition in KT3.B.1, must be coherently designed in deep relationship and strong consistency with the above scenario in order to complement and integrate the latter with the IT strategic go-to-marked vision and approach. Taking into account the key role of WP2.2, coherence and consistency between the two level of implementation will be ensured by a process entailing the agreement of this work package on the implementation guidelines provided by KT3.B.1.

In this frame the policy baseline documents generated by WP2.2 on epSOS Governance Structure[4] and the Use of Project Joint Activity Reserve Fund will provide guidance to KT3.B.1 in the implementation process.

KT3.B.1 must set out the implementation guidelines considering the strategic choices drawn by the baseline governance structure, namely those which recall the following principles[5]:

1. **Co-ordinate across all interoperability areas**
2. **Engage of industry** and of PN administrations with the goal of establishing a permanent mechanism and an ecosystem for secure **technical and organisational sustainability**
3. **Rationalise and optimise use of resources**
4. **Design jointly – implement locally** safeguarding the end-to-end model.

In addition to these Policies, WP2.2.1 should consider the guideline expressed by PSB related to the specification and development of epSOS-1, as a basis for development in epSOS-2, to assure the reuse of already implemented solution both to safeguard the PNs investments and reduce the risk for brand new developments and piloting.

[4]"Policy epSOS Governance Structure" document, 11.03.2011, adopted by the PSB on 22nd March 2011.

[5] Refer to Policy epSOS Governance Structure" for more details

For each of the above points WP2.2 is asked to make sure that they translate into project policies which the Implementation Strategy will follow. Specifically on the 4th principle., KT3B1 team asks WP2.2 to create a policy which ensures that the PN's investment for implementation according to a common design is safe and future-proof.

# 2 epSOS Lesson learned Implementation strategy review

## 2.1 Followed approach

The epSOS architecture was designed in a way that each functional building block is either

- provided by a national infrastructure (e.g. HCP authentication)
- implementable by an existing IHE profile (e.g. IHE XCPD)
- designed as a clearly separated original epSOS functionality (e.g. epSOS TRC Assertion)

All of these interoperability building blocks are described in the epSOS technical documentation (see figure 1):

- epSOS D3.4.2 common component specification defines the normative NCP-2-NCP interface that solely consists of IHE profiled transactions (white puzzle pieces)
- epSOS D3.9.1 implementation guide additionally provides a non-normative specification of a software architecture made of a number of epSOS software components (yellow puzzle pieces)
- epSOS D3.3.2 architecture and epSOS D3.7.2 security services define the expected behaviour of functionality that is to be provided by the national infrastructures (green puzzle pieces)

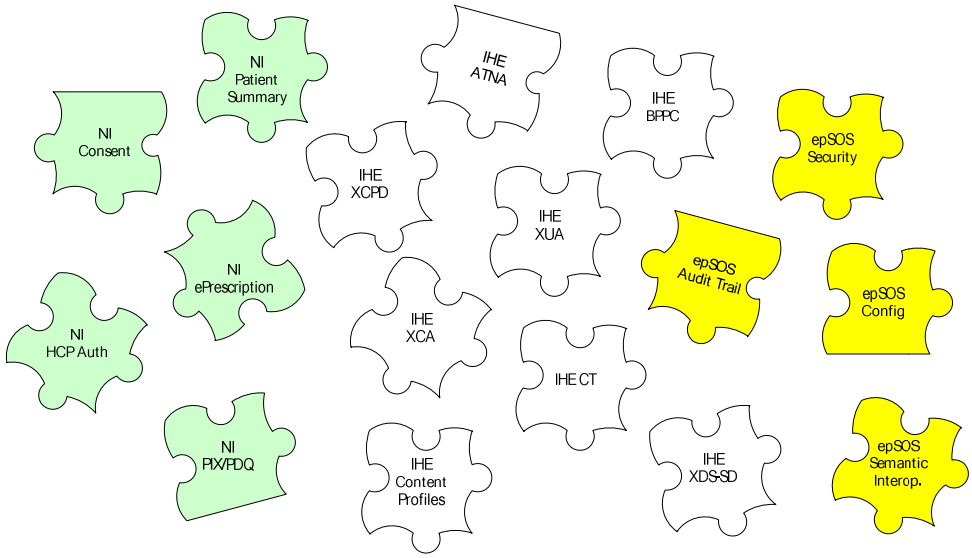



Figure 1: epSOS Functional Building Blocks

## 2.2 **Original Approach: IHE-Based Software**

The major reason for choosing IHE profiles as the basis for epSOS was the industry claimed that a huge portfolio of IHE-compliant products were available from industry that could serve as a »backbone« for an epSOS NCP. As it was an objective of epSOS to enable competition between vendors in order to allow member states to choose among different offers, a deployment strategy was defined by WP3.4 as sketched in figure 2:

- epSOS does not do common implementation of IHE profiles; this field is solely given to vendors who spent efforts in developing respective solutions which have proven to be mature. It is assumed that a single vendor (or a small group of vendors) who provides all required IHE profile implementations acts as a major integration partner of a single member state.

- epSOS I has done a common development of software for all epSOS original functionality (CCD = common components development). These components were implemented by epSOS industry partners, funded by epSOS and provided as open source. Each vendor who is running an integration project with a member state can take these components and link them with his existing IHE capable software modules.

- epSOS only provides a normative specification for the NCP-2-NCP interface. National infrastructures (NI) span a wide range of interfaces and standards and the way to “interface“ cannot be normalized. Therefore the integration of the software modules to enable an NCP integrated to a national infrastructure is an individual activity to be performed by each member state and its industry partners.

Figure 2: epSOS NCP Deployment – as it was planned

Among different offers from different consortia for speeding up the NCP development by providing commonly usable components, the epSOS PSB chose the Fraunhofer-ELGA-Tiani (FET) proposal which was built upon the deployment

model as sketched in figure 2. Together with industry partners CareCom, Gnomon, NetSmart and PosAM a reference implementation of an NCP was provided that built upon TIANI off-the-shelf IHE software components.

## 2.3 **Achieved Result: NCP-in-a-Box**

In order to allow for a parallel development of glue components between a national infrastructure and the common software components for an NCP, epSOS member states asked the FET team to provide a specification for the NCP "back " interface towards the national infrastructure. FET followed this request and defined a respective WebService programming interface based on the existing Tiani solution (Tiani National Infrastructure Interface). Obviously none of the member states planned for a close integration of an NCP into the existing services, they rather preferred to treat the NCP as a "black box" with a defined functionality that could be treated as a semantically enriched stub for cross-border sharing of medical data. In addition the provided interface solely focuses on epSOS core functionality and makes limited assumptions on the deployment of data managing components within the national infrastructure. However, this new interface has not been subject of rigorous design and testing as was applied to the normative epSOS NCP-2-NCP interface where robustness, platform-independence and long-term viability were considered.

Figure 3 sketches how the final NCP software components deployment in epSOS 1 looks like. Additional "TIANI Ni If" components had to be created (Orange) to support the specified „back" interface, while still requiring the national infrastructure to develop specific components to adapt itself to the specified „back" interface. But due to the encapsulation of semantic services and epSOS-specific security concerns within the NCP „box" this „back" interface is rather simple and just introduces a „thin" adaptor layer.

### 2.3.1 **Central Services**

Connected to the concept of NCP-in-a-Box, epSOS 1 has defined and implemented the so called "Central Services", with the purpose of keeping under a centralised management the relevant NCP configuration data.

In particular the epSOS Central Reference Terminology Repository is the heart of epSOS interoperability, keeping the reference terminologies (under epSOS responsibility) and their translation/transcoding for each PN (under each PN's responsibility). epSOS Terminology is based on international Coding systems, but no interoperability standard has been considered adequate to epSOS peculiarities.

Figure 3: NCP as a Black Box

## 2.4 Assessment: ”IHE-Based Software Backbone” vs ”NCP in a Box”

Table 1 gives an overview of the pros and cons of both approaches with respect to various criteria.

| Criteria | Assessment |
|---|---|
| Development Effort/Cost | For the »NCP in a Box« two interfaces must be specified: the normative NCP-NCP-interface and the “back”-interface towards the national infrastructure. This additional “back” interface was recently specified by the primary vendor (Tiani). With every extension of epSOS services, both interfaces have to be extended. This effort is covered by the provider of the »NCP in a Box«, Evolution of the national infrastructures will require additional changes to the “back”-interface. The integration effort at MSs is reduced.<br>For the IHE-Based software components only the normative NCP-NCP-interface is needed. Effort for integration of the provided components is with the MS. Evolution of requirements to the NCP-NCP-interface creates effort for the component provider and the integrating MS. |
| Reuse | The »NCP in a Box« is reusable as a monolith designed primarily for epSOS services. Selected IHE-Based Software Components” can be reused more flexibly by the MSs in another context. |
| Cost of Installation and Operation | The »NCP in a Box« is delivered as an Off-the-Shelf product that needs to be interfaced with the national infrastructure, while the » NCP Based on IHE Components« approach requires each PN to set up an integration project. For the PN the »NCP in a Box« was much cheaper to install and operate – on short term. Long term cost depends on the maintenance process that will be established with the provider of the »NCP in a Box« and by its impact on the open market. |

| | |
|---|---|
| Impact on market | Enhancement of »IHE-based Software Components« with further epSOS specific functionality would require investment by the provider with the prospect of extending their present customer base.<br>epSOS can potentially create a European market for a turn-key »NCP in a Box« with the vendors charging the PN directly. |
| Sustainability | If treated as a product the »NCP in a Box« is sustainable because the respective vendors will – in their own interest - take responsibility for the evolution of the interfaces. The market is likely to be initially small to reach this sustainability but can increase by reusing NCPs for sharing also non-epSOS related data between European regions and existing regional networks<br>For the »Off-the-shelf IHE Software components« approach there is no normative »backward« interface and therefore each additional requirement at the borderline between NI and NCP must be defined by each PN Nevertheless these components have a large market and will be maintained commercially or open source over the long-run at very low cost (but even with all risks of open source software maintenance). The epSOS specific components may attract more specialized vendors. |
| Lock-Ins | The »NCP in a Box« can be in theory exchanged: if a new vendor makes a better offer to a PN, that PN would be able to switch to this vendor if such a “back” interface would be standardized and supported by all vendors in a common fashion). Unfortunately, there is lock-in today with a vendor specific “back interface” creating a lock-in. The »IHE-based Software Component« approach interweaves IHE based Component, epSOS specific components and National specific integration. In both cases, the PN would need to set its own back interface or component level interfaces and use those as seen best fit. The NCP-to-NCP IHE profiles and standards-based interface remains the fundamental truly open foundation to minimize lock-in. |
| Flexibility | The »Off-the-shelf IHE Software Component« approach offers PNs a higher flexibility as there is no restricting interface in between NI and NCP. With the »NCP in a Box« PN only get NCP core functionality – no more and no less. |
| Security Policy | As a box the »NCP in a Box« can be hardened and evaluated against defined security criteria. With the off-the-shelf IHE software component approach the components can be better integrated with the native security environment of the NI. The reduction of the software layers simplifies evaluation of single – yet PN specific – components’ implementations. |
| Effort for Operations | The »NCP in a Box« can be operated under the existing security policy. Required administrative and operational tools (e.g. security handbook, operations guidelines) only have to be developed once.<br>The »off-the-shelf IHE software components« allows the reuse of the NI deployment and operations strategy and respective guidelines and handbooks already developed by each PN. |
| epSOS Annex-I Compliance | The designer of the »NCP in a Box« is responsible for compliance with Annex-I core principles. With off-the-shelf IHE Components more responsibility is assumed by the PN. |

Lessons Learnt and hints for the future:

From a PN perspective the »NCP in a Box« has offered a turn-key solution, which provides sufficient functionality for low costs and with minimum risks. The effort for connecting existing national services was low and common requirements on secure operations can be covered by common security policies and operations guidelines. From the assessment it is not clear to which extent this solution is somehow considered less sustainable than the »IHE – Based Software Components« solution – especially if one considers that the »NCP in a Box« could be deployed as a managed product with a clear business model.

Sustainability of NCP in a Box might assume that there is either a PN Consortium to ensure maintainability and evolution of a shared solution among a set of PNs, or that there is enough of a market for vendors of epSOS „NCP-in-a-box“ solutions without having the PN require different operation environments, software architectures, and different models of integration into their national infrastructure.

From an industry perspective the »IHE Based software components« approach offers much better business opportunities and is better suited to open new markets. The higher flexibility of this approach allows for a deeper integration with national services and can as such foster the development of additional bilateral cross-country services on top of the epSOS platform but outside of the epSOS project

The alternative with IHE-based standard software components was not used by epSOS 1, for reasons that need to be analysed. Was it because neither Industry nor IHE Europe were keen in advertising and supporting a satisfactory offering of off-the-shelf components? Was it because the sustainability was not the priority, but the launch of initial pilots? Was it because the epSOS interoperability specifications were so complex to navigate, that PN and Vendors did not feel comfortable to proceed independently (e.g. because the off-the shelf-IHE software components did not hide IHE grouping requirements and implementation specifics (e.g. ebRIM) from the NI)? Was it because the level of parallel development that needed to be done in a short time span both on the national infrastructure side and on the support of the NCP-2-NCP interoperability was felt too difficult for new implementation teams ? Was it because the PN wanted to minimize their short-term investment? It was probably a little of all of the above.

Options for epSOS PNs to decide on:

1. Deliver only NCP specs and leave procurement and integration to the PNs who comply to the NCP-NCP-interface only.
2. In addition to 1. specify an “NCP in a Box” with a normative NCP-NCP-interface and a sample “back”-interface, no implementation. Procurement for the epSOS interfacing is left to the PN. Vendors may offer components only or an integrated “NCP in a Box” with a “back”-interface supporting or not the sample “back”-interface.
3. In addition to 1. and 2. epSOS provides a proof of concept “NCP in a Box”. More options may stimulate product development on the market.

Industry team cautioned against the challenge for epSOS to develop and maintain a sample “back”-interface that may be used across all PN software development environments, and the choices made for hiding or exposing services depending on the security environments.

## 2.5 **Detected issues**

The implementation approach used fo epSOS 1 was effective in reaching in a reasonably quick time frame a proof of concept implementation for more than 10

pilot PNs. It helped the ramp-up of the implementation teams in each PN by allowing them to remain rather independent from the development and integration of a significant part of the NCP specific capability. It hid the fragmentation, inconsistencies and complex organization of the NCP-to-NCP specifications. The test tool development was also able to proceed in parallel while reducing the testing effort.

However, it revealed some limitations associated with the “single source” nature of the solution. During testing, when an error was detected, the testing activities where halted while it was being fixed on the shared NCP in a box. Some non-compliance to the specifications may remain undetected if they are too subtle for the conformance test tool to detect, and be identified only when another implementation is being introduced. The necessity for each member state implementation to adapt to the “de facto” back interface of the NCP in a box is inducing additional layers of software. But foremost, the lack of competition is constraining all MS to adopt the same implementation model, a sole source product, which may be more complex to maintain and to evolve, as their national infrastructure evolves and specific national policies are applied in a production mode to the operation of the NCP.

# 3 epSOS Future Implementation & Testing Strategy

Two options have been considered based on the lessons learnt from the implementation strategy used for epSOS I and the strategic objectives of epSOS 2 as understood. We will first review the general policies in section 3.1.that drove the definition of these options.

## 3.1 General policies

- **Software Implementation in epSOS 2:** epSOS 2 plans to move from a proof of concept pilot to a sustainable environment and does not want to assume the operational responsibility to fund and manage, as epSOS deliverables, implementation software components. This was performed in epSOS I to meet the tight project pilot timelines and the lack of established NCP implementation teams in the various participating nations.

- **Operationalize epSOS 2:** Per the epSOS 2 DoW: "Phase 2 of epSOS will further consolidate, scale up and operationalise the presently available epSOS building blocks and services". We interpret "operationalize", in the context of shaping a future implementation and testing strategy, to mean that, the epSOS 2 implementation and testing strategy has to be organized in way that is best sustainable after the end of epSOS 2, in the absence of an EU funded Large Scale Project and meet the breadth of national IT environments from over 20 member states and associated nations.

## 3.2 Options assessment

Two options related to the organization of the epSOS implementation by the participating nations have been considered:

1. The creation of a **Software Development Consortium** independent from the epSOS project, but governed by the participating nations interested in pooling their resources. This Consortium would be in charge of designing, procuring and/or developing a set of epSOS Software Components that Participating Nations may chose or not to use in implementing their epSOS interfacing per the epSOS interoperability[6] specifications and associated policies.
2. The fostering of a **Software Solutions Ecosystem** in which industry support and open source communities contributions would offer a choice of tested software components and solutions that Participating Nations would rely upon in their implementation of their epSOS interfacing. epSOS as a project would foster the awareness of PNs need for cross National/Regional border Services and apply its leadership in organizing a "competitive

[6] Interoperability covers both the normative interface and the expected behaviour along the full end-to-end flow of data.

dialogue" between interested solutions providers and PNs. Lessons learned from the attempt to organize this in epSOS 1 would be carefully analysed and errors not repeated.

Both of these options move the common software components development activities outside of epSOS. This includes activities such as defining an NCP software architecture, programming interfaces specifications, software development process and methodologies, maintenance and integration. It refocuses epSOS on its core governance role in coordinating the evolution of its technical and policy specifications, the availability of a testing platform and business planning (pilot and operational acceptance, introduction of new services, etc.).

The epSOS 1 lesson learnt about the different software implementation models, for a country NCP and its design and integration with evolving national infrastructures, should enable Participating nations to choose among the following software design and implementation models:

1. *NCP as a black box:* On the basis of the epSOS NCP-to-NCP-interface specification, the entities committed to deliver such an NCP black box are responsible to select and integrate its software components as they choose and in a way hidden by the NCP "back" interface they chose to support based on their customer's need (e.g. java, .net, web services, etc.).
2. *NCP as a transparent box:* Only the NCP-to-NCP interface is specified by epSOS, and on its basis, the entity responsible to deliver such an NCP as a transparent box, is responsible to integrate the necessary software components, either as independent elements or as an integrated box. Back interfaces either at the component level of the box level are provided.
3. *NCP built from off-the-shelf components:* Only the NCP-to-NCP interface is specified by epSOS. Vendors provide a tool box, with modularization and deployment guidelines that demonstrate how their existing products/solutions can be integrated with a national infrastructure to support a NCP.

It appears that each one of these implementation strategies is of value and is likely to be used at different points in time, or given the national constraints in policies and architecture of the national infrastructure:

The two organizational options (Software Consortium or Ecosystem) can support the emergence of any or all of these implementation approaches. Staying away from software architecture and development platforms used across the core of the PN eHealth projects has been found the best sustainable long-term solution to develop and maintain interoperability across a broad range of implementations.

## 3.3 **Major goal: allow development of EU market solutions**

Through direct involvement at the national level and the involvement of a large industry team including various SMEs at the European level this project will offer "opportunities ... for innovative SMEs in the ICT sector ... to improve their products, services and business processes. It does so by contributing to the creation of wider market opportunities ... for SMEs." It will thereby "open new opportunities and support the growth and development of innovative SMEs that can then benefit from wider markets for the diffusion of their innovations."

By the present involvement of a large industry team including various SMEs active across Europe the LSP will "support experience sharing across regions and sectors on the means to ensure the wider uptake of ICT by SMEs."

To achieve this goal of epSOS 2, it is necessary that:

- The epSOS interoperability specifications be aligned to the broader needs of the support of ePrescribing and Patient Summaries not only across-EU countries, but also across regions within one country, hence significantly enlarging the market potential for epSOS compliant software components and "in a box" NCP solutions.
- The barrier of entry into the epSOS ecosystem be kept at an as low as possible level so that SMEs may compete effectively. This implies that the epSOS specifications and testing process be well documented, simple to access, transparent and aligned with a more generic approach (e.g. aligned with existing processes such as those from IHE, and the direction set by the EU HITCH project).
- Where possible, availability of open source and commercial software components supporting the standards and profiles selected by epSOS be identified and documented to facilitate their use by Participation Nations.
- Reduce the effective overall software complexity to develop epSOS compliant interfaces by the Participation Nations. This should reduce the costs to achieving quality interfaces, to maintaining the NCP related software.

Having listed these statements, it remains the responsibility for each PN to develop their own strategy

## 3.4 **Proposed Implementation strategy**

In this section the above two organizational options for the software development are analysed and refined. A number of common conditions are critical for either one of these options to proceed successfully:

1. Milestone date established, for stable and simple to read interoperability specification approved
2. Milestone date established, for availability of "lab" interoperability test tools
3. Milestone date established, for Projectathon testing

4. Milestone date established, for start of pre-pilot testing
5. Milestone date established, for start of clinical use
6. epSOS has a maintenance process for its specification and responds in a timely manner to questions.
7. The migration process from epSOS 1 to epSOS 2 and, in general to any future service deployment has to be considered as a basic requirement for medium/long term sustainability.
8. Other ?

### 3.4.1 **Software Development Consortium**

In this proposal, a number of epSOS Participating Nations would choose to join forces in a Consortium where they would invest the necessary resources and governance with the objective to jointly develop a number of software components for their use in the development of their NCP. Such a consortium would be distinct from the epSOS Project and follow the same epSOS interoperability specifications, as would any other epSOS Participating Nation not member of this Consortium. This Consortium would be responsible to decide if it would use a “make” or a “buy” (or combination) implementation strategy. The Consortium could select or not vendor solutions.

For this approach to work, the following requirements are critical:

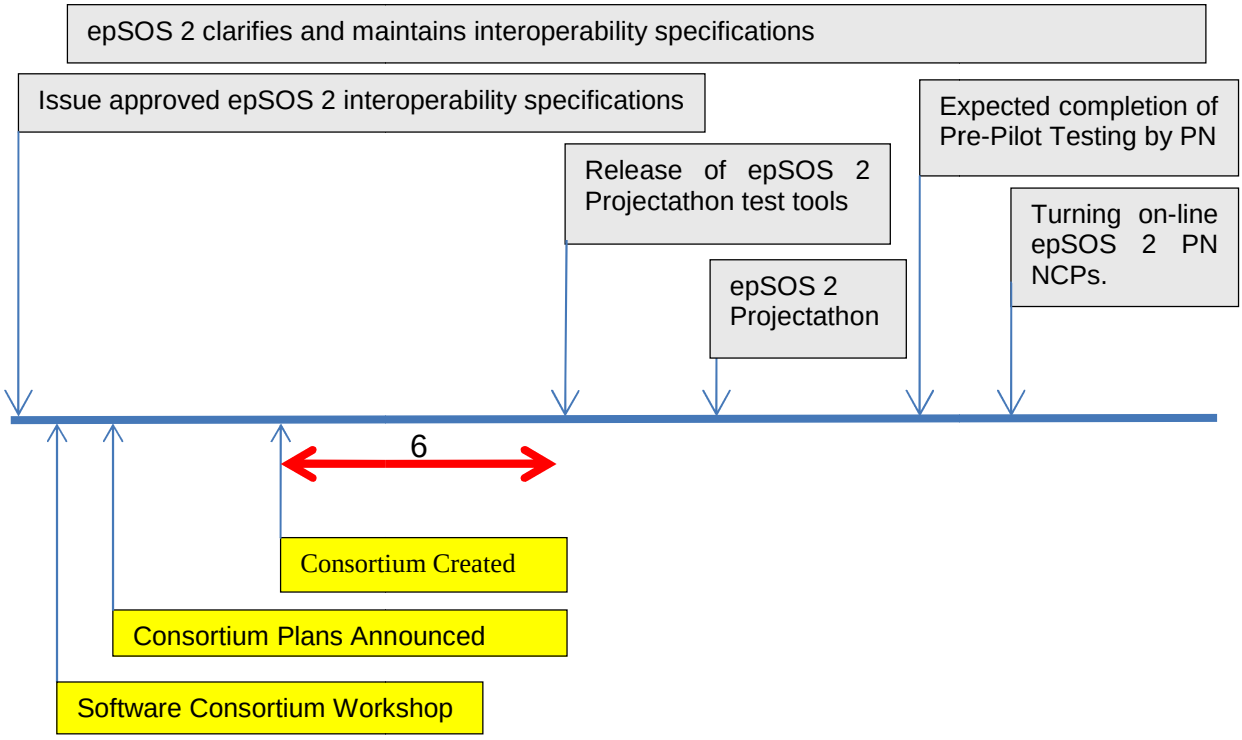
- the consortium has established itself and sufficient resources are available
- the consortium committed itself to provide an NCP that can be used by all PNs. No JARF funding should be expected for this,
- the “back” interface and/or component interfaces of the NCP are defined and agreed with epSOS Project Domain (PD) 3. However “back” interfaces are not the responsibility of epSOS: they will be decided and maintained by the Software Consortium.

The following steps are expected to be performed:

1. epSOS announces key milestone dates of epSOS 2 project:
   a. issue for approved epSOS 2 interoperability specifications
   b. release of epSOS 2 Projectathon test tools
   c. foresee the creation of epSOS architecture support team for PNs
   d. epSOS 2 Projectathon event
   e. expected completion of Pre-Pilot Testing by PN
   f. turning on-line epSOS 2 PN NCPs.
2. epSOS to host a “Software Consortium Workshop” where interested PNs (no industry) that are ready to invest resources in the creation of such a consortium meet and set the funding model and governance for this consortium.
3. Pre-consortium reports to epSOS PSB creation plan. This is necessary in order to identify major risk as early as possible, and being able to go for a contingency plan, to be defined. Consortium announces creation and plan

for software development (specific list of components, packaging of components, date available for PN participating in Consortium. Announce plans and calendar for issuing an RFP to industry

4. Consortium creation deadline set at 6 months before date of release of epSOS 2 Projectathon test tools.
5. epSOS to provide support for clarifications and maintain interoperability specifications in a responsive way for test tool development and Software Consortium.




### 3.4.2 **Fostering of a Software Solutions Ecosystem**

In this proposal, the epSOS 2 project would organize an activity to act as a neutral coordinator for the emergence of a suitable ecosystem where epSOS Participating Nations, industry and open source teams would declare respective commitments or interest to work together. In principle, no software development for the PN epSOS interfacing would be funded directly by the epSOS project (only test tools would), although leveraging as a starting point the Fraunhofer/Elga/Tiani epSOS software components. This would apply the principles of competitive dialogue processes among declared interested parties. A process to facilitate the emergence of this ecosystem:

1. Invite software providing entities (commercial and open source) to an ecosystem solutions workshop hosted by epSOS.
2. epSOS invites all Participating Nations to the same ecosystem solutions workshop.

3. Each PN engages a competitive dialogue on the definition of epSOS specific software components versus non-epSOS specific software components with the software providing entities interested to meet with them.

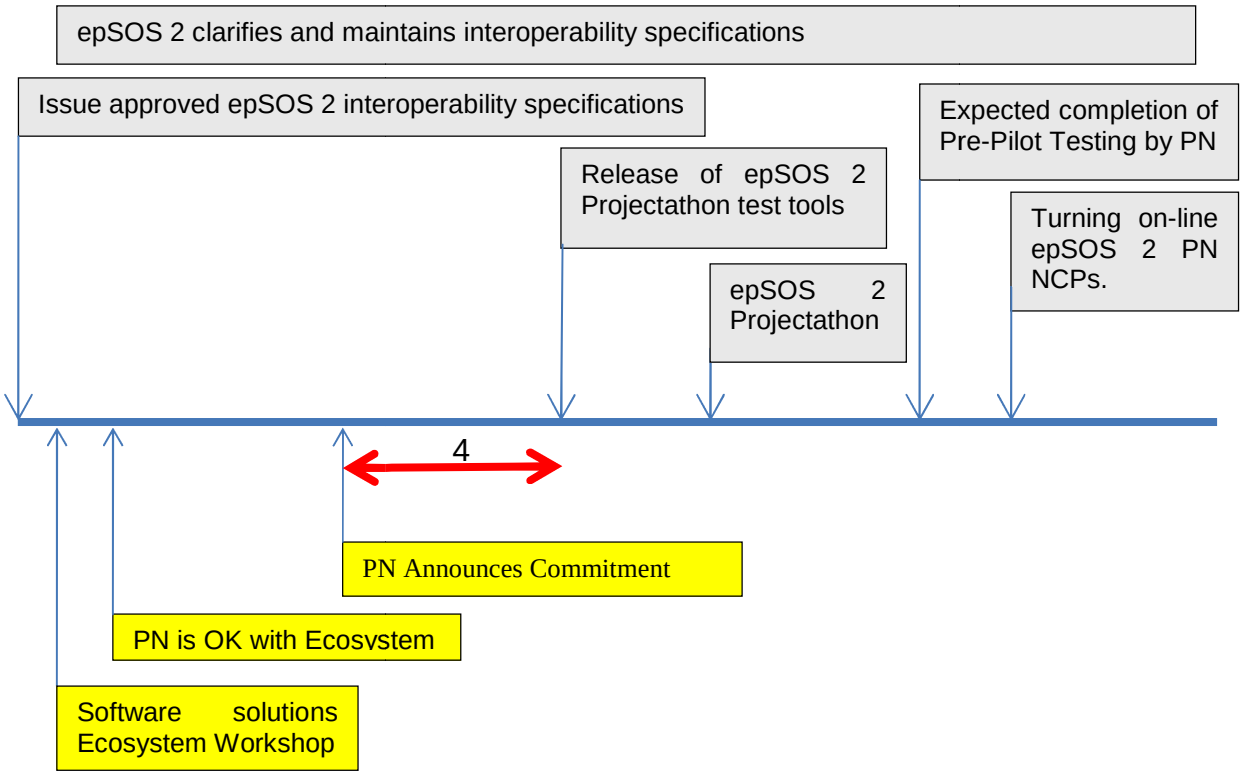
The general strategy is to not require (but allow) software providers to offer a set of software components as an "NCP in a transparent box". This is important to broaden the choices for PN and respect vendor market focus. The epSOS specific software components would likely require more analysis and proactive approaches (possibly with targeted initial epSOS funding).

- For this approach to work, the following requirements are critical:
    - epSOS would organize this "marketplace" between PN representatives/ potential buyers and vendors/open source team interested.
    - Early enough, given the milestone, to allow sufficient planning by all parties for meeting the agreed milestone dates.
    - These parties could interact one-to-one in any way they want to align their interest and strategies. Of course this is not a tendering process, just an RFI style activity.
    - The failed experience with assembling a cross-vendor catalogue of software components in epSOS 1 would not be repeated. The analysis of the cause of the failure and a recommendation of countermeasures will be performed.
- Each PN may invite other vendors (or group of vendors) to participate in this process.
- There is no need for epSOS to establish a framework that allows PNs and vendors to synchronize integration efforts and to fix discovered software inconsistencies. This would be a joint responsibility between the PNs and the vendors and other teams.

The following steps are expected to be performed:

1. epSOS announces key milestone dates of epSOS 2 project:
    a. issue for approved epSOS 2 interoperability specifications
    b. release of epSOS 2 Projectathon test tools
    c. epSOS 2 Projectathon event
    d. expected progress and completion of Pre-Pilot Testing by PN, controlled by epSOS
    e. turning on-line epSOS 2 PN NCPs.
2. epSOS to host a "Software Solutions Ecosystem Workshop" where interested PN that are ready to acquire software solutions (specific components, NCP-in-a-box, etc) participate and meet with vendors/integrators/open source/consortia interested by PN customers.

3. PN individually report to PSB, no later than one month after workshop their comfort to proceed with this approach and to procure their epSOS connection solution. This is necessary in order to identify major risk as early as possible, and being able to go for a contingency plan, to be defined.
4. PN need to confirm conclusion of their solution development no later than 4 months before date of release of epSOS 2 Projectathon test tools.
5. epSOS to provide support for clarifications and maintain interoperability specifications in a responsive way for test tool development and ecosystem implementers.




## 3.5 Impact analysis on epSOS / PNs / Industries

Unlike in epSOS 1, where timely start of the pilots and short-term risks were among the most important element in the implementation strategy, in epSOS 2 the focus should better balance schedule with operationalization and sustainability for Participation Nations.

Participating Nations need effective software solutions for implementing their epSOS compliant interface. Because the responsibility to develop, maintain and operate the software applications that support in part these Participating Nations NCP functionality. If such software solutions are to be provided by vendors and/or

open source teams, Participating Nations need assurance of availability, relevance and sustainability. In return these software solution providers need assurance of a credible demand by the Participating Nations.

Industry realizes that epSOS interfacing represents a rather limited market. However, epSOS has two critical impacts on the eHealth market that highly motivate industry. First epSOS has high visibility across Europe for advancing the maturity of the European eHealth market. Second, epSOS use cases, are reasonably close to the cross-regional interoperability within a country, hence enlarging the market for epSOS software and solutions is possible.

The following table summarizes the pros and cons of the two proposed approaches.

| **Criteria** | **Fostering of a solutions ecosystem** | **Software Development Consortium** |
|---|---|---|
| Development of EU market solutions | Broader | Limited |
| Risks for PNs | Medium | Low.<br>This may turn to high for the Project if the Consortium fails: all PNs adopting this solution will fail |
| Risks for Industry | Medium | Low |
| Open Source engagement | In competition with Industry | Easier |
| Flexibility of SW solutions for PN | High | Low, unless shown as a peculiarity of the Consortium |
| Robustness and Quality | Hard to be predicted | Hard to be predicted |
| Sustainability | Risk of non-synchronized NCP evolution and higher effort for agreeing on spec changes | Further development of epSOS depends on single consortium and its will to put efforts into maintenance |

# 4 Guidelines to specification and testing

## 4.1 Guidelines to Technical specifications

EPSOS 1 SPECS WILL BE KEPT AS MUCH AS POSSIBLE, TO AVOID REINVENTING THE WHEEL AND THROWING AWAY THE ALREADY DEVELOPED / TESTED SOLUTIONS.

- epSOS 2 extensions of the existing use cases such as multiple sources for a PS or the transmission of data to country A have been analyzed in epSOS-1 and considered with the architectural design. Therefore we do not expect major changes in the existing architectural patterns.
- But: especially the transmission of data from B to A will raise requirements for end-to-end security (esp. end-to-end authenticity as no PN will update their national data bases with data where the originator is anonymous and/or cannot be directly authenticated). The needed safeguards must be designed in a way that they also cover the existing open issue on end-to-end security (esp. confidentiality) in data transmission from A to B. There are some new ideas on how this could be done without affecting the existing specs too much. These will be further elaborated in epSOS 2 WP3.A.

EPSOS 2 SPECS SHOULD ADD NEW FUNCTIONALITIES POSSIBLY IN AN INCREMENTAL WAY WITH RESPECT TO EPSOS 1 SPECS, KEEPING BACKWARD COMPATIBILITY.

- In a first run in summer 2011 epSOS 2 picks up the core functionalities and happy cases of the new use cases and old use cases extensions; it focuses on additional end-to-end security safeguards to be integrated with the existing design. Exceptional conditions and bells-and-whistles of the new use cases will be analyzed in common with the pending epSOS-1 wish-list and feed-back from the pilots in order to consolidate first and then to integrate optional features into the specs. It must be clear that only those optional features will be integrated that match with the existing design and standards choice.
- A set of rules must be defined for assessing whether an epSOS extension to an existing standard/profile should be published on the international, European or national level. In order to increase the sustainability of the specs all epSOS transactions that are relevant for other projects should be published and maintained outside epSOS along the IHE levels (international, European, national).
- The epSOS technical documentation must be consolidated and re-arranged. redundancies must be minimized and experience from the pilot development and testing on “who needs what information” must be considered.
- In epSOS 2, we need to be careful not to rule out any implementation options. Interoperability specifications might not be sufficient: for instance,

central services, semantics specifications are also relevant. The detailed component (NCP-in-a-box) specifications and advice are nice-to-have not must-have.

- epSOS 2 specifications and implementation documents (as deliverable of WP3.A and WP3.B) should include code examples for developers, to help understanding specifications.

## 4.2 Impact for a sustainable deployment and testing strategy

The identified implementation strategies are not in contradiction with the hypotheses upon which D3.9.2 “Testing Strategies and tools” was defined and that were refined and applied in D3.10.1: Test Results.

Both organizational options (i.e. Software Development Consortium and Software Solutions Ecosystem) foster the development of partially common software for all PNs, and then the adaptation/interfacing of these common software to the individual PNs. From the perspective of testing strategy, the important issue in this respect is the thorough testing of common software according to the epSOS specifications, before their adaptation by the PNs. When this is not secured, several PNs will face exactly the same issues due to the common software during pre-PAT or PAT testing. In order to achieve the testing of common software before releasing them to the PNs, the testing team and the common software development team (be it either the consortium or the ecosystem) should have good contact points and act in cooperation.

epSOS 1 has provided a good story to tell around assurance and testing. This is really important but on-line tools and PATs have given us a very practical way forward which I think we should build upon. This allows more flexibility for new suppliers to be able to bring solutions to market.

Based on epSOS 1, epSOS 2 testing strategies, should:

- Identify several test phases, giving to the PN the task and the responsibility to perform them, demonstrating the compliance to epSOS specification and requirement
- Appoint a Third Party (in epSOS 1 IHE Europe) to develop Testing Tools to verify the compliance of the implemented solutions to epSOS specifications
- Establish face-to-face (Projectathon - PAT) and on line testing events / sessions (PAT-on-Line), organized by third parties, to verify the compliance of solutions / services implemented by PNs or Vendors to epSOS Specification
- Run a Pre-Pilot-Testing process with the two-fold goal
    - Perform end-to-end functional testing to identify critical issues, understand and evaluate the clinical risk, propose corrective actions

- Demonstrate the compliance of a service to start treating real patient data

The decision of introducing the PAT-on-Line concept will allow a more flexible and cheap testing process, because PNs and Vendors should not wait for the next PAT to validate systems (service compliance and interoperability), nor too frequent PATs should be funded by epSOS.

The decision to increase the link between the epSOS Projectathon and the IHE Connectathon should allow synergies and the enforcement of the defined ecosystem, if IHE and epSOS specs will become closer and closer.

As a tendency line, if the epSOS specifications are endorsed by International specification bodies like IHE and HL7, epSOS profile tests might become IHE profile tests, avoiding the need for epSOS specific PAT, allowing a long term sustainability.

# 5 Conclusion

epSOS 1 defined three implementation strategies, leaving to PN the role of specifying and implementing, or leaving complete freedom to the market opportunities and open competition, or jointly develop the full proof of concept.

All the PNs opted to adopt the last one, minimizing the risk of non interoperability and covering the lack of the National Infrastructure.

This solution, valid for epSOS 1, shows some limits as for medium long term sustainability.

WT3.B.1 identified that epSOS core responsibility is and remains to specify and support testing for compliance to the epSOS Interoperability Architecture.

The open question is whether epSOS 2 should consider supporting the definition of an “informal” epSOS Software Architecture which includes the specification of a “back-interface”.

The proposed implementation strategies for epSOS 2 offer opportunities to create/enforce the eHealth interoperability ecosystem (through the establishment of a Consortium or through the open competition) to assure market opportunities which might allow sustainability for PNs and Vendors.

The trick is to be able to create an environment in which industry can compete and PNs can choose their preferred way forward (together or apart) and how do we provide specifications, tools and support to enable this in a way that allows for future growth.

Open or Closed source approach may be freely chosen by PNs. However epSOS is in favour of Open Source approach, in line with EC and (some) PN eGov guideline, which may ease the ecosystem creation and long term sustainability.

From the epSOS side, scenarios and specifications and decision on what it had to be provided to PNs, have always to be defined in compliance with the policies defined by WP2.2, safeguarding the PNs investment in epSOS 1, and adopting international standards.

In case of failure of the selected alternative between the Consortium and the Ecosystem, a recovery plan has to be established, to protect the epSOS project LSP, through a JAB-funded development. In this case, open source approach will be preferential.

This implies a proactive co-operation with Standardisation Bodies fostered by the WP3.D activities.

Testing Strategy should follow the paradigm of assuring interoperability through the verification performed by a third independent party who exploits testing tools and procedures developed with the epSOS support.

The concept of reuse in the testing leads to exploitation of the tools and expertise developed and consolidated by IHE Europe in epSOS 1.

In order to close the loop, the generic policies proposed by WP2.2 will need to be carefully instantiated to the needs of concreteness of the epSOS 2 implementation and testing strategy.

# Appendix A Abbreviations

Terms and Definition used in this document are included in the epSOS. In order to ease the reading, most common abbreviation are reported in this appendic abbreviations.

| | |
|---|---|
| CCD | (epSOS) Common Component Design |
| CDA | Clinical Document Architecture |
| eCRTS | epSOS Central Reference Terminology Server |
| eD | eDispensation |
| EDQM | European Department for the Quality of Medicines |
| eP | ePrescription |
| FET | Fraunhofer ISST / Elga and IT consortium |
| GUI | Graphical User Interface |
| HCP | Health Care Professional |
| HCPO | Health Care Provider Organization |
| HLDD | High Level Design Document |
| ID | Identifier |
| IHE | Integrating the Health Care Enterprise – Europe |
| IT | Industry Team |
| JAB | Joint Activity Budget |
| JDBC | Java Database Connectivity |
| JWG | Joint Working Group of Work Packages 3.8 and 3.9 |
| LSP | Large Scale Pilot |
| MS | Member State |
| MTC | epSOS Master Translation/Transcoding Catalogue |
| MVC | epSOS Master Value Sets Catalogue |

| | |
|---|---|
| NC | NationalConnector |
| NCP | National Contact Point |
| NCP-A | National Contact Point of Country A |
| NCP-B | National Contact Point of Country B |
| NI | National Interface |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PAP | Policy Administration Point |
| PD4 | Project Domain 4 |
| PDF | Portable Document Format |
| PDP | Policy Decision Point |
| PEB | Project Executive Board |
| PEP | Policy Enforcement Point |
| PID | Patient Identity |
| PMT | Project Management Team |
| PN | Participating Nation |
| PoC | Point of Care |
| POJO | Plain Old Java Object |
| PoU | Purpose of Use |
| PS | Patient Summary |
| PSB | Project Steering Board |
| SAML | Security Assertion Markup Language |
| SME | Subject Matter Expert |
| SOAP | Simple Object Access Protocol |
| SQL | Structured Query Language |

| | |
|---|---|
| SSL | Secure Socket Layer |
| STS | Security Token Service |
| TPM | Technical Project Manager |
| TRC | Treatment Relationship Confirmation |
| TSAM | Terminology Services Access Manager |
| TSL | Trusted Service List |
| URL | Uniform Resource Locator (world wide web address) |
| WSDL | Web Services Description Language |
| WP | Work Package |
| WS | Web Service |
| XFRM | Transformer |
| XCA | Cross Community Access |
| XDR | Cross-entreprise Document Reliable Interchange |
| XML | eXtensible Markup Language |
| XUR | Cross-Enterprise User Authentication |

# Definitions

| | |
|---|---|
| Central Common Services | A set of central services jointly used by NCPs. |
| Circle of Trust | See epSOS Glossary. |
| Common Software Components | Software components of the NCP-in-a-Transparent-Box |
| Country A | See epSOS Glossary |
| Country B | See epSOS Glossary |
| eDispensing (eD) | See epSOS Glossary. |
| ePrescription (eP) | See epSOS Glossary. |
| epSOS Central Reference | Web tool (based on the HealthTerm system |

| | |
|---|---|
| Terminology Server (eCRTS) | developed and maintained by CareCom) to allow every MS to develop, validate, archive and download to the NCP the MVC and MTC. |
| epSOS Master Translation/Transcoding Catalogue (MTC) | This is the epSOS Master Value Sets Catalogue which contains, in addition to the original terms, their translation in different languages corresponding to the respective Member States and the possible cross-referencing (transcoding) with other code system that are used at the national level. The translation and the cross-referencing (transcoding) is a national responsibility. Providing the content of each country's contribution to the epSOS Member States is under epSOS' responsibility. |
| epSOS Master Value Sets Catalogue (MVC) | Collection of terms used within certain parts of the pivot documents (either parts describing the patient demographics or the clinical problems for example) based on known code systems such as ICD-10, SNOMED CT, ATC, EDQM, UCUM, etc. |
| High Level Design Document (HLDD) | Document describing the concept and high level architecture of NCP-in-a-Transparent-Box |
| Interoperability Architecture | epSOS Interoperability Architecture shall include not only the NCP-to-NCP interoperability specification, but also critical end-to-end requirements/policies and other elements such shared data distributed by shared services-e.g. MTC/MVC). The possible specification of components and of back interface has not to be considered as mandatory part of the epSOS Interoperability Architecture. |
| National infrastructure | It represents all entities where patient or HCP or Health Care records are managed in member states. |
| NationalConnector (NC) | Entity that encapsulates the Nation-Specific NCP Components. The NationalConnector is implemented as a black box having its subcomponents hidden from the NCP |
| Nation-Specific NCP Components | The components of the NCP that will not be developed in common but are still part of the NCP |
| NCP gateway | A gateway system under the control of the NCP that manages all epSOS transactions and which connects the National Infrastructure (NI) to the epSOS backbone. It is a point of entry/exit to/from the NCP, acting on behalf of a HCP (at a PoC) who requires access to a patient's medical data through epSOS, or acting as |

| | |
|---|---|
| | service broker of an epSOS data provider |
| **NCP-in-a-Transparent-Box** | A modular set of software components (Common Software Components) intended to facilitate a NCP implementation that can be used completely or partly by any MS to fulfil NCP obligations. This implementation is not mandatory. |
| Requirements | Definition of all relevant needs (business, functional, non functional, technical and technological) for system specification and implementation |
| Software Component | Software that can be installed or replaced only as an entity to create a scalable implementation (e.g. component can provide directory services, data storage, provisioning, etc.) |