Submitted to the EC on 03/05/2016

COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT Policy Support Programme (ICT PSP)

e-CODEX

e-Justice Communication via Online Data Exchange

ICT PSP call identifier: CIP-ICT-PSP-2009-4
ICT PSP main Theme identifier: CIP ICT PSP 2010 5.2 3: E-JUSTICE SERVICES
Project full title: e-Justice Communication via Online Data Exchange
Grant agreement n°: 270968

D7.6 Architectural Hands on Material
(Update of D7.4)

Deliverable Id : D7.6
Deliverable Name : Architectural Hands on Material
Status : Finalized
Dissemination Level : Public
Due date of deliverable : February 2016
Actual submission date :
Work Package : WP7
Organisation name of lead partner for this deliverable : Italian Ministry of Justice and CNR
Author(s): Marco Velicogna, Giampiero Lupo, Christine Lewis, Madalina Adam, Giulio Borsari, Francesco Contini, Gemma del Rey Almansa, Jose Matías González Bolivar, Zoï Kolitsi, George Pangalos, Yiannis Salmatzidis, Enrico Francesconi, Ernst Steigenga, Natalie Nickel
Partner(s) contributing : DE, ES, GR, IT, NL, RO, UK

Abstract: The Deliverable provides a quick introduction and reference guide for new and potential e-CODEX partners. It describes briefly what e-CODEX is about and identifies which documents a new partner should consult for more detail. It outlines e-CODEX key standards and architecture guidelines, its high level architecture and basic components. An overview of the lessons learned from the experiences of piloting (at architectural level) is also provided. In particular, it describes the technological, organisational and legal issues which new partners will need to address in order to join the project.
## History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes made</th>
<th>Modified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>13/01/2014</td>
<td>Deliverable structure</td>
<td>Velicogna, Lupo, WP1, MB</td>
</tr>
<tr>
<td>0.5</td>
<td>19/05/2014</td>
<td>Assemblage and editing of the 1st draft version for review</td>
<td>Marco Velicogna, Giampiero Lupo, Christine Lewis</td>
</tr>
<tr>
<td>0.6</td>
<td>27/06/2014</td>
<td>2nd version with revisions after the first review cycle</td>
<td>Marco Velicogna, Giampiero Lupo</td>
</tr>
<tr>
<td>0.7</td>
<td>24/09/2014</td>
<td>Revisions after the second review cycle and addition of Chapter 5 on &quot;process and data modelling for e-CODEX services&quot;</td>
<td>Marco Velicogna, Christine Lewis</td>
</tr>
<tr>
<td>0.8</td>
<td>19/11/2014</td>
<td>Revisions after the third review cycle</td>
<td>Marco Velicogna, Ernst Steigenga, Christine Lewis</td>
</tr>
<tr>
<td>0.9</td>
<td>27/11/2014</td>
<td>Document finalization</td>
<td>Marco Velicogna, Giulio Borsari</td>
</tr>
<tr>
<td>1.0</td>
<td>29/12/2014</td>
<td>Final editorial amendments</td>
<td>WP1</td>
</tr>
<tr>
<td>1.1</td>
<td>22/04/2016</td>
<td>Document update from D7.4 to D7.6</td>
<td>Marco Velicogna, Giampiero Lupo, Giulio Borsari</td>
</tr>
<tr>
<td>1.2</td>
<td>29/05/2016</td>
<td>Revisions after review cycle</td>
<td>Marco Velicogna</td>
</tr>
<tr>
<td>2.0</td>
<td>03/05/2016</td>
<td>Final editorial amendments</td>
<td>WP1</td>
</tr>
</tbody>
</table>
## Table of contents

**HISTORY** ........................................................................................................................................... 2
**TABLE OF CONTENTS** .......................................................................................................................... 3
**LIST OF FIGURES** ............................................................................................................................... 5
**LIST OF TABLES** ................................................................................................................................. 6
**LIST OF ABBREVIATIONS** .................................................................................................................... 7
**EXECUTIVE SUMMARY** ....................................................................................................................... 9

### 1. INTRODUCTION ................................................................................................................................. 10
  1.1. SCOPE AND OBJECTIVE OF DELIVERABLE .................................................................................... 10
  1.2. WP7 GENERAL OBJECTIVES AND VISION ..................................................................................... 10
  1.3. METHODOLOGY OF WORK .............................................................................................................. 10
  1.4. RELATIONS TO INTERNAL e-CODEX ENVIRONMENT ..................................................................... 10
  1.5. RELATIONS TO EXTERNAL e-CODEX ENVIRONMENT .................................................................... 11
  1.6. QUALITY MANAGEMENT .................................................................................................................. 12
  1.7. RISK MANAGEMENT ......................................................................................................................... 13
  1.8. STRUCTURE OF THE DOCUMENT ................................................................................................... 13

### 2. INTRODUCTION TO e-CODEX ............................................................................................................ 15
  2.1. WHAT IS e-CODEX? ......................................................................................................................... 15
  2.2. e-CODEX GOVERNANCE LANDSCAPE ............................................................................................ 17
      2.2.1. e-CODEX PROJECT ORGANISATION ....................................................................................... 22

### 3. e-CODEX STANDARDS AND ARCHITECTURE GUIDELINES AND THEIR IMPLEMENTATION ...... 24
  3.1. INTEROPERABILITY FRAMEWORK ..................................................................................................... 24
  3.2. ARCHITECTURAL GUIDELINES .......................................................................................................... 26
  3.3. GUIDELINES: FUNDAMENTAL REQUIREMENT; GENERIC BUSINESS REQUIREMENTS; USE OF MULTILATERAL SOLUTIONS ......................................................................................................................... 26
  3.4. ARCHITECTURE DEVELOPMENT METHOD ....................................................................................... 27
      3.4.1. ITERATIONS ................................................................................................................................. 27
      3.4.2. ARCHITECTURAL DECISIONS BASED ON RESOURCE AVAILABILITY ..................................... 27
      3.4.3. TAILORING OF THE METHOD ..................................................................................................... 28

### 4. ARCHITECTURAL DECISIONS AND COMPONENTS .......................................................................... 29
  4.1. ARCHITECTURAL OVERVIEW ........................................................................................................... 29
  4.2. TECHNOLOGICAL COMPONENTS ...................................................................................................... 29
      4.2.1. THE GATEWAY ........................................................................................................................... 32
      4.2.2. THE CONNECTOR FRAMEWORK .................................................................................................. 33
      4.2.3. e-CODEX EXCHANGE INFRASTRUCTURE TECHNICAL SECURITY ........................................... 34
      4.2.4. THE NATIONAL GATEWAY AND CONNECTOR TESTING PROCEDURES ................................ 35
      4.2.5. PILOT REQUIREMENTS ............................................................................................................... 36
      4.2.6. SERVICE PROVIDER .................................................................................................................. 36
4.3.  CIRCLE OF TRUST AGREEMENT ................................................................. 37

5.  PROCESS AND DATA MODELLING FOR E-CODEX SERVICES: FROM LEGISLATION TO ELECTRONIC CROSS BORDER PROCEDURE ........................................................................... 40

5.1.  FEASIBILITY ........................................................................................................ 40
5.2.  PROCESS ANALYSIS ............................................................................................ 41
5.3.  DATA MODELLING AND ANALYSIS ................................................................... 44
5.4.  PRODUCTION OF XML SCHEMA DEFINITIONS ................................................. 45
5.5.  MAPPING .............................................................................................................. 46
5.6.  SUSTAINABILITY ................................................................................................. 46

6.  PRACTICAL IMPLEMENTATION ............................................................................ 47

6.1.  INTRODUCTION TO EXPERIENCES FROM USE CASES AND ON-GOING PILOTS ................................................................. 47
6.1.1.  CIVIL LAW CASES ....................................................................................... 47
6.1.2.  CRIMINAL LAW CASES ............................................................................... 48
6.1.3.  SYNCHRONOUS COMMUNICATION ................................................................ 51
6.2.  KEY TECHNOLOGICAL AND LEGAL STEPS TO GO LIVE ................................ 51
6.3.  KEY ORGANISATIONAL STEPS TO GO LIVE .................................................... 53

7.  HOW TO START? REFERENCE PACKAGES ......................................................... 57

8.  SUPPORTING MATERIAL (ANNEXES) ................................................................ 61

8.1.  SECURITY AND DATA PROTECTION ................................................................. 61
8.2.  LONG TERM SEMANTIC SUSTAINABILITY PILLARS DESCRIPTION .................... 62
8.2.1. IDENTIFIERS ................................................................................................ 62
8.2.2. CORE LEGAL CONCEPTS ............................................................................. 62
8.2.3. DOMAIN-DOCUMENT MODEL ..................................................................... 63
List of Figures

Figure 1 e-CODEX Partners............................................................................................................................................. 16
Figure 2 e-CODEX and related initiatives (Source: Velicogna and Lupo 2016) ......................................................... 22
Figure 3 The ELF layers of intervention....................................................................................................................... 25
Figure 4 e-CODEX high-level infrastructure representation ..................................................................................... 30
Figure 5 e-CODEX e-Delivery solution generic flow of a message ............................................................................ 31
Figure 6 e-CODEX National solution example (adapted from e-CODEX Deliverable D5.11 Concept of Implementation) ................................................................................................................................................. 37
Figure 7 Coherence between business, routing and data in support of cross border legal procedures .......................................................... 41
Figure 8 International business transactions for FD 2008/909 .................................................................................... 42
Figure 9 Business collaborations in Small Claims ......................................................................................................... 42
Figure 10 Business transactions within BC-001003 Filing a Claim ........................................................................... 43
Figure 11 Business Transaction and its business documents .......................................................................................... 44
Figure 12 Concepts from Small Claims .......................................................................................................................... 45
Figure 13 Domain-Document model ............................................................................................................................... 63
# List of Tables

Table 1 Abbreviations.................................................................................................................. 8  
Table 2 Quality Checklist .......................................................................................................... 12  
Table 3 Risks ............................................................................................................................. 13  
Table 4 Steps to create XML Schemas.................................................................................... 45  
Table 5 Reference documents.................................................................................................... 57  
Table 6 The concepts from the example related to a Core Vocabulary or a Core Legal Concept (in development)........................................................................................................ 63
## List of Abbreviations

<table>
<thead>
<tr>
<th>Acronym /abbreviation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASiCS</td>
<td>Associated Signature Containers</td>
</tr>
<tr>
<td>BPSS</td>
<td>Business Process Specification Schema</td>
</tr>
<tr>
<td>CCBE</td>
<td>Council of Bars and Law Societies of Europe</td>
</tr>
<tr>
<td>CCTS</td>
<td>Core Components Technical Specification</td>
</tr>
<tr>
<td>CEF</td>
<td>Connecting Europe Facility</td>
</tr>
<tr>
<td>CfC</td>
<td>Coordination for Configuration</td>
</tr>
<tr>
<td>CIP</td>
<td>Competitiveness and Innovation Framework Programme</td>
</tr>
<tr>
<td>CMS</td>
<td>Case Management System</td>
</tr>
<tr>
<td>CNR</td>
<td>National Research Council of Italy</td>
</tr>
<tr>
<td>CNUE</td>
<td>Council of the Notariats of the European Union</td>
</tr>
<tr>
<td>Connector</td>
<td>e-CODEX DOMIBUS Connector</td>
</tr>
<tr>
<td>CTP</td>
<td>e-CODEX Central Testing Platform</td>
</tr>
<tr>
<td>DOMIBUS</td>
<td>DOMain Interoperability BUS. Name of the sample implementation of an ebMS 3 message handler done by e-CODEX to connect national back-end systems and the European e-Justice Portal and consisting of two components, the Gateway and the Connector.</td>
</tr>
<tr>
<td>e-CODEX</td>
<td>e-Justice Communication via Online Data Exchange</td>
</tr>
<tr>
<td>e-IDAS</td>
<td>eIDAS – Electronic Identification and Signature (Electronic Trust Services) regulation</td>
</tr>
<tr>
<td>e-SENS</td>
<td>electronic Simplified European Networked services</td>
</tr>
<tr>
<td>EAW</td>
<td>European Arrest Warrant</td>
</tr>
<tr>
<td>ebBPSS</td>
<td>ebXML Business Process Specification Schema</td>
</tr>
<tr>
<td>ebMS</td>
<td>Electronic Business Message Service Specification</td>
</tr>
<tr>
<td>ebXML</td>
<td>Electronic Business using eXtensible Markup Language</td>
</tr>
<tr>
<td>EIO</td>
<td>European Investigation Order</td>
</tr>
<tr>
<td>EPO</td>
<td>European Payment Order</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>ESCP</td>
<td>European Small Claim Procedure</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>eu-LISA</td>
<td>European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice</td>
</tr>
<tr>
<td>FAL 2</td>
<td>Find-A-Lawyer 2 project</td>
</tr>
<tr>
<td>Gateway</td>
<td>e-CODEX DOMIBUS Gateway</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>Acronym /abbreviation</td>
<td>Explanation</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IDABC</td>
<td>Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens</td>
</tr>
<tr>
<td>INEA</td>
<td>Innovation &amp; Networks Executive Agency</td>
</tr>
<tr>
<td>IRSIG-CNR</td>
<td>Research Institute on Judicial Systems of the National Research Council of Italy</td>
</tr>
<tr>
<td>ISA</td>
<td>Interoperability Solutions for European Public Administrations</td>
</tr>
<tr>
<td>ITTIG-CNR</td>
<td>Istituto di Teoria e Tecniche dell'Informazione Giuridica of the National Research Council of Italy</td>
</tr>
<tr>
<td>LSP</td>
<td>Large Scale Pilot project</td>
</tr>
<tr>
<td>LSSG</td>
<td>e-CODEX Legal and Security Sub-Group</td>
</tr>
<tr>
<td>MB</td>
<td>Management Board</td>
</tr>
<tr>
<td>Me-CODEX</td>
<td>Maintenance of e-CODEX project</td>
</tr>
<tr>
<td>MOJ</td>
<td>Ministry of Justice</td>
</tr>
<tr>
<td>NIF</td>
<td>National Interoperability Framework</td>
</tr>
<tr>
<td>p-modes</td>
<td>Processing Modes</td>
</tr>
<tr>
<td>PCT</td>
<td>Processo Civile Telematico</td>
</tr>
<tr>
<td>PD</td>
<td>Primary Deputy</td>
</tr>
<tr>
<td>PEPPOL</td>
<td>Pan European Public Procurement OnLine</td>
</tr>
<tr>
<td>RDF</td>
<td>Resource Description Framework</td>
</tr>
<tr>
<td>REM</td>
<td>Registered Electronic Mail</td>
</tr>
<tr>
<td>s-TESTA</td>
<td>Secure Trans European Services for Telematics between Administrations</td>
</tr>
<tr>
<td>SPOCS</td>
<td>Simple Procedures Online for Crossborder Services</td>
</tr>
<tr>
<td>STORK</td>
<td>Secure Identity Across Borders Linked</td>
</tr>
<tr>
<td>Trust-OK token</td>
<td>The Trust-OK token is a document generated by the e-CODEX DOMIBUS Connector and indicates the result of the connector validation of the sender signature and certificate or information regarding the authentication process of the advanced electronic system used.</td>
</tr>
<tr>
<td>VRD</td>
<td>Vehicle Registration Data</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>XPath</td>
<td>XML Path Language</td>
</tr>
<tr>
<td>XSD</td>
<td>XML schema definitions</td>
</tr>
<tr>
<td>XSLT</td>
<td>Extensible Stylesheet Language Transformations</td>
</tr>
</tbody>
</table>

*Table 1 Abbreviations*
Executive Summary

The e-CODEX project is a Large Scale Project (LSP) in the domain of e-Justice.\(^1\) Its main goal is to improve the cross-border access of citizens and businesses to legal justice in Europe as well as to improve the interoperability between legal authorities within the EU. For this purpose the project will provide a pan-European interoperability layer using common technical standards for connecting existing national as well as European legal systems.

This document provides an introduction and reference guide for new and potential e-CODEX partners. The document presents an overview of the e-CODEX project and deals briefly with its legal, technological, semantic and organisational issues. It also provides references and links to useful documentation for future partners. In particular, the deliverable outlines e-CODEX key Standards and Architecture guidelines (IDABC Architecture Guidelines and ISA - Interoperability Solutions for European Public Administrations\(^2\))\(^3\), its high level architecture and basic components. An overview of the lessons learned from the experiences of piloting (at architectural level) is also provided.

\(^1\)See also http://www.e-CODEX.eu/home.html

\(^2\) The ISA programme is the follow-on of IDABC which came to an end on 31 December 2009. The ISA programme is focusing on back-office solutions supporting the interaction between European public administrations and the implementation of Community policies and activities. For more information see http://ec.europa.eu/idabc/servlets/Doc6ffa.pdf?id=31770.

\(^3\) Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. For more information see http://ec.europa.eu/idabc/en/home.html.
1. Introduction

1.1. Scope and Objective of Deliverable
The scope of the document is to provide clear and simple information to new e-CODEX partners by describing the project and providing references to key project documentation. Architectural Hands on Material also describes how e-CODEX has been designed. More details about other aspects of the project are described by WP2 in the marketing material. Detailed installation and setup guides are described within the prototype work package. This guide is part of e-CODEX’s approach for sustainability and aims to ensure that Member States not yet participating in the e-CODEX project will be able to in the future.

1.2. WP7 General Objectives and Vision
The overall project structure is separated into different work packages which take into account existing building blocks from a number of areas such as the e-Justice Portal, CIP projects (e.g. PEPPOL, STORK and SPOCS), other on-going projects such as ‘Concept for Cross-border Electronic Filing and Delivery for the European Electronic Payment Order’ led by Austria and national projects as appropriate. WP7 provides guidance on how to integrate these assets and best practice with development activities to ensure technical interoperability.

1.3. Methodology of Work
This document is an update of D7.4 Architectural Hands on Material. Activities related to the drafting of D7.4 deliverable involved several e-CODEX partners through telephone calls and exchanges of e-mails. Preparatory work has been carried out to define the structure of the document with strict coordination between WP7 coordinators and WP1. A WP7 conference call was then organised to discuss the structure of the document with all partners involved in WP7 activities and to verify the availability of partners to be involved in drafting the deliverable or in providing useful materials. The Austrian, Greek, Romanian, Spanish and United Kingdom teams offered their support to the Italian team, who coordinated the drafting of this deliverable. The teams worked on drafting specific sections of the document according to their competence. The Italian team, with the support of the United Kingdom team, assembled and revised the deliverable. The draft documents were then circulated within the e-CODEX mailing lists (WP7, LSSG, WP1, MB and PD), revised and further circulated for a second round of comments and revisions. Following a suggestion from WP6, during the second revision cycle, a chapter on process and data modelling in e-CODEX drafted by the Dutch team was added to the deliverable. Due to this relevant addition, a third review cycle was deemed necessary and carried out before submission to the European Commission. The activities have been carried out in strict coordination with the leaders and representatives of all other WPs. D7.4 was finalised in November 2014. D7.6 updates D7.4 by taking into account the decisions, actions and achievements that have taken place between the finalisation of D7.4 and the end of the e-CODEX project in May 2016.

1.4. Relations to Internal e-CODEX Environment
Representing an introduction to the e-CODEX project and its main deliverables, the document is related to previous work of all WPs. WP7 worked in collaboration with WP2, WP3 and the technical
Work Packages (4-6). WPs provided information, documentation and assistance to draft the document. Information and documents refer to the main technological, organisational, semantic and legal aspects of the project.

1.5. Relations to External e-CODEX Environment

The deliverable takes into account information from existing building blocks of running CIP projects (e.g. PEPPOL, STORK, SPOCS), the e-Justice Portal and other EU co-funded and national projects. It also takes into account the role of the e-SENS project, whose objective is to consolidate, improve, and extend technical solutions to foster electronic interaction with public administrations across the EU, which will carry on the results of e-CODEX and other Large Scale Pilot projects and contribute to their sustainability. Moreover, the deliverable provides information to e-CODEX’s external stakeholders and to potential new partners.
1.6. Quality Management

The quality of this deliverable was ensured by following the agreed approach of identifying key issues to be discussed, agreeing on the document structure, finding the key competences needed to draft it and through intense cycles of review, resulting in extensive participation from most of e-CODEX’s partners.

<table>
<thead>
<tr>
<th>Category</th>
<th>Remarks</th>
<th>Checked by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6.1.1.1.1.1. Conformance to e-CODEX template</td>
<td>The document is conformant to e-CODEX template.</td>
<td>EQM, WP7, WP1</td>
</tr>
<tr>
<td>Language &amp; Spelling</td>
<td>The document’s language and spelling has been checked.</td>
<td>EQM, WP7, WP1</td>
</tr>
<tr>
<td>Delivered on time</td>
<td>The document has been delivered with a slight delay. The delay is mainly due to dependence on other deliverables and from the requirement to provide a deliverable as up-to date as possible.</td>
<td>WP7, WP1</td>
</tr>
<tr>
<td>Each technology description contains the correct elements</td>
<td>Item checked.</td>
<td>WP7</td>
</tr>
<tr>
<td>Consistency with description in the TA and in other e-CODEX deliverables</td>
<td>Item checked.</td>
<td>WP7, WP1</td>
</tr>
<tr>
<td>Contents is fit for purpose</td>
<td>Item checked.</td>
<td>WP7, WP1</td>
</tr>
<tr>
<td>Contents is fit for use</td>
<td>Item checked.</td>
<td>WP7, WP1</td>
</tr>
<tr>
<td>Commitment within WP</td>
<td>Item checked.</td>
<td>WP7, WP1</td>
</tr>
</tbody>
</table>

Table 2 Quality Checklist
1.7. Risk Management

The main risks for this deliverable are summarised in the table below:

<table>
<thead>
<tr>
<th>Description</th>
<th>Probability</th>
<th>Impact</th>
<th>Priority</th>
<th>Response</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensibility of the document for external stakeholders.</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Team worked on simplifying the concepts of the e-CODEX project.</td>
<td>WP7</td>
</tr>
<tr>
<td>The need to update the document for new and potential partners will not end with its submission or the end of the project.</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>The document should be updated in follow-up projects (e.g. Me-CODEX) and initiatives</td>
<td>WP7, WP1</td>
</tr>
</tbody>
</table>

**Table 3 Risks**

1.8. Structure of the document

The rest of the document is structured as follows:

Chapter two provides an introduction to the e-CODEX project, the technological infrastructure developed and the project governance.

Chapter three presents the key e-CODEX Standards and Architecture guidelines that have been used and applied in the pilots, including lessons learned from piloting (at the architectural level). It also provides an overview of the Interoperability Framework (European Interoperability Framework for European public services). The Architecture guidelines are based on IDABC Architecture Guidelines for Trans-European Telematics Networks for Administrations. e-CODEX partners took into account an update to these guidelines, the ISA - Interoperability Solutions for European Public Administrations.

Chapter four provides an overview of e-CODEX’s high level architecture and basic components including a description of the main features and functions of the e-CODEX DOMIBUS Gateways, e-CODEX DOMIBUS Connectors (from now on Gateways and Connectors), service providers and

---


6 The ISA programme is the follow-on of IDABC which came to an end on 31 December 2009. The ISA programme is focusing on back-office solutions supporting the interaction between European public administrations and the implementation of Community policies and activities. For more information see http://ec.europa.eu/idabc/servlets/Doc6ffa.pdf?id=31770.

7 The e-CODEX DOMIBUS is a sample implementation of an ebMS3 message handler done by e-CODEX. Member States can use this solution or use other implementations following the e-CODEX requirements. The connection to the national back-end systems and the European e-Justice Portal is channelled by a so-called Gateway. An e-CODEX message flow would start at the back-end application A which sends the message to Gateway A, then sends it to Gateway B, which finally sends it to back-end application B. The functionality necessary for message
network(s) and the legal agreement establishing the technical conditions for the secure transmission of judicial documents and data between e-CODEX partners.

Chapter five describes how process and data modelling (provisioning) for e-CODEX services is carried out in order to support electronically processed cross border legal procedures.

Chapter six introduces experiences from the e-CODEX pilots including short examples of real use cases, a pilot preparation checklist and some key lessons learned to help implementation and piloting. Chapter seven provides a ‘reference package’ of e-CODEX key documentation drafted by various e-CODEX Work Packages.

Finally, the annexes provide a classification of Standards in use within e-CODEX, legal references and EU legal background, and use cases and a description of e-CODEX long-term semantic sustainability pillars.

---

exchange within the Justice domain is not part of the ebms3 / AS4 standard. This is realised in a software component called Connector, which also builds the bridge to the back-end applications.

8 e.g. verify actual practices and discrepancies from the letter of EU Regulations and their general interpretation, involve internal and external users, etc. with some real-life examples.
2. Introduction to e-CODEX

2.1. What is e-CODEX?

As outlined in the European e-Justice Strategy, information and communication technologies (ICT) can be used in the administrative procedures of judicial systems to provide a distinct advantage in terms of improving effectiveness, cooperation between legal authorities and, most importantly, citizens access to justice. This is true both at national and European level.

In line with this strategy, the European Commission co-financed the e-CODEX project to “improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU.”

In a nutshell, the project aims at providing an easier and safer (electronic) access to legal information and procedures in other EU Member States for businesses and citizens; strengthening cross-border judicial cooperation and providing greater effectiveness for cross-border procedures through common standards and greater interoperability of information systems.

e-CODEX is a 66 months, EU co-funded project with a budget of €24m (EU contribution: €12m) running from Dec 2010 to May 2016. It involves 20 countries, mainly through their Ministries of Justice or their representatives, and other institutions such as the CCBE (Council of Bars and Law Societies of Europe), CNUE (Council of the Notariats of the European Union) and the National Research Council of Italy (CNR). e-CODEX features in the Strategy on European e-Justice 2014 – 2018, which has been endorsed by the Council of the European Union and the European Parliament.

---

9 [http://www.e-CODEX.eu/about-the-project.html](http://www.e-CODEX.eu/about-the-project.html)

10 e-CODEX is funded through the ICT Policy Support Programme under the Competitiveness and Innovation Framework Programme (CIP).

11 Based on the adoption of the multiannual action plan on e-Justice 2009- 2013.
The e-CODEX project aims to improve interoperability between legal authorities within the EU with minimum impact on existing national ICT solutions. In this context transport of data and documents is a key element of the solution. Any functionality to be developed for a cross-border e-Justice service necessarily means transport of information from one country to another. The e-CODEX infrastructure translates national standards of documentation to the e-CODEX standard through mapping to ensure reliable transportation of the data. The technology is being piloted in live use cases (i.e. with real parties and real cases). Civil pilots already live include European Payment Order (based on Regulation (EC) 1896/2006), European Small Claims procedure (based on Regulation (EC) 861/2007) and Business Registers (based on Directive 2012/17/EU). Criminal live piloting began with the exchange of sensitive data regarding cross-border crime in the EURegio region within the context of the Mutual Legal Assistance pilot. The pilot was then extended to the European Investigation Order (based on Directive 2014/41/EU). In addition, at the end of the project, the Financial Penalties use case (based on Framework Decision 2005/214/JHA and Directive 2015/413) is in the final stages before going live.

---


13 EURegio: region at the border between Germany (North Rhine-Westphalia), The Netherlands and Belgium

14 [http://www.youtube.com/watch?v=icsac-TQIQQ](http://www.youtube.com/watch?v=icsac-TQIQQ)

15 Natalie Nickel et al. (2016) e-CODEX Deliverable D1.16 Final sustainability report and recommendations (Update of D1.12 Sustainability Plan)
More specifically and from a **technological perspective**, e-CODEX is a multilateral, content agnostic e-delivery infrastructure that uses building blocks from previous EU Large Scale Projects to develop a single pan-European interoperability layer for access to cross-border e-Justice services. This e-delivery infrastructure may be adapted for more generalised use in the government sector within the LSP called electronic Simplified European Networked services (e-SENS), aiming to deliver reusable and tested building blocks for the Connecting Europe Facility (CEF).

The e-CODEX architecture enables the interconnection of service providers through national Gateways and Connectors. No central component is involved in the communication. Additionally, where no national access is provided, the general public should be able to access the infrastructure through the EU e-Justice portal, which is intended as a central entry point for citizens, business and legal professions and should be available from summer 2016.

**e-CODEX services** follow agreed judicial procedures based on EU Regulations and Decisions (e.g. European Payment Order, European Small Claim etc.). While these procedures provide a certain level of standardisation, their functioning relies on national organisations (e.g. courts), procedures (e.g. notification, payment of fees) as well as technologies and specific frameworks (e.g. e-identification, e-signature etc.). When electronic communication crosses national borders, mutual trust and acceptance of the national systems that manage such communication is needed.

To support this, the e-CODEX project has drafted an agreement called the **Circle of Trust** (see Chapter 4.3), signed by all piloting partners. This established a firm basis to recognise exchanged electronic information with a minimum level of organisational requirements needed for operational and technical matters related to, or in connection with, the functioning of the e-CODEX system. The extension of the Agreement beyond the end of the project and the piloting phase is part of the long term sustainability effort, which is one of the scopes of the Permanent Expert Group on e-CODEX related issues established by the Working Party on e-Law (e-Justice) of the Council of the European Union.

### 2.2. e-CODEX Governance landscape

In the last years of the project e-CODEX has extended considerably beyond the people and organisations directly involved in the project and in the use of its services. In order to understand the

---


17 CEF project funded by the European Commission is devoted to stimulate and support projects of common interest for the deployment and operation of digital service infrastructures. For more information please see [http://ec.europa.eu/digital-agenda/en/connecting-europe-facility](http://ec.europa.eu/digital-agenda/en/connecting-europe-facility).


20 Natalie Nickel et al. (2016) e-CODEX Deliverable D1.16 Final sustainability report and recommendations (Update of D1.12 Sustainability Plan)

future evolution of e-CODEX, it is therefore important to have a perspective of the main elements and
events that characterise the project governance and which are not limited to the project itself. This is
particularly relevant given the fact that the project itself formally ends in May 2016 while at the same
time e-CODEX will continue to move forward.

From the very beginning e-CODEX has been in close contact to existing standardisation bodies in order
to provide a solution based on widely accepted standards. In particular, it tried to involve
representatives and professionals of different standardisation organisations such as ETSI and OASIS
into the specification phase in order to make the right decisions and use the standards accordingly.
Also, as previously mentioned, the experience with standards coming from previous LSP projects has
been taken into account. 22

Furthermore, e-CODEX has been in close contact with the latest large-scale project e-SENS (Electronic
Simple European Networked Services), which started in 2013 aiming at consolidating the building
blocks developed by all previous large-scale projects (e.g. e-Signature, e-Identity, e-Delivery and e-
Documents which are relevant in the legal area). e-SENS and especially its e-Justice domain team are
building upon the results of e-CODEX to “identify more specific demands of potential users of
electronically available legal procedures” 23 and are working on extending the piloting activities to
additional judicial areas (e.g. family law, administrative law etc.). Besides this, e-SENS is taking into
account the e-CODEX sustainability action plan 24 and will consider the requirements and actions which
need to be met or carried out to ensure the maintenance and sustainability of the e-CODEX technical
components. e-CODEX is, to some extent, expected to answer some of the challenges posed by its
sustainability, so this can only be acted on by e-SENS in due time. The work on sustainability will
therefore continue in the e-SENS project extension phase during the course of 2016 and early 2017. 25

At a higher EU political level, the discourse generated by the need to ensure the long-term
sustainability of e-CODEX has much increased its institutional visibility and therefore its potential
impact on fields that are outside its sphere of influence as a simple ‘tool’ to support cross-border
communication. As part of this dialogue, e-CODEX sustainability has emerged as a relevant component
to achieve the Digital Agenda for Europe objectives. This has resulted in the explicit mention of e-
CODEX “in the Strategy on European e-Justice 2014–2018 26 and the associated Action Plan 27, both of
which have been endorsed by the Council of Ministers of the European Union and the European
Parliament”. 28

Furthermore, the Council of the European Union (Justice and Home Affairs), in its meeting on

23 e-SENS, Technical Annex, WP5.3 e-Justice Piloting S. 102
24 In e-SENS D3.3 „Report on the integrated view of the LSP strategies” and D3.4 “Preliminary proposal for a
governance body” the e-CODEX sustainability action plan was used as a sources. Furthermore e-CODEX
sustainability experts have been surveyed
25 Natalie Nickel et al. (2016) e-CODEX Deliverable D1.16 Final sustainability report and recommendations (Update of D1.12 Sustainability Plan)
26 See 17006/13
27 See 9714/14
4 December 2014, identified and underlined the need to establish a sustainable framework for the technical solutions developed in the context of the e-CODEX project. In particular, Council (Justice and Home Affairs) “invited the Commission to finalise its internal reflections and submit to the Council solutions for the sustainability of the e-CODEX project in the short and longer terms, on the aspects concerning the future governance of e-Justice at EU level, including the possibility of using an existing EU agency”. The topic of e-CODEX sustainability was addressed again at the informal Justice and Home Affairs ministerial meeting on 30 January 2015. As a result of this high level EU political discourse, the “Council (Justice and Home Affairs) established the expert group on e-CODEX related issues on 15 June 2015”.

Since then the expert group has worked in cooperation with the e-CODEX Management Board and the Commission to find a viable solution for the e-CODEX sustainability “taking into account the principles of voluntary action, decentralisation, interoperability and independence of the judiciary, and the need to take into account the interests of those Member States not currently participating in the e-CODEX project”. While the medium-term sustainability of the technical generic components could be ensured by the “Connecting Europe Facility” (CEF), the e-CODEX system was seen as more than just the sum of the technical parts. In particular, three solutions for the long term were discussed:

1. Firstly, the Commission could be invited to assume responsibility for the continued maintenance of the e-CODEX solutions. However, the Commission may not be optimally equipped for such a form of operational management.
2. A second option could be to assign these responsibilities to one or more Member States. Comparable experiences have, however, shown that this can create structural, organisational and technical difficulties (e.g. the Schengen Information System). Therefore such an approach might not be a viable solution.
3. A third option would be to entrust an existing agency with these tasks. For this purpose, three agencies were identified as possible candidates, eu-LISA, ENISA and INEA.

The Council Expert Group on e-CODEX related issues and the e-CODEX Management Board have worked to identify criteria for involving an existing European agency for the purpose of sustaining and maintaining e-CODEX components. As it has already emerged, the entrusting of the e-CODEX solution maintenance and long-term sustainability has implications which go beyond those one would expect if the object was simply a support tool. In addition to technical capabilities, it is important that the governance of the agency respected and ensured the independence of the judiciary. Accordingly, the “Management Board of e-CODEX has approached eu-LISA, ENISA and INEA to check their respective interest, willingness and approach towards acting as a partner for the sustainability of e-CODEX”. At the same time, it was also recognised that “if an EU agency is made responsible for the full lifecycle of development and operational management of the e-CODEX solutions in the short term and, after due consideration, for the full lifecycle of development and operational management of the

29 Ibidem.
30 Ibidem.
interoperability of decentralised IT systems in the area of e-Justice in general in the long term, a specific legislative instrument to be submitted by the Commission will be necessary”.

As a result of this process, the expert group on e-CODEX recommended that the “Management Board of e-CODEX start contact with eu-LISA, in full cooperation with the Commission, with a view to it taking care of the maintenance of e-CODEX at a date to be agreed between all parties, though preferably no later than 1 August 2018”. It further stressed that “between the end of the e-CODEX project and the uptake by a European agency the maintenance of the e-CODEX assets have to be ensured”, and it underlined that “A first step in this direction was taken by the Commission in its latest call for proposals for an Action Grant on e-Justice”. In its meeting on 3-4 December 2015, the Council of the European Union (Justice and Home Affairs), adopted the roadmap on the sustainability of e-CODEX and “confirmed the importance of a new co-financed project covering the maintenance of the e-CODEX assets”.

Following this lead, a group of e-CODEX leading Member States used the e-Justice call to apply for funding with a proposal for a new project called Me-CODEX (Maintenance of e-CODEX) covering the maintenance of the e-CODEX assets specifically related to the e-Justice service provision. The overall goal of Me-CODEX is to ensure a swift and sustainable transition of the e-CODEX project towards long-term sustainability. It is intended as a bridge between the closure of e-CODEX and the handover to a potential agency that will take responsibility for the daily maintenance of the solutions, on-going development and support to EU Member States and associated countries. The expected result of Me-CODEX is therefore to outline the necessary requirements to an agency that will be charged of ensuring the long-term sustainability of the e-Justice solutions that have been developed by e-CODEX. To ensure the approach undertaken by Me-CODEX to maintain e-CODEX is viable, the consortium will work in collaboration with a number of on-going initiatives. In particular, close collaboration with the Connecting Europe Facility (CEF) should ensure that all the necessary technical components used within e-CODEX are maintained and enhanced where possible. Furthermore, Me-CODEX plan to benefit from its current links with the CEF team of DIGIT and DG CONNECT to position the sustainability needs of Me-CODEX and take part in discussions regarding the future sustainability of all digital service infrastructures and building blocks. This alignment will be key in ensuring a viable and sustainable long-term solution for the maintenance of all e-CODEX solutions and beyond. Furthermore, due to the e-Justice Portal role in providing an entry point for the citizens of “most of the MS”, the involvement of DG JUSTICE in the activities related to e-CODEX solutions maintenance and evolution seems also to be needed.

36 Ibidem, p.9
37 Ibidem, p.9
39 Exact geographic scope to be defined in the future legal act.
40 Natalie Nickel et al. (2016) e-CODEX Deliverable D1.16 Final sustainability report and recommendations (Update of D1.12 Sustainability Plan)
While the area of influence of e-CODEX has extended, a constellation of activities in the e-justice domain have spurred on from the e-CODEX achievements. To cite three initiatives that started at the beginning of 2016:

1. The CCBE, within a EU co-funded project, is planning to connect Find a Lawyer 2 (a tool that allows lawyers to verify e-ID in cross border procedures) to e-CODEX. “Within the framework of e-CODEX, FAL 2 will provide the necessary solution to ensure that the person claiming to be a lawyer is indeed a qualified lawyer in his/her home jurisdiction and is, thus, able to fill in claims on behalf of the client through e-Justice procedures available, for instance, under e-CODEX”. More concretely, a use case on Lawyer2Court communication consisting in testing the participation of lawyers in EPO via the European e-Justice Portal using the outcome of the projects FAL2 and FAL3 has been initiated and will be finalised in the context of the expected Me-CODEX project.

2. Pro-CODEX (Connecting legal practitioners national applications with e-CODEX infrastructure), a EU co-funded project, that has begun to investigate the possibilities and create conditions to make e-CODEX and the applications used by legal professionals (lawyers and notaries) at national level interoperable. e-CODEX has been designed to provide general solutions and is well tailored on meeting national courts’ needs, while the e-Justice Portal should provide a solution for non-repetitive players. At the same time, with exceptions, these solutions are not integrated with the applications that legal practitioners use to manage their business in different member states. At present, private companies providing these systems do not seem interested in developing e-CODEX interfaces due to the limited number of users. In this perspective, Pro-CODEX will provide the means to extend the user bases of e-CODEX investigating the issues related to the connection of legal professionals applications to e-CODEX infrastructure and develop running pilots in a limited number of countries.

3. The ‘API for Justice’ EU co-funded project, coordinated by the Dutch Ministry of Justice aims to open up the infrastructure for cross border legal services provided by e-CODEX and the European e-Justice portal, by means of an API (Application Programming Interface). This would make it possible for third parties to build applications which use the e-CODEX services.


43 As the work to link FAL2 with e-CODEX will take more time than first expected, the work on FAL3 needs to be postponed. This means that the testing of the Lawyer2Court use case will be done after the end of e-CODEX. Source: e-CODEX Deliverable D3.13 Update of D3.4 Test Findings of Tests.
2.2.1. **e-CODEX project organisation**

Because the organisation of the e-CODEX project will end soon, a short description of the distribution of tasks and competences may help in understanding the results and processes which led to them. The e-CODEX project distributed its tasks and competences in seven core work packages covering various aspects including coordination, communication, technological development and implementation, testing and operational aspects in real live systems.

In particular, the three work packages that deal with the overall project coordination, high level architecture and piloting are:

- **WP1 - Project administration and sustainability** – deals with project progress monitoring and quality assurance, budget monitoring and Community funds allocation. The work package manages and maintains contacts with the European Council and Commission.

- **WP3 - Piloting and experimenting** – has the task of selecting, implementing and testing e-justice services based on the components developed in the ‘technical’ work packages (WP4, WP5 and WP6). WP3 monitors technical testing of components before the piloting stages go live.

- **WP7 Architecture**—focuses on high-level architectural issues such as the identification of high-level and common functional requirements (what the system is supposed to do) and non-functional requirements (how the system should be) and high-level decisions (e.g., the reuse of pre-existing components). WP7 also supports the coordination of the activities of technical work packages (WP4, WP5 and WP6 activities).

A single work package, **WP2 – Communication** –, is dedicated to the activities of communication and sharing of information about e-CODEX to stakeholders and potential partners.
Three work packages are dedicated to technical aspects of the e-CODEX project. These work packages cover three areas of development of the core technical interoperability components.

- **WP4 - e-Signature and e-Identity**: deals with identity for natural and legal persons, roles, mandates and rights/e-Signatures. The work package works on issues such as user authentication and authorisation. It is in charge of the development of the Trust-Ok Token.

- **WP5 - e-Delivery and e-Payment**: deals with issues regarding exchange of documents and data. It manages the development and implementation of e-CODEX e-delivery infrastructure (Gateway and Connector). The work package works on the implementation of building blocks and on the update of software components, as well as any related e-Payment services for each pilot use case, in collaboration with the e-Justice portal.

- **WP6 - Documents and Semantics**: Document standards – mainly deals with issues of semantic interoperability. In particular, it works on the semantic aspects of the documents and metadata involved in the project.

Aside of the work packages, two other bodies play a fundamental role in the project governance: the Management Board and the General Assembly.

The **Management Board** includes, among other actors, the project coordinator and the WP leaders. The body monitors the effective and efficient implementation of the project, supports the project coordinator in preparing meetings with the European Commission and makes proposals to the General Assembly in relation to relevant topics such as rearranging tasks and budgets. The Management Board is responsible for the proper execution and implementation of the decisions taken in the General Assembly, to which it is accountable.

The **General Assembly** is composed of one representative per partner with each country having one vote. It is the ultimate decision-making body of the project. The General Assembly meets twice a year. The body mainly ratifies decisions and proposals from WPs and the Management Board.

During the project’s activities the necessity of dealing with particular tasks and bringing together experts in specific fields brought about the creation of specific sub-groups and special ad hoc units. In particular, the **e-CODEX Legal and Security Sub-Group (LSSG)**. The LSSG is composed of legal experts from within the project but also from outside, with experience in EU and Member States’ law. It deals with mapping of the EU and national norms that are relevant for the project’s aims. It also studies how EU laws are interpreted and implemented by various Member States. Furthermore, it promotes the harmonisation and interpretation of EU law and its application in Member States. The LSSG drafted the “Circle of Trust” agreement (see section 3.3) which has been signed by partners participating in the pilots.
3. e-CODEX Standards and Architecture guidelines and their implementation

3.1. Interoperability framework

The e-CODEX partners relied on the EIF (European Interoperability Framework for Pan-European e-Government Services)\[^{44}\] for European public services version in order to support the interoperability of different system’s components (see fig. 2).\[^{45}\]

The EIF supports cross-border and cross-sector interoperability and guides public administrations in reaching this objective. It also supports the integration of various National Interoperability Frameworks (NIFs) by indicating common elements such as principles, policies, guidelines, recommendations and standards. EIF can be considered as a ‘meta framework’ that establishes generic principles in common between several NIFs which are, in general, more detailed and often prescriptive. The EIF promotes and supports the delivery of European public services by fostering cross-border and cross-sector interoperability and guiding public administrations in their work to provide European public services to businesses and citizens. It also complements and ties together the various National Interoperability Frameworks (NIFs) at European level. The e-CODEX project focused on four EIF layers of intervention: legal interoperability, organisational interoperability, semantic interoperability and technical interoperability.

Reaching legal interoperability refers to the reduction of incompatibilities between legislation in different Member States. The e-CODEX team worked in particular on analysing the discrepancies between national legislation and the European procedural norms. Moreover, an agreement between e-CODEX Member States, called the “Circle of Trust” deals with the issue of legal interoperability establishing that partners providing services via e-CODEX may trust each other in terms of confidentiality, e-Identification and e-Signature.

Organisational interoperability refers to the cooperation between organisations to achieve mutually agreed goals and implies integrating business processes and related data exchange. Semantic interoperability aims at ensuring that the precise meaning of information that is shared between parties is understood and preserved throughout these exchanges. Therefore it consists of developing vocabulary to describe data exchanges and ensuring that all communicating parties understand data elements in the same way.

Technical interoperability refers to technical aspects of linking information systems. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange. In the e-CODEX environment, the team made use of formalised specifications and standards mainly pursuant to EU Directive 98/34.\[^{46}\]

e-CODEX Deliverable D7.1 (Chapter 5) shows the e-CODEX perspective on interoperability layers with reference to EIF. EIF also shows 12 general principles of good administrations.

- Principle 1: Subsidiarity\[^{47}\] and proportionality.

---

\[^{44}\] http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529

\[^{45}\] e-CODEX Deliverable D7.1 Governance and Guidelines Definition


\[^{47}\] Subsidiarity is a basic principle of the IDA(BC) architecture. It refers to the autonomy of the business partners that make use of the internetworking architecture. While business partners exchange or share information, they...
The 12 principles describe the context in which European public services are decided and implemented. Moreover, they complement one another regardless of their different natures, e.g. political, legal or technical.

![Figure 3 The EIF layers of intervention](http://ec.europa.eu/idabc/servlets/Doc3470.pdf?id=19280)

---

Cooperating partners with compatible visions, aligned priorities, and focused objectives

- Aligned legislation so that exchanged data is accorded proper legal weight
- Coordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal
- Precise meaning of exchanged information which is preserved and understood by all parties
- Planning of technical issues involved in linking computer systems and services

Political Context

- Legal Interoperability
- Organisational Interoperability
- Semantic Interoperability
- Technical Interoperability

---

must be able to choose their own policies and practices (i.e. technological approach, legal framework, principles of management, etc.). The internetworking model of the IDA(BC) architecture offers and safeguards this autonomy by means of separation between a central, common infrastructure, the EuroDomain or Internet, and the local networks of the business partners, the LocalDomains. Access to the common infrastructure is offered by network interfaces called EuroGates or by Internet Service Providers.

3.2. Architectural guidelines

The e-CODEX architecture has been designed following the Architecture Guidelines for Trans-European Telematics Networks for Administrations, Version 7.1 (IDABC)\(^{48}\) and the follow-on ISA guidelines.

First, decentralised responsibility that allows business partners concerned with trans-European networks to organise the data processing systems, the networks, the technological approach and the legal framework in a way best suited to their practices. The decentralised responsibility also means autonomy of the business partners to select the architecture of their own IT solutions, the service provider, policies and legal framework. At the same time, the partners’ architectural and technological solutions must adhere to e-CODEX standards, while policies and legal framework must match the EU regulations the e-CODEX services are built upon.

Second, the use of a web service model as a key technology for setting up interoperable services which refers to reusable services based on standard interfaces and protocols that any application, running on any web-enabled infrastructure, can be designed to support.

Third, the guidelines support the separation between a central, common infrastructure, the EuroDomain or Internet, and the local networks of the business partners, the LocalDomains. Access to the common infrastructure is offered by network interfaces.

Fourth, the guidelines also support the reusability of components, which brings economy of scale and shorter implementation time. In the e-CODEX environment this supports both the “reuse” of national systems already implemented which will be kept unchanged (unless a partner decides to build its system from scratch) and also the e-CODEX components which are reused and adapted from other EU and open source projects and are intended to be reused by other EU projects (e.g. e-SENS).

Fifth, the guidelines indicate the advantages to opt for a multilateral solution instead of bilateral solutions.

The IDA guidelines influenced the team’s choices in terms of architecture design leading to a reduction in modification of national systems, the conversion to e-CODEX standards performed by National Gateways and a system based on full trust of other Member States on confidentiality, e-Identification and e-Signature.

3.3. Guidelines: Fundamental Requirement; Generic Business Requirements; Use of Multilateral Solutions

The fundamental and generic business requirements of the e-CODEX Architecture are provided in e-CODEX Deliverable D7.1.\(^{49}\) The fundamental requirements specify a decentralised architecture and interoperability between heterogeneous systems. A decentralised responsibility involves business partners organising their data processing systems and networks in a way best suited to their practices. On the basis of this principle, Member States maintain their current national systems and connect them to the e-CODEX architecture, which has the main aim of “translating” data from national standards to the e-CODEX standards. The fundamental requirements also indicate the importance of reaching interoperability between heterogeneous systems achieved via a common architecture at European level. This is also a direct consequence of a decentralised architecture.

\(^{48}\) The guidelines support a set of technical and organisational specifications.  

\(^{49}\) Chapter 3.5.2 of e-CODEX Deliverable D7.1 Governance and Guidelines Definition
Generic Business Requirements address the following information process elements:

- First, data exchange with regard to users who need to exchange, share and manage information inside the user community with trusted partners or outside the user community with external non-trusted partners.
- Second, data collection that refers to data gathered from distributed sources into a European data collector (hosted e.g. by Commission, Agencies, etc. Given the specific requirements of the current e-CODEX use cases this element has not yet been developed).
- Third, data dissemination with reference to the data centrally stored, accessed from distributed points by query/answer processes (given the specific requirements of the current e-CODEX use cases this element has not yet been developed).
- Fourth, data sharing regarding users who need to search, query, access and optionally retrieve information wherever this information is located (given the specific requirements of the current e-CODEX use cases this element has not yet been developed).
- Fifth, the element of alert. This refers to a type of communication based on a kind of “push” mechanism. In this case, communication follows a certain event and reaches its recipient within a defined time scale.

e-CODEX architecture is also based on the use of multilateral solutions. Interoperability partners establish collaboration agreements and develop common solutions instead of implementing bilateral arrangements, because this would create the need for maintenance of a multitude of solutions and agreements.

3.4. Architecture Development Method

The e-CODEX team relied on the TOGAF (Open Group Architecture Framework) guidelines as an architecture development method. With reference to the TOGAF guidelines, e-CODEX Deliverable D7.1 indicates the following methodological aspects.

3.4.1. Iterations

This regards the iteration cycles for the revision of e-CODEX software and architecture. Following TOGAF methodology, WP7 has maintained an on-going coordination with WP3 and technical WPs in order to adapt the architectural model to changing requirements.

3.4.2. Architectural decisions based on resource availability

The e-CODEX team relied on the principle of reusable components. Therefore, the architecture implementation had the aim of using the resources available from current national systems. The

---

50 e-CODEX Deliverable D7.1 Governance and Guidelines Definition, Chapter 3.5.2
51 See e-CODEX Deliverable D7.1 Governance and Guidelines Definition, Chapter 5
52 http://pubs.opengroup.org/architecture/togaf9-doc/arch/
53 e-CODEX Deliverable D7.1 Governance and Guidelines Definition, Chapter 3
54 The iteration and revisions cycle interested also the e-CODEX deliverables which, in their updated versions, crystallise the evolving high level architectural decisions on technical and methodological aspects.
creation of an overarching architecture framework influenced and guided the work of the other technical work packages (WP4, 5 and 6).

3.4.3. Tailoring of the method
The e-CODEX team worked on the adaptation of TOGAF methodology on the basis of resources available. For example, division of work in Work Packages represents what TOGAF calls an “Enterprise Architecture Capability” with WP7 being the architecture board.
4. Architectural Decisions and Components

4.1. Architectural overview
This section describes the main e-CODEX technological components, its legal basis and their governance. The following paragraphs provide more detail on the main components of the e-CODEX architecture: the National Gateways and Connectors, which constitute the e-Delivery infrastructure. User interface\(^{55}\) with the e-Delivery infrastructure is provided by a Service Provider, which is a national system maintained by a piloting country or by the European Commission (the European e-Justice Portal). In addition, e-CODEX has also developed a default implementation of the Connector framework that works ‘out of the box’ and without any further adaptations, called a Standalone connector.\(^{56}\)

The organisational and legal issues that arise due to connections between very different justice systems and e-Justice systems has been managed by an agreement called the Circle of Trust that binds the piloting countries. The Circle of Trust provides a mechanism for the recognition of information exchanged across borders between partners in e-CODEX.

As architectures, their technological components and the Circle of Trust agreement will need to change with time in order to adapt to external changes and to improve. This chapter also provides a short description of e-CODEX governance mechanisms.

4.2. Technological components
As previously mentioned, from a technological perspective e-CODEX is a multilateral, content agnostic, e-Delivery infrastructure that uses building blocks from previous large scale projects to develop a single pan-European interoperability layer to support cross-border e-Justice services. The e-Delivery infrastructure consists of two main elements, which are the Gateway\(^{57}\) and the generic Connector framework handling the e-CODEX specific functionalities and components. Once the Gateways and National Connectors are up and running they provide the e-Delivery functionalities required to get pilots running.

The main function of the Gateway is the exchange of messages with other Gateways while the National Connector carries out the adaptations required by its corresponding Service Provider (see Figure 4 e-CODEX high-level infrastructure representation, including two national examples and the e-Justice portal access for EU citizens, companies and legal practitioners who do not have access to /prefer not to use a national solution).

---

\(^{55}\) Within the components provided by e-CODEX no user interface exists. User interaction is foreseen only in the national end systems connected to the e-CODEX components.

\(^{56}\) Rödlich F., González M. (2016) e-CODEX Deliverable D5.13 WP5 Final Report

\(^{57}\) The Gateway has been developed building on Holodeck (a B2B free open-source software for B2B messaging, based on the OASIS specifications for ebXML Messaging version 3 and AS4 profile), but is now evolving independently.
The generic flow of a message through the e-CODEX e-Delivery solution is sketched in Figure 5 e-CODEX e-Delivery solution generic flow of a message. The description of the various components of the figure and of the data and information flows is provided in the following paragraphs.
The following sections provide a more detailed description of the technical components, including reference to technical functionalities, testing procedures and pilot requirements.
4.2.1. The Gateway

**Technical functionalities**

The Gateway of the e-CODEX project is a piece of software that is responsible for several tasks. The basic functionality of the Gateway is for e-Delivery, which is the exchange of messages between partners. This functionality is performed by the whole set of modules within the Gateway.

Each Gateway’s features, and modules that provide it, are listed below:

- Compliance with a set of standards:
  - ebMS 3.0 standard: Gateway interchange messages complying with the ebXML standard. The message transformation takes place in the Connector. The Connector then forwards the content to the Gateway (Webservice or JMS interface). The Gateway then creates an ebMS message, which is in ebXML format.
  - Standard ETSI-REM TS 102 640-2 V2.1.1 for the implementation of evidences (for messages exchanged between Gateways): a) evidence by the sending Gateway; b) evidence by the recipient Gateway; c) evidence by the recipient Connector.
  - Core Components Technical Specification (CCTS) meta models and rules necessary for describing the structure and contents of conceptual and physical/logical data models, process models, and information exchange models.

- p-modes configuration: the way ebXML messages are sent and processed between two Gateways is defined by the p-modes files. The p-modes Configuration tool is used for managing these files.

- Security: The Security module signs and encrypts the communication between the different Gateways.

- Reliability: The Reliability module implements Reliability and Quality of Service configurable behaviour (AS4 is used here – not WS-Reliability or WS reliable messaging).

- Logging: the Logging module enables the administrator to configure log levels and choose the log medium to be used (database or file).

- Web service interfaces: The Backend interface for communications with the national Connector is implemented in the web service interface. Communication between Connector and Gateway is performed through a web service interface. Starting with Version 2, a Java Messaging Service Interface is provided.

For further detail of the modules that make up the Gateway and their implementation you should go to e-CODEX Deliverable D5.11 (Concept of Implementation).\(^\text{58}\)

**Installation procedures**

The Gateway software is provided by e-CODEX as a software package ready to be installed and used. The e-CODEX starter kit describes where to find the software of the Gateway and gives references to other documents needed in this context, e.g. the Installation manuals. Sustainability of the e-CODEX Gateway is described in the Sustainability Plan.\(^\text{59}\)

\(^{58}\) The document can be downloaded at http://www.e-CODEX.eu/

\(^{59}\) e-CODEX Deliverable D1.16, Sustainability Plan (update of D1.12 and D1.7). The document can be downloaded at http://www.e-CODEX.eu/
4.2.2. The Connector Framework

Technical functionalities

According to its particular settings, each e-CODEX participant must perform some adaptations to the messages. The Connector Framework provided by e-CODEX is a generic set of modules which aims to provide the common functionality which is needed by every piloting MS. The MS specific parts will need some specific and dedicated implementation using well-defined interfaces and most participants have found it relatively easy to make these adaptations.

The Connector framework implements two workflows, one for sending messages from the national backend system to the Gateway (outgoing workflow) and the other one for receiving messages from the Gateway and forwarding them to the national backend system (incoming workflow).

The Connector consists of a controller that implements and controls the whole workflow between the components. The connection of the Connector to the national Backend System must be provided by the MS and be configured as a plugin. For internal use, e.g. storing message IDs, a small database is needed. Deliverable D5.12 (Developed Modules) chapters describe the components in more detail.

The incoming workflow consists of the following steps:

1. The Connector queries the pending messages from the Gateway and downloads them.
2. Then the Trust-Ok token\(^{61}\) of the incoming message is validated and a piece of evidence is created and sent back to the Gateway to inform whether the message has been accepted or rejected.
3. Afterwards the content is transformed (if necessary) to the national format and the message is sent to the national backend system.
4. It is MS specific how the Connector checks if the message has been delivered to the national system. A timer starts and when it expires with no news from the national backend system it considers that the message has not been delivered. (evidence: Delivery/NonDelivery)
5. The real retrieval of the message by the end recipient is also expected and the result is also sent back as an additional piece of evidence (Retrieval/NonRetrieval) to the Gateway. A second timer analogous to the former is used here.

\(^{60}\) The document can be downloaded at http://www.e-CODEX.eu/

\(^{61}\) The Trust-OK token is a document in PDF (human readable) and in an XML (machine readable) format that is included in the ASICs envelope (see chapter 5.2.2) and that indicates the result of Connector’s validation of the sender signature and certificate or information regarding the authentication process of the advanced electronic system used. The result of the validation (trustworthy - not trustworthy) is indicated in the Trust-OK token document. The message is sent independently from the result of the validation. The idea behind the Trust-OK token is to provide the possibility for the receiving party (e.g. a judge) to recognise documents that have been filed by using a trustworthy advanced electronic system based on signature or authentication.

By using the token in accordance with the “Agreement on a Circle of Trust”, the receiving party does not need to validate the signature and the certificate itself. Regardless of the signature assessment by the Trust-OK token, the receiving party still has the right and is granted the means to revalidate the signature independently (Deliverable 4.8: Concept for Implementation of WP4 (Update of D4.2); the document can be downloaded at http://www.e-CODEX.eu/).
The outgoing workflow consists of the following steps:

1. The Connector queries the pending messages from the national backend system and downloads them.
2. Afterwards the content is transformed (if necessary) to the e-CODEX format.
3. The Trust-OK token is created by checking the signed PDF or, in the case of an advance electronic system, by default.
4. The ASiCS container, an envelope in which the form and the attached pdf documents are included, is also created.
5. A piece of evidence to inform the national backend system on the progress of the message is created. In case of errors, a rejection evidence is sent back to the national subsystem immediately (evidence: SubmissionAcceptance/Rejection).
6. The National Connector forwards -via the backend web service- to the Gateway the message content, the ASiCS container and the Evidence. The Gateway collects them and creates the message according to the ebMS 3.0 standard.
7. The National Connector then waits for the acceptance of the message from the Gateway to forward the evidence with the confirmation of acceptance for the national backend system. A timer starts and if it expires NonDelivery and NonRetrieval Evidence will be send to the national backend system.

Standalone Connector:
As previously mentioned, e-CODEX has also developed a default implementation of the Connector framework, which works out of the box without any further adaptations. This version exists for all piloting MS which do not have any national system in place to be connected to e-CODEX but still want to participate within e-CODEX.  

Installation procedures
The source of the Connector Framework components is available on the NEXUS server as well as on the Joinup homepage. Within the source you will find additional documentation describing the different methods and parameters in more detail.

To download, install and start the Connector Framework please refer to the Quick Start Guide and the appropriate Installation Manual. In particular, the guide on how to configure the Connector is included in the Connector Framework Installation Manual.

4.2.3. e-CODEX exchange infrastructure technical security
As a default, e-CODEX communication between Gateways takes place over the Internet. Security of e-CODEX over Internet is amongst other means, provided by the TLS and 2-way SSL protocol (in 5th layer of OSI model). Compared to the use of private networks, the usage of the Internet for e-CODEX exchanges means that the network is open for all participants allowed by the e-CODEX community.

62 The acceptance evidence originates from the receiving MS, see steps 4 and 5 of the Connector incoming workflow.
64 Based on Moelker et al. (2015) e-CODEX WP7 Report - e-CODEX exchange infrastructure technical security analysis - v1.0
The default e-CODEX infrastructural interchange implementation foresees multiple means for confidentiality assurance:

- Deployment of 2-way SSL will prevent ‘man-in-the-middle attacks’ for both sending and receiving partner are identified and authorised by mutually agreed certificates.
- Through operation on a public network ‘Internet’ privacy is obtained by channel encryption resulting in a temporary private section on this channel for the duration of the exchange of a certain message.
- In addition to the transport channel being encrypted, the messages themselves are also signed.
- Further security means are provided by the possibility to encrypt message content on top of the previously mentioned message encryption and channel encryption.

Unlike default usage of the Internet where anyone can connect to anyone on any topic at any given time, adopting the ebMS standard for communication will restrict the usage to mutually acknowledged and authorised partners, each operating in a predefined business context. This in combination with the security provisions mentioned above will prevent information being compromised or being sent to unintended recipients.

For specific procedures, the use of s-Testa has been considered but not piloted as the default infrastructure technical security has been assessed as adequate for the present security requirements.

### 4.2.4. The National Gateway and Connector testing procedures

Deliverable “5.5 Description of tested functions and the outcomes” establishes a common protocol for testing. The testing activity covers message flows from the national Connector of the issuing Member State to the national Connector of the receiving Member State. Once a piloting country has the Gateway and the Connector up and running, it has to follow and fill out the test sheets provided by WP3 in order to document the Gateway-to-Gateway and Connector-to-Connector tests. Another option is to use an automatic testing tool (Central Testing Platform - CTP).

#### 4.2.4.1. Central Testing Platform (CTP)

During the tests for the first pilot - EPO - it was recognized that the test time could be shortened considerably by giving the piloting partners the chance to make all functional and use case specific tests before starting the tests with other partners. It was therefore decided to develop a Central Testing Platform as a separate tool simulating a complete e-CODEX infrastructure for all use cases and to provide a full e-CODEX test environment for sending and receiving test messages for all the existing e-CODEX pilots. One of the main difficulties was to setup such a tool very quickly after recognising its importance. Fortunately Greece volunteered not only to implement the CTP but also to host it and

---

65 s-TESTA (Secure Trans European Services for Telematics between Administrations) is the European Community’s own private, IP-based network dedicated to inter-administrative requirements and providing guaranteed performance levels. s-TESTA has been created to offer a telecommunications interconnection platform that responds to the growing need for secure information exchange between European public administrations. [http://ec.europa.eu/idabc/en/document/2097/5644.html](http://ec.europa.eu/idabc/en/document/2097/5644.html)
provide access to all piloting partners. The CTP started with the EPO use case and then extended to include Small Claims, Mutual Legal Assistance and Business registers.  

4.2.5. Pilot requirements

The Connector Framework must be “customised” to the e-CODEX participant requirements/environment, but from a pilot use case point of view only the use of the XML schemas defined by e-CODEX is relevant. Pilots require adaptations in the Content Mapper module.

The e-CODEX Gateway is content agnostic. Therefore, only the way that messages are handled needs to be considered from a pilot use case point of view. This is defined by the p-modes files.

For each pilot use case, any event affecting the business processes (new actors, new documents, modification to the process, etc...) requires the p-modes to be created or modified.

Please refer to the document “roles and responsibilities for piloting” which contains detailed procedures on how to become a piloting participant.

4.2.6. Service provider

A Service Provider is an application that is maintained by the piloting countries (i.e. the national solution which allows e-filing of national cases which has been adapted to satisfy e-CODEX requirements or an ad-hoc solution) or by the European Commission (the European e-Justice Portal). In order to be a Service Provider a system must be able to deliver a service in conformity with e-CODEX standards (security standards, privacy, etc.) in the field of e-justice and be connected to a Gateway through a Connector of an e-CODEX partner.

Its main functions are to create, send and receive the documents and data required by one or more e-CODEX enabled services, and allow electronic signing or authentication of the user if an authentication-based advanced electronic system is used. The advanced electronic system can be either based on an electronic signature or authentication and must have the following characteristics:

1. The document is uniquely linked to the user;
2. The system is capable of identifying the user;
3. The document is created using means that the user can maintain under his control and any subsequent change of the data is detectable.

A Service Provider can be a governmental solution or a private solution. In other words, depending on the use case, or on the role of the user, the Service Provider can be a national application maintained by the participating country’s government, the e-Justice portal or another application used by legal professionals. In order to be connected, the system must undergo an audit from the MS owner of the Gateway and Connector. The figure below (Figure 6 e-CODEX National solution example) demonstrates the Austrian governmental solution.

68 D3.3 Documented System Requirements and Specifications
69 Cf. e-CODEX Deliverable D7.5 Requirements Finalisation & D3.11 Described Test Scenarios
70 Source: e-CODEX Deliverable D5.11 Concept of Implementation.
4.3. Circle of Trust agreement

The Circle of Trust is an agreement drafted by the e-CODEX Legal and Security Sub-Group and signed by the e-CODEX piloting parties. While on-going EU legislative action, especially e-IDAS and the e-Justice Regulation, are likely to address such general and specific conditions for establishing trust and mutual acceptance of national systems, at the time when the e-CODEX pilots are taking place such legal frameworks are not in place. As a result, when exchanging information across borders, piloting partners71 in the e-CODEX project currently lack a legal basis to recognise the information exchanged. The approach taken in the project was to elaborate these needs and set them out in an Agreement, which was adopted by the e-CODEX General Assembly and will cover the duration of all e-CODEX piloting activities. The “Agreement of the Circle of Trust” forms therefore a firm basis for the recognition of information exchanged across borders between piloting partners in e-CODEX. When partners are ready to join a pilot they must declare to the e-CODEX Coordinator that they comply with the terms of this agreement (declaration of accession). This agreement may become redundant and needs to be amended if a European regulation or other legislation enters into force.

The concept of the Circle of Trust is simply that if the information is trusted by the state where it originates from, then it may also be trusted by the receiving state/s, subject to certain conditions. A Circle of Trust is understood as the mutual recognition between Member States of electronic data, documents and signatures within the existing legal framework. In order to fall within the scope of the

71 For piloting partner it is meant a Member State or an Organisation that wants to participate in an e-CODEX pilot by developing its National e-CODEX building blocks. The participation in the pilot does not end with the testing stage of the pilot but continues during the live phase. At this stage, the service implemented is up and running and can be utilised by the users.
Circle of Trust, the document must originate from an advanced electronic system and must be accompanied by a Trust-OK token issued by the Sending Connector, indicating whether the Document is considered as trusted or untrusted in the original country of trust.

Both signature-based and authentication-based Advanced Electronic Systems are accepted. The specific requirements for electronic documents and the Trust-OK token are set out in the Circle of Trust Agreement and its Annexes.

The establishment of a Circle of Trust creates the conditions that will allow the Receiving Gateway, upon receipt of a message from the Sending Gateway, to forward the message to the receiving Connector without requesting further authentication from the Sender. The receiving Connector shall process the message in accordance with the laws of the Receiving State. In relation to the sending party, the receiving state shall have no obligation to carry out a verification of the authenticity and integrity of the document(s) but may rely on the information provided by the Trust-OK token.

Traceability and trust is also supported by means of evidences. For each message, each of the Sending Connector and the Receiving Connector shall issue time evidences as further detailed in the agreement in order to allow the sender and the recipient to identify the points of time that are legally relevant.

The parties to the agreement agree and undertake to use all their best efforts to cooperate effectively and in a timely way to strengthen the functioning of the e-CODEX System. For this purpose, they appoint Contact Points who are responsible for the operational and technical matters related to or in connection with the functioning of the e-CODEX System. They also set up their Gateways within the e-CODEX System and they communicate and exchange information in order to avoid any risks associated with non-receiving or non-sending of messages or the partial or total failure of the e-CODEX System.

Security and data protection issues are considered very important by e-CODEX partners. The relevant provisions at EU-level and at national level have to be respected. This is why the parties of the agreement have to make sure that they adopt all necessary technical and organisational measures to guarantee personal data security and prevent the alteration or loss of, or unauthorised processing of or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).

All e-CODEX project partners who are piloting in at least one of the pilots must become partners to the agreement. The agreement is open for all countries participating in the e-CODEX project (Member States of the European Union and Associated Countries).

Any amendment of the Circle of Trust Agreement requires approval by the General Assembly in accordance with the Consortium Agreement. However, amendments to Annex 2 (the list of piloting partners who have acceded to the Agreement) does not require such an approval but is maintained by the e-CODEX Coordinator, who will distribute the list to the e-CODEX partners after each accession or termination by a piloting partner.

It is important to note that the Circle of Trust Agreement is only valid for the duration of the e-CODEX project. With the connection to the European e-Justice Portal and the Me-CODEX project, a proposal for the extension of the Circle of Trust agreement was formulated and accepted. At the same time,
during the e-CODEX Legal and Security Sub-Group meeting of the 25th of January 2016 the participants discussed the potential need to amend the content of the Trust OK Token but agreed not to make any changes due to the limited time available before the end of the project. It was nevertheless recognised that this issue will most likely rise again after the end of the project (in the Me-CODEX project). The need for an amendment of the Circle of Trust due to the implementation of the eIDAS Regulation has also been discussed. The regulation provides for a mutual recognition of e-signatures for national online service offered by or on behalf of a public sector body if the foreign e-signature is of the same security level.

The Implementing acts of the eIDAS regulation regarding trust services should eliminate the need for the Circle of Trust agreement as far as electronic signatures are concerned, but not in regard to advanced electronic systems. Accordingly, after the end of e-CODEX project there will be the need to monitor further developments carefully and adjust the legal agreements or technical systems or both if necessary. 


75 Natalie Nickel et al. (2016) e-CODEX Deliverable D1.16 Final sustainability report and recommendations (Update of D1.12 Sustainability Plan)
5. Process and data modelling for e-CODEX services: from legislation to electronic cross border procedure

Because e-CODEX aims to support the electronic processing of cross border legal procedures with minimal impact on national ICT systems, it is essential to achieve a shared understanding of the actual transactions and relevant data used by all parties involved in the procedure. What follows is a description of the process that governs the ‘process and data modelling’.

There are three stages for electronically processed cross border legal procedures in e-CODEX:

1. Establish the feasibility of the legislation to be electronically processed
2. Process analysis, based on ebBPSS from the ebXML stack
3. Data modelling and analysis, based on CCTS

We can explain this better using a story to describe the different stages. The story is fictional but based on real cases.

Franz von Liebensfels from Klagenfurt rented an Opel Astra on the Internet for use in Portugal. He collected the car from the Rental Car company’s office in a street in the centre of Lisbon. Due to the existence of damage to the vehicle he decided to go to the company’s office at the airport and the employee agreed to the change. The employee inspected the Opel Astra and discovered damage to the windscreen. Mr Liebenfels assured him that this was already there when he had collected the vehicle. The consumer subsequently saw that his credit card had been charged with the sum of € 400. He decided to file a claim against Rental Car at the court of Lisbon using the European Small Claim Procedure.

The following sections (5.1, 5.2 and 5.3) describe the three stages. The rest of the chapter describes in further detail how e-CODEX deals with relevant elements for achieving mutual equal understanding of data in legal procedures currently and sets out a path for the future.

5.1. Feasibility

The decision on the feasibility of any legislation to be supported by electronic means in e-CODEX is prepared by the work package on piloting, in e-CODEX this is WP3. This first stage is not technical at all. The feasibility of any procedure to be processed electronically is decided upon mainly by the policy goals of either the Member States, the European Commission or less commonly by the European Parliament. The criteria that are taken into account are:

1. Number of supporters
2. Extensibility
3. Involvement of all Work Packages
4. Not already covered by existing/planned projects

---

77 http://www.unece.org/cefact/codesfortrade/ccts_index.html
5. Expected volume
6. Category of beneficiaries
7. Legal basis
8. Countries willing to participate in the use case.

Depending on the legislation at hand additional criteria might be necessary to decide on the feasibility for a procedure to be supported by e-CODEX. Once the feasibility of the digitalisation of a legal procedure is concluded and embraced the next steps are definitely of a more technical nature. Figure 7 expresses the mutual dependency of process, data and transport (or routing).

![Diagram](image)

**Figure 7 Coherence between business, routing and data in support of cross border legal procedures**

5.2. Process analysis

e-CODEX follows the ebXML standard to achieve interoperability. Part of the standard is ebBPSS for process analysis. Process analysis requires people involved in handling the legal procedure to participate in describing the process. The knowledge and experience gained from regular handling of cross-border legal procedures is essential to develop digital solutions with added value. The basic steps in the process analysis are:

1. Describing the context of the legal procedure:
   a. Analysis of the legislative foundation of the cross border legal procedure
   b. Identifying experts on the cross border legal procedure from Member States
2. Scoping of the process
3. Modelling of the process
4. Defining the business transactions:
   a. Listing the information needed for each transaction to be processed successfully
5. Reporting on the outcome of the process analysis

Figure 8 presents graphically the outcome of the process analysis, in this case for the claim of Franz von Liebensfels following the European Small Claims Procedure 861/2007.

![Figure 8](Image)

Once the scope of the process has been decided upon, the next stage is to determine the process steps. The process steps are called Business Collaborations (see Figure 9).

![Figure 9](Image)

The process analysis shows the business collaboration listed underneath for the exchange of information between Member States.

---

78 Scope visualization based on idef0. See http://www.idef.com/idef0.htm for more information
1. BC-001002: Court retrieval.
2. BC-001003: Filling a claim.
3. BC-001004: Deciding.

Each business collaboration is supported by business transactions. The business transactions related to BC-001003 are pictured in Figure 10.

![Figure 10 Business transactions within BC-001003 Filing a Claim](image)
Figure 11 Business Transaction and its business documents

The process of handling information in documents and messages between parties involved within the Member States is out of scope for the process analysis by e-CODEX. It must be clear that for the proper digital processing of a cross border legal procedure a comparable analysis is required for information exchange within a Member State.

5.3. Data modelling and analysis

e-CODEX uses a 3-level framework towards semantic interoperability. The framework consists of a conceptual model, a logical model and the technical or physical model. Every level of abstraction serves a different objective. Most of all, semantic interoperability serves the alignment of business and IT. The conceptual model will guide and support business and IT to create the foundation for the exchange of information through experience and using previously known and used concepts. For the composition and reusability of concepts, the logical model facilitates the design process by selecting, composing, fine tuning and coding logical elements to use in messages supporting the execution of legal procedures. The logical model is domain oriented and therefore use-case centric. The physical (or technical) layer is exclusively related to the use case or project.

The business transactions and the information required, as formulated in the business documents, create the starting point for data analysis in e-CODEX. The procedure describes the steps that have to be taken and not how these steps are executed. The actual execution of these steps will be dependent on the choice whether or not a ‘standardised approach’ for the creation of schemas is chosen and if so, what standard will be applied. The procedure distinguishes between roles, responsibilities and tasks. The steps to create XML schemas are summarised in Table 4.
<table>
<thead>
<tr>
<th>Step</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Process articulated information requirements with process analyst responsible for the use case description</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2. Check if existing building block for a certain (set of) information elements required for the use case are available for reuse in your semantic library</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>3. Reuse or extend available building block, according to agreed standards, NDR, etc. Else create new building block</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>4. Add definition and source for newly created information entities</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5. Add properties for newly created information entities</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6. Add code lists</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7. Select the use case required building blocks from your library into a XML Schema concept</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>8. Delete the information entities contained in the selected building block, but not relevant for the XML Schema</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>9. Generate the XML Schema to be implemented by participants</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Table 4 Steps to create XML Schemas**

1 = scenario where a semantic library is used and maintained for creating XML Schemas
2 = scenario where concepts / information entities and code lists are created specifically for one use case and not necessarily reused in other use cases.

### 5.4. Production of XML Schema Definitions

As a ‘best practice’ e-CODEX has established a core team of data modellers responsible for creating, editing and extending the concepts. The core team either identifies or creates the concepts based on the information requirements from a use case and the separate business transactions. Figure 12 shows the concepts and the relations between the concepts for Small Claims.

![Figure 12 Concepts from Small Claims](image)

Once a concept is created, it is presented to a semantic user council formed of representatives from all stakeholders from specific use cases to approve the definition of a concept before deployment. Approved concepts are deployed in schemas that carry the information as identified in the business transactions. The schema creation group will put the approved and selected concepts into the XML
schema definitions (XSD). The schema creation group is also responsible for the validation of the XSDs. Figure 3 represents the process of data analysis and XSD production.

5.5. Mapping

Mapping is a transformation process within a MS. The responsibility for mapping is with the MS, not with e-CODEX. The MSs decide when, if and how messages are transformed from the European level to the national solutions. As this can be a very time consuming activity specialists from MSs must be involved as early as possible in this process. Although not within its responsibility e-CODEX facilitates the ‘national data mapping’ through mapping workshops. For transforming XML data from one XML format to another XML format three different approaches are demonstrated in the workshops:

1. **Peek and Poke using XPath expressions**
   
   This approach uses an empty template file which conforms to the structure that is defined for the output XML data. Values from the input XML data are retrieved using XPath expressions (Peek) and filled in the template file using XPath expressions (Poke).

2. **Transformation using XSLT**
   
   This approach uses an XSLT template-processing engine (the processor) to produce the output XML data. The XSLT template processor takes the input XML data, plus one or more XSLT style sheet modules, and processes them to produce an output document. The XSLT style sheet contains a collection of template rules: instructions and other directives that guide the processor in the production of the output document.

3. **Transformation using DataBinding**
   
   DataBinding is the ability to marshal objects into XML and the inverse, i.e. to un-marshall XML back into objects. In this approach the input XML data is un-marshalled into objects. These objects are used to programmatically create new objects for the output that will be marshalled into the output XML data. The object classes for both the input XML format and the output XML format can be generated from XML schemas making it easy to keep the object definitions synchronised with the XML Schema definitions.

5.6. Sustainability

e-CODEX created a long term strategy for the establishment of semantic interoperability to support the digital processing of cross border legal procedures. The aim of the long term strategy is twofold. The first aim is to guarantee the correctness of the processing of cross border legal procedures. The second aim is harmonising legal concepts to enable faster deployment of these procedures. The long term strategy builds upon existing methodologies and instruments.

The long term strategy consists of four pillars:
1. A Governance model
2. The Core Legal Concepts
3. Semantic interoperability, which is deployed through a Domain and Document Model
4. Naming convention for the unique identification of concepts and forms.

The Governance model, intended as the proposed steps that govern the creation of the semantic interoperability layer, has been described in this chapter. For further details on the other pillars see Chapter 8.2.
6. Practical implementation

This chapter provides some basic information for new piloting partners. This information is needed in order to set up a Gateway and Connector, to connect to the e-CODEX infrastructure and to go live with one or more e-CODEX use cases. This entails the technical, legal and organisational steps required to join the e-CODEX e-delivery infrastructure and preparing and implementing a live e-CODEX use case. The following sections will introduce the use cases that e-CODEX is piloting with, a check list that refers to two e-CODEX documents fundamental for piloting, the “Roles and responsibilities for piloting” and the “Quick Start Guide”, and a set of lessons learned from the on-going live piloting.

6.1. Introduction to experiences from use cases and on-going pilots

The e-CODEX project addresses in particular some of the weaknesses that have been identified when exchanging judicial documents in cross-border cases. Its aim is to provide an infrastructure that facilitates the secure exchange of documents between Member States, thus reducing delays and improving access to justice in Europe.

The technological solutions provided have been designed in line with current technological developments within the European e-Justice field so countries wishing to join the project at a later stage can easily adopt them.

e-CODEX’ pilots focused in particular on three main areas of interest: Civil Law Cases, Criminal Law Cases, and Synchronous Communication applied to business registers. In the sections below, each area of interest and the relative e-CODEX use cases are briefly introduced.

6.1.1. Civil Law Cases

The objective of pilots in the Civil Claim area is to simplify and speed up cross-border claims in civil and commercial matters. The aim is to allow processing of civil claims on-line in cross-border cases, and enable electronic delivery of related documents. In the Civil Law Cases area two trans-border civil procedures have been identified: the European Payment Order (EPO) and Small Claims.

6.1.1.1. European Payment Order (EPO).

The EPO procedure is based on Regulation (EC) No 1896/2006 of the European Parliament. The procedure has the aim of allowing the recovery of uncontested monetary claims in cross-border cases by creating a harmonised European Payment Order procedure.

The EPO e-CODEX pilot connects the respective national filing systems via e-CODEX infrastructure thus enabling electronic cross-border filing to the competent court in another piloting Member State. The prerequisite of a system to be connected to the e-CODEX infrastructure is that documents exchanged through the system have to be at a minimum created by an “advanced electronic system”\(^{79}\) or signed with an advanced electronic signature.

\(^{79}\) The system can also be named “advanced signature system”. Neither of the terms/phrases are defined legally. The exact definition of which kind of signature is needed can be found in the specific regulations for the different uses cases. Further legal requirements are described in D3.12 Documented System Requirements and Specifications (update of D3.3).
The pilot also foresees the implementation of a new functionality in the European e-Justice Portal. The functionality will allow citizens to fill the application-form for a European Payment Order and to submit this application directly in electronic format to the competent court in a Member State participating in the pilot.

The following countries are currently participating in the e-CODEX pilot for the European Payment Order procedure: Austria, Estonia, Germany, Greece, Italy, and Poland with the actual exchange of legally valid documents and communications between parties and courts (live), while France and Malta are currently in the final stages before going live.

In the deliverable D3.11 and D7.5 (Governance and Guidelines Definition), the process modelling of the EPO use case is described. The process modelling is a document prepared by the WP6 team that describes the objective of the use case, the steps involved, the solutions required for its implementation and provides the basis for drafting the pilot’s functional requirements. The document is based on the EPO standard framework and on the application of the regulation in the national contexts. In D3.11 and D7.5 (Governance and Guidelines Definition), functional and non-functional requirements are also included.

6.1.1.2. Small Claims (SC)

The Small Claims use case is based on Regulation (EC) No 861/2007 of the European Parliament. The regulation provides a procedure that allows a money claim to be filed to a European court where the value of the claim does not exceed €2,000 excluding interest, expenses and disbursements.

The Small Claims Procedure operates on the basis of standard forms. It is a written procedure unless an oral hearing is considered necessary by the court. This pilot has the aim of enabling European Union citizens and companies to process civil claims and deliver related documents online. For systems connected through the e-CODEX infrastructure participating in the pilot, the prerequisite is an advanced electronic signature.

The following countries are currently participating in the e-CODEX pilot for Small Claims: Austria and Poland are live, while Czech Republic, France and Malta are currently in the final stages before going live.

The process modelling of the Small Claims use case is described in the deliverable D3.11 and D7.5. The process modelling illustrates the use case’s objectives, the steps involved and the solutions required. In D3.11 and D7.5, functional and non-functional requirements are also included.

6.1.2. Criminal Law Cases

e-CODEX pilots in the Criminal Law Cases area have the aim of improving and speeding up cross-border prosecution practices through digitisation. The pilot will look at the electronic exchange of documents and judicial cooperation acts of EU Member States between relevant judicial authorities.

The following use cases have been selected: Mutual Legal Assistance (Secure Cross-border Exchange of Sensitive Data, EURegio and the European Investigation Order), European Arrest Warrant (EAW); Mutual Recognition of Financial Penalties.
6.1.2.1. Mutual Legal Assistance

The Mutual Legal Assistance pilot includes a number of initiatives aimed at cross-border communication between judicial authorities which have been developed in different stages of the e-CODEX project and which achieved different level of completion.

Secure cross-border exchange of sensitive judicial data

This initiative, which was then superseded by the EURegio and European Investigation Order ones and never implemented, focused on two areas:

1. Freezing and confiscations based on Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence and
2. Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders. In this area, the pilot would have digitalised the procedure that allows a judicial authority of a Member State to request the enforcement of a freezing or confiscation order to a second Member State’s judicial authority.

Please refer to deliverable D3.11 and D7.5, Governance and Guidelines Definition, for the process modelling of the Secure cross-border exchange of sensitive judicial data use case (Chapter 2.1.2), its accurate description and the illustration of functional (Chapter 3.5) and non-functional requirements (Chapter 4).

EURegio

Related to the secure cross-border exchange of sensitive judicial data use case is the EURegio initiative. EURegio is a pilot proposed by the Ministries of Justice of Belgium, the Netherlands and North Rhine-Westphalia (DE), whose aim is the digitalisation of data exchange for criminal matters within the EURegio cooperation framework. The goal of this cooperation, established in the border areas of Belgium, Germany and the Netherlands between national prosecuting authorities, is to curtail, as far as possible, the offenders’ freedom resulting from opening the borders within the scope of the Schengen process and the different legal systems. e-CODEX will support the cooperation in terms of electronic exchange of requests for legal assistance (currently up to 5000 per year), follow-up correspondence and enquiries for information in criminal cases. The service provides a secure data transmission channel which ensures the unique authentication of the sender and the recipient and the establishment of common data standards in order to allow further processing of the data sent by the respective national judicial case management systems. EURegio bears a strong resemblance to the European Investigation Order (EIO, see the following paragraph on Mutual Legal Assistance), which entails exchanges between investigating judges. Thanks to this, once the decision to implement the use case was taken, the forms that are used for the EURegio exchanges have been very quickly developed on the basis of the work already developed for EIO. Given the status of implementation of the two procedures and the minor complexity of the EURegio exchange, EURegio was piloted first. Germany and the Netherlands are live since November 2015.

European Investigation Order

The existing framework for gathering of evidence is too fragmented and complicated. A new approach is therefore necessary to replace all the existing instruments in this area: a comprehensive system for obtaining evidence in cases with a cross-border dimension, taking into account the flexibility of the
traditional system of mutual legal assistance. This new approach is based on a single instrument called the European Investigation Order (EIO). It proposed a procedure that would allow an authority in one member state (the "issuing authority") to request specific criminal investigative measures be carried out by an authority in another member state (the "executing authority"). The EIO has a horizontal scope and therefore applies to almost all investigative measures. The European Investigation Order (EIO) pilot takes advantage of the experience of EURegio pilot and serve as model for the civil law pilot Taking of Evidence (EC 1206/2001; amended by EC 1103/2008). The EIO was formally adopted as a Directive in April 2014, with MS having until 22 May 2017 to comply with its provisions. Germany and the Netherlands are live while Belgium, France, Greece and Spain are currently in the final stages before going live.

6.1.2.2. European Arrest Warrant (EAW)

The EAW pilot is based on the Council Framework Decision 2002/584/JHA of 13 June 2002 that provides the EU judicial procedure for the arrest and surrender by another Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order. The e-CODEX EAW use case implements the electronic transmission of the European arrest warrant (issued by the requesting Member State competent judicial authority) to the executing authority, and the exchanges between the issuing and the executing authority. The deliverable D3.11 and D7.5 presents the process modelling of the EAW use case and it also includes the functional and non-functional requirements. Before reaching the piloting stage, and following thorough discussions, it was decided to shelve the work on EAW on the ground that the objective of the pilot was sufficiently covered by other cross-border tools.  

80 e-CODEX Deliverable D3.13 Update of D3.4 Test Findings of Tests

6.1.2.3. Mutual Recognition of Financial Penalties

The Financial Penalties use case is based on Framework Decision 2005/214/JHA of 24 February 2005 and on Directive 2015/413. The procedure regards the obligation to pay a sum of money on conviction of an offence imposed in a decision (Framework Decision 2005/214/JHA). Offences may be the participation in a criminal organisation, terrorism, trafficking in human beings, trafficking in arms, swindling, trafficking in stolen vehicles, rape or even penalties for road traffic offences.

The decision imposing a financial penalty is transmitted from the "issuing state", i.e. the Member State that delivered the decision, to the "executing state", i.e. the Member State that executes the decision in its territory. The decision is transmitted to the competent authorities of the Member State where the natural or legal person has property or income, is normally resident or, in the case of a legal person, has its registered office.

The e-CODEX pilot for financial penalties will focus in particular on traffic offences in a country other than the one in which a car is registered and on the Directive 2015/413/EU of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences. The Directive sets up a procedure for the exchange of information between Member States in relation to eight road traffic offences (speeding, non-use of a seat-belt, failing to stop at a red traffic light, drink-driving, driving under the influence of drugs, failing to wear a crash helmet, use of a forbidden lane and illegally using a mobile telephone). The Member States may thus access each other's national data concerning vehicle registration in order to determine the person

80 e-CODEX Deliverable D3.13 Update of D3.4 Test Findings of Tests
liable for the offence. The Directive provides a list of the data elements necessary to conduct the search, of the data elements provided as a result of the search and a template for an information letter to inform the owner, the holder of the vehicle or the otherwise identified person suspected of committing the road-safety-related traffic offence in case the Member State of the offence decides to initiate follow-up proceedings in relation to the road-safety-related traffic offences listed in the Directive. The e-CODEX pilot will digitise this procedure.

France and Netherland participate in the e-CODEX pilot for the Mutual Recognition of Financial Penalties. The deliverable D3.11 and D7.5 (Governance and Guidelines Definition) includes the process modelling of the Financial Penalty use case, its description and the illustration of functional and non-functional requirements.

6.1.3. **Synchronous Communication**

The objective of pilots in the Synchronous Communication area is to allow cross border machine-to-machine communication, in general without human interaction. It should be noted that the term “synchronous” is not used here in the technical sense of synchronous web service communication.

6.1.3.1. **Interconnection of Business Registers**

This use case has been proposed for the extension phase of e-CODEX to demonstrate the interoperability of synchronous communication and is based on Directive 2012/17/EU amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers (see also Framework Decision 2005/214/JHA of 24 February 2005). The Directive 2012/17/EU has two pillars. The first is to create a system allowing for accessing to information in the Member States’ registers through the European e-Justice portal. The second pillar allows communication between the Member States’ registers.

e-CODEX centres its efforts at first on digitising the procedure for cross-border mergers. This procedure regards the notification in a Member State’s business register of a dissolving company due to a merger taking effect and the reply of a second Member State’s business register with a confirmation of receipt of the notification. Austria, Ireland and Italy are currently participating live in the e-CODEX pilot.

The deliverable D3.11 and D7.5 presents the process modelling of the Synchronous Communication use case and it also includes the functional and non-functional requirements.

6.2. **Key technological and legal steps to go live**

While the decision to start with e-CODEX is always made at an organisational level, and thereafter organisational, technological and legal steps tend to intertwine, here we decided, for sake of clarity, to separate the mainly technological and legal steps from the organisational ones and to present them in this order.

To get involved in the piloting, new partners should start with e-CODEX “Roles and responsibilities for piloting” document which provides an overview about:

1. Parties involved;

The document is dedicated to technicians of countries and infrastructure providers participating in e-CODEX piloting or planning to do so.

The document also indicates the preconditions for participating in one or more e-CODEX use cases. These regard the following actions:

1. The first step to become a partner of the e-CODEX piloting environment is to inform the WP3 coordinator, in order to get access to the e-CODEX Environment to start testing with other e-CODEX infrastructure providers.
2. Sign the Circle of Trust document (e-CODEX Agreement on a Circle of Trust adopted by the e-CODEX General Assembly on the 20th of February 2013).
3. Set up the Gateway and Connector infrastructure and connect it to the National Service Provider system(s).
5. Tests to be done before going live:
   a. An initial phase of internal tests by developers;
   b. Integration tests of components (Gateway and Connector); business tests of National Service Provider (producing a document and sending it to the national Gateway);
   c. Gateway to Gateway tests and Connector to Connector tests between countries; end-to-end tests.
   d. For the last two test types, a documentation of successful execution has to be provided to WP3.
   e. On-site visits for live demonstrations of WP3.
6. Create and maintain the test environment as well as the production environment, i.e. all up and running.
7. Indicate the successful completion of all tests and the documentation of these tests (Quality Assurance) has to be sent to WP3. At this point the decision will be made if the new infrastructure provider is ready to participate in productive message exchanges within e-CODEX.
8. Preparation to go live: Download\(^\text{82}\), install, configure and set up Gateway\(^\text{83}\) on a separate Server and send all necessary information to the CfC (Coordination for Configuration).
9. Going live: 14 days after providing the necessary configuration files, the new infrastructure provider is part of the e-CODEX production system.

The “Roles and responsibilities for piloting” document also indicates the actors that will support the implementation of e-CODEX components in the piloting countries. Work packages WP4, WP5 and WP6 are responsible for the implementation and release of these components. The work package

\(^{82}\) https://secure.e-CODEX.eu/nexus/content/groups/public/org/holodeck/holodeck/

\(^{83}\) https://www.jol.nrw.de/bscw/bscw.cgi/d3610205/Installation%20Instructions.docx
responsible for a component will run tests to prove that the specified technical requirements are met. The results of the tests are published in the e-CODEX deliverables concerned with testing.

Please refer also to the “Roles and responsibilities for piloting” document for a detailed schemas of the workflow for new e-CODEX infrastructure providers.

6.3. Key organisational steps to go live

The project aims to develop a viable technological infrastructure for the cross-border exchange of data and documents in the justice domain. Moreover it takes into account the need for organisational actions to support the implementation of procedures and provision of services. In July 2013, Austria, Estonia, Germany and Italy started piloting the European Payment Order (EPO) based on the outcome of the work within the different e-CODEX work packages. In 2014 Greece joined the piloting. The key lessons presented here are derived from our experiences of live piloting of EPO procedure and the preparation for the piloting of other use cases (e.g. EURegio) and provide guidelines to help implementation and piloting of new participating partners (e.g. with some real-life examples).

Lessons learned regard the piloting checklist, testing of pilots and dissemination activities. These range from verifying actual practices, discrepancies from the general interpretations of EU Regulations, and involving internal and external users, etc.

Key steps:

1. Follow a pilot preparation checklist:
   - Build on and refer to the e-CODEX ‘Level of Support’ (renamed “Roles and responsibilities for piloting”) document & Quick Start Guides

2. Focus on starting the pilot with Member States that have a better chance of providing of real-life cases:
   - Check historical data of conventional (paper) cases and take into account the direction of travel (e.g incoming and outgoing cases).

3. Focus on time-management and personnel:
   - Assign at least one dedicated person to testing and communication with both external (other piloting countries) and internal (court-side, lawyer-side) collaborators.
   - Allow at least two months for testing. Do not forget that no matter how carefully you plan your deployment goals, the successful completion of testing highly depends on your partners’ time availability.
   - Ensure that proper legal arrangements are made (Circle of Trust, co-existence of “paper” and “electronic” procedure where applicable, and interfaces between paper and electronic procedure are set up where needed).

4. Setting up the Gateway and Connector:
   - Use Quickstart Document (provided by WP5).

5. Testing the Gateway and Connector:
   - Use of automatic testing tools such as the ones being hosted by Greece (a password-protected website where a partner can request a test message to be automatically sent when needed).
   - Consult WP5 concerning technical difficulties.

6. Mapping existing national schemas to e-CODEX (or creating new ones):
   - Use e-CODEX Schemas & documentation.
   - Use Forms and XPath document for each scenario (provided by WP6):
7. Validating forms before performing end2end testing:
   - Consult previous end2end test files and pre-completed EPO test forms (PDFs accompanied by their respective e-CODEX valid XML files) from countries already in piloting mode.
   - Consult mapping examples, currently being created (effort initiated by AUTH/Greece to translate test forms into XML, will be ultimately completed by WP3 & WP6).

8. Verify the actual practices concerning the off-line procedure, which will be electronically enabled through the use case as they may differ quite broadly from what would be expected reading the law or looking at the experience of other partners.

9. Dissemination activities:
   - Plan local dissemination activities to users (e.g. lawyers, judges and court personnel) well in advance and get direct feedback.
   - Support for the development of new procedures and practices can be required, especially from the courts and public prosecutor offices.

10. Not all communication requirements are formally foreseen:
    - E.g. FreeFormLetter is now part of the EPO Schemas and has proved to be a worthwhile tool in exchanging e-CODEX messages when the required form was not provided by the EU Regulation.

In addition, there are some lessons learned from the experience of single piloting countries, from the involvement of national stakeholders that get in touch with the European project and from the experiences of the first users that try to use the system.

In Italy a number of lessons came from the efforts of the Italian Ministry of Justice and its partners IRSIG-CNR and ITTIG-CNR to assess the actual practice using the paper based procedure and involving stakeholders during the implementation and piloting stage. These activities allowed information to be gathered on the organisational issues regarding the application of the EPO procedure in Italy and its use by Italian lawyers. In particular IRSIG-CNR conducted:

- Preliminary organisational analysis on Italian Payment Order Online.
- Analysis of the European Payment Order (application of Italian courts and lawyers).
- Involvement of stakeholders: Court of Milan (Judges and Court Service) and the Bar Association of Verona.
  - Involvement of Court of Milan for Piloting.
  - Connection of already functioning PCT (Processo Civile Telematico).
  - Presentation of the project, objectives and “how it works” in a set of meetings (Italian MoJ, IRSIG-CNR, ITTIG-CNR).

The involvement of stakeholders is fundamental for a piloting country in order to gather information on organisational issues that regard courts’ application of the European procedure, the use of the procedure by lawyers and the issues that they may encounter. In Italy, the preliminary analysis showed a number of problems affecting the EPO implementation including the low level of procedural standardisation within the courts, the scarce number of EPO claims that Italian courts receive, the difficulties for parties and lawyers in assessing which is the competent court and the payment of fees. Piloting countries have to be aware of these organisational issues in advance in order to deal with them before introducing the technology. There is often not a single way in which the off-line procedure to be piloted has been implemented. There are many, resulting from different interpretations and enactment of EU and national norms and of the local context.
These issues can be dealt with by an organisational (and legal) approach that focuses on the procedure and its real application in the courts and not simply by introducing technology.

Properly managing the technological and organisational complexity is key to the success of the project. For this purpose, the EURegio participants (Belgium, North Rhine-Westphalia (Germany) and the Netherlands) decided to follow a gradual approach and to start piloting with the initial and most important step of the procedure, the Mutual Legal Assistance (MLA) request. Furthermore, once the case is registered by the addressed authority, additional information including the case file number is sent back through the e-CODEX infrastructure. The following steps of the EURegio procedure are then carried out off-line.

Since no official form for a MLA request is available, a form was defined which contains all necessary information to start an investigation. In doing so, the upcoming EIO was taken into account. In this way, while already benefiting from the electronic transmission of a MLA request and gaining real life experience, the practitioner in the EURegio have time to discuss and decide on the next steps towards a fully supported electronic procedure.

In order to properly debug a freshly installed system (Gateway and Connector), a peer with a working system must send a variable number of test messages. This can prove difficult to set up, since it is difficult to predict exactly when these messages are needed. For this purpose, Greece set up a simple password-protected website where e-CODEX partners can “request” a test message to be automatically sent to them when needed. This is a simple script that copies a pre-defined test folder (containing a test message) to the outgoing messages folder of the Greek Connector. While e-CODEX partners implementations may differ, the core concept is very simple and an effective time-saver. This automatic testing tool can be easily adapted to send test messages to future piloting countries as well.84

While the EPO forms provided by the EU regulation cover most of the procedure’s information needs, some events are not covered by them (e.g. in the event of bankruptcy of the defendant, etc.). Austria provided an example of the approach used within their national system to deal with such cases, based on a free text form and standard text messages that can be inserted in such form. Based on this example, e-CODEX has begun developing a number of standard messages that can be used in such cases, translated by each partner in their language(s).

Estonia developed a web based interface connected to e-CODEX that allows citizens to file EPO claims to piloting countries’ courts based on the use of their national system of electronic signature. This allowed some useful insights in the development of this kind of services for one-time users of the service when a user contacted the Estonian helpdesk because he was trying to file an EPO claim to Germany, but he was not successful. The user complained that the electronic procedure was too complicated for him. Difficulties regarded the large form to fill and the many error messages that were generated. The Estonian Ministry of Justice’s contact person, acting as a helpdesk in this case, provided the user with a detailed manual but unfortunately the manual wasn’t enough for him. He still was not able to fill in the form correctly and gave up on filing the claim electronically and filed the claim on paper. The electronic procedure was too complicated for an occasional user.

84 I. Salmatzidis and I. Pagkalos, Greek EPO Pilot: Report on Current Status and Lessons Learned so far. e-CODEX WP3, 14/02/2014
On the basis of this experience, Estonia divided the form to be filled by the users into smaller parts so that if there is an error in the form the user will learn it straight away. The experience acknowledges that the error messages have to be clearer for the one-time user to make sure he understands where he has made a mistake. Moreover, detailed instructions have to be provided in advance.

The user also complained that payment information was not available in advance so that he had to contact the German court to know how the payment of the court fee was handled. The information on payment of court fees that can be retrieved in the e-Justice Portal is not easy to find and a link to this information should be included in the national system.
7. How to start? Reference packages

The following table includes the abstracts of the documents most important for incoming partners. Please refer to these deliverables in order to gather information on the e-CODEX project and piloting.

<table>
<thead>
<tr>
<th>Document</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>e-CODEX Circle of Trust Agreement</strong></td>
<td>The agreement is a document by which the Parties intend to define and establish a Circle of Trust for the crossborder exchange of documents and data within all e-CODEX use cases for the duration of the pilots. The Agreement will firstly be adopted by the General Assembly of the e-CODEX project. When Partners are ready to join a pilot they must declare to the e-CODEX Coordinator that they comply with the terms of this Agreement (declaration of accession).</td>
</tr>
<tr>
<td><strong>e-CODEX Level of Support</strong> (renamed “Roles and responsibilities for piloting”)</td>
<td>This document contains information about procedures and rules regarding setup and maintenance of an e-CODEX infrastructure.</td>
</tr>
<tr>
<td><strong>European Interoperability Framework for Pan-European e-Government Services</strong></td>
<td>The European Interoperability Framework (EIF) is a set of recommendations, which specify how Administrations, Businesses and Citizens communicate with each other within the EU and across Member States borders. The EIF 1.0 was issued under the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens programme (IDABC).</td>
</tr>
<tr>
<td><strong>e-CODEX Deliverable D1.16 Sustainability Plan (update of D1.12 and D1.7)</strong></td>
<td>European LSPs are by their nature “Pilots”, which implies that their duration is limited in time. The need to plan for the time after the project’s end is therefore evident. This deliverable defines what is meant by “sustainability”, describes how e-CODEX ensures sustainability for its project results and lists the technical components for which long-term maintenance needs to be provided and how that can be done. It also highlights some of the decisions within the project that have an impact on maintenance and lists some actions specifically targeting sustainability.</td>
</tr>
<tr>
<td><strong>e-CODEX Deliverable D3.11 &amp; 7.5 Requirements Finalisation and Description of Test Scenarios (Update of D3.2 and D7.2)</strong></td>
<td>The objective of this deliverable is to map the requirements of the use cases that have been selected for e-CODEX piloting, and set up scenarios for testing the system. This is done through process modelling describing the objectives, steps, supporting elements, and the solutions required for the implementation of each use case, a definition of the high level and common functional...</td>
</tr>
</tbody>
</table>
requirements and non-functional requirements and a description of the test scenarios for the piloting of each use case.

This work is an update of the deliverable D3.2 and D7.2, initially submitted in 2012. The aim of the update is not to focus on the existing content, but to reflect the extension of e-CODEX and the inclusion of a new use case dedicated to Synchronous communication applied to business registers. Therefore updates concern mainly this new use case, with the exceptions of the use case dedicated to Secure cross-border exchange of sensitive data and the postponed Financial penalties use case. At the time of the first submission, it was not possible to complete all the parts on these use cases, which has now been done in this update.

<table>
<thead>
<tr>
<th>e-CODEX Deliverable D3.6 System Manuals (Implementation, Operations and Maintenance) and D3.9 Definition of Operations and Maintenance processes and requirements</th>
<th>This deliverable is in particular intended for countries that would like to participate in one or more use cases established by e-CODEX. The objective is to provide the information required to understand the e-CODEX architecture as well as a prescriptive guide to complete local implementation. It contains an introduction to the architectural basis of e-CODEX, the common technical and administrative requirements for the use cases, a description of the incident-, release-, security- and availability management as well as a description of any use case specific requirements. Clear references are provided to existing documentation for more in-depth reading to make the guide more user-friendly and focused.</th>
</tr>
</thead>
<tbody>
<tr>
<td>D4.8 Concept for implementation</td>
<td>This deliverable provides an up-to-date description of modules and building blocks that have been realised, descriptions of detailed processes and requirements and the mapping of the processes to the functionalities of the solution.</td>
</tr>
<tr>
<td>D4.10 Developed Modules and Building Blocks</td>
<td>This deliverable provides information about modules and building blocks developed by e-CODEX WP4, concentrating on the different functionalities of the e-CODEX Trust Library and especially on the Trust OK-Token.</td>
</tr>
<tr>
<td>e-CODEX Deliverable 5.11 Concept of Implementation</td>
<td>The main goal of this document is to describe a convergence approach for building an electronic transport infrastructure able to fulfil the requirements of the Justice domain and which building blocks could be reused in other sectors. The solution described in this document incorporates the inputs arising from a convergence effort in cooperation with the European Commission, other LSPs and standardization organisations. This effort is intended</td>
</tr>
</tbody>
</table>
to create the foundation to design and develop a basic implementation of a cross-border European e-Delivery solution.

The present document will serve as the basic reference to start the development of the pilot implementation of a general electronic transport infrastructure that enables the exchange of documents in different sectors although specially focused on the judicial domain. The challenge faced is to have an operative solution running before end of 2012 based on cutting edge standards like ebMS 3.0, ETSI REM and WS-stack.

This is a living document, as the specifications it contains should be updated according to the experience and results obtained during the next development and integration phases.

| e-CODEX Deliverable D5.12 Developed Modules | The main goal of this document is to give an overview about the two main deliverables of WP5, which are the GW and the Generic Connector Framework. It describes shortly the structure of this deliverables and the dependencies to other deliverable. |
| D6.9: Update D6.3: Concept of implementation of WP6. | Introduces the methodology for modelling (incl. modelling steps), refines requirements and gives functional specifications for the individual building blocks. This deliverable also contains the long-term strategy of WP6. Initial findings from the development and testing and integration phase are concluded. |
| D6.11: Update of D6.4/D6.10: | This document describes how e-CODEX modules have been developed and presents the results of modelling. It contains the development and the schemas for the use cases. |
| e-CODEX Deliverable D7.1 Governance and Guidelines Definition v2.0 | This deliverable describes the activities carried out by e-CODEX Work Package 7 to set up an architecture governance structure for the e-CODEX project and provide a description of such structure. It also provides a reference of the Standards and Architectural Guidelines to improve interaction, exchange and cooperation among European public administrations across borders and across sectors for the delivery of e-CODEX services. Furthermore, this delivery sets the general framework for the e-CODEX methodology discussion. The actual methodology, which provides a framework and guidelines describing how to document the architecture and specifications so that the necessary types and levels of documentation fit together, is provided in an appendix as it is conceived as a document which will evolve during the course of the project. Lastly, Delivery 7.1 presents e-CODEX high-level scenario models |
of use cases, and discusses the e-CODEX security policy, which provides the basic principles for a secure operational environment and the development of a ‘Circle of Trust’ among actors, citizens, businesses, legal practitioners and the judicial authorities, specifying the obligations of the parties.

| e-CODEX Deliverable D7.3 High Level Architecture Definition | This document is a consolidating deliverable, summarising the high level architectural decisions taken so far within e-CODEX and providing clear indications as the component model is concerned. In other words, it provides an answer to questions such as: Which techno-institutional components does e-CODEX reuse? What needs to be done at National level and what by e-CODEX? Who builds what (i.e. Gateways, XML etc.)? While this is a technical document it may provide a valuable source of information for e-CODEX external environment. |
8. Supporting material (Annexes)

8.1. Security and data protection

Security and data protection issues are of particular importance in e-CODEX. The relevant provisions at EU-level and at national level have to be respected. Parties must therefore adopt all necessary technical and organisational measures to guarantee personal data security and prevent the alteration or loss of, or unauthorised processing of or access to data. Detailed security requirements and guidelines for ensuring authenticity, integrity, availability and confidentiality of the e-CODEX system and processes can be found in the respective deliverables (http://www.ecodex.eu).

For example:

a. Security Requirements for Connectors
   - A Connector needs to be set up in a secure and protected domain.
   - The Connector has to use an electronic certificate provided by an official trust authority for signing the ASICS container which is sent from the Connector to the Gateway. The certificate shall be compliant to the X.509 standard.
   - The underlying operating system has to be kept up to date with regard to necessary updates and patches, especially those with regard to security.
   - The receiving Connector has to process the document(s) and the Trust-OK token in accordance with the laws of the receiving Member State.
   - Only authorised and authenticated persons (by means of user-Id and password) must have access to the Connector.
   - The operating authority of a Connector must monitor the Connector permanently and has to inform the other e-CODEX partners as fast as possible in case of a failure of the local Connector. In the case of such a failure the operating authority has to undertake all measures so that the failure is cleared as fast as possible.

b. Security Requirements for Gateways
   - A Gateway needs to be set up in a secure and protected domain.
   - Only dedicated point to point internet connections secured by electronic certificates provided by an official trust authority between two Gateways must be allowed. The certificates shall be compliant to the X.509 standard.
   - The recommended software of the Gateway is the one provided by the e-CODEX project. The operating authority has to take care that the Gateway is always updated according to the published software version of the Gateway.
   - The underlying operating system has to be kept up to date with regards to necessary updates and patches, especially those with regards to security.
   - Authenticity and Integrity must be sufficiently protected
   - The exchange of messages and other information between the Gateways has to be done in encrypted form. A Gateway has to be monitored by the operating authority so that any risk of non-receiving, non-sending of a message and any risk of data loss can be avoided.
- Only authorised and authenticated persons (by means of user-id and password) must have access to the Gateway.
- The operating authority of a Gateway must monitor the Gateway permanently and has to inform the other e-CODEX partners as fast as possible in case of a failure of the local Gateway. In the case of such a failure the operating authority has to undertake all measures so that the failure is cleared as fast as possible.

8.2. Long term semantic sustainability pillars description

e-CODEX’s long term strategy for the establishment of semantic interoperability to support the digital processing of cross border legal procedures consists of four pillars:

1. A Governance model (intended as the proposed steps that govern the creation of the semantic interoperability layer, and which is described in Chapter 5)
2. The Core Legal Concepts
3. Semantic interoperability, which is deployed through a Domain and Document Model
4. Naming convention for the unique identification of concepts and forms.

8.2.1. Identifiers

As this topic can be handled with just a few words it comes first. The W3C standard URI is used to uniquely identify concepts and forms. The unique identification in e-CODEX will follow the ISA approach for the concepts. The forms will be identified according the URN:lex naming convention.

8.2.2. Core Legal Concepts

Inspired by ISA’s Core Vocabularies, harmonisation of legal concepts in European legislation through the introduction of Core Legal Concepts is desirable. For generic legal concepts the Core Legal Concepts are meant to describe the minimum set of attributes allowing additions to meet any necessary nuance. The minimum set of attributes harmonises these legal concepts. The Core Legal Concepts will, like ISA Core Vocabularies, be defined in writing and modelled in XML and RDF.

e-CODEX noticed that currently each time a legal procedure is taken up for electronic proceeding, basic legal concepts like ‘claimant’, ‘defendant’ and ‘court’ have to be analysed and modelled to match exactly the definition in the legislation at hand. Notwithstanding the necessity for nuances in legal matters, the aforementioned legal concepts are of such generic nature that harmonisation seems possible and desirable. For generic legal concepts, the Core Legal Concepts are meant to describe the minimum set of attributes allowing additions to meet any necessary nuance. The minimum set of attributes harmonises those legal concepts. The idea is to harmonise data definitions to the benefit of electronic proceeding through the introduction of Core Legal Concepts. Also, Core Legal Concepts would enable faster electronic deployment of cross border legal procedures. The table underneath provides an idea of potential Core Legal Concepts based on the example narrative.

<table>
<thead>
<tr>
<th>Directly identified concept from narrative</th>
<th>Deduced concept from narrative</th>
<th>Core Vocabulary</th>
<th>Core Legal Concept (draft)</th>
</tr>
</thead>
</table>

62
8.2.3. Domain-document model

Semantic interoperability is deployed through a distinction between a Domain Model and a Document Model. The latter serves to instantiate a document e.g. a form belonging to a specific use case. The Domain Model is used for providing meaning to the document in its context. Figure 13 shows the relation between the ‘concepts’ at the domain level and their deployment in the instantiations in the document, in e-CODEX terms understood as an instantiation at the physical level.

8.2.3.1. Small Claims Document Logical Model excerpt in RDF/XML

The code underneath is an example of how an instantiation of a Small Claim might look like if represented in RDF. Up to summer 2014, e-CODEX has no experience in deploying RDF in a production environment.
<?xml version="1.0"?>
<rdf:RDF
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:ESCP="http://{URI root}/def/EuropeanSmallClaims#">
    <rdf:Description rdf:about="[FormAinstanceURI]#id1">
        <rdf:type rdf:resource="ESCP#Court"/>
        <ESCP:hasCourtName>Court of Lisbon</ESCP:hasCourtName>
        <ESCP:hasCourtAddress>Rua Polo Sul 43, Lisboa</ESCP:hasCourtAddress>
        <ESCP:hasCourtCountry>Portugal</ESCP:hasCourtCountry>
    </rdf:Description>
    <rdf:Description rdf:about="[FormAinstanceURI]#id2">
        <rdf:type rdf:resource="ESCP#Claimant"/>
        <ESCP:hasClaimantName>Franz von Liebenfels</ESCP:hasClaimantName>
        <ESCP:hasClaimantAddress>Museumstrasse 12, Klagenfurt</ESCP:hasClaimantAddress>
        <ESCP:hasClaimantCountry>Östenreich</ESCP:hasClaimantCountry>
    </rdf:Description>
    <rdf:Description rdf:about="[FormAinstanceURI]#id3">
        <rdf:type rdf:resource="ESCP#Defendant"/>
        <ESCP:hasDefendantName>Rental Car</ESCP:hasDefendantName>
        <ESCP:hasDefendantAddress>Avenida Sol 1345, Lisboa</ESCP:hasDefendantAddress>
        <ESCP:hasDefendantCountry>Portugal</ESCP:hasDefendantCountry>
    </rdf:Description>
    ...
</rdf:RDF>