Submitted to the EC on 03/08/2012

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

D7.3 High Level Architecture Definition

Deliverable Id :	D7.3
Deliverable Name :	High Level Architecture Definition
Status :	Version 1
Dissemination Level :	
Due date of deliverable :	31.10. 2011
Actual submission date :	03.08.2012
Work Package :	WP7
Organisation name of lead partner for this deliverable :	Ministry of Justice - Italy
Author(s):	Giulio Borsari, Marco Velicogna, Albert Kappe, Alexander Weber, Liisa Nikkarinen, Zoi Kolitsi, Andreas Symeonidis
Partner(s) contributing :	IT, DE, EE, NL, GR

Abstract:
This document is a consolidating deliverable, summarizing 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 build 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.

History

Version	*Date*	*Changes made*	*Modified by*
0.1	29.02.2012	Initial draft chapter 3 Architectural Decisions	Alexander Weber, Liisa Nikkarinen
0.1	01.03.2012	Initial draft chapter 4 Component Model	Albert Kappe, Zoi Kolitsi, Andreas Symeonidis
0.1	09.03.2012	Initial draft executive summary chapter 1 Introduction	Marco Velicogna
0.1	02.04.2012	Initial draft chapter 2 Architectural Overview	Marco Velicogna
0.2	11.04.2012	Merge of different content/ chapters, executive summary, introduction and chapter 2	Giulio Borsari, Marco Velicogna
0.3	04.05.2012	Inclusion of comments received by MB, added chapter 4.4	Giulio Borsari, Marco Velicogna
0.4	23.05.2012	Inclusion of comments received by partners	Giulio Borsari, Marco Velicogna
0.5	26.06.2012	Inclusion of comments received by partners and authors revised chapters	Giulio Borsari, Marco Velicogna
0.6	17.07.2012	Merge of different contents	Giulio Borsari, Marco Velicogna
1.0	03.08.2012	Decision 30 agreed – final version	-

Table of contents

HISTORY **2**
TABLE OF CONTENTS **3**
LIST OF FIGURES **4**
LIST OF TABLES **5**
LIST OF ABBREVIATIONS **6**
EXECUTIVE SUMMARY **7**
1. INTRODUCTION **9**
1.1. SCOPE AND OBJECTIVES OF THE DELIVERABLE 9
1.2. WP7 GENERAL OBJECTIVES AND VISION 9
1.3. METHODOLOGY OF WORK 9
1.4. RELATIONS TO INTERNAL E-CODEX ENVIRONMENT 10
1.5. RELATIONS TO EXTERNAL E-CODEX ENVIRONMENT 10
1.6. QUALITY MANAGEMENT 10
1.7. STRUCTURE OF THE DOCUMENT 10
2. ARCHITECTURAL OVERVIEW **12**
2.1. E-CODEX INFRASTRUCTURE COMPONENTS 12
3. ARCHITECTURAL DECISIONS **17**
3.1. GENERAL DECISIONS 17
3.2. SIGNATURES & AUTHENTICATION 23
3.3. TRANSPORT 26
3.4. DOCUMENT TYPES & DATA MODELLING 29

List of Figures

Figure 1 – e-CODEX High level architecture schema 12
Figure 2 – e-CODEX Components 13
Figure 3 - e-CODEX building blocks from the piloting country perspective 15
Figure 4 – High level use cases scenario (Adapted from D7.2 Requirements Finalisation & D3.2 Described Test Scenarios) 16
Figure 5 – Governance structure for architectural decisions 17
Figure 6 – Interoperability layers (source: European Interoperability Framework (EIF) for European public services fig 4.1) 19

List of Tables

Table 1: Abbreviation 6
Table 2: Supporting working-groups compositions and roles..... 10

List of Abbreviations

Acronym	*Explanation*
BSCW	Basic Support for Cooperative Work
CCBE	Council of Bars and Law Societies of Europe
CCTS	Core Components Technical Specification
CIP	Competitiveness and Innovation framework Programme
D7.3	Deliverable Number 7.3
ebMS	Electronic Business Messaging Services
EAW	European Arrest Warrant
EC	European Commission
EPO	European Payment Order
epSOS	Smart Open Services for European Patients
EQM	External Quality Manager
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technologies
ICT PSP	ICT Policy Support Programme
LSP	Large Scale Pilot
MB	Management Board
NIEM	National Information Exchange Model
OASIS	Advancing Open Standards for the Information Society
PEPPOL	Pan-European Public Procurement Online
SPOCS	Simple Procedures Online for Cross- Border Services
STORK	Secure idenTity acrOss boRders linKed
TA	Technical Annex
WP	Work Package
XML	

Table 1: Abbreviation

Executive summary

What is e-CODEX about?

Within the European Union, as a result of the growing integration and greater mobility of goods and people, the importance of cross-border judicial activities and procedures is increasing. More cooperation between different national judicial systems is needed. ICT can provide an important tool to support the resulting data exchange, communication and cooperation needs. In this context, the **e**-Justice **C**ommunication via **O**nline **D**ata **Ex**change project (e-CODEX), carried out by 19 partners[1], aims to improve European cross-border access to justice for citizens and businesses as well as the interoperability between legal authorities within the EU.

The objective is to use Information and Communication Technologies (ICT) to make cross-border judicial procedures more transparent, efficient and economic both in civil and criminal matters. The e-CODEX effort is therefore not only to ease access to information, but also the ability to process cross-border cases efficiently through electronic means.

To reach this ambitious goal, a fully technically interoperable European e-Justice system must be designed. The technical solutions envisaged within this context must respect both the principle of independence of the judiciary and of subsidiary. The e-Services and infrastructure that Member States have already established cover specific requirements of national legal systems. Generally, these national solutions are the result of considerable investments and cannot simply be replaced through new centralized approaches. The objective of the e-CODEX project is neither to re-invent the wheel nor to duplicate one national solution at the European level. Its ambition is to build on these national solutions in order to build a pan-European interoperability layer, which will connect the existing systems. The project is developing common approaches and standards in several areas. Within the project, effective solutions will be tested through working prototypes and via the piloting of several judicial use cases. This will take place also through a strong collaboration and reuse of components developed within existing European Large Scale Projects (LSP) such as EPSOS, STORK, PEPPOL and SPOCS.

Five use cases have been selected, divided into two pilots:

Pilot 1: Civil Claims: European Payment Order (EPO) and Small Claims

Pilot 2: Cross-border Mutual Legal Assistance: Mutual recognition of financial penalties, Secure cross-border exchange of sensitive data, and European Arrest Warrant (EAW).

D7.3

This document is a consolidating deliverable, summarizing the high level architectural decisions taken so far within e-CODEX (in particular D7.1 and D7.2&D3.2, but also taking into account D3.1, D3.3, D4.1, D 4.1.1, D4.2, D5.1, D5.2, D6.1, D6.2) and providing clear indications as the component model is concerned.

---

[1] The 19 partners are either being or representing their national ministries of justice of 14 European Member States and Turkey, plus the Council of Bars and Law Societies of Europe (CCBE), the Conseil des Notariats de l'Union Européenne (CNUE) and the National Research Council of Italy (with two institutes, IRSIG-CNR and ITTIG-CNR). Belgium is represented by two partners.

As a reading of the document will show, the main high-level architectural issues have been solved, and processes to solve the ones still open have been initiated. In some cases it was recognized the impossibility of defining working solution ahead of time and it has been decided to test the possible options in the pilots in order to empirically find the more suitable and efficient solutions.

Risks

The major risks within the project are different in kind, impact and probability. A first major risk raises from the complexity of existing MS techno-institutional systems that need to be made interoperable. Solutions must not be just technological but also compatible with the MS legal system and user friendly. In order to confront this risk, longer than initially anticipated information gathering, but also discussion and negotiation has been required. A second major risk rises from the heterogeneity of partners' contributions from both a quantitative and qualitative perspective. This has been addressed for clarifying to the project management. Risks external to the consortium lay in the dependency with other LSPs and EU portal as regards the maturity and availability of their technical developments and in the complexity in finding a solution that is simple enough from a user perspective to be adopted.

Next steps[2]

The e-CODEX project has now entered its second year. During the course of this second year, the project will need to transform its paper-based activities to the writing of code and development of the e-CODEX building blocks. This therefore calls for the need to:

- Finalise the system requirements, including investigating further legal requirements deriving of the national law of the piloting states
- Carry on the e-Delivery convergence effort and pursue the effort to re-use and adapt solutions from other co-funded projects
- Address the topic of e-Signatures, regardless of the state of advancement of the new signature directive
- Establish a circle of trust
- Specify, develop and connect the e-CODEX transport platform to the European e-Justice Portal
- Conduct the enlargement of the e-CODEX project to further European countries and assess the need for an extension into time
- Engage stakeholders and raise the profile of e-CODEX providing information on e-CODEX high level architecture
- Alignment of the developments from different WPs
- Definition of the integration tests

[2] Adapted from D1.6, 22.02.2012, Page 13

1. Introduction

1.1. Scope and objectives of the deliverable

This document is a consolidating deliverable, summarizing the high level architectural decisions taken thus far within e-CODEX by WP7 *Architecture* but also by the technical work packages WP4 *e-Identity and signature*, WP5 *e-Delivery and e-Payment*, and WP6 *Document Standards and Semantics*, and working in strict collaboration with WP3 *Piloting* and WP1 *Project Management*.

It is intended to provide a synthetic guideline both for internal e-CODEX use, and for external information. Many of the decisions presented in this document can respond to issues or proposals which have been introduced by the various deliverables which have preceded it, including, at a higher level, D7.1 and D7.2&D3.2, but also D3.1, D3.3, D4.1, D 4.1.1, D4.2, D5.1, D5.2, D6.1, D6.2. Furthermore, this document provides indications on the features of the gateway-based architecture that has been selected. The function of the gateways is to separate national and EU portal solutions from e-CODEX allowing them to exist independently. It converts messages from the national or EU portal format to a format supported by e-CODEX and *vice versa*.

1.2. WP7 General Objectives and Vision

As the overall project structure is separated into different work packages and will take into account existing building blocks from running CIP projects[3] and national projects, there is a need to provide an overall guidance on how to integrate these assets and best practices with development activities to ensure the overall technical interoperability. The architecture work package (WP7) focuses on the architecture, design and validation of the common specifications and building blocks. The leader of WP7 is responsible for the architectural integration of building blocks and for the setup of an architecture governance structure.

1.3. Methodology of Work

The activities have been carried out through face to face plenary meetings and telephone conferences. Working-groups have been created in order to deal with specific questions and parts of the deliverable. The roles and composition of these working-groups were discussed and agreed upon in the plenary meetings. These groups are:

- High Level Use Cases working-group
- Process modelling working-group
- Legal and Security subgroup
- Functional Requirements working-group
- Non-functional Requirements working-group

[3] Potential building blocks may come from PEPPOL, STORK, SPOCS, the e-Justice Portal or other projects such as the Austria-lead project "Concept for Cross-border Electronic Filing and Delivery for the European Electronic Payment Order.

The table below shows the working-groups' compositions and roles.

Participant	High Level Use Cases working-group	Process modelling working-group	Legal and Security subgroup	Functional Requirements working-group	Non-functional Requirements working-group
JM NRW	Support	Support	**Responsible**	**Responsible**	Support
AUTH Greece	Support		Support	Support	Support
MoJ Italy	Support	Support	Support	Support	
RIK/JM Estonia		Support	Support	Support	
MoJ France	**Responsible**	Support	Support	Support	
MoJ Turkey					Support
MoJ Netherlands		**Responsible**	Support		**Responsible**
BMJ Austria		Support	Support		Support

Table 2: Supporting working-groups compositions and roles

1.4. Relations to Internal e-CODEX Environment

As this document is a consolidating deliverable, summarizing the high level architectural decisions taken so far within e-CODEX and providing clear indications as the component model is concerned, its preparation has been carried out in collaboration with all e-CODEX WPs and partners. This has allowed the verification of the consistency between the decisions taken so far at various levels and increase coordination with the various e-CODEX efforts and initiatives.

1.5. Relations to External e-CODEX Environment

While working on the present deliverable, WP7 has been careful to keep up with the indications deriving from the strong relations developed between e-CODEX and other LSPs, in particular to interoperability projects such as STORK, PEPPOL and SPOCS, and with the EU Commission (in particular -but not only- in relation to the e-Justice Portal).

1.6. Quality Management

Document quality is ensured through the involvement of the e-CODEX External Quality Manager, authors open discussion (through face-to-face meetings, telephone conferences and e-mail exchanges), and a cycle of partners document review to check technical and legal issues but also readability.

1.7. Structure of the document

D1.1 *Guidelines on how to write a good deliverable* have set up a formal structure any deliverable is expected to follow.

The deliverable 7.3 (High Level Architecture Definition) is structured as follows:

1. Introduction

2. Architectural Overview
3. Architectural Decisions
4. Component Model

2. Architectural Overview

The overall architecture of e-CODEX is based on the idea that the use of information and communication technologies can support cross border communication between the different parties in civil and criminal judicial procedures. E-CODEX technical and organisational choices build on the idea of creating a *'circle of trust'* (providing a basis for the Judicial authorities to trust the information provided by e-CODEX gateways) among the judicial authorities involved. As e-CODEX analysis has shown, without such *circle of trust*, the complexity of the task would be too high to be managed in order to produce a working solution.[4]

2.1. e-CODEX infrastructure components

Figure 1 – e-CODEX High level architecture schema

[4] Cf. D7.2 (Requirements Finalisation) & D3.2 (Described Test Scenarios), page18

The above picture provides a simplified representation of the e-CODEX high-level architecture, including the main actors, components and their interconnections.

In essence, e-CODEX allows the electronic exchange of data and documents between the main actors of cross border judicial activities (e-CODEX users). The representation applies to all use cases that have been selected for the piloting phase of the project: European Payment Order (EPO), Small Claims, Mutual Recognition of Financial Penalties, Secure Cross-border Exchange of Sensitive Data, and European Arrest Warrant (EAW).

The e-CODEX infrastructure allows an e-CODEX user to submit files, data and documents. The **e-CODEX users** for civil cases are typically the claimant, the defendant, their lawyers and the court of origin. While for simplicity claimant and defendant (and respective lawyers) in *Figure 1* appear to be in the same Country (A), they are typically in different Countries. In the criminal cases users can be judicial authorities such as public prosecutors, judges or even members of the police forces.

The e-CODEX architecture includes four main building blocks: the e-CODEX Service Provider, the e-CODEX Connector, the e-CODEX Gateway and the e-Delivery platform. Figure 2 provide a more detailed representation of the e-CODEX building blocks.

Figure 2 – e-CODEX Components

An e-CODEX user creates, submits and receives his/her files though his/her national system (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 through the e-Justice portal. Such systems, for the purpose of e-CODEX act as **e-CODEX Service Providers**. In order to be an e-CODEX service provider the system must be able to deliver a service in conformity with e-CODEX standards (security standards, privacy…) in the field of e-justice and be connected to an e-CODEX gateway through an e-CODEX Connector of an e-CODEX member. An e-CODEX Service Provider may be a governmental solution or a private solution. In other words, depending on the use case, or on the role of the user, the e-CODEX 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.[5]

The **e-CODEX Connector** performs two main functions: 1) it transforms the outgoing documents received from the e-CODEX Service Provider from the national standard to the e-CODEX standard and adds a trust-ok token to the documents. The trust-ok token provides the results of electronic

[5] D3.3 Documented System Requirements and Specifications, 11.05.12 page 13

signature verification or a statement guaranteeing that the document was issued by an *advanced electronic system* that is capable of identifying the user and that ensures that the document is uniquely linked to the user and is created using means that the user can maintain under his control and any subsequent change of the data is detectable. According to the principle of the circle of trust, the responsibility for the implementation and the control of those characteristics lies with the Member State whose party to a procedure uses the system.[6] The receiving country can then trust the documents and is not required to validate them again.[7] 2) It transforms the incoming documents received by the e-CODEX gateway from the e-CODEX standard to the national standard, it verifies the trust-ok token and that no data has been changed.

The e-CODEX Connector might also perform protocol and semantic translations. Member States' are free to decide at what stage in their infrastructure they will perform these actions if they are necessary at all.

The **e-CODEX gateways** are national (and the e-Justice portal) "channels" or systems for data transmission between two communication partners. e-CODEX gateways are under the responsibility of an e-CODEX members. The gateways are required to fulfil specific security requirements within their operation but also for the communication with others. These gateways act as interfaces between national systems (or the e-Justice portal) and the e-Delivery platform. Accordingly, they perform different functionalities, such as establishing a connection to other gateways and connectors, format the content of a message to be sent to the eBMS3.0 standard and extract the contents of a received eBMS3.0 message,[8] providing a transport signature and providing a timestamp for outgoing messages and checking of the transport signature, providing of a timestamp and sending of an acknowledgment of receipt for incoming messages.

The **e-Delivery platform** is responsible for the secure and reliable transport of data and files from one e-CODEX gateway to another. It has been decided to adopt a decentralized architecture. If a technical need will emerge in the future, a central hub will then be considered. To allow access to all potential users, the system will use the Internet with encryption to ensure a secure connection. Further investigations on s-Testa from legal and technical perspective should be done. The final solution should be able to run over any IP network including s-Testa. In principle, the e-CODEX e-Delivery platform will be "content agnostic, however it remains to be discussed if delivery evidences are business documents and therefore part of the content (the payload) or if they are rather an integral part of the transport infrastructure".[9]

Figure 3 provide a representation of all building blocks from a piloting countries perspective:

---

[6] D3.3 Documented System Requirements and Specifications , 11.05.12 page 16

7 e-CODEX Deliverable 5.3 Concept of Implementation v0.9

[8] D4.2: Concept for Implementation of WP4, 30.05.2012

[9] D5.2 Reusable Assets 02.12.2011, Page 25

Figure 3 - e-CODEX building blocks from the piloting country perspective

A representation of the electronic cross border judicial communication exchange process supported by e-CODEX is provided in the swim lane diagram below (*Figure 4*):

Figure 4 – High level use cases scenario (Adapted from D7.2 Requirements Finalisation & D3.2 Described Test Scenarios)

3. Architectural decisions

The complexity of the e-CODEX Large Scale Pilot project necessitates that organizational, architectural or technical decisions have to be written down and disseminated through the deliverables. Especially architectural decisions have a fundamental effect on many areas of the project. This section of deliverable 7.3 will highlight the major architectural decisions that have been made thus far.

One way to define an architectural decision is to first define the problem or requirement. This can be done by the technical work packages WP4, WP5 and WP6 or by WP7 directly. The architecture work package, WP7, is always included early on in the process and participates in the discussion with all other involved work packages to clarify the definition of the requirement or problem.

Once the problem has been properly defined and a possible solution has been agreed upon by the work packages, it is presented to the management board. The management board then has the final say on how to proceed.

Figure 5 – Governance structure for architectural decisions

The table-based list below contains the major architectural decisions made by e-CODEX up to this point.

3.1. General decisions

Decision 1	Interoperability framework
Description	'An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public

	services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.' *Source*: *European Interoperability Framework (EIF) for European public services, page 2 Chapter 1.2.3* http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf (accessed on May 09th, 10:53 CEST)
Decision	An interoperability framework will be used in the e-CODEX project.
Reason / Benefit	Create a standard for cross-border interoperability to guide public administrations -and other organizations involved in the public services provision- in their work to provide European public services to businesses and citizens.

Decision 2	**Interoperability layer**
Description	Interoperability, within the context of European public service delivery, is intended as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.' *Source:* Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:260:FULL:EN:PDF) (accessed on May 09th, 10:58 CEST); see also *European Interoperability Framework (EIF) for European public services, page 2 Chapter 1.2.2* http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf (accessed on May 09th, 10:53 CEST) The Interoperability layer distinguishes four levels of interoperability: *Legal interoperability* *Organisational interoperability* *Semantic interoperability* *Technical interoperability*
Decision	A set of Core Interoperability Agreements covering all 4 Interoperability Layers will be defined and agreed upon in order to facilitate interoperability across the Pan European Member States
Reason / Benefit	The complexity of a cross border service implementation requires a high level of interoperability. This makes it necessary to develop a detailed layer system for interoperability.

Figure 6 – Interoperability layers (source: European Interoperability Framework (EIF) for European public services fig 4.1)

Decision 3	**Internet vs. sTesta**
Description	For the network infrastructure there is a choice to be made between sTesta and the internet. sTesta is the European Community's own private network, isolated from the internet and allowing officials from different Ministries to communicate at a Pan-European level. It uses the IPsec protocol to guard against the interception of messages. Outside access to the sTesta network is not possible.
Decision	It was decided that e-CODEX e-Delivery should use a secure communication channel over the Internet whose endpoints are protected by authentication schemes that offer the levels of security as required by the type of information to be protected for the initial piloting phase. Further investigations on s-Testa from legal and technical perspective should be done. The final solution should be able to run over any IP network including s-Testa.
Reason / Benefit	sTesta might not be available to all participants and through the use of encryption a secure connection between participants can be guaranteed using the internet.

Decision 4	**Topology**
Description	Gateways are endpoints for national systems to connect. Gateways provide the communication with other gateways. Point to point connection between the gateways is favoured for the preparation of the pilot phase. It has been decided to use a decentralized architecture. If a technical need will emerge in the future, a central hub will then be introduced.

Decision	A point to point connection between the gateways is favoured for the preparation of the pilot phase.
Reason / Benefit	To standardize the communication between participants and to limit the architectural influence from national systems.

Decision 5	Requirement to the e-Justice Portal

Description	There are several requirements in connection with the EU e-Justice Portal that were described in the document "e-Justice Portal and e-CODEX Pilots" that was submitted to the EC on 2011-08-25. The below listed requirements will have to be fulfilled by the e-Justice Portal:
	• Information about the judicial procedures associated with the e-CODEX pilots must be updated in the static pages of the e-Justice Portal.
	• For lawyers, the European e-Justice Portal needs to connect to the "Find a lawyer" application provided by CCBE in order to validate the role of the lawyer.
	• The e-Justice Portal should implement the user-interface for all judicial forms needed for the submission and execution of the e-CODEX pilot procedures using the already existing "dynamic forms" capability of the e-Justice Portal.
	• The European e-Justice Portal needs to implement a new electronic interface (according to the e-CODEX architecture) to send and receive judicial forms as e-CODEX messages (via the European e-CODEX Gateway) to/from the competent destination court:
	  ○ Convert judicial input forms into e-CODEX (input) messages (XML envelope, XML payload and optional attachments)
	  ○ Send (input) messages to e-CODEX
	  ○ Receive (output) messages from e-CODEX
	• Different types of response messages will have to be displayed to the user.
	• Create secure user mailboxes (for citizens, businesses and legal professionals and possibly also for courts) to be able to receive asynchronous responses.
	• The ability to digitally sign electronic forms with digital signatures is essential.
	• A European e-CODEX gateway similar to a national e-CODEX gateway and based on the same interfaces shall be set up.
	• Integration of online payment via direct bank or credit card access or via payment service provider should be provided.
	• The ability to locate the competent destination court for a specific MS and Proceeding Type (e.g. small claims and EPO) automatically via a Web service (possibly from the European Court Atlas).

Decision	The above requirements will be communicated to the e-Justice Portal.
Reason / Benefit	The e-Justice Portal needs to be able to provide the same basic features as

	the national solutions. e-CODEX and DG Justice have both agreed to that.

Decision 6	**Language/Translation e-Payment**
Description	Language of information on e-payment which is not in an (official) language of the receiving MS (or one that the addressee understands) may be rejected. The translation of documents related to e-Payment is under the responsibility of the claimant.
Decision	No action is taken by e-CODEX. e-Payment was not chosen as pilot for e-CODEX. Therefore the translation is not in the primary use of e-CODEX but as added feature.
Reason / Benefit	This is in accordance with the framework decision that documents have to be in the language of the competent court because this is part of the judicial procedure.

Decision 7	**No storage of message content**
Description	The e-CODEX system will transport messages to the receiving e-CODEX Gateway. The public IP address of each MS gateway will be known, so each MS can filter the access to their e-CODEX Gateway. After a successful message transmission including the corresponding notifications the original message must be deleted and only the log information for statistical purposes is stored.
Decision	The e-CODEX exchange platforms architecture will only store information on the exchange, never on the content of information exchanged.
Reason / Benefit	Messaging needs to be reliable and secure and comply with existing privacy laws.

Decision 8	Confidentiality of information exchange
Description	The confidentiality of the transported data between gateways must be ensured. In order to achieve this: • A secure network protocol, such as TLS [RFC2246] or IPSEC [RFC2402], provides transient confidentiality of a message as it is transferred between two adjacent network nodes. • The e-CODEX transport platform and the connected services will defend against SQL injection, cross-site scripting, cookie poisoning, OWASP[10] Top 10, XML schema poisoning, XML bombs, malware, routing detours, and rate-based transaction control. • The architecture's physical equipment will be secured. • Persistent confidentiality and privacy can also be achieved by additionally encrypting the content of the messages.
Decision	Member State solutions have to respect the e-CODEX security policy.
Reason / Benefit	The confidentiality policy is based on e-CODEX Security Policy and in conformance to EIF v2.0 (3.2.2. The Secure Data Exchange Layer) It must be noted that due to the scope of e-CODEX, which deliberately does not cover the part of communication between national solution and gateways, it must be explicitly stated that end-to-end Security (with regard to integrity and confidentiality) cannot be guaranteed. Especially end-to-end encryption will not be delivered by e-CODEX and is subject to national governance. Additional / parallel security provisions must be taken at national level in order to achieve the required level of end-to-end security required. All e-CODEX data flows must be adequately protected, covering both the Member States' requirements and the agreed e-CODEX minimum standards on this matter.

3.2. Signatures & Authentication

Decision 9	Signature on PDF
Description	In some Member States the human readable portions (mostly PDF files) are to be signed and in some Member States (see Netherlands) the XML portion of the message is signed.
Decision	All Member States must have the ability to sign at least PDF-files. When sending XML with stylesheet and PDF only a signature on the PDF is required. Signing of XML with stylesheet is optional (no rejection will take place).

[10] See The Open Web Application Security Project at: https://www.owasp.org/

Reason / Benefit	e-CODEX must balance the contradicting requirements of allowing citizens to sign according to their national law and to guarantee the interoperability.

Decision 10	**Signature Formats**
Description	There are different signature formats in use in the Member States.
Decision	The sender of a document (i.e. claimant or defendant) will apply signatures according to its national law. If a format other than the reference formats (XADes, PADes, CADes, DSS and ASiC-S) is used, then the Member State has to guarantee the possibility to validate those signatures as stated by Commission decision 2011/130/EU.
Reason / Benefit	e-CODEX must guarantee interoperability.

Decision 11	**e-Signature validation**
Description	If an electronic signature is required, the signature can be verified through the DSS (Digital Signature Service) for e-Signatures. It can validate all e-Signatures that support the requirements in Commission Decision 2011/130/EU and will make use of a trusted list[11]. The user will be able to sign all content necessary for the use case (see ALL-RQ-F-001). The e-Signature validation will be done at the sending e-CODEX Gateway, but it should be noted that successful validation is not mandatory for the message to be sent. After the signature is validated a Trust-OK Token is added by the e-CODEX Gateway. Should the system not be able to validate the signature the message will be sent anyway, but the Trust-OK Token will give clear indication.
Decision	e-CODEX validates signatures on the sending side and adds a “Trust-OK” token.
Reason / Benefit	The receiving country does not have to verify signatures.

Decision 12	**Circle of Trust**
Description	The issuing state adds a “Trust Ok”-token to the message if the user is “authenticated” or has electronically signed. If the “trust ok”-token is not provided, the gateway is not allowed to send the message. No verification of signatures will take place at the receiving end (circle of trust). The receiving MS has to accept the message.
Decision	The receiving country trusts the validation done in the sending country.

[11] Whether e-CODEX will need a trusted list in its own or the EU TL will be enough is under investigation by WP4.

Reason / Benefit	Through the use of the "circle of trust" the responsibility of verifying the signature lies with the sending country. The process does not have to be repeated in the receiving country.
Source	Tallinn, December 2011 - Paris, December 2011 - D7.2-D3.2

Decision 13	**Advanced Electronic System**
Description	As e-CODEX Service Provider for the civil use cases, e-CODEX will accept and will only accept an 'advanced electronic system'. An advanced electronic system is an electronic system which meets the following requirements: (a) the created document is uniquely linked to the user; (b) the system is capable of identifying the user; (c) the document is created using means that the user can maintain under his control; and (d) any subsequent change of the data of a created document is detectable;
Decision	According to the principle of the circle of trust, the responsibility for the implementation and the control of the four requirements above lies with the Member State whose party to a procedure uses the system
Reason / Benefit	National Systems that have strong authentications don't have to sign.

Decision 14	**Primary user access**

Description	The National Infrastructure in the Member States participating in e-CODEX and the e-Justice Portal should address the security requirements for user access management for the different types of primary users: citizens, legal persons, legal professionals (representing a citizen or a company for a specific case) and in particular should be able to identify:
	• "Natural Persons", e.g. citizens
	• "Legal Persons", e.g. companies, institutions
	  ○ Companies are normally represented by one or several "Natural Persons", which can be found in the European Business Register (EBR)
	• "Legal Professionals", e.g. lawyers, notaries
	  ○ They can represent other "Natural Persons" or "Legal Persons". The assertion of the role is sufficient. For lawyers the role will be checked connecting to the "Find a Lawyer" application provided by CCBE, if available..

Decision	Sufficient user access management for the different types of users is a prerequisite in order to identify, authenticate and authorize e-CODEX users and implement the e-CODEX security policy. Roles will not be checked.

Decision 14	Primary user access
Reason / Benefit	According to e-CODEX Security Policy and in conformance to EIF v2.0 (3.2.2. The Secure Data Exchange Layer) See also “e-Justice Portal support to e-CODEX Civil Pilots”, chapter "3.2 Ability to authenticate, and authorize European citizens, businesses and legal professionals".

Decision 15	Verification of role
Description	Communication actors could have special identities which are very useful for the process. This special identity could allow such an actor to start the process in representation of another actor. A pre-condition of the verification of the actor’s role is a real time up-to-date role-list.
Decision	For lawyers the role will be checked connecting to the “Find a Lawyer” application provided by CCBE, if available.
Reason / Benefit	The CCBE is working in a function to the Find-A-Lawyer that will allow verifying the lawyer's role. During the implementation of this service CCBE expect to work closely with e-CODEX and the e-Justice portal

3.3. Transport

Decision 16	Message size
Description	From the e-CODEX transport platform perspective there is no limit on message size. Limits come from the legislation and technical infrastructure of different Member States which might have set an upper limit or message size.
Decision	There is no size limit on messages sent through the e-CODEX transport platform, but Member States can specify Business Rules to regulate the message size. The p-modes specify the business rules for transportation between two gateways. For the piloting phase a limit of 5MB has been set.
Reason / Benefit	The size limit should be dependent on the receiving country. When supplying messages via a national transport infrastructure, it is the responsibility of the participating member states to ensure size limits are not exceeded.

Decision 17	ebMS
Description	The ebMS specification defines the technical interconnection, including

	security standards and the message structure. A detailed description can be found in the ebXML Messaging Core Specifications[12] and a more comprehensive summary in *D5.2 Reusable Assets*.
Decision	The e-CODEX e-Delivery transport infrastructure will be based on the OASIS **eb**XML **M**essaging **S**ervice (ebMS) standard.
Reason / Benefit	The goal was to provide a cross border communication via gateways, similar to the existing LSP PEPPOL and SPOCS solutions. The OASIS ebMS standard allows creating such a cross border communication. ebMS also fits all other requirements of e-CODEX and the other LSPs. Therefore a proposal for e-Delivery convergence based on ebMS was created by the LSPs.

Decision 18	**Transport Signature**
Description	The e-Signature (transport signature) is a measure to provide message integrity between gateways. A signature applied to the hash of the message by the gateway assures that the message has not been changed during transport. The authenticity of a message (header and payload) must be guaranteed.
Decision	All message routed through the e-CODEX transport platform carry a transport signature.
Reason / Benefit	The system guarantees that documents and messages exchanged between the gateways are guarded against tampering during transport.

Decision 19	**Notification/evidence**
Description	For the transport of judicial data, a notification system becomes necessary. This system contains Notices of receipt with the time stamps delivered by a time stamping solution and Delivery- and Notice Notifications, which produce notices for the user. The evidences and the format of these that are required by the judicial data exchange are specified based on the ETSI REM standard, which is the same concept as used by SPOCS.
Decision	All messages routed through the e-CODEX transport platform will be time stamped. The e-CODEX system will be able to receive / log and produce / send out notices of receipt.
Reason / Benefit	e-CODEX will provide reliable exchanges in the judicial domain at two levels: technical and business. This will take into account legal deadlines of the use cases and when the corresponding time periods start. These deadlines and points in time are

[12] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features Committee Specification 02, http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html, 12 July 2007

	determined by national regulation, and the relevant information should be made available for the user.[13] On the other hand the user needs to be aware of the successful delivery of a claim. This gives the user the legal certainty that an action by the court will be taken. The e-CODEX on itself cannot provide Business notifications. Business notifications will in most cases be initiated in the case management applications that reside within the MS and are out of control of the e-CODEX infrastructure. They are however an essential part of the e-CODEX functionality as a whole.

Decision 20	**Statistics information**
Description	The system needs to obtain and store information about the e-CODEX exchange infrastructure usage, especially in case of further litigation. Details on reporting of statistical information based on log entries as well as monitoring are provided in D5.3 (chapters 4.3.2.3, 4.3.2.6, 4.3.2.7)
Decision	The e-CODEX transport platform will collect statistical data and store access logs. No personal data will be stored. Thus, any IP address will only be stored in its anonymous form.
Reason / Benefit	Statistics information will allow the gauging of the performance of the technical systems.

Decision 21	**No End-to-End encryption**
Description	The term End-to-End encryption means that the encryption during the transport of a package or data-container will only decrypted at the final recipient. This requires a single transport platform for the whole communication process.
Decision	No end-to-end encryption is provided by e-CODEX infrastructure; for specific needs, sender and recipient can adopt encryption mechanisms on their own (e.g. exchanging public cryptographic keys).
Reason / Benefit	As the ebMS communication is between gateways only, a complete end-to-end encryption is not foreseen and will not be provided by e-CODEX. According to the ebMS version 3.0 standard, the communication between the MSH (i.e. the gateways) will be encrypted.

[13] This issue is being discussed by LSSG and WP7

3.4. Document Types & Data Modelling

Decision 22	**No Data Containers**
Description	Container format specifications describe how different data elements/files (including metadata) are bundled up in one computer file. Transport containers include the information, payload like attachments and metadata for the transport. Instead of encrypting each element, only the container has to be encrypted. Each element/file within the container must still be signed individually.
Decision	
Reason / Benefit	We do not need transport containers between gateways because bundling is handled by the transport infrastructure. A compelling legal reason to use containers was not identified. If there is a need for containers nationally, it's the Member States' responsibility and therefore out of scope for e-CODEX.

Decision 23	**Container formats for signatures**
Description	Specifications also allow for detached signatures to be used. In these cases, the signature is held separately from the file it was computed for, and might need to be bundled through the use of a container.
Decision	The ASIC-S container is adopted.
Reason / Benefit	If multiple files and their detached signatures are included in the same message envelope, it may become difficult to pair a file and its signature. The ASIC-S container keeps together the readable files for the final user, and it guarantees the integrity of them.

Decision 24	**Formats**
Description	The e-CODEX transport platform places no restrictions on the formats included in the message, but Member States can specify Business Rules to regulate which message formats they accept. The piloting countries may have specific restrictions for additional formats in specific use cases. These restrictions need to be known. <u>Behaviour when messages could not be accepted:</u> • National e-CODEX service providers (and the e-Justice Portal) should provide a document to the software implementers with the business rules which formats are accepted • Users should be informed prior to sending the message in the e-Justice

	Portal • Initiators of communication should be urged to obey the business rules • Final check on receiving side Error message when sending unsupported formats
Decision	At least PDF shall be supported by all participating countries. PDF/A will be further investigated. XML for the form contents.
Reason / Benefit	Parties should be able to read the documents exchanged through e-CODEX.

Decision 25	**Relationship between XML and PDF**
Description	It is important to distinguish between short and long term strategy: • Short term: PDF and XML as payload in messages, translate legal into functional requirements, market XML + XSLT to legal domain. • Long term: In the future it might be feasible to use XML + XSLT as open standards, supporting machine processing and transformation to human readable files, widely used in applications. XML and XSLT are well supported and will be around for a long time.
Decision	The PDF document is the legally binding part of the message for the pilot phase. XML and XSLT will be further examined.
Reason / Benefit	XML + XSLT are easier to process on the receiving end and can be input into a system through automatic procedures.

Decision 26	**XSLT on the e-Justice portal**
Description	**XSLT** (Extensible Stylesheet Language Transformations) is a descriptive, XML-based language used for the transformation of XML documents. The original document is not changed. Instead, a new document is created based on the content of an existing one. XSLT is most often used to convert data between different XML schemas or to convert XML data into web pages or PDF documents. These files then become readable for humans again and can be displayed on web pages like the e-Justice Portal. The European e-Justice Portal [14] is conceived as a future electronic one-stop-shop in the area of justice to make citizens' life easier by providing information on justice systems and improving access to justice throughout the EU, in 22 languages. For this, the portal provides dynamic forms for the European Payment Order and Small Claims procedures. The XSLT standard can be used to convert the XML version of these forms to a human-readable

[14] https://e-justice.europa.eu

	PDF or a set of web pages.
Decision	WP6 will not develop XSLTs to create PDFs from the XML data. This is an European e-Justice Portal requirement.
Reason / Benefit	The European e-Justice Portal is out of e-CODEX's competence since the portal's ownership is with the European Commission, DGJLS.

Decision 27	**Transformation at national gateways**
Description	Member States have different standards in place for structured data (XML data). The e-CODEX format developed by WP6 is primarily intended for use between gateways.
Decision	Transformation of data for import into the national systems is under the responsibility of the respective MS. It can be performed at e-CODEX connector level, but is not necessarily so. MS could do so at application level.
Reason / Benefit	Every national system is different and only the responsible organisations within the country know how the data has to be transformed.

Decision 28	**Use case centered approach**
Description	While it would be desirable to create a universal data model that covers all possible applications in justice, this is probably not feasible within the given timeframe.
Decision	The e-CODEX data modelling will focus on those data needed for the e-CODEX use cases, while trying to use an approach that is universally applicable to new use cases.
Reason / Benefit	The use case centred approach ensures that the e-CODEX data model can be finished in time for implementation.

Decision 29	**Role of ontologies**
Description	Ontologies can be used to identify the basic concepts needed for the e-CODEX data modelling.
Decision	No final decision has been made yet. The decision has been to distinct between a short term and a long term solution. The short-term solution is to abstain from using an exhaustive conceptual model as it the time to develop such a model does not meet the requirement to start piloting in November 2012. The long-term decision is to start to investigate the necessity and the requirements for a conceptual model. This investigation is due to start after

	the successful start of the operational phase of the pilot, planned in November 2012.
Reason / Benefit	The development of a conceptual model is time consuming because of necessary discussions and development of methodological and procedural guidelines. The need to support the execution of cross-border legal procedures from November 2012 on urges WP6 and e-CODEX to distinct between short term and long-term strategy.

Decision 30	**Niem/CCTS**
Description	Niem and CCTS are competing methodologies for the creation of data models. Both are under consideration for use in WP6.
Decision	Regarding the choice between NIEM and CCTS for data modelling WP6 has chosen CCTS to be applied for the **short-term implementation**, although MB still has to approve this decision. A final decision on the standard for data modelling (CCTS/NIEM) will be based on an investigation, which is due to start after the successful start of the operational phase of the pilot, planned in November 2012.
Reason / Benefit	The need to support the execution of cross-border legal procedures from November 2012 on urges WP6 and e-CODEX to distinct between short term and long-term strategy.